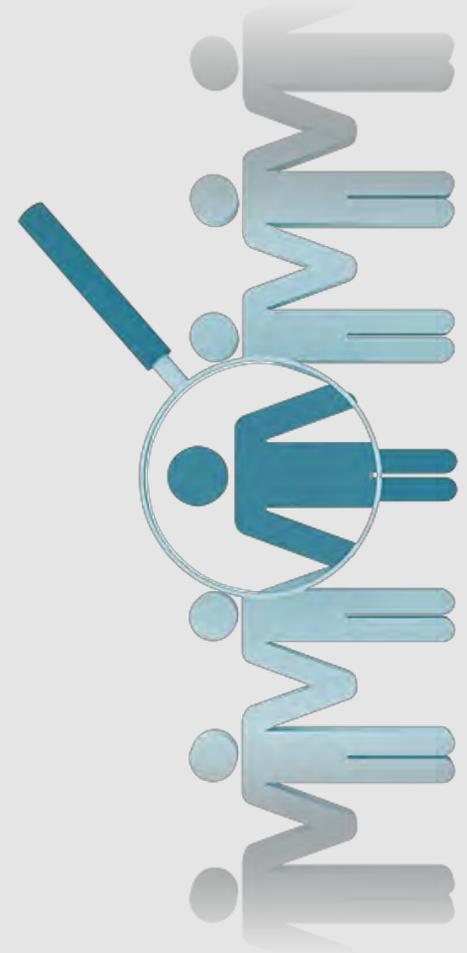




# TABLE OF CONTENTS

1	Threats to Identity –2019-2020
3	Self Assessment
6	Opt Out of Search Engines and Other Databases
8	Opt Out of Public Records and Data Aggregators
10	Google Alerts
12	Online Registration
14	Anonymous Email Services
16	Twitter
22	Instagram
28	Facebook
42	Amazon
51	Pinterest
57	Snapchat
65	TikTok
71	YouTube
76	LinkedIn
84	PlayStation
90	Hidden Apps
92	Mobile Payment Apps
94	Dating Apps
96	Fitness Tracking Apps
104	iOS Settings
109	Android Settings
114	Zoom
119	Traveling Safely with Smartphones
120	Identity Theft
122	Keeping Your Kids Safe Online
124	Photo Sharing Services
128	Smartphone EXIF Removal
130	Lock Down Your Computer
132	Securing Your Wireless Network
135	Delete Browser Artifacts (Cookies, Cache & History)
142	Additional Resources



# IDENTITY THREATS SMART CARD

## Top Data Breaches of FY 20 That You Should Be Aware Of

- ◆ Facebook - Sept 2019 & April 2020
- ◆ T-Mobile - Nov 2019 & March 2020
- ◆ Wawa — Dec 2019
- ◆ Microsoft – Jan 2020
- ◆ MGM - Feb 2020
- ◆ Marriott - March 2020
- ◆ Zoom - April 2020
- ◆ National Cardiovascular Partners - April 2020
- ◆ Nintendo - April 2020
- ◆ Mathway - May 2020
- ◆ Claire’s - June 2020
- ◆ Twitter Bitcoin Attack - June 2020

**\*\***Two researchers have discovered four billion records on at least 1.2 billion people left open on an unsecured server impacting an estimated hundreds of millions of people. The data however, doesn't include sensitive information such as passwords, Social Security numbers, or credit card numbers. It does, nevertheless, contain profiles of hundreds of millions of people that do include home and cell phone numbers, associated social media profiles like Twitter, Facebook, and LinkedIn, work histories which appear to have been scraped from LinkedIn, almost 50 million unique phone numbers, and 622 million unique email addresses.

## Things to Consider

- ◆ When buying a new car don't leave all the paper work in the glove compartment or elsewhere in the car . Criminals who break into cars can use that information to steal your identity, not just your car.
- ◆ Consider posting travel (vacation) photos and information after you return from your trip so criminals don't know you are away and your house is empty.
- ◆ If you are buying or selling something online and it seems too good to be true, chances are it is. A simple Google search of the situation might end up saving you a lot of time and hard earned money.
- ◆ Consider turning off your Wi-Fi as soon as you get into your car to leave your house. #habitscanbegood
- ◆ Consider how many people have access to public Wi-Fi, then consider only using privately secured Wi-Fi.
- ◆ Consider an open-phone policy with your children so you can access their phone anytime and without notice. Remember: if you are "friends" with your kids online that's only half the battle...it's important to check on their accounts to see who and what they are talking about. #keepingourkidssafe
- ◆ It's always great to donate, but consider verifying the authenticity of a charity and/or website first. Perhaps visiting an official website or calling the official number.
- ◆ Gamers: consider who you are communicating and sharing information with and perhaps limit online gaming interactions to only people you have met face to face.
- ◆ Consider logging off of your email and social media accounts when you are not using them, especially on your computer. Doing so will limit the access and abilities of an intruder if they are able to hack in. #protectyourdata

## What to Lock Down

- ◆ Any PII Information
- ◆ Your credit report
- ◆ Your child's credit report
- ◆ Your social media accounts (recommend utilizing smartcards to lock accounts down )

### In Cases of Identity Theft:

- ◆ Notify your bank & credit card companies
- ◆ Change all passwords including on social media
- ◆ Report ID Theft to [www.FTC.gov](http://www.FTC.gov)
- ◆ Let friends and family know in case the criminal now has access to your emails and social media accounts
- ◆ File a Police report

## Actions to Take in 2020

- ◆ Recommend turning on Two Factor Authentication for all devices and accounts that allow such an option
- ◆ Update your devices' virus protection and your passwords
- ◆ Clear cookies and browser history frequently
- ◆ Update , Update , Update!!! Make sure to allow your device to update to ensure you have the most up to date security measures
- ◆ Make sure you backup all your devices.
- ◆ Encrypt your emails
- ◆ Never save credit or debit card information to devices, apps, or accounts for quick and easy checkout
- ◆ Verify those emails; most official business emails will not ask for your PII or Password...check those links
- ◆ Don't accept friend requests from strangers
- ◆ Consider using a VPN

# IDENTITY THREATS SMART CARD

## Actions for the Physical World

- ◆ Be aware of your surroundings
- ◆ Use checks sparingly
- ◆ Invest in a home safe
- ◆ Shred documents, bills, and any mail
- ◆ Do **not** give out your SSN
- ◆ Be mindful of shoulder surfers (whether on your phone, computer, at an ATM, etc.)
- ◆ Be mindful of credit card skimmers at ATMs and Gas pumps
- ◆ Use a locked mailbox
- ◆ Check financial statements frequently
- ◆ Read medical statements
- ◆ Use credit cards instead of debit cards
- ◆ Be sure to sign the back of any credit or debit card



## Useful Resources and Links

<https://www.identityforce.com/blog>

<https://www.common sense media.org/privacy-and-internet-safety>

<https://www.ftc.gov/>

<https://identity.utexas.edu/>

<https://www.getsafeonline.org/>

<https://staysafeonline.org/>

<https://www.idtheftcenter.org/>

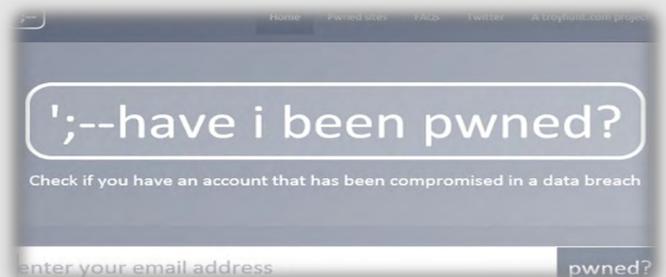
<https://www.irs.gov/>

<https://www.usa.gov/identity-theft>

<https://www.consumer.gov/articles/1015-avoiding-identity-theft>

<https://www.transunion.com/fraud-victim-resource/child-identity-theft>

Be sure to check out <https://haveibeenpwned.com/> to see if your personal data, via your email address, has been compromised in any data breach. Not all data breaches are included on this website but it's a great start to owning your Identity.



Checking data breaches monthly or quarterly will help to ensure you do not fall victim to identity theft.



**KEEP CALM**  
**Treat your password**  
**Like your toothbrush...**  
**Never share it**  
**and change it often!**

# HOW TO CONDUCT A SELF-ASSESSMENT



## Your Online Presence

One of the easiest ways for people (e.g. potential employers, criminals, etc.) to get information about you is through your existing online presence. There, they can learn about you with just a few clicks of the mouse and a quick Internet search. It is therefore important for you to know just what is out there publicly available about you, and how you might reduce any unwanted information.

Review your social media accounts and available data aggregator websites to determine what, if any negative or unwanted information is out there about you. Remember, your close contacts, including family members may have also, unintentionally exposed information about you. It is important to also review what others may have posted about you especially if you have been tagged, directly linking you to a post and making you much easier to find.

## Search Engines

Search yourself using various search engines such as Google, DuckDuckGo, etc. for the differences and benefits of each (for a few examples of popular search engines please see the third page). Please note that Google appears to yield the most accurate results for people searches and captures more relevant information.

Prior to researching, ensure you are not logged into any of the search engine sites such as Google or Yahoo. Be sure to delete your browser history and clear cookies before you begin and when you have completed all your research.

These next instructions are related to the Google search engine, but can be applied to most other search engines.

Start with basic personal information such as First and Last Name. If you have a common name, you may want to search First, Middle, and Last Name, or your name associated with a City and State, Home Address, or an associated organization. Please see the examples below:



## Search Engines Continued...

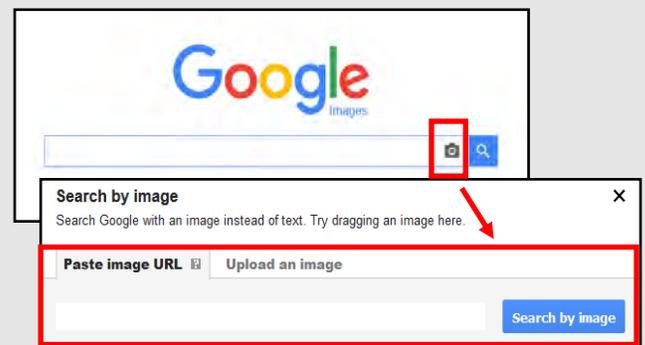
Please note that search terms **within quotations marks " "** will yield results that have the same terms in the **same order** as the ones inside the quotes. So "John Edward Smith" will not necessarily return the same results as "Edward, John Smith."

Google does support Boolean logic, however you might, instead decide to use its own search operators which can be found here: <https://support.google.com/websearch/answer/2466433?hl=en>

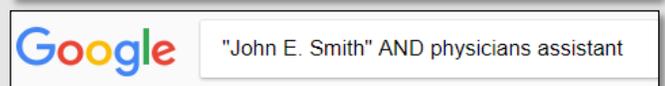
You will also want to search your email addresses, usernames, and phone numbers within quotation marks.

If your search results continue to include items that are not relevant, use the **dash sign** to **exclude** certain search terms like this: "John Smith" -Pocahontas

You may want to conduct an image search on any photos you have used as profile pictures on social media accounts or posted to other places online. The reason for this is to ensure that advertisers and/or any other company or individual hasn't taken your picture for their own personal use. To conduct an image search using Google, go to **images.google.com**, click the camera icon, then select Upload an image. Select the image you want to use to start your search.



Collectively the search engine results will give you an idea of the information that can be quickly collected on you. For example, you may have found and information about previous work experience, hobbies (e.g. races, sporting events), or schools (e.g. graduation announcement). Use that information to conduct further searches such as:



Assume that the information you post and share is visible to everyone in the world.

# HOW TO CONDUCT A SELF-ASSESSMENT



## Boolean Match Logic

Boolean Search is a way to organize your search using a combination of keywords and the three main Boolean operators (AND, OR and NOT), to produce more accurate and more relevant results.<sup>(1)</sup>

- a) AND
- b) OR
- c) NOT
- d) “ ”
- e) ( )



## Social Media Search

Take an inventory of the social media accounts that you currently maintain. Some examples include, Facebook, Instagram, LinkedIn, Twitter, etc.

First, without being logged in to any social media accounts, conduct open source searches on yourself to see what is viewable to the public. Remember, if your social media accounts don't show up during your open source searches that doesn't mean your account is completely private. It's important to check out the smartcards to help you lock down your accounts to your own personal satisfaction.



Next, login to those accounts and thoroughly review your profile for sensitive information and consider removing unnecessary data:

- ◆ Review your profile to see what data is available to the public (address, employment, phone number, etc.)
- ◆ Check any photos that you have posted or have been tagged in (this can be done through your Activity Log if using Facebook)

\* See Facebook, Instagram, Twitter and LinkedIn Smart Cards to learn how to properly set privacy settings.

## People Finder Open Source/Fee

### Required Sites

Conduct searches on various data aggregator sites.

Examples include:

- ◆ www.ussearch.com
- ◆ www.spokeo.com
- ◆ www.beenverified.com
- ◆ www.intelius.com
- ◆ www.radaris.com

You can conduct an initial search for free, but all of these sites require payment to access a full report. These sites require no special authorities; anyone with Internet access and a credit card can purchase reports, so it is a good idea to be familiar with the information that can be discovered through them.

If you find information that you do not want publicly available in any of the reports, contact the organization to request that your information be opted out.

Once you've opted out of or suppressed any sensitive information you have found, consider setting up Google Alerts so that you're notified if the information reappears.

## Relatives

Though you may have found most of your information conducting your individual search, it might be a good idea to conduct a light search on friends and family members. Remember, they may have posted information about you that an adversary may be able to access.

- ◆ Ensure nothing posted on any of the accounts indicates or outright displays personal information you don't want discovered.
- ◆ Ask immediate family members (spouse, children, etc.) to review their account settings and postings to ensure that they have not inadvertently posted personal information about you or themselves.
- ◆ Provide family and friends with copies of our Smartbook or Smart Cards to help them with locking down their accounts and devices.

Search engines are the best place to start a self assessment. They can help to provide you a quick idea as to how much information there is about you online.

# HOW TO CONDUCT A SELF-ASSESSMENT



## Examples of Common Search Engines

### www.google.com

Google is a search engine that specializes in Internet-related services and products. These include online advertising technologies, search, cloud computing, and software. The majority of its profits are derived from AdWords, an online advertising service that places advertisements near the list of search results.

### www.bing.com

Bing is the second largest search engine in the U.S. Searches conducted using Bing generally yield similar results to Google, however Bing's image search capability (<https://www.bing.com/images>) is considered superior by most.

### www.duckduckgo.com

DuckDuckGo is a search engine that distinguishes itself from other search engines by not profiling its users and by deliberately showing all users the same search results for a given search term. Does not store or compile any of your data to include searched data or personal information (meaning it will not learn from your searches in the same way that Google will). DuckDuckGo emphasizes getting information from the best sources rather than the most sources, generating its search results from key crowdsourced sites such as Wikipedia and from partnerships with other search engines like Yandex, Yahoo!, Bing, and Yummly.

### www.searx.me

Searx is a metasearch engine, aggregating the results of other search engines while not storing information about its users.<sup>(2)</sup>

### https://archive.org

The Internet Archive is an American digital library with the stated mission of "universal access to all knowledge." It provides free access to collections of digitized materials, including but not limited to; websites, software applications, music, videos, moving images, and millions of public-domain books.

## Examples of Common Social Media Sites

- [www.facebook.com](http://www.facebook.com)
- [www.linkedin.com](http://www.linkedin.com)
- [www.myspace.com](http://www.myspace.com)
- [www.twitter.com](http://www.twitter.com)
- [www.tumblr.com](http://www.tumblr.com)
- [www.classmates.com](http://www.classmates.com)
- [www.instagram.com](http://www.instagram.com)
- [www.vk.com](http://www.vk.com)
- [www.pinterest.com](http://www.pinterest.com)
- [www.flickr.com](http://www.flickr.com)
- [www.meetup.com](http://www.meetup.com)
- [www.youtube.com](http://www.youtube.com)
- [www.snapchat.com](http://www.snapchat.com)
- [www.reddit.com](http://www.reddit.com)
- [www.tiktok.com](http://www.tiktok.com)

## Additional Examples of People Finder Open Source/Fee Required Sites

- ◆ [www.truthfinder.com](http://www.truthfinder.com)
- ◆ [www.findpeoplesearch.com](http://www.findpeoplesearch.com)
- ◆ [www.privateeye.com](http://www.privateeye.com)
- ◆ [www.peoplefinders.com](http://www.peoplefinders.com)
- ◆ [www.usa-people-search.com](http://www.usa-people-search.com)
- ◆ [www.spokeo.com](http://www.spokeo.com)
- ◆ [www.locateplus.com](http://www.locateplus.com)
- ◆ [www.peakyou.com](http://www.peakyou.com)
- ◆ [www.thatsthem.com](http://www.thatsthem.com)
- ◆ [www.familytree.com](http://www.familytree.com)
- ◆ [www.instantcheckmate.com](http://www.instantcheckmate.com)
- ◆ [www.zabasearch.com](http://www.zabasearch.com)
- ◆ [www.peoplelookup.com](http://www.peoplelookup.com)
- ◆ [www.publicrecords.com](http://www.publicrecords.com)
- ◆ [www.whitepages.com](http://www.whitepages.com)
- ◆ [www.reversegenie.com](http://www.reversegenie.com)
- ◆ [www.yasni.com](http://www.yasni.com)
- ◆ [www.social-searcher.com](http://www.social-searcher.com)
- ◆ [www.infospace.com](http://www.infospace.com)
- ◆ [www.lullar.com](http://www.lullar.com)
- ◆ [www.publicrecordsnow.com](http://www.publicrecordsnow.com)
- ◆ [www.findoutthetruth.com](http://www.findoutthetruth.com)
- ◆ [www.truepeoplesearch.com](http://www.truepeoplesearch.com)
- ◆ [www.checkpeople.com](http://www.checkpeople.com)
- ◆ [www.peoplelooker.com](http://www.peoplelooker.com)
- ◆ [www.persopo.com](http://www.persopo.com)
- ◆ [www.peoplefinder.com](http://www.peoplefinder.com)
- ◆ <https://carsowners.net>
- ◆ <https://allpeople.com>

If you post something on your social media account, it may show up on search engine search results. Remember to set your privacy settings.

# OPTING OUT OF SEARCH ENGINES & OTHER DATABASES



Google isn't the web; it's only a search engine for finding data on the Web. If you want to remove something, find the source of the content and who controls it.

## Google

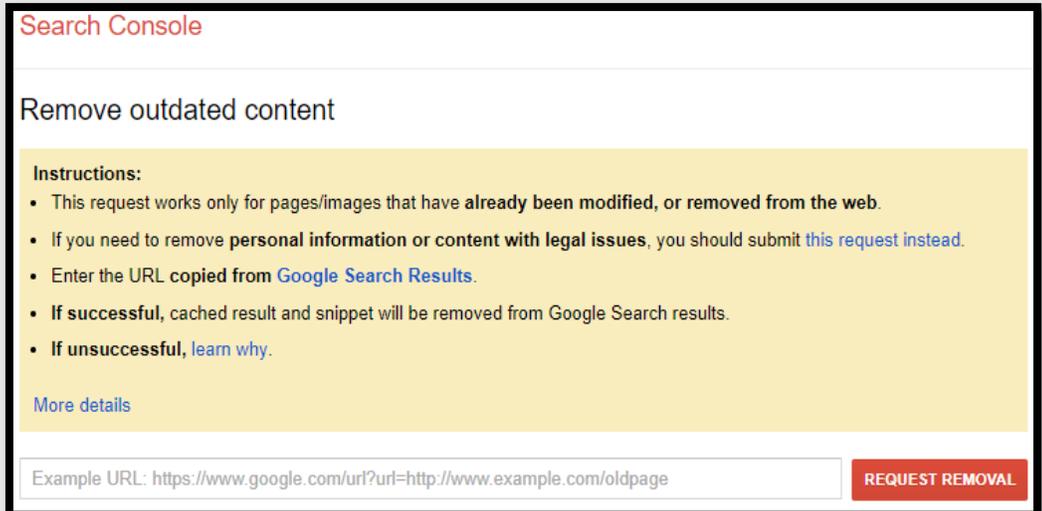
<https://www.google.com/webmasters/tools/removals>

While conducting a “Self Assessment” (see the Self Assessment card) you may find Google Search Results (websites) that you wish to remove.

Find the URL associated with the “Search Result” you wish to remove and paste the URL in the “Request Removal” box (see URL above and picture to the right).

It is **important** to note that a “Search Result” cannot be removed so long as the information and URL remain active on the original Webmaster’s page. In order to remove your information from Google you must first contact the Webmaster where the information resides and ask that it be removed. Once you obtain confirmation that the information has been removed, you can then “Request Removal” from Google.

On the “Search Console” page, you can also track you requests to determine if Google has accepted the removal request.



## Bing

<https://www.bing.com/webmaster/help/bing-content-removal-tool-cb6c294d>

To remove a search result or cache from Bing, go to the above URL and follow the steps located on the Bing website, under “Removing Outdated Cache”.

Like any search engine, it is important to note that your information cannot be removed from Bing prior to it being removed from the active website via the websites Webmaster. You will also need to create and sign into Bing with your Microsoft account (formerly Windows Live ID) in order to submit your request and track its progress.



## Acxiom

<https://isapps.acxiom.com/optout/optout.aspx>

What kind of books do you read? What kind of shoes do you buy? What type of information do Marketers have on you?

Acxiom Corporation is a database marketing company. The company collects, analyzes and sells customer and business information used for targeted advertisements. Good news! Opt Out of this service simply by following the link shown above. #protectyourdata



# OPTING OUT OF SEARCH ENGINES & OTHER DATABASES



## BeenVerified

<https://www.beenverified.com/f/optout/search>

Public government records are available from official public records custodians or repositories to anyone who requests them. In addition to public records, personal information may be commercially acquired from credit reporting agencies or utilities. BeenVerified is one of many online data brokers that purchases and collects publicly available information that is resold to anyone as a report.

BeenVerified provides a quick and easy process to allow you to remove your information from their People Search results. Using the above link, you can search their database, select your record, and verify your request to opt out by clicking on the link in their verification email. After you verify, they will send you an email confirming that the record you selected has been opted out and will instruct their data partners not to return the record in future People Search results.

BeenVerified uses your email address to send you an email to verify your request to opt out. They will not sell the email address that you provide as part of the opt-out process, or use it for any other purpose, without your prior consent. There is no charge to remove your data from BeenVerified's People Search results. Once you receive their email confirming that they have processed your opt-out request, your request will be reflected in their People Search results the next time their server refreshes. In most cases, this will take 24 hours to take effect and then they encourage you to check for yourself.

Once you receive their email confirming that they have processed your opt-out request, your request will be reflected in their People Search results the next time their server refreshes. In most cases, this will take 24 hours to take effect and then they encourage you to check for yourself.

Once your opt-out has been processed, they will instruct their data partners not to return the record you opted out in future People Search results. At this time, they only provide an opt-out for their People Search service. Therefore, it is possible that your name will appear in search results for the other search services available through BeenVerified even after you opt out of People Search.

There may be times when one of their data partners provides a new record that is different enough from your existing, opted out record that they cannot match this new record to the existing record opted-out record and will create a new one. Accordingly, if you have previously opted out and see a new record about you appear in their People Search results, contact them at [privacy@beenverified.com](mailto:privacy@beenverified.com) and they will help you remove that record as well. It is important to occasionally check BeenVerified to ensure the opt-out process is continuing.

## People Finders

<https://www.peoplefinders.com/manage>

Upon request, Peoplefinders can block the records they have control over in their database from being shown on PeopleFinders.com. Unless otherwise required by law, they will only accept opt-out requests directly from the individual whose information is being opted-out and they reserve the right to require verification of identity and reject opt-out requests in their sole discretion. Of course, they are unable to remove any information about you from databases operated by third parties. They do not accept opt-out requests via fax or mail.

They are not obligated by law to block the records they have control over in their database from being shown on PeopleFinders.com. Despite this, they will endeavor to comply with any such requests to block the records they have control over as described above. Please note, they have no control over public records, and do not guarantee or warrant that a request for removal of or change to personal information as described above will result in removal of or change to all of your information from PeopleFinders.com. Further, they are not responsible for informing third parties with whom they have already shared your personal information of any changes. Just because PeopleFinders.com is associated with a separate aggregator does not mean they will contact them on your behalf to remove your information you must visit each site.

## Google Analytics Opt Out

<https://tools.google.com/dlpage/gaoptout/>

To provide website visitors the ability to prevent their data from being used by Google Analytics, they have developed the Google Analytics opt-out browser add-on for the Google Analytics JavaScript (ga.js, analytics.js, dc.js).

If you want to opt-out, download and install the add-on for your web browser. The Google Analytics opt-out add-on is designed to be compatible with Chrome, Internet Explorer 11, Safari, Firefox and Opera. In order to function, the opt-out add-on must be able to load and execute properly on your browser. For Internet Explorer, 3rd-party cookies must be enabled.

Get Google Analytics Opt-out Browser Add-on

# Opting Out of Public Records and Data Aggregators



This process will not delete your data, only suppress it. These sites update periodically and reintegrate new information. You need to repeat every six to nine months.

- ◆ Conduct research to see what records each data aggregator has collected about you and your loved ones.
- ◆ Some data aggregators may have information about you and your family under multiple listings; you may need to repeat the removal process described below for each listing.
- ◆ Have ALL the required information prepared before you begin the removal process. Also, follow ALL necessary steps to complete the removal process; you may need to mail or fax information to the aggregator.
- ◆ Understand that incorrect information may be a good thing and that it might not be necessary to “fix”.
- ◆ Do not think removing your information from certain data aggregators will suppress everything that’s available about you. Information in data aggregators about family member and associates may still contain information about you.
- ◆ Don’t think you have to delete/suppress all your information on these sites. Remember, some information on data aggregator sites is “normal” since it is collected from places such as Public Records and Credit Bureaus.
- ◆ Do not remove information on other family members. If there is information that you believe is harmful to you, contact your family member and help them to go through the removal process.

Search for your name, names of family members, email addresses, phone numbers, home addresses, and social media usernames using some of the data aggregator links below. Once you have reviewed your information and identified what needs to be removed (if any), you should record your findings to facilitate the removal process. Please note, the information presented here about how to remove personal details from data aggregators is subject to change. Opting out will not remove your information indefinitely.

## Individual Data Aggregator Removal Links

PrivateEye, Veromi, PeopleFinders, and PublicRecordsNow are all owned by the same parent company, Confi-Chek.com. You must still opt out of each individually.

- Opt out of PrivateEye by completing the form at:
- <https://www.privateeye.com/static/view/optout/>
- Opt out of Fastpeoplesearch by completing the following steps at: <https://www.fastpeoplesearch.com/removal> and by visiting the Peoplefinders opt out (url below).
- Opt out of PeopleFinders and Public Records Now by visiting: <https://peoplefinders.com/manage/>
- Opt out of USA People Search by visiting: <https://usa-people-search.com/manage>



## Radaris

To opt out of Radaris follow the instructions at: <http://radaris.com/page/how-to-remove>



## Group Removal Data Aggregator Links/Information

Intelius owns, or is affiliated with, the below sites. When you request removal of your records, also request removal from this network of sites. Opt-out of Intelius online at <https://www.intelius.com/optout>. Of the Intelius affiliates, the following require a separate opt out process where you must fax your ID and a letter containing the information you want removed to **425-974-6194**:

- Peoplelookup, and Phonesbook
- Use the following language on the coversheet:  
*“As per your privacy policy, please remove my listing from iSearch, ZabaSearch, Public Records, PeopleLookup, PhonesBook, LookupAnyone, and all other affiliated people search sites. Thank you for your help with this personal security issue.”*



## US Search/Spock/Lookupanyone

Opt out of US Search by visiting <https://www.intelius.com/opt-out/submit/>. Search for your name and click on the appropriate listing. Print the cover sheet and mail or fax a state issued ID or drivers license to the listed address or fax number. <http://www.ussearch.com>



# Opting Out of Public Records and Data Aggregators



Changing or suppressing your information could cause you problems getting credit. It is important to know what is worth suppressing and what is worth keeping. #themoreyouknow

## Family Tree

FamilyTreeNow allows you to opt out at: <https://www.familytreenow.com/optout>. The entire process takes place in four simple steps, where you must first select your record and then verify it is in fact your record. After you have found and confirmed your record, you simply click “Opt-Out” and you will have completed the process.

It is important to note that if you found your FamilyTreeNow record on a search engine like Google, FamilyTreeNow has a process for its remove, which can also be found using the link above where you will find additional information under “Notes”.



## TruePeopleSearch

To opt out of TruePeopleSearch simply go to: <https://www.truepeoplesearch.com/removal> and follow the three step process.



## WhitePages

To opt out of Whitepages, search for your information using your first name, last name, city, and state. Once you have located your record copy the URL and paste it here, [https://www.whitepages.com/suppression\\_requests/](https://www.whitepages.com/suppression_requests/). Next, follow the steps to complete the removal process. This process will require a phone call from WhitePages (computer generated) in order to complete the process.

<http://www.whitepages.com>



## MyLife

Call MyLife at **888-704-1900**. Press 2 to speak to an operator. Have the following information ready: name, age, date of birth, email, current address, and a previous address. Tell the representative that you want your listing removed and provide the information you want deleted. A second option is to request opt out via email at: [privacy@mylife.com](mailto:privacy@mylife.com). Be sure to specifically request your information is removed from Wink.com as well as MyLife.com. Once they confirm the removal, the listing will be off the site in 7-10 days.



## Been Verified

BeenVerified allows you to opt out at <https://www.beenverified.com/faq/opt-out/>. Search for your listing and claim it by selecting the “>” on the right side of your record. Enter your email address. You must click the opt out link within the email sent to your account. <http://www.beenverified.com/>



## PeekYou

To opt out of PeekYou, fill out the form at: <http://www.peakyou.com/about/contact/optout/index.php>. Select **Remove my entire listing** under **Actions**. Paste the numbers at the end of your profile’s URL in the UniqueID field. Fill in the CAPTCHA, and you’re all set. You’ll get an immediate email confirming you’ve sent in your opt out form and a second email in a few days or weeks to tell you that it has been deleted.

<http://www.peakyou.com>



## USA People Search

To opt out of USA People Search, go to <https://www.usa-people-search.com/manage/> and search for your information. Once you have located your record select “That’s the One.” The next page will be a confirmation that you would in fact like to Opt Out of the USA-people-search database, click the agreement blocks at the bottom of the page and it will complete the Opt Out Process.



## InstantCheckMate

To opt out of InstantCheckMate, follow the instructions at: <http://instantcheckmate.com/optout>  
You can opt out by mail or online.  
You must provide them an email address to send the record removal to.

<http://www.instantcheckmate.com/>



# HOW TO SET UP GOOGLE ALERTS



## Background

Google Alerts is a free Google feature that monitors the internet for mentions of any topic a user specifies. Google collects and packages all instances of these mentions and delivers them to the user continuously (as soon as Google recognizes the mention), daily or weekly. For instance, you may choose to be notified anytime your name is mentioned in an article, when a specific job title is posted, or when your business is mentioned.

## Step 1: Open the Website

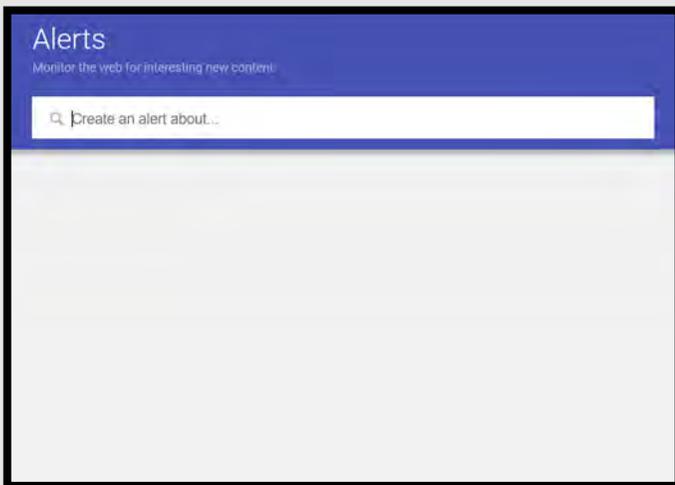
To begin, type “Google Alerts” into your search engine, or you can go directly to the website <http://www.google.com/alerts>. It might be helpful to bookmark this page for easier access in the future.

Tip: You can use the search box like you would in Google Search, but avoid general terms or the vast majority of the results will be wildly unnecessary and difficult to sift through. You can use *advanced search commands*, surround the search in quotes for *phrase searches*, *search on a specific site only*, etc.

## Step 3: Create the Alert

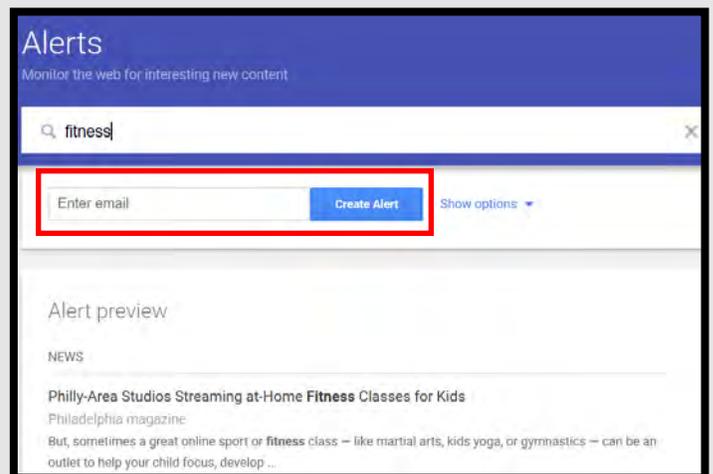
Enter a valid email address, where Google will send you the results of your query. Then complete the process by clicking on the “Create Alert” button. (If it doesn’t ask for your email, you are likely already logged into your Google Account, and will receive the emails in the associated email account). You will receive an email from Google Alerts asking you to confirm or cancel this request. Once you confirm the request, you will begin receiving your alerts. Your first basic Google Alert is now complete. See Step 4 to learn how to further specify search parameters.

Help keep your identity safe by staying up to date on new data breaches - create an Alert for "Recent Data Breach" and monitor results for your information. #databreach



## Step 2: Enter Your Search

Under “Alerts” (highlighted below), enter the topic you would like to receive alerts about. As soon as you begin typing, a sample of your first alert will appear. If you are not getting the results you want, you can change your input right away. You may decide to set an alert for your own name to help monitor what might be out on the internet about you, especially after you have reviewed the “Self-Assessment card”.



Tip: Emails from Google Alerts are sent from [google-alerts-noreply@google.com](mailto:google-alerts-noreply@google.com). You might set up an email filtering rule for messages from that address so that they’re sorted into a special folder instead of in your inbox, where they can easily cause cluttering.



# HOW TO SET UP GOOGLE ALERTS



Help keep your identity safe by staying up to date on new data breaches - create an Alert for "Recent Data Breach" and monitor results for your information. #databreach

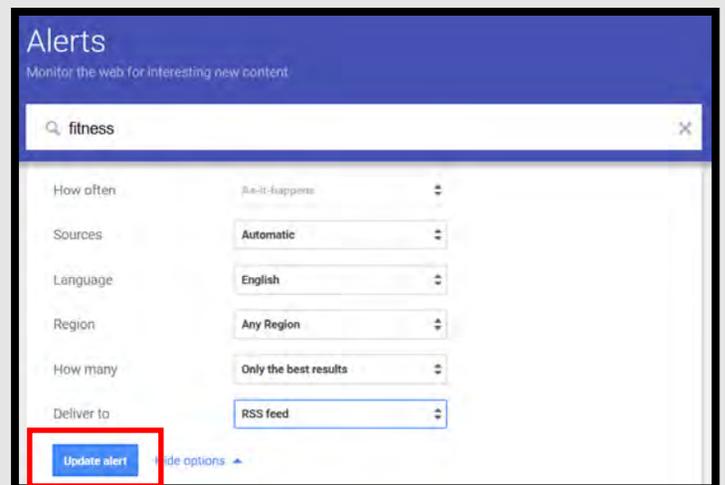
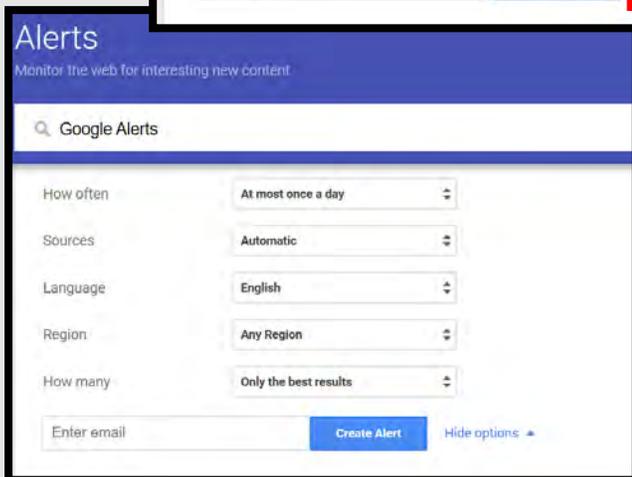
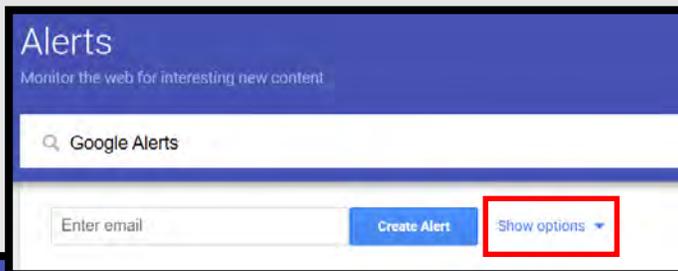
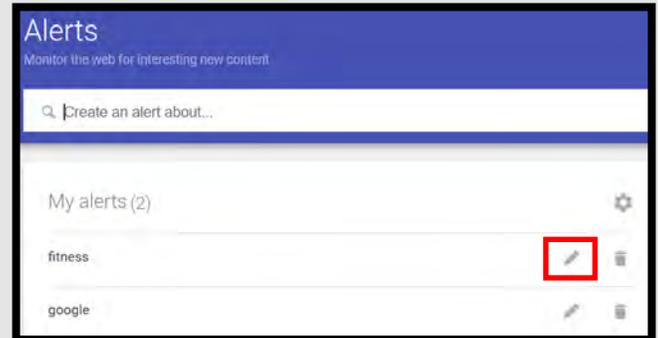
## Step 4: Choose Search Parameters

Select "Show options" to adjust:

- How often you want to receive alerts (choose as it happens, once per day, or once per week)
- The source of the search (e.g., Video, News, Web, Books)
- The language of the source website
- The region in which the search should take place (like the U.S., Egypt, Spain, etc.)
- How many search results you want to see (only the best results or all search results)
- Where to deliver the Google Alerts data (your email address or an RSS feed)

## Modify Alerts

If you would like to modify your current alerts complete the following steps. Select the "Edit" button next to the alert you wish you modify (see the Pencil icon as highlighted below). You may now change the alert keywords, as well as any of the search parameters listed. To finish, select "Update alert" at the bottom.



## Delete Alerts

If you ever wish to delete one or more of your alerts, you can do so easily by clicking the "Trash can" icon next to the alert you wish to delete..





# ONLINE REGISTRATION SMART CARD

Only fill in the minimum required identity information to help limit what human hackers can find out about you. #stopidentitytheft

Online services include sites that require users to register and create personal profiles prior to using their service. Best practices include:

- ◆ Review the terms of service for each site to determine their privacy policy and data sharing agreements with third party entities.
- ◆ Avoid filling in optional identity fields for online profiles; only fill in the minimum required identity information.
- ◆ Never give online services access to your social security number or physical address.
- ◆ Turn down options to upload and share your existing contacts during registration.
- ◆ Check and, if necessary, change privacy settings to protect your personally identifiable information immediately after completing the registration process.

## Identify Elements of Social Networking Site (SNS) Accounts

Online identity can be described as an aggregate of accounts and account-related activities associated with a single person. Common identity elements required by SNS for creating accounts and participating in their online services are shown below.

### First & Last Name

First and last name are mandatory for almost all SNS accounts. In order to better protect yourself, it is important to make sure your account is locked down and consider having a profile picture that is something other than your photo.

### Username

Username is unique to each user account, unlike first and last name which can be shared across multiple users. **DO NOT** include personally identifiable information, such as last name or birthday, when creating your username.

### Birthday

Birthdays are used to verify the user's age and customize age-appropriate content for the user on the site. This information is sometimes published on the SNS profile and must be removed retroactively.

### Gender

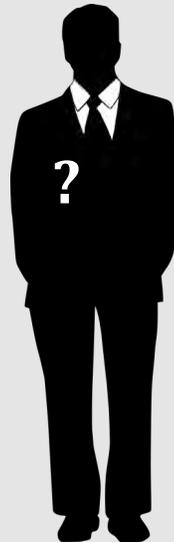
Gender is a common field to fill out on the registration page, used mostly for future content customization. Whenever possible, avoid making a distinction when signing up for your account.

### Company/Employment Information

Company and employment information are required for professionally-oriented SNS services, where the main purpose is to meet and build your network with other people in your field.

### Location: Address, Zip Code, Country

Location information is required to various levels of granularity depending on the service. It may include address, zip code, and/or country.



### Sexual Orientation / Relationship Status

These fields are most often required in **online dating sites**, where the main purpose is to meet people.

### Email Address

Email is the 2nd most common requirement for creating a SNS account. It is used to **verify your account** during registration and often used as a credential during future log-ins.

### Mobile Phone Number

Registering for email accounts frequently requires a verifiable phone number. Refrain from using services that require phone numbers or opt to use an alternative method to verify accounts.



# ANONYMOUS INTERNET & MESSAGING SERVICES



Anonymous email accounts offer no overt or obvious connection to your identity, typically require no personal information to register, and retain little data usage. These accounts should be accessed and used in conjunction with an anonymous IP address.

## “Do’s and Don’ts”

- \* Do always use a secure browser and VPN that anonymizes your IP address when accessing anonymous email services. Be sure your browser is updated regularly.
- \* Do remember, although the tools anonymize you, if you have to pay with traditional means, you can be identified through that transaction.
- \* Do use VPN services. They anonymize your IP address, although you will have to submit personal data to sign up for the service.
- \* Do **not** access more than one account in a single browser session, and never access popular services such as Google or Yahoo in the same session.
- \* Do **not** include personal details in your communication that can be used to identify you, such as your name, phone number or address.
- \* Do **not** use anonymous email services on any device that requires personal logins, such as a smart phone with linked accounts.

## “Using Tor to Anonymize Your IP Address”

Tor Browser is a free, open source web browser that uses a volunteer network of virtual tunnels and a layered encryption process to anonymize your IP address. Note that Tor anonymizes the origin of your traffic and encrypts everything inside the Tor network; however, it *cannot* encrypt the data after it comes out of Tor at the destination. Tor can be installed according to the instructions below

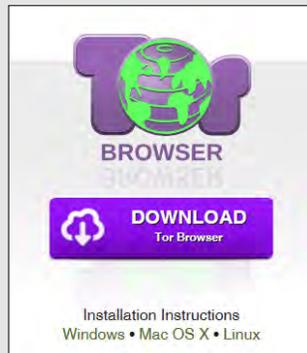
Warning! Tor is generally used when someone needs to hide their computer’s identity or location. It should not be used as a default search engine for everyday internet browsing. Never visit social networking sites or enter any personal data on any website using the Tor Browser — it is poorly regulated and leaves your information extremely vulnerable to theft.

No matter how many tools you use to mask your IP, your payment or signup information could identify you.

Visit [torproject.org](https://torproject.org).

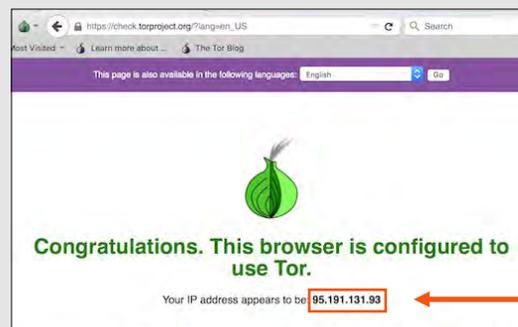
Download and Install the **Tor Browser Bundle** to your hard drive or a flash drive.

1

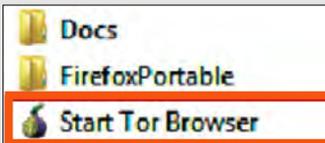


Ensure your Tor Browser is providing you with an anonymous IP address.

3



IP address

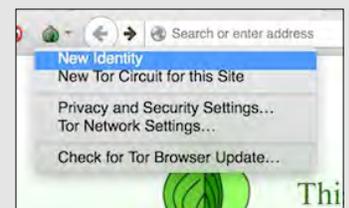


Launch the **Tor Browser** which can be found at the location you saved the bundle to. Double-click “**Start Tor Browser**”.

2

To use a new IP address, click the and select “**New Identity**”. Please note that doing this will close all of your currently opened tabs.

4



# ANONYMOUS INTERNET & MESSAGING SERVICES



There are many email and messaging options out there that can provide a means to send and receive messages anonymously or semi-anonymously. The right service for you will depend on the primary nature of your communications, the cost, and the information you are willing to provide.

Provider	Service	Primary Use	Data Retained	Data Sharing	Cost
<b>Hide My Ass!</b>	VPN Temporary Email	Freely surf the web (VPN). Receive emails and use the inbox for websites that you do not necessarily trust that require you to provide an email address.	IP address, cookies, payment details, username, password, and actual emails. HMA asks for an existing email address at signup but this is optional.	They do not sell personal data to 3rd parties unless required by law. They do share information with members of AVG Group.	VPN as low as \$6.99. Email is free.
<b>CloakMy</b>	One time message and chat service	One time messaging and chat. You have to send the recipient a unique URL to go retrieve the message.	Logs IP addresses	None, does not share or sell information to others	Free
<b>ProtonMail</b>	End to end encrypted email	Fully encrypted email, emails are encrypted client side so they are fully encrypted when they get to the Proton servers in Switzerland	Optional additional email upon sign up for account recovery purposes.	Proton if compelled, which they never have been could only hand over encrypted emails. They do not retain the keys to encryption, the client does.	Free
<b>HushMail</b>	Email host	HushMail is an email host just like Gmail or Yahoo. It is accessible through Tor and it does not require personal information to register.	Browser type, operating system, IP address, credit card information when purchasing product. Retains email messages for up to 18 months, encrypted or non-encrypted.	Logs user IP addresses. They have also turned over user data to U.S. authorities in the past due to court orders.	\$49.98/year
<b>Signal</b>	Encrypted text messaging	Send one-to-one and group messages, which can include files, voice notes, images and videos, and make one-to-one voice and video calls	Signal users must invite each other using mobile number. The service can encrypt messages but not necessarily anonymize users. The encryption is on the users device rather than the company servers	The messages can be set to self destruct after being read. The app does not retain the message. Signal says it will share information with Third Party service providers, and for legitimate legal purposes.	Free
<b>Wickr</b>	Encrypted text messaging	End-to-end encryption and content, expiring messages, including photos, videos, and file attachments and place end-to-end encrypted video conference calls	Wickr users must invite each other using mobile number. The service can encrypt messages but not necessarily anonymize users. The encryption is on the users device rather than the company servers	The messages can be set to self destruct after being read. The app does not retain the message	Free
<b>Mailinator</b>	Temporary Disposable Email	Use the Mailinator address anytime a website asks for an email address. Can only receive email.	No signup required.	Mailinator is a public domain so anyone can read an email if they know what address was used. Use odd names to avoid heavily used inboxes.	Free

Disposable email services allow you to send untraceable, disappearing emails.

# TWITTER SMART CARD



## Do's and Don'ts

- Don't provide any identifiable information (e.g. name, hobbies, job title, etc.) on your profile or in your Tweets.
- Don't link your Twitter account to any third party applications such as Facebook, LinkedIn, or fitness apps.
- Don't allow Twitter to access your location. Disable location services when posting images on whichever device you are using whether it be iOS, Android or uploading them from your computer.
- Don't allow people you do not know in real life to follow you. Only maintain connections with people and pages you know and trust.
- Do be careful when using hashtags # in Tweets as it allows users to index and associate your Tweet with a particular topic.
- Do ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- Do use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- Do use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.

Twitter accounts are hacked all the time. Make sure to use a strong password that is changed periodically as well as 2FA #safetyfirst

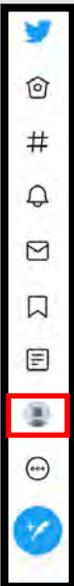
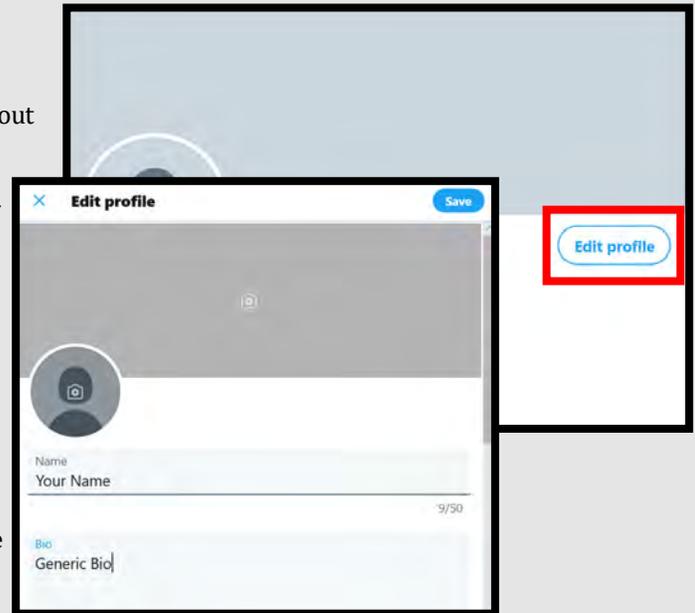
### Personal Computer (PC) Version

Let's start to lock down your account by first checking out what your "Profile" says about you.

Click the "Profile" icon at the lower left of the screen — this is likely your profile picture.

Click "Edit Profile" as shown to the right.

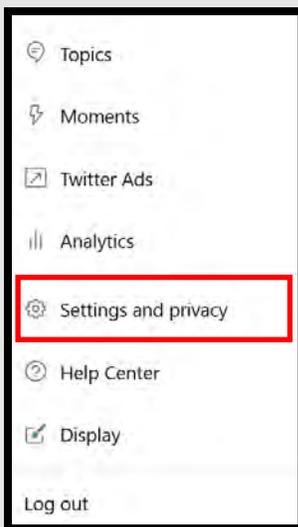
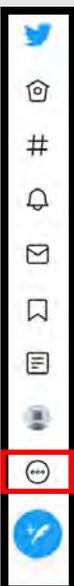
First, notice the "Profile Image" and "Header Image" sections. It is recommended that you do **not** use photos of yourself for your profile and header photos. These are viewable to the public and present an unnecessary vulnerability. Alternative options include avatars and landscape or other types of photos that are not personal and do not contain identifying information within them.



Below the "Profile Image" section are the "Name", "Bio", "Location", "Website" and "Birthday" sections. These are **not** required to be filled in, and it is recommended that you leave them blank or generic. Even if you use inaccurate location data, it is possible for someone to tie the data back to you by using data aggregator sites. Personally identifiable information (PII) is often used as a means to gain access to certain accounts (banks, credit cards, school etc.). Thus, providing even your birthday could help an identity thief steal your identity.

Now, let's move on to the "Settings and Privacy" tab on the same menu at the left hand side of your screen. (see left)

All of these settings need to be separately updated on all the various devices you use to access Twitter, including Android phone, iPhone, and home computers. Twitter is programmed differently on each of these devices, and the settings will not automatically transfer among them. Also, set your "Location" to "Off" on ALL devices.



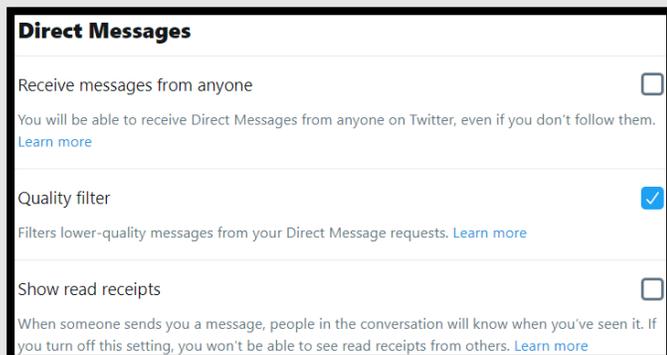
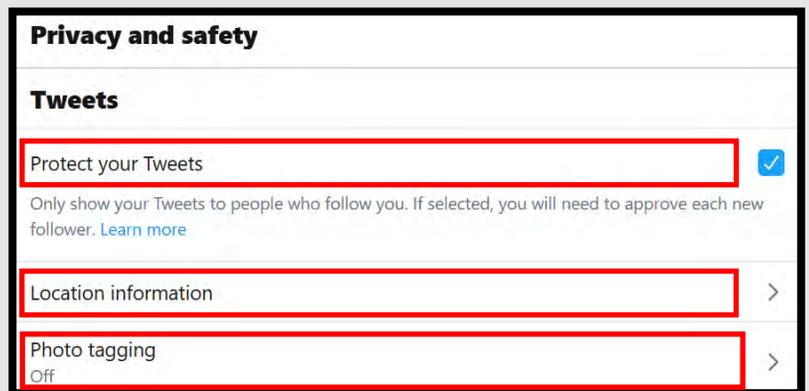
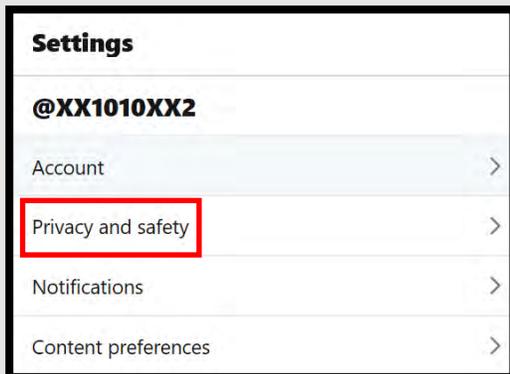
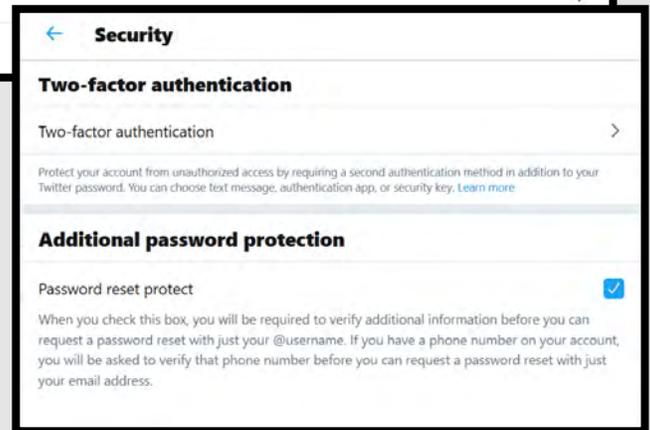
# TWITTER SMART CARD



## Personal Computer (PC) Version

Once in “Settings and Privacy” you can re-view your “Account” information, including “Security” settings and how data, such as your “Username” is displayed. Remember to stop and think about what your “Username” says about you, what is it giving away? In the “Account” section, select “Security”. “Two-factor authentication” is the most secure option, and is recommended for your account. Choose your preferred “Two-factor authentication” option, most likely “Text Message”. Also ensure “Password reset protect” is checked. These settings add layers of protection to prevent your account from being hacked.

Next, go back to the left column, under “Settings” and select “Privacy and Safety” (see below). All the sections in RED (below right) are recommended settings that should be selected. Check the box for “Protect your Tweets”, click on “Location information” and make sure the box on the next screen is **unchecked**. Ensure “Photo tagging” is “Off”. Remember it is always better to control your information than it is to allow someone else to decide for you.



Let’s scroll to the middle of the page and locate the “Direct Messages” section. Uncheck the first and last boxes in this section in order to limit incoming messages from people you do not know.

**Note:** In addition to the information you share with it, Twitter will use your Tweets, content you’ve read, Liked, or Retweeted, and other information to determine what topics you’re interested in, your age, the languages you speak, and other signals. The purpose is generally to show you more relevant content.

Parents! Following your child’s school is important for updates, but if your account isn’t locked down, anyone can see which school your child attends. #lockitdown

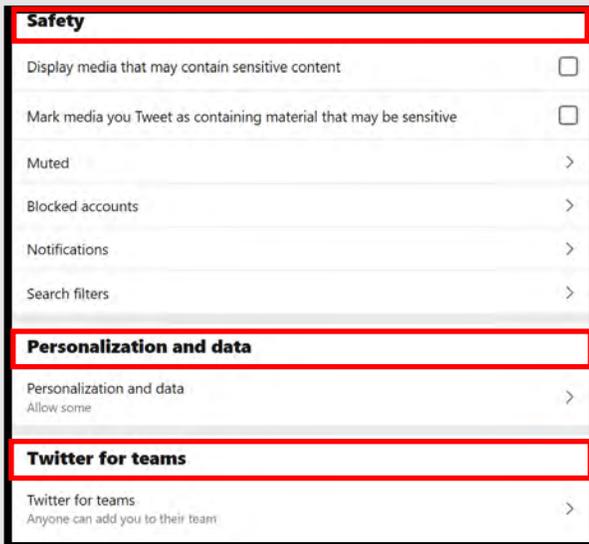
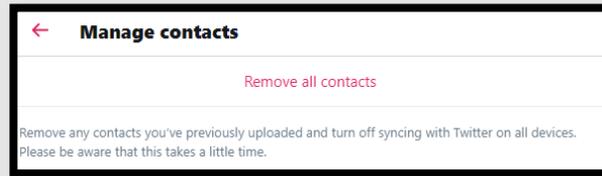
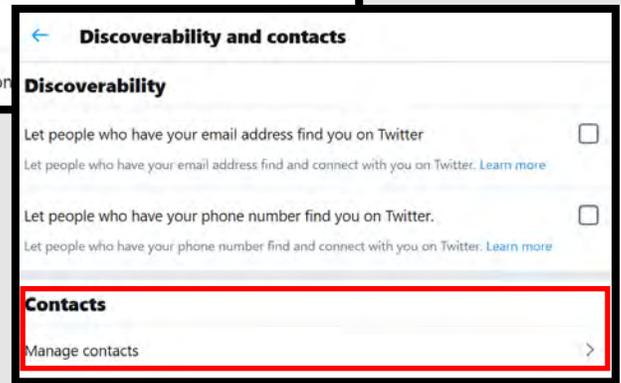
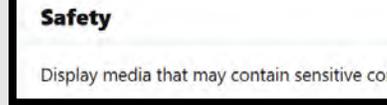
# TWITTER SMART CARD



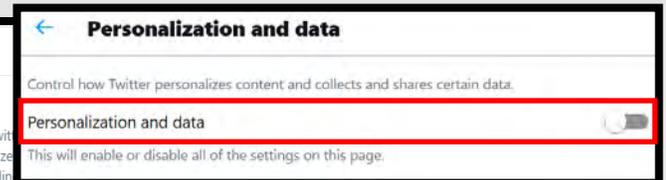
## Personal Computer (PC) Version

Next is the “Discoverability and contacts section” (see right). Ensure both boxes under “Discoverability” are unchecked. It is best to maintain as much control as possible of who is connecting with you.

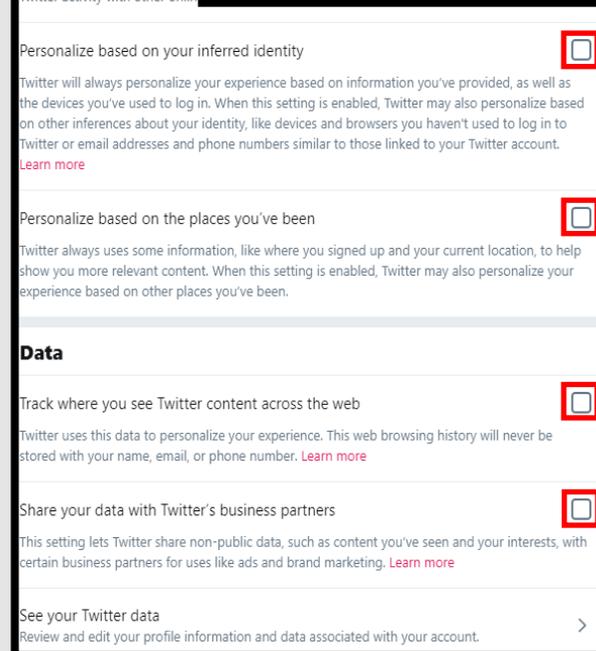
Now click the “Contacts” section. Here you can review and remove any contacts Twitter has collected. It is recommended that you not synchronize any of your accounts together, to include any email accounts with contact information in them. Synchronizing your email accounts allows Twitter to do more than just upload your contacts — Twitter uses the information to learn more about you and your contacts. You should not synch accounts, “Remove all contacts,” if there are any in this section, and remember to keep your identifying information off your own Twitter account, in case your contacts try to import your data to any of their accounts.



Below the “Discoverability and contacts” section is the “Safety” section (left). You may want to review this section in order to better control the types of content you see, and more importantly to control what is displayed on your *child’s Twitter* account.



Next, go to the “Personalization and data” section and disable the “Personalization and data” switch, as shown to the right. This will stop Twitter from collecting data regarding your preferences, locations, behaviors and activities. It is recommended that you fully disable this function. Twitter will always collect some data on you from your account, for instance based on your Tweets, comments, and engagements within the app. But where you can limit such collection, it is advised that you do, in order to control as much as possible, the extent to which your information is passed around the Internet.



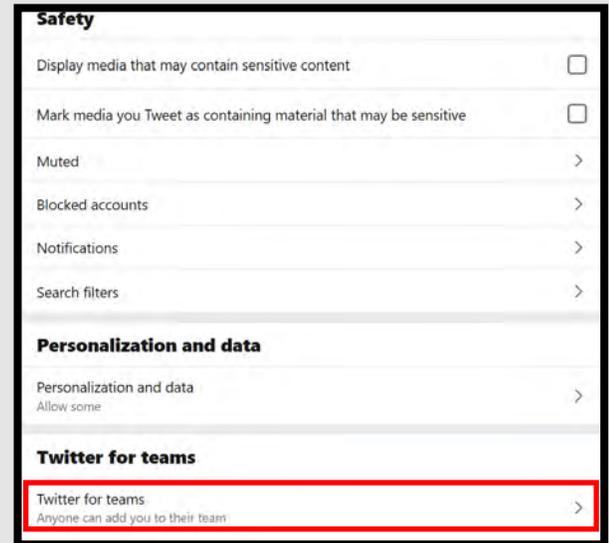
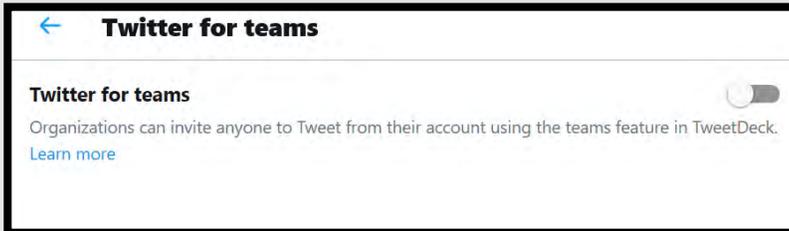
Parents! Following your child’s school is important for updates but if your account isn’t locked down anyone can see which school your child attends. #lockitdown

# TWITTER SMART CARD



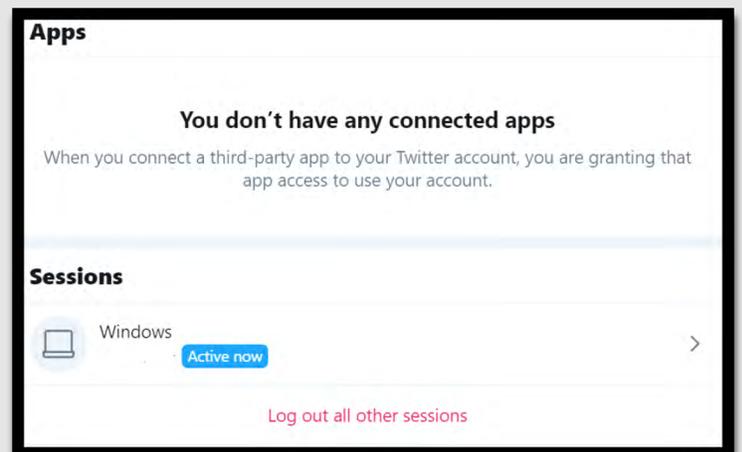
## Personal Computer (PC) Version

Finally, identify the “Twitter for teams” section. It is important to stay in control of who has access to your profile. We recommend you turn the “Twitter for teams” switch off. This will make it so no one can add you to a team without your permission.



In order to manage your Apps and/or sessions go to “Account” and on the right hand column select “Apps and Sessions”. Here you can go through any apps you may have granted access to your Twitter account and revoke access. Limit which apps have access to your account and your personal information.

**App Permissions:** Third-party apps may request access to perform different actions using your Twitter account. Apps with “read access” can view your profile info, Tweets, and account settings. Apps with “read and write” access can view the above information, as well as update and manage your profile and account settings, and post, delete, and engage Tweets on your behalf. Always keep an eye on your “Connected Apps”, especially what permissions they have.



### What are my privacy options?

If you do not want Twitter to show you interest-based ads on and off of Twitter, there are several ways to turn off this feature:

- Using your Twitter settings, visit the **Personalization and data** settings and adjust the setting **Personalize ads**.
- If you are on the web, you can visit the Digital Advertising Alliance’s consumer choice tool at [optout.aboutads.info](https://optout.aboutads.info) to opt out of seeing interest-based advertising from Twitter in your current browser.

If you do not want Twitter to show you interest-based ads in Twitter for iOS on your current mobile device, enable the “Limit Ad Tracking” setting in your iOS phone’s settings. If you do not want Twitter to show you interest-based ads in Twitter for Android on your current mobile device, enable “Opt out of Ads Personalization” in your Android phone’s settings.

If you prefer to opt out of Twitter’s interest-based ads, follow these instructions: go to **optout.aboutads.info** which will then take you outside of Twitter to the Digital Advertising Alliance page where you can not only opt out of ads from Twitter but other ads that might be using your “cookies” to track you. You do need to be logged into Twitter in order to remove the interest-based ads from your account. Additionally, if you are blocking your cookies, you may have to allow access to them prior to beginning the removal process.

# TWITTER SMART CARD



## Mobile Device Version

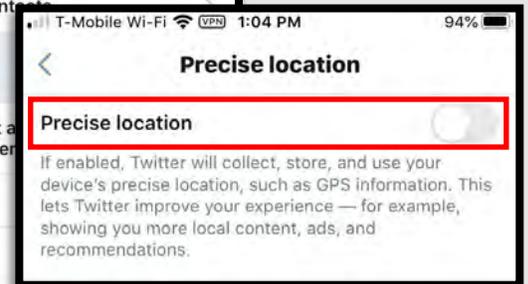
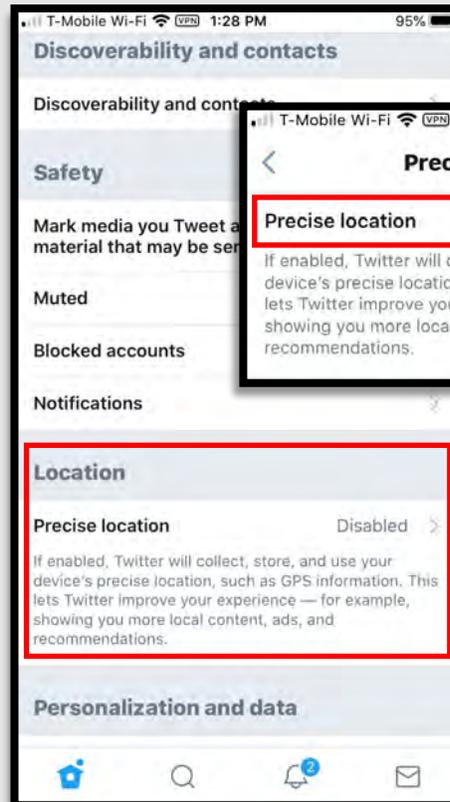
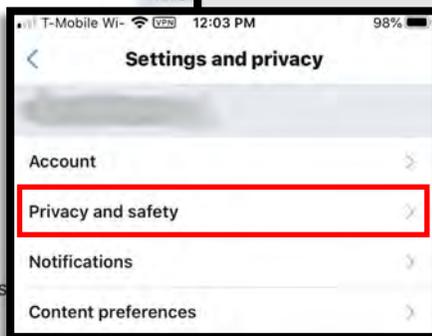
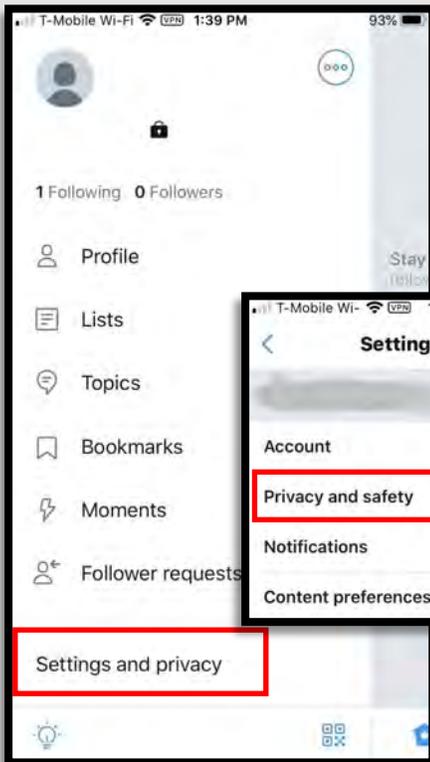
\* Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.

If you frequently access Twitter on your mobile device, you will want to ensure all of the above procedures are completed. Additionally, you will want to accomplish one lockdown feature that is ONLY available on your smart device—the “Precise Location” feature. It is important to turn this feature off because it allows Twitter access to your location for advertisements and photo geo-tagging. Getting to the “Settings” section on your smart phone is one of the biggest differences between the computer-based and phone-based accounts and is shown in the screenshots displayed on this page.

iPhone users: select the “Profile” icon at the top left of the screen, then select “Settings and Privacy” at the bottom of the menu. Next, select “Privacy and Safety”, scroll all the way down to “Location”, and “Precise Location” to ensure it is disabled. (see images)

Android users: getting to the “Settings and Privacy” section is similar to the computer based version. Once you are in the “Settings and Privacy” link, select “Privacy and Safety” then scroll down to the bottom of the page and select “Precise Location.” It is recommended that you turn this function to “disable” and then select “done.” (images not provided, but similar)

Always check to make sure your location settings are locked down on Twitter. This means both on your smart device in the “Settings” section, and via the App.



#TheMoreYouKnow

#DataSecurity

#dataprivacy

#identitytheft

**Hashtags #** are used to index key words and topics on Twitter, think of them as the topic of your “tweet” or “post”. Understand that if your account is public and you use a hashtag on a tweet, anyone who does a search on that hashtag may find your tweet. People use hashtags as a way to improve crowdsourcing requests. When you add a hashtag to a tweet, Twitter adds the message to the hashtag group so more users see your “tweet”. Even if your Twitter account is private and your tweets are protected, be cautious of what you post online. Accounts can be compromised and settings can mistakenly be disabled.

# TWITTER SMART CARD



## Indicators of Possible Account Compromise:

Do you think your account may have been compromised or hacked? Have you noticed any of the following:

- \* Unexpected Tweets posted by your account
- \* Direct Messages sent from your account that you did not initiate
- \* Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- \* A notification from Twitter stating that your account may be compromised
- \* A notification from Twitter stating that your account information (bio, name, etc.) has changed
- \* Your password is no longer working or you are being prompted to reset it. \*If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , Twitter advises you take the following actions:

- ◆ Delete any unwanted Tweets that were posted while your account was compromised
- ◆ Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- ◆ Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- ◆ Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Twitter account
- ◆ Be sure to check that your email is secure. It may be worth changing the password to both your Twitter account and the email associated with your Twitter account.

If you need to report **Spam/Fake Accounts/Harassment**: Go to <https://help.twitter.com/en/contact-us>

If your account was hacked: <https://help.twitter.com/en/safety-and-security/twitter-account-hacked>

Also, if you find that your account has been hacked, it is best to let Twitter know by filling out the "Hacked Account" form located on the forms site at: <https://help.twitter.com/forms>

If you cannot log in to your email account, Twitter has provided links to each email accounts "having trouble signing in" page for your convenience. <https://help.twitter.com/en/managing-your-account/cant-access-my-accounts-email-address>

If you still need help or have questions, you can contact Twitter using their Support handle @TwitterSupport.

**A six character password can be cracked in one second**

**Important Message from Twitter:** Changing an account's password does not automatically log the account out of Twitter for iOS or Twitter for Android applications. In order to log the account out of these apps, sign in online and visit "Apps" in your settings. From there you can revoke access for the application, and the next time the app is launched, a prompt will request that the new password be entered.

If you frequently receive password reset messages that you did not request, you can require that your email address and/or phone number must be entered in order to initiate a password reset. Find instructions and information about resetting your password.

PASSWORD LENGTH	POSSIBLE COMBINATIONS	TIME TO CRACK		
		S = SECONDS	H = HOUR	Y = YEAR
4	45697	< 1 S		
5	1 188 1376	< 1 S		
6	3 089 15776	< 1 S		
7	8 031 810 176	~ 4 S		
8	20 882 706 4576	~ 1.5 M		
9	54 295 036 78976	~ 45 M		
10	141 167 770 956 53376	~ 19 H		
11	367 034 448 698 7780	~ .1 Y		
* 12	954 289 566 616 822 000	~ 1.5 Y		
13	248 115 287 320 374 E4	~ 39.3 Y		
14	645 099 747 032 972 E5	~ 1,022.8 Y		
15	167 725 934 228 573 E7	~ 26,592.8 Y		
16	436 087 428 994 289 E8	~ 691,412.1 Y		
17	1 133 827 315 385 15 E10	~ 17,976,714 Y		
18	294 795 102 000 1390 E10	~ 467,394,568 Y		

# INSTAGRAM SMART CARD

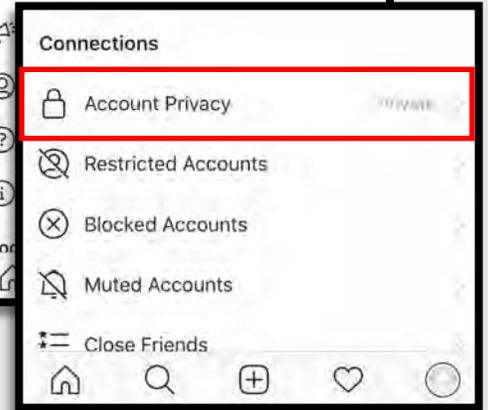
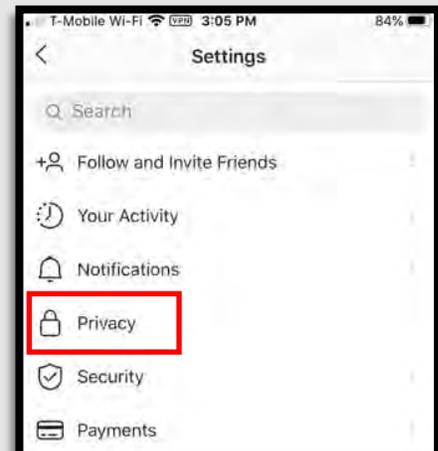
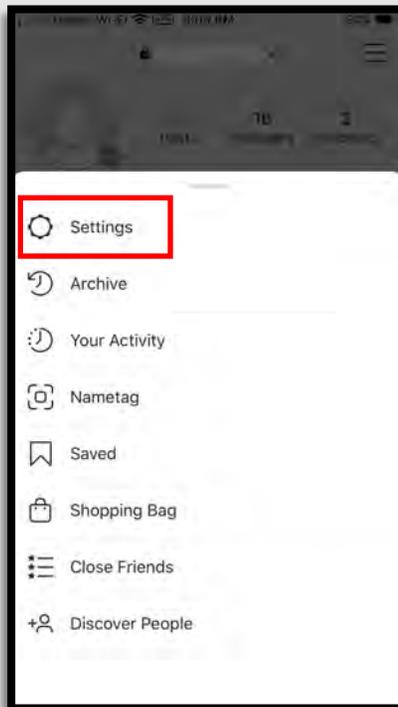


## Do's and Don'ts

- Don't use geo-location tags—this will prevent others from seeing your location. Instagram deletes metadata from a photo the moment of uploading; however, geo-tags that give your location pose a personal security risk.
- Don't establish connections with people you do not know. Understand that people are not always who they say they are online.
- Don't forget to remind family members to take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- ♦ Do use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- ♦ Do remember there are privacy concerns when using your name and birthdate when registering for free services, such as apps and social media. It is not necessary to use your real name or birthdate when creating an account.
- ♦ Do change your password periodically and turn on Two-Factor Authentication to help keep your account secure.

## Mobile Device Version

\* Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.



Instagram now gives you the ability to update your settings on either your mobile device or computer! First, it is recommended to set your account to "Private". In the mobile application, head to the bottom of the interface to the "Profile" icon (noted above) and select it. Next, select the "Menu" icon located at the top right of your screen. Select the first option, "Settings", then select "Privacy." (**Android:** "Settings" located bottom of "Menu" section.) Next, under "Connections", half way down the menu, select "Account Privacy", then turn "On" the "Private Account" toggle. If you are on your computer, the "Settings" icon will be located right next to the "Edit Profile" tab. From there, go back to the "Privacy" tab.

Do not allow your teens and preteens to accept followers that they do not know personally. Instagram has a plethora of fake accounts. #stophumantrafficking

# INSTAGRAM SMART CARD



## Mobile Device Version

\* Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.

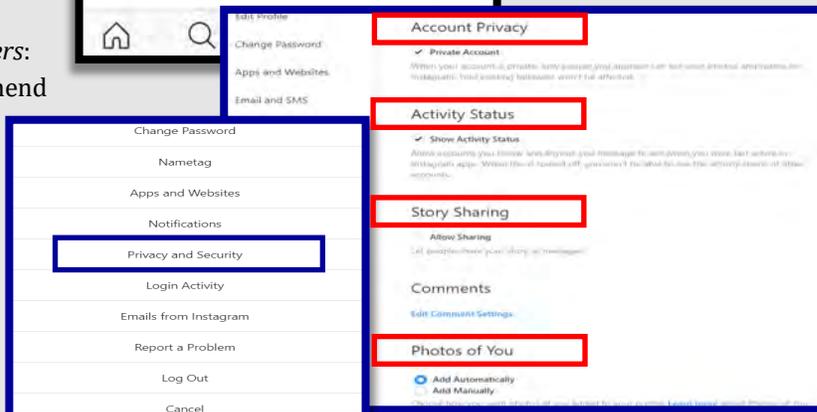
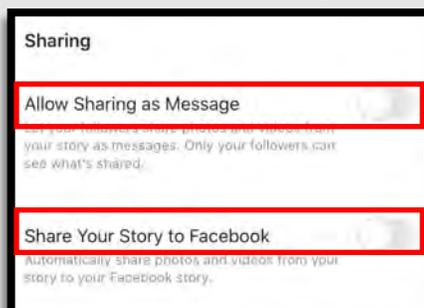
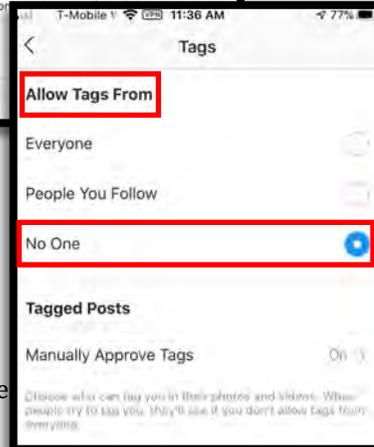
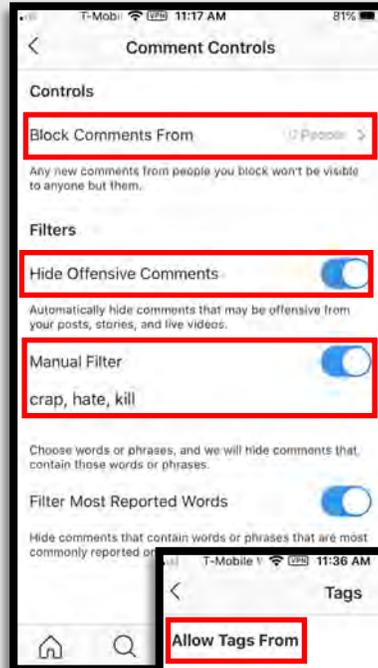
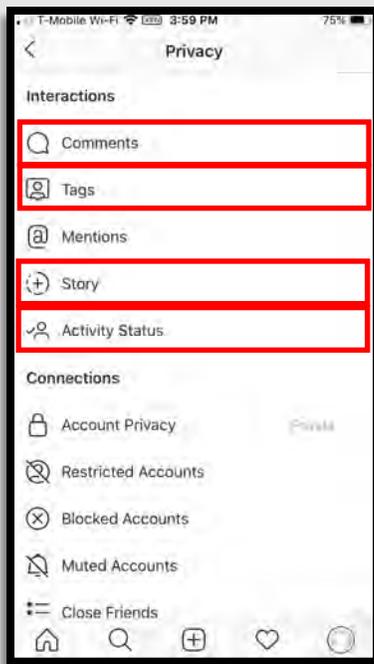
There are many useful features under the “Privacy” tab. First under “Privacy”, choose “Comments”, then “Controls”. Especially for children’s/teen’s Instagram accounts, you may want to filter the kinds of feedback allowed on their posts. Here, you can block comments from certain people, and filter out offensive comments including specific words you designate yourself. (see left)

Next, you want to make sure you are in full control of pictures of you that are online - for this, review the “Tags” menu. From the “Privacy” menu, select “Tags”.

For best security, identify “Allow Tags From” and select “No One”, which will allow no one to tag you in their photos. Alternatively, choose “People You Follow”. Also, under “Tagged Posts”, ensure that “Manually Approve Tags” is noted “On”, or select this option and toggle it “On”. (see left)

In “Privacy” you will also see “Activity Status”. This function allows users to see when and possibly where you are, while active on Instagram. If you do not want users to know when you are active you can select “Activity Status” and then toggle “On” to “Off.”

The remaining items under the “Privacy” tab allow you to restrict, block, and mute Instagram accounts as you see fit. Once you have adjusted the “Privacy” settings on your mobile device, it is a good idea to check them on your computer Instagram account as well, to ensure your preferences have been updated. To get to “Settings”, from “Home Page”, select your “Username”, then select the “Settings” icon next to the “Edit Profile” button. (see left boxes in blue for computer application.)



*Android users:* under “Account Data”, you can view all changes to your account—use this feature as an activity feed to ensure actions taken on your account have been your own.

Next, head to “Story” listed under “Privacy” (see above). Identify the section titled “Sharing”, toward the bottom of the page. Here you will be able to turn off the “Allow Sharing as Message” function, which allows others to share stories that you have posted. It is also recommended that you take a second to ensure the “Share Your Story to Facebook” function is “Off”.

*Android users:* we recommend setting “Allow Resharing to Stories” to “Off” as well.

80% of Instagram users are from outside of the US. Therefore it is extremely important to vet your followers before you trust them with your profile. #trustbutverify

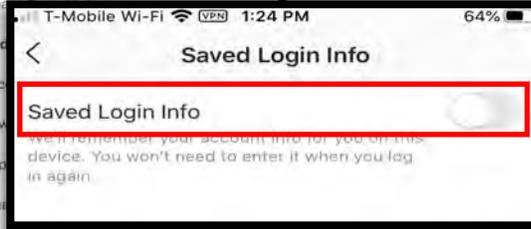
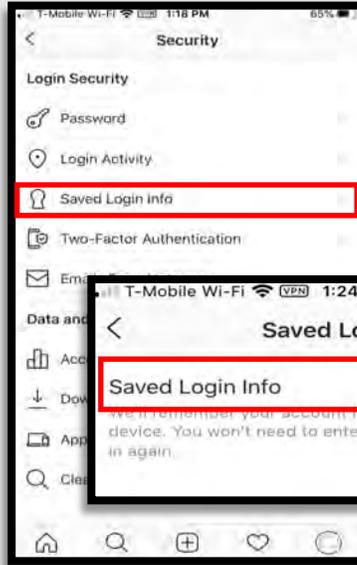
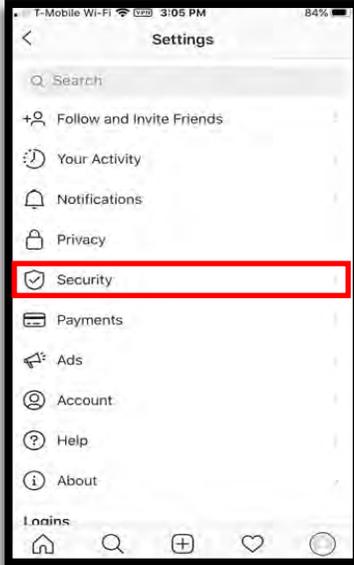
# INSTAGRAM SMART CARD



## Mobile Device Version

\* Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.

Teenagers use Instagram more than any other social networking site. It is important to know who they know and what they are talking about. #keepthemsafe

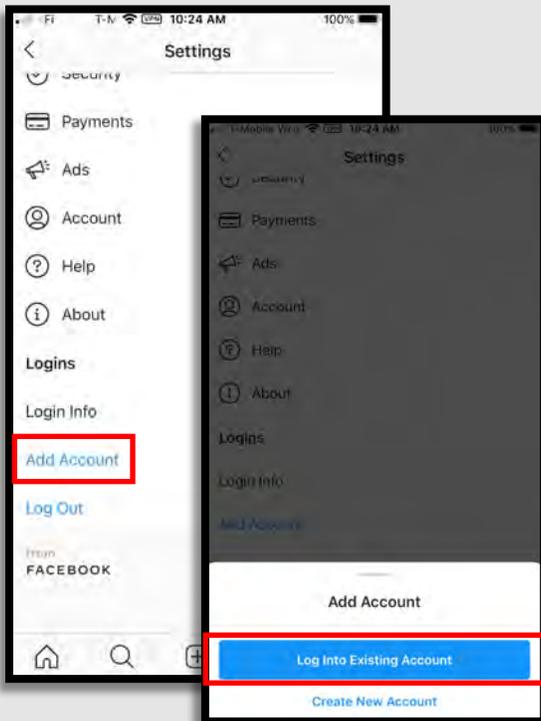
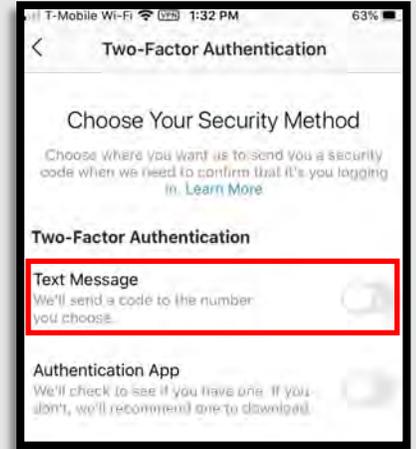


With your “Privacy” secured, the next important feature to address is “Security” on your Instagram account. Back under “Settings”, select “Security”, right under the “Privacy” section you just completed. First, select “Saved Login Info”, then ensure the toggle is set to “Off”. This way, if someone steals your phone, they will not also have instant access to your Instagram account.

“Next, under “Security”, select “Two-Factor Authentication.” It is recommended that you choose this function in order to better protect your account. On the following screen, select “Get Started”, then choose your preferred authentication method, probably “Text Message”.

## Adding Accounts

There is a function located in “Settings”, called “Add Account”, by which you can add unlimited additional accounts to your mobile device. For instance, a parent would be able to add the child’s account to theirs here, and monitor activity. Depending on the settings of the account, you may be able to access the added account without entering a password.



The dangers of this feature are significant for teenagers, who are not inclined to consider security and worse case scenarios. No one should allow others to “Add Account”. In fact, you should try not to access your account on someone else’s mobile device, and always remember to log out, especially when using a different device. Dangers of this situation include: friends can post on your behalf, on your account; friends can send messages on your behalf; friends can do all these things when they become angry with you. The dangers are obvious when considering common teenage behavior.

# INSTAGRAM SMART CARD

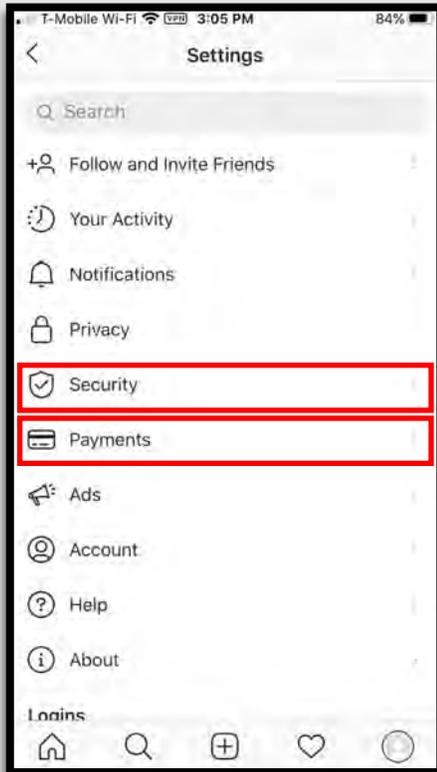
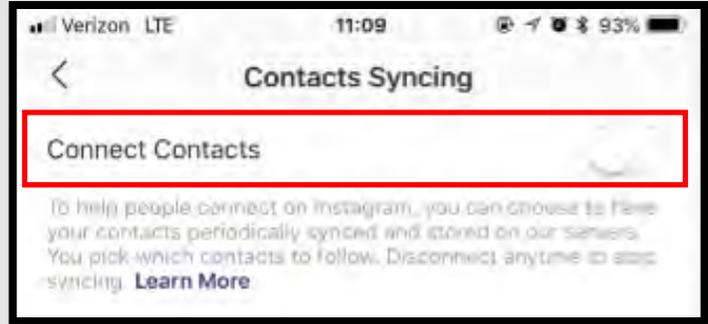


## Mobile Device Version

\* Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.

Teenagers use Instagram more so than any other social networking site. It is important to know who they know and what they are talking about. #keepthemsafe

Next, head back to the “Settings” menu and select “Account” then “Contacts Syncing”. It is recommended that you forbid Instagram from uploading your contacts by turning “Off” the “Connect Contacts” option.

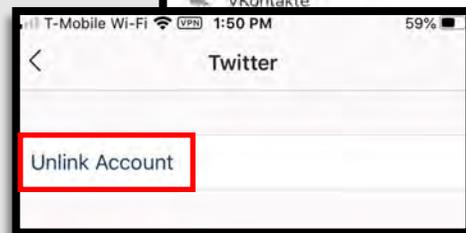


Finally, back under “Settings”, notice the option for “Payments”. (see left) This feature allows you to add a “Payment Method” to your Instagram account. It is not advisable to store credit card or any other payment information on your account.

Next, let’s go back to the “Account” menu (under “Settings”) and scroll down to the “Linked Accounts” tab. Here you want to make sure you have not linked any of your social media accounts to Instagram.



If you have, you will see the username of the particular account to the left of the arrow. The example (right) is clear of connections. If you have any accounts linked,

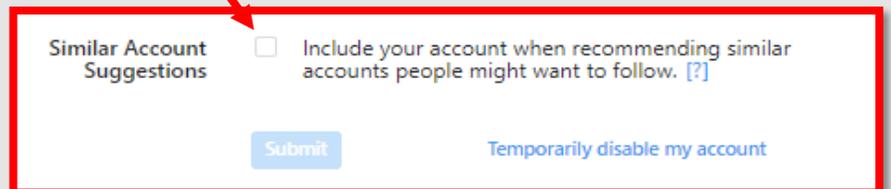
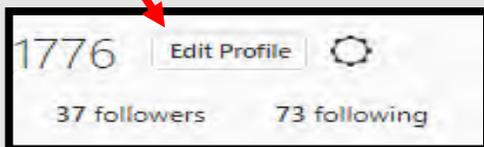


simply select the arrow next to the social media app and unlink the account by selecting “Unlink Account”. Please do check this, even if you believe you have never manually linked an account, just to make sure.



Instagram (on your personal computer / laptop) has a feature that allows it to push your profile to other users as “suggested users to follow”, it is recommended you disable this feature. First, select the “Profile” icon, then select the “Edit Profile” button. Once there, scroll to the bottom of the page and find “Similar Account Suggestions” and deselect the box if checked. Once deselected, Instagram will no longer be allowed to push your profile to other users as “suggested users to follow.”

\*This feature may not show on all Android devices. It is NOT available on iPhone, but you can lock it down on your computer.



# INSTAGRAM SMART CARD



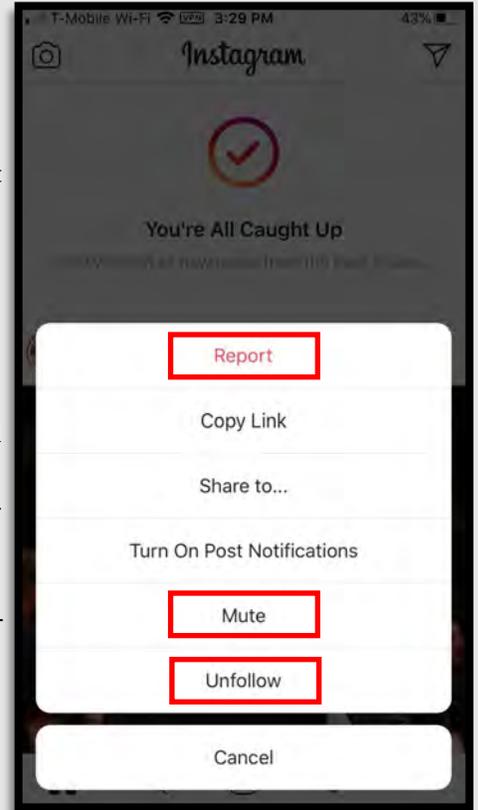
## Mobile Device Version

\* Images are of iPhone Operating System (iOS), but the steps apply equally to Android Operating System (aOS), as differences between the two are negligible.

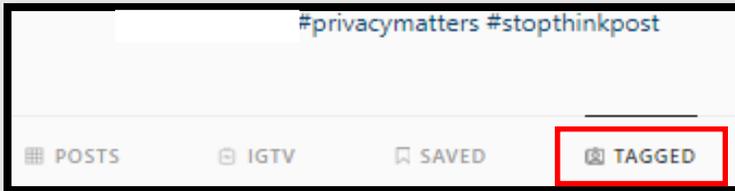
Instagram allows you to have more than one account loaded at a time. Talk to your kids about sharing their usernames and passwords with their friends. #protectourkids



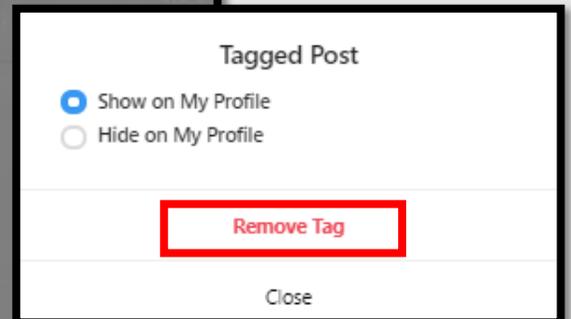
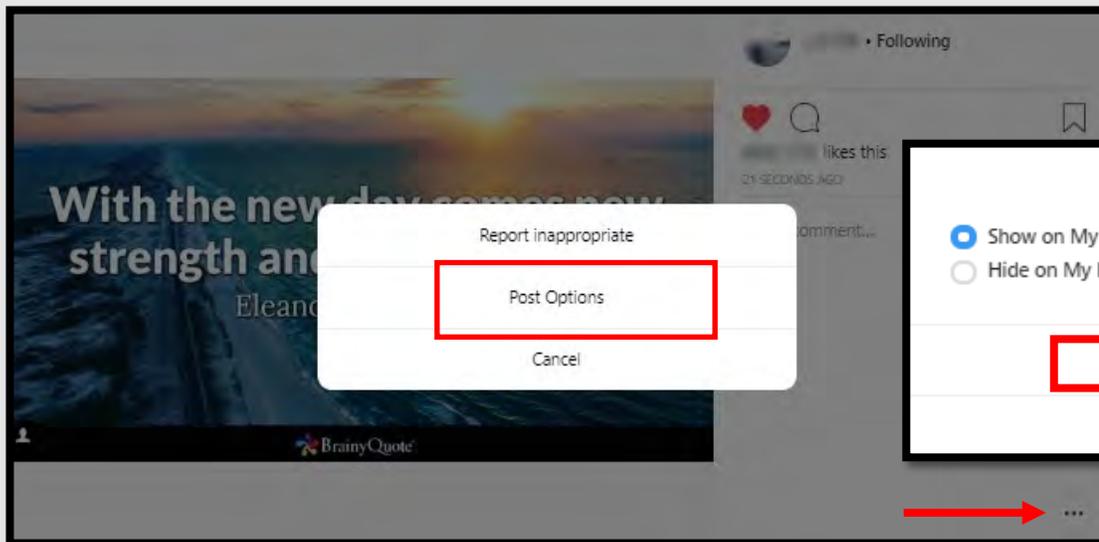
Instagram allows you to report, or remove from your feed, any offensive post you come across. Simply select the menu button at the top right corner of the post and select which option best applies to that particular post from the drop-down menu. You have options to “Report” the offensive post, “Mute” the account that posted it for a select period of time, or “Unfollow” the person who posted it. When you report a post, Instagram will ask you for more information as to why you are reporting it, and then offer suggestions to improve your Instagram experience.



Removing unwanted tagged photos/posts is important. If you have a profile that is “Private,” you are on the right track to controlling your online image. Understand that even if your profile is private, if you tag or comment on a post from a public profile, your tag or comment will be viewable to all.



In order to remove a tag of yourself from someone else’s post you can follow these steps. First, go back to your “Profile” icon and select the “Tagged” icon (see left). Next, select the post you are tagged in that you wish to un-tag yourself from. Find and select the menu at the bottom of the post (shown at the bottom of the page by a red arrow), then select “Post Options.” Next, you can “Remove Tag” simply by selecting the link highlighted here in red. \*This may not be available on all devices, such as iPhone, but it is available on computer.



# INSTAGRAM SMART CARD



## Indicators of Possible Account Compromise:

**Do you think your account may have been compromised or hacked? Have you noticed any of the following:**

- \* Unexpected posts posted by your account
- \* Direct Messages sent from your account that you did not initiate
- \* Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- \* A notification from Instagram stating that your account may be compromised
- \* A notification from Instagram stating that your account information (bio, name, etc.) has changed
- \* Your password is no longer working or you are being prompted to reset it. \*If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , it is advised you take the following actions:

- ◆ Delete any unwanted posts that were posted while your account was compromised
- ◆ Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- ◆ Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- ◆ Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Instagram account
- ◆ Be sure to check that your email is secure. It may be worth changing the password to both your Instagram account and the email associated with your Instagram account. \*If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.

If you need to report **Spam/Harassment**: Go to [https://help.instagram.com/contact/383679321740945?helpref=page\\_content](https://help.instagram.com/contact/383679321740945?helpref=page_content)

If your account was hacked: <https://help.instagram.com/>, then go to "Privacy and Safety Center," "Report Something," and finally select "Hacked."

Also, if you find that someone is impersonating you on Instagram: Go to <https://help.instagram.com/>, then go to "Privacy and Safety Center", "Report Something," and finally select "Impersonation Accounts."

If you still need help or have questions, you can always contact Instagram by: [https://help.instagram.com/contact/272476913194545?helpref=faq\\_content](https://help.instagram.com/contact/272476913194545?helpref=faq_content)

number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	5tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:  
 k – Thousand (1,000 or 10<sup>3</sup>)  
 m – Million (1,000,000 or 10<sup>6</sup>)  
 bn – Billion (1,000,000,000 or 10<sup>9</sup>)  
 tn – Trillion (1,000,000,000,000 or 10<sup>12</sup>)  
 qd – Quadrillion (1,000,000,000,000,000 or 10<sup>15</sup>)  
 qt – Quintillion (1,000,000,000,000,000,000 or 10<sup>18</sup>)

If you received an email from Instagram letting you know that your email address was changed, you may be able to undo this by using the revert this change option in that message. If additional information was also changed (example: your password), and you're unable to change back your email address, then you should report the account to Instagram.

# FACEBOOK SMART CARD

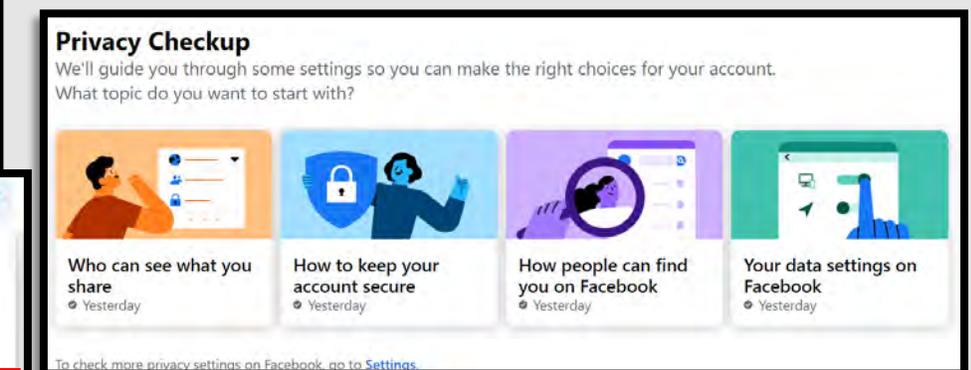
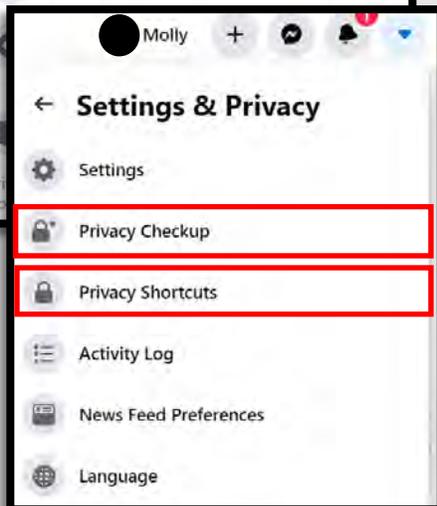
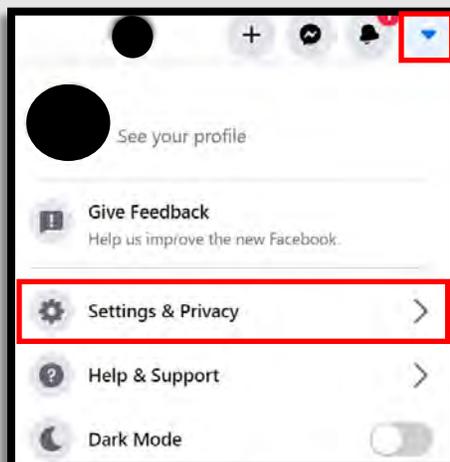


## Do's and Don'ts

- ◆ Do use pictures of something other than yourself for cover and profile photos. Cover and profile photos are viewable to the “Public”. Remember if you change your profile picture you must change the privacy setting from “Public” to perhaps “Friends”, Facebook will not do it for you.
- ◆ Do use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.
- ◆ Do select “Only Me” or “Friends” for all available settings options. Ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- ◆ Don't add your birthdate, location, phone number, or other personal details to your profile. If you do add this information make sure you set it so that it is not “Public”.
- ◆ Don't link your Facebook account to any third party applications such as Twitter, LinkedIn, or gaming apps.
- ◆ Don't establish connections with individuals you do not know and trust. Understand that not everyone is who they say they are.
- ◆ Don't discuss specific details online, keep discussions general. When posting pictures, ensure that no personal information can be seen in the background. For instance, if you are posting a picture of your car you will want to make sure the license plate is not showing.

## New Design & Quick Privacy

Facebook published a new platform design in 2020, with the purposes of providing a simplified user experience closer to the mobile app version, faster performance, and new features. Facebook's new design provides several privacy and security updates, most notably more access to information and explanations regarding your options. The information provided in these pages will walk through the entire process of locking down your Facebook account. However, if you are in a hurry, you can access an abbreviated version of Facebook's privacy and security options by going through the “Privacy Checkup” and “Privacy Settings” features on your account. Start at your “Home Page”, select the “Down Arrow” in the top



Next, select “Privacy Checkup”, and walk through each box on the screen that follows. Again, it is an abbreviated version of the manual provided here, we recommend you work though this whole Card at your convenience. You could also use this feature to complete easy quick checks on a regular basis, for instance each month, just to make sure you stay on top of changes.

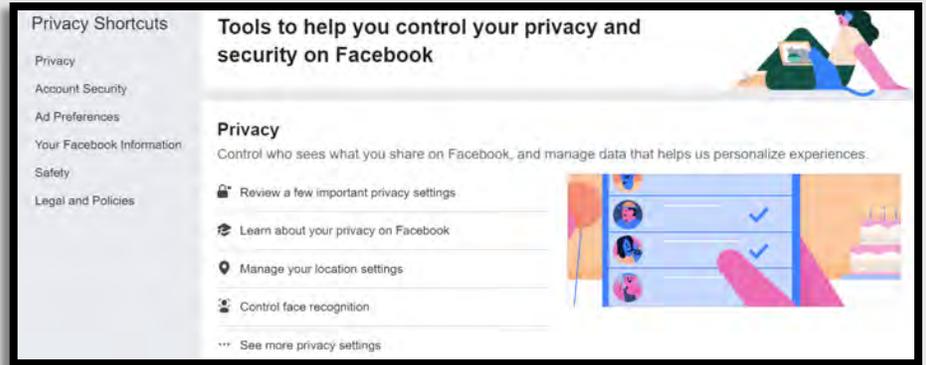
Facebook quizzes could be taking more from you than you realize, Think twice about finding out which Star Wars character you are. #keepyouridentitysafe

# FACEBOOK SMART CARD



## Personal Computer (PC) Version

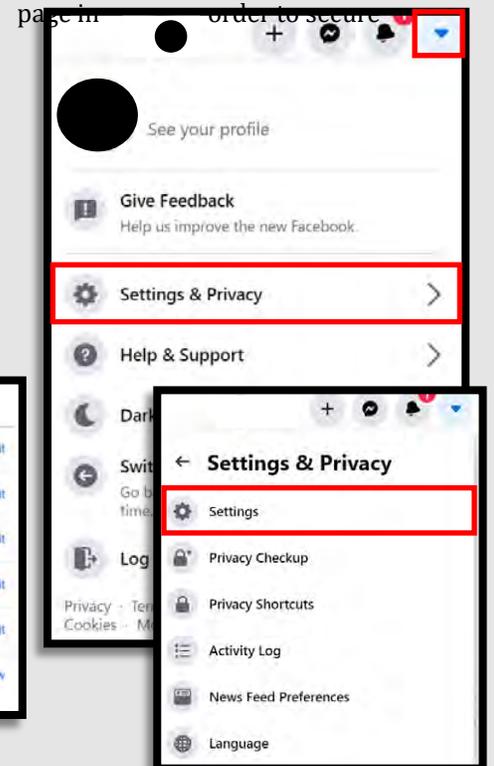
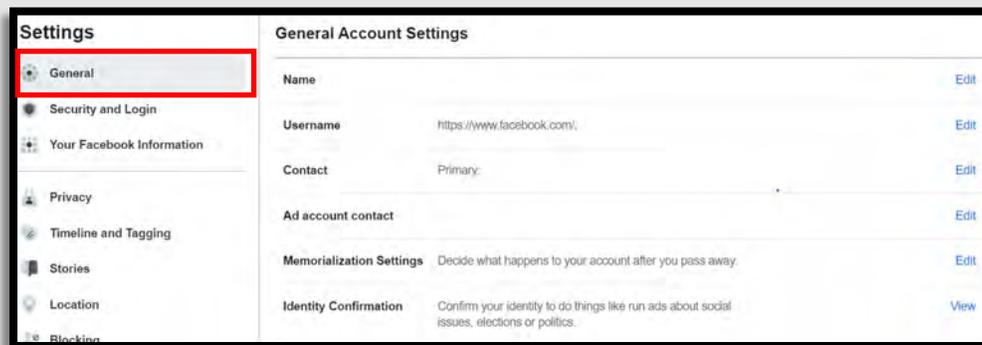
Secondly, you can select “Privacy Shortcuts” (see previous page), which will take you to the page seen here to the right. Here, you can go through some additional privacy information (all of which will be covered in the coming pages), and access useful information about things like privacy, how Facebook’s ad policy and processes work, and resources for parents. Again, feel free to go through this information, but also complete the full Card, beginning below, for our most thorough lock down guidance.



Facebook continuously works to enhance its privacy efforts and better protect user data. As a result, many settings have changed and more have been added. To begin, click the “Down Arrow” at the top right corner of the Facebook screen. From the drop down, select “Settings and Privacy”, and then “Settings”. You will want to go through each menu item on the next

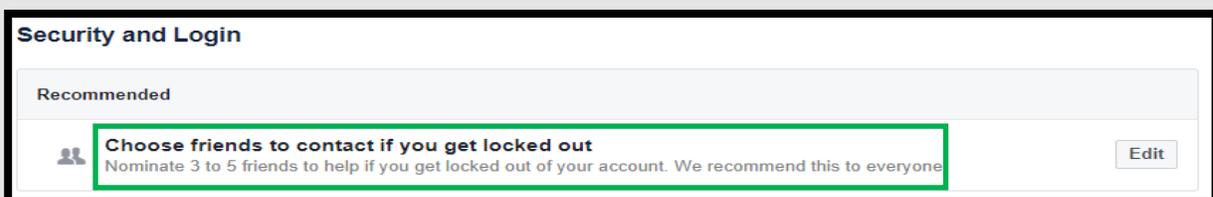
## General Account Settings

Starting in the “General” section (see below), go through and review your information. Remember, your “Username” (which is located in the URL) will be “Public” on Facebook, just as your “Name” is. In this section you can add a new email address and phone number, direct what happens with your account when you die, and direct Facebook ads to a new email address.



## Friends can help if you get locked out!

Next, head back to the left-hand column and select “Security and Login”. Here you can check and update your security settings and see all the places that Facebook thinks you are logged in at. First look at the “Recommended” section, shown below. It is recommended that you choose friends that can help you to log in to Facebook should you ever become locked out.



It is not possible to lock down someone else's account so it is important to note the privacy setting on a post before you "Comment" or "React" to each post. #privacymatters

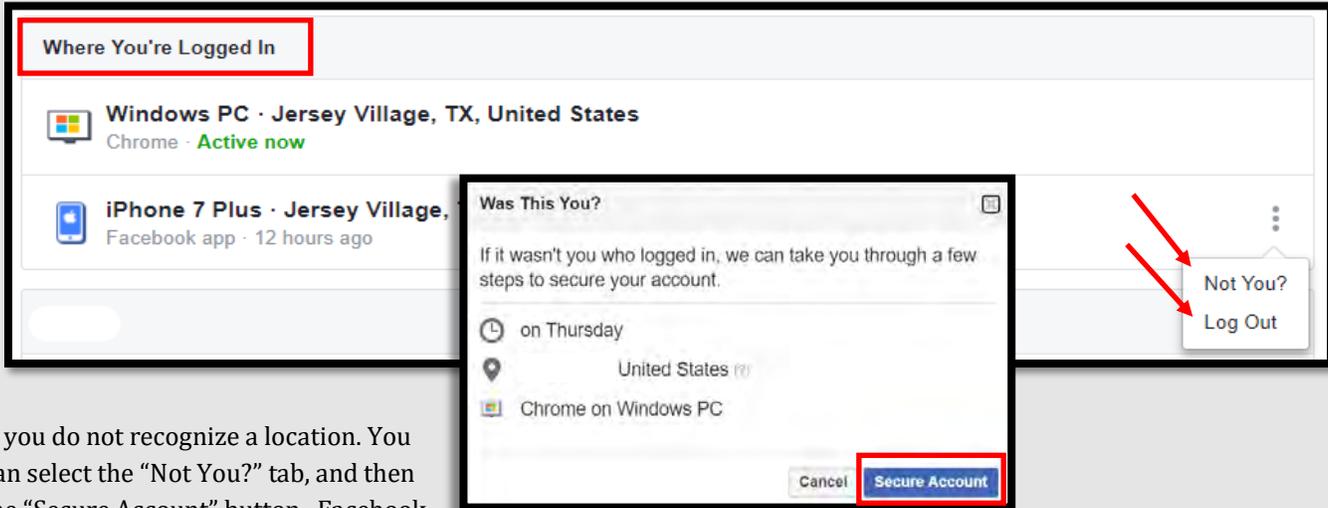
# FACEBOOK SMART CARD



## Personal Computer (PC) Version

### Login & Two Factor Authentication

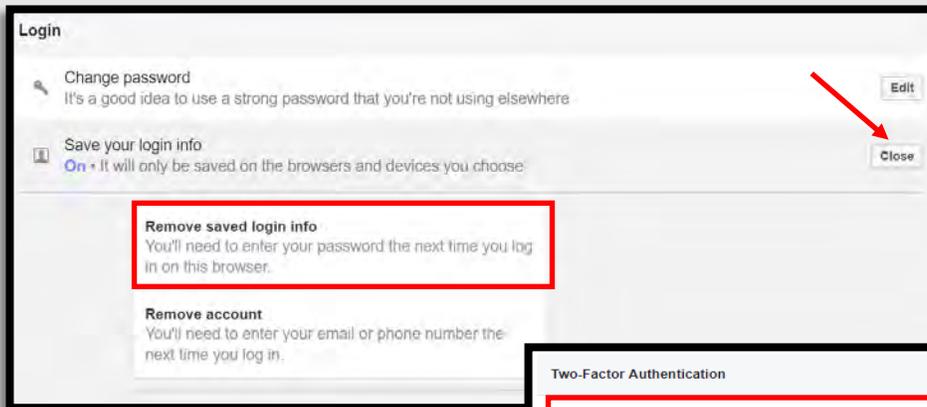
Once you have selected your friends as an additional security measure, scroll to the “Where You’re Logged in at” box and look to ensure you recognize each location Facebook says you are logged in from. Some of these locations can be repetitive based on how many times you log in or for each different session.



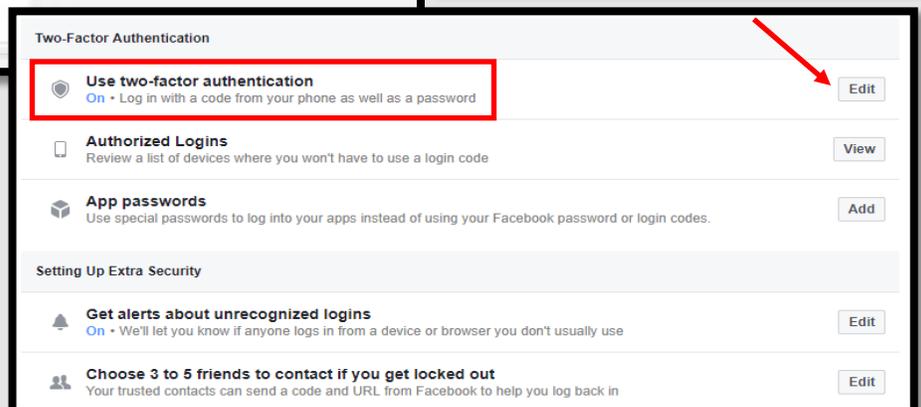
If you do not recognize a location. You can select the “Not You?” tab, and then the “Secure Account” button. Facebook will take you through some steps to help you ensure your account is secure.

Next, under “Login”, and “Save your login info”, you have the choice to keep yourself logged in on any device you choose. We recommend that you NOT enable this function, and instead choose to log in each time you open Facebook. This way your account is secure even if you lose your computer or mobile device. Select the “Edit” button to the right, and then select “Remove saved login info”.

An unrecognized login location can be the result of a few different things. First, when signing in via mobile device, you may be routed through an IP address that doesn't reflect your actual location. Second, Facebook may have inaccurate information. Third, you may remain logged into a device that you logged onto in an alternate location. And finally someone else could have unauthorized access to your Facebook account. If an unrecognized location seems to be due to unauthorized access it is recommended that you immediately go in and change your password on both Facebook and your email account.



We recommend that you enable “Two-factor Authentication” in order to equip your account with the highest level of security available. Click on the “Edit” button to the right of “Use two-factor authentication”, and choose the security method you prefer or are most familiar with. A security code will be sent to you for entry each time you log in.



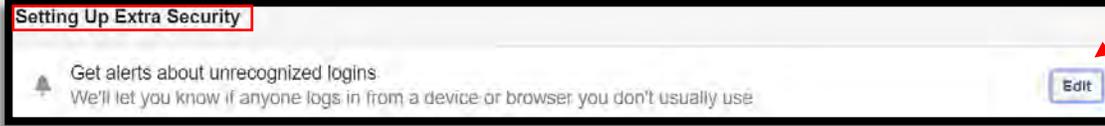
It is not possible to lock down someone else's account so it is important to note the privacy setting on a post before you “Comment” or “React” to each post. #privacymatters

# FACEBOOK SMART CARD

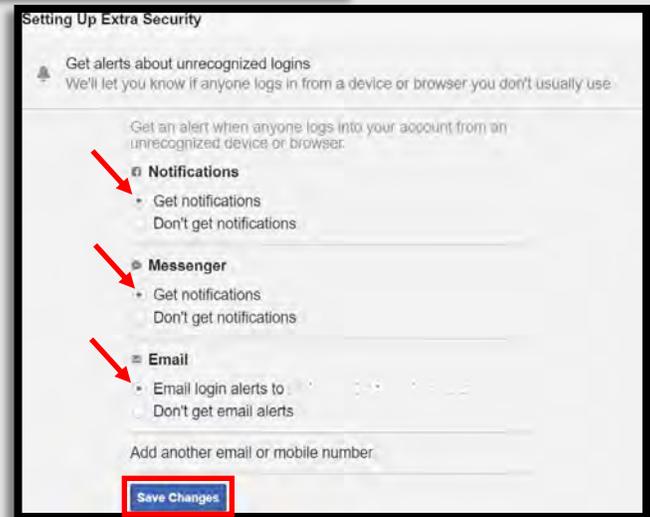


## Personal Computer (PC) Version

Never become complacent with your Privacy settings. Checking your settings once a quarter could help to keep your information safe online. #updateyourprivacysettings

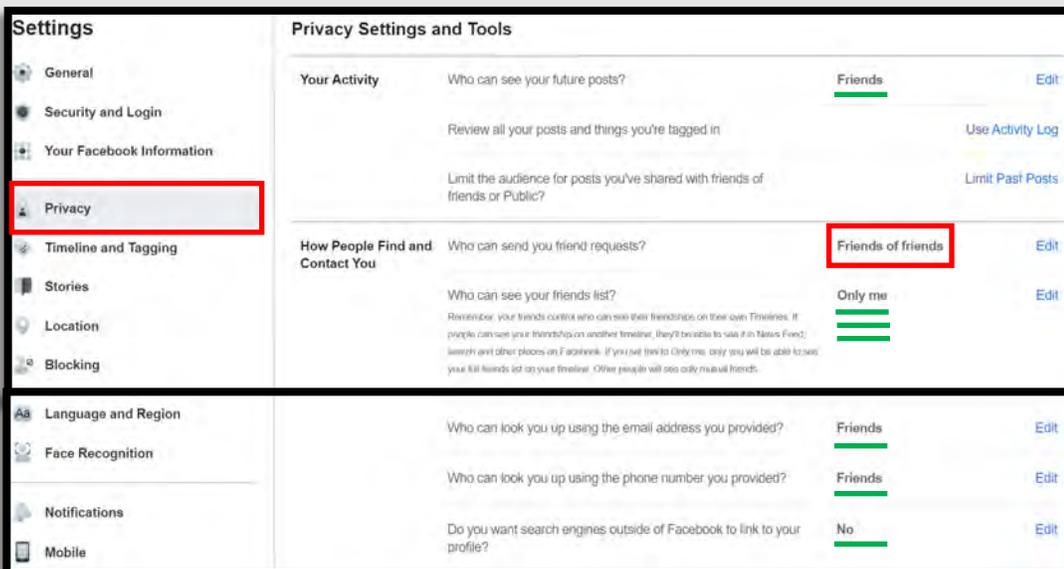
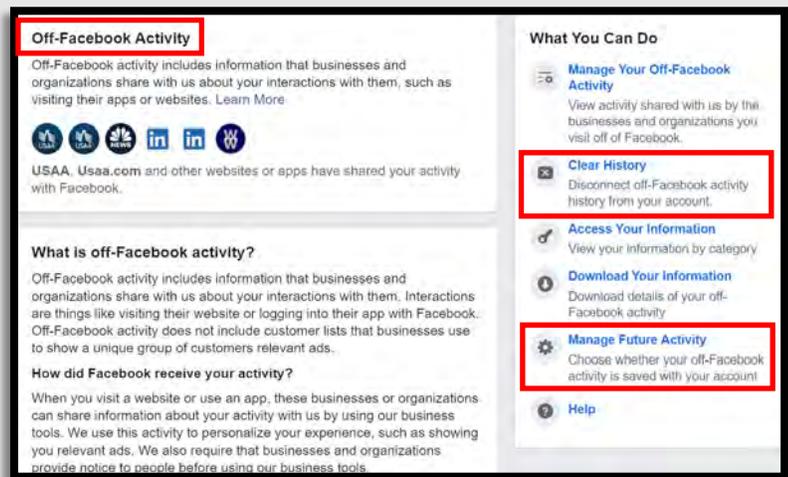


Finally, it is a good idea to request notification in the case that someone logs into your account without your permission. To do this, under “Setting Up Extra Security”, and “Get alerts about unrecognized logins”, to the right, click the “Edit” button. Then select the buttons under “Facebook Notification”, “Messenger” and/or “Email” to direct where you would like to receive such messages. To complete, click on the “Save Changes” button.



Next, go back to the column on the left hand side and select “Your Facebook information”. Here you can easily manage the information you have allowed onto Facebook or delete your account entirely. \* Time Saver...both the “Access Your Information” and “Activity Log” sections take you to the same “Activity Log” page, and allow you to manage your information.

**Next select “Off-Facebook Activity” and clear your history. It is highly recommended that you forbid Facebook from tracking your “Offline Activity. Select “Clear History” and click on the “Clear History” button on the pop-up. Also consider selecting “More Options”, then “Manage Future Activity” in order to limit the kinds of information Facebook can collect from your “Off-Facebook Activity “ in the future. Follow the prompts to “Manage Future Activity”.**



Now look at the tabs on the left and find the “Privacy” section. Completing this section is one of the most important aspects to keeping your information safeguarded on Facebook. This section puts you, the user, in charge of decisions about where your data goes and who can see it. Take some time here to ensure each section is set to your preference. **\*\* Guidance for the image to the left “Privacy Settings and Tools” page is found on the following page. \*\***

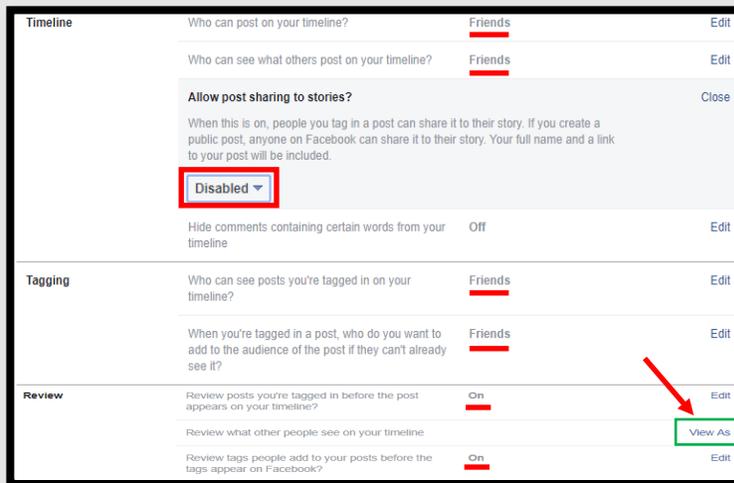
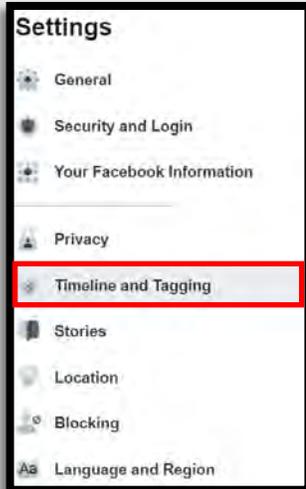
# FACEBOOK SMART CARD



## Personal Computer (PC) Version

**\*\* This paragraph applies to the “Privacy Settings & Tools” page image above, or on the previous page. \*\*** We recommend no category be set to “Public”. Preferable settings are noted below. We recommend choosing “Only Me” wherever possible, but understand that this sometimes undermines the social purpose of Facebook. Still, we strongly recommend you leave the “Only Me” setting for “Who can see your friends list” in order to protect yourself and your social network—this list simply gives away too much information about you. Where you cannot leave “Only Me”, the next best option is to choose “Friends”. Finally, we recommend you do NOT allow Facebook to link other search engines to your profile.

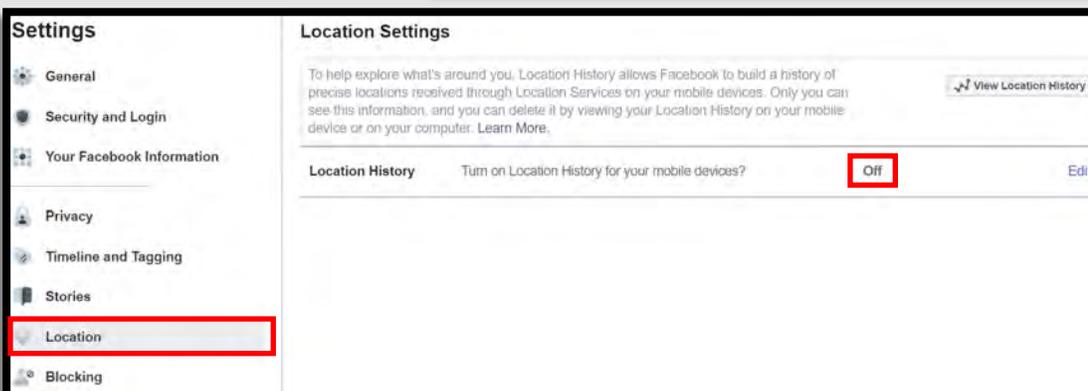
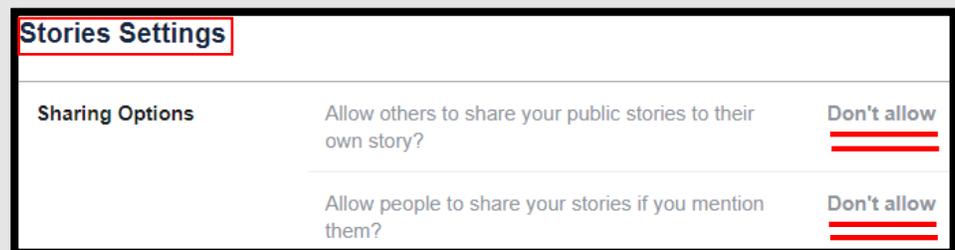
### Privacy & Stories



Next, back under “Settings”, right under “Privacy”, you will find “Timeline and Tagging”. Take a few moments here to make sure you agree with all the settings. Some recommendations for this section are the following: ensure nothing is set to “Public”; make sure to turn “On” each section under “Review” so that no one can tag you in anything without your permission.

Under “Review”, you can also view your profile from the perspective of the public, or people who are not your “Friends”. Simply select “View As”. While reviewing your profile from the public perspective, take note of anything you see that you might want to lock down later, such as old profile pictures.

Since the “Stories” function has become more popular, it is important to remember it also needs to be locked down. Facebook has created a new feature that prohibits others from sharing your “Stories”. Select “Stories” from the “Settings” menu, and set both “Sharing Options” to “Don’t Allow”.



In the “Location” section make sure Facebook shows your location is “Off”. You must also turn your location settings to “Off” on each of your mobile devices to ensure the pictures/ data you post do not contain geolocation information.

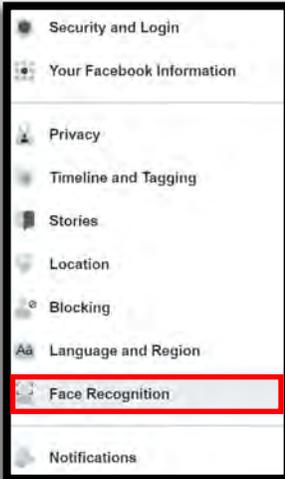
Letting people know where you are at the exact moment you are there can be an extremely dangerous choice. #thinkbeforeyoupost

# FACEBOOK SMART CARD

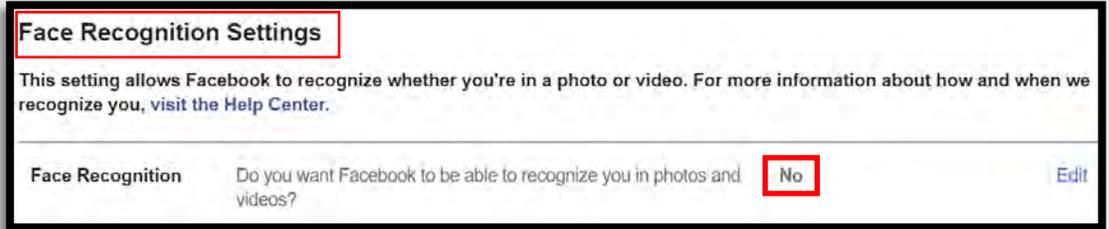


## Personal Computer (PC) Version

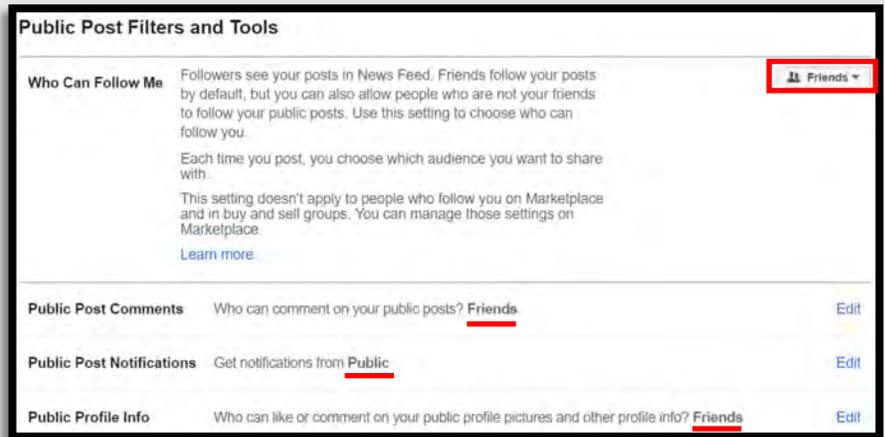
Managing your Facebook Profile is important. Equally as important, is knowing what other users are saying about you. #ownyourprofile #fbtagging



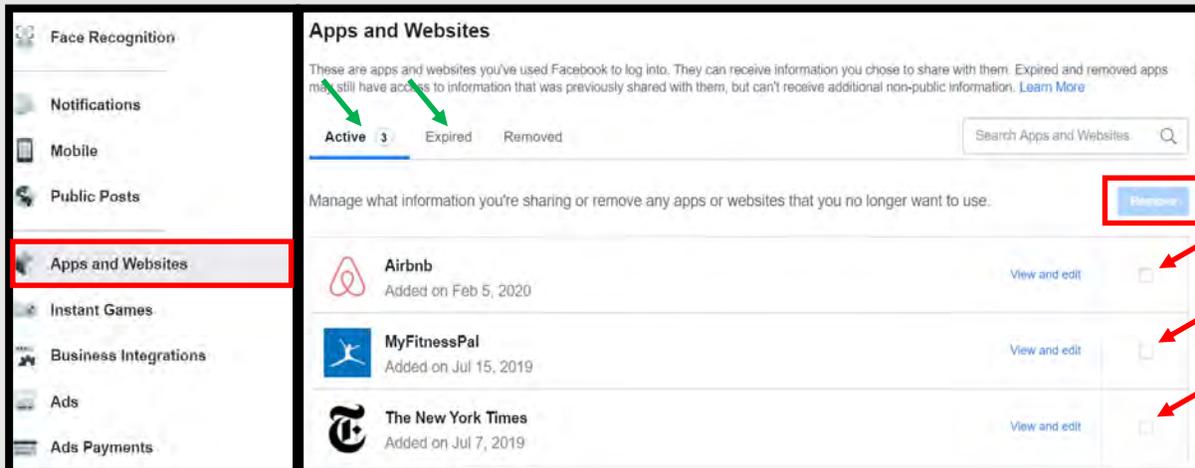
Do you want Facebook to be able to recognize your face in pictures? Neither do we! Recommended setting for this section is easy — “No”.



Next, in the “Public Post Filters and Tools” section, under “Public Posts” in “Settings” let’s review public filtering. It is recommended that you do not let the “Public” follow you. Remember, allowing the “Public” to follow you means anyone with a Facebook profile, and possibly even without one, can see what you are posting.



Now let’s clean up all the “Apps and Websites” that Facebook has been allowing to use your information. Here you can review all the applications you may have allowed access to your Facebook account. Select “Apps and Websites”, in the “Settings” menu.



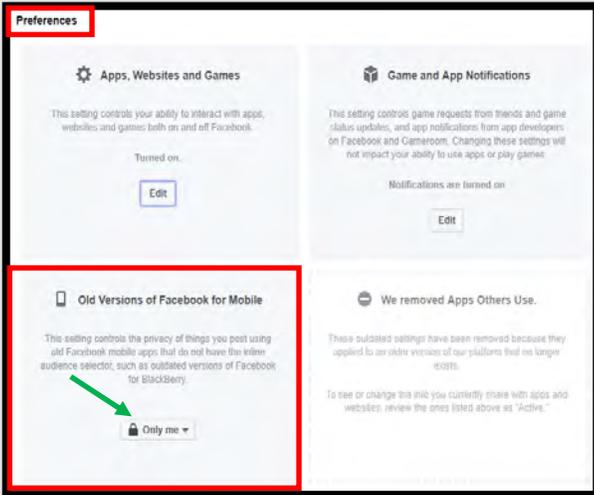
If you find apps that you no longer wish to have access, simply check the box and then select “Remove”. Make sure to do this for the “Active” and “Expired” sections tabs at the top of this box.

# FACEBOOK SMART CARD



## Personal Computer (PC) Version

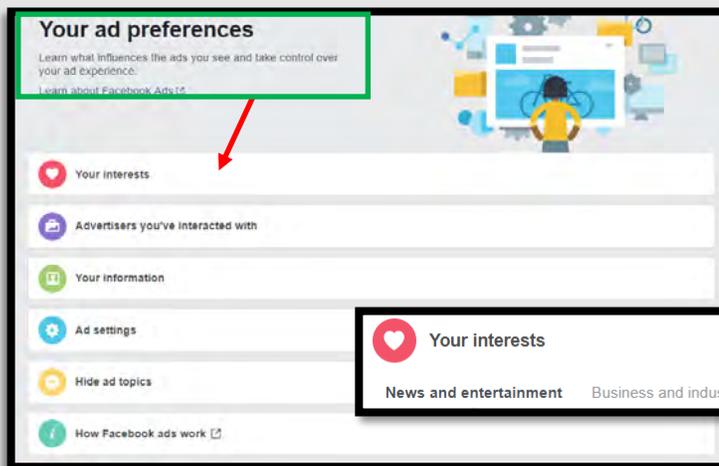
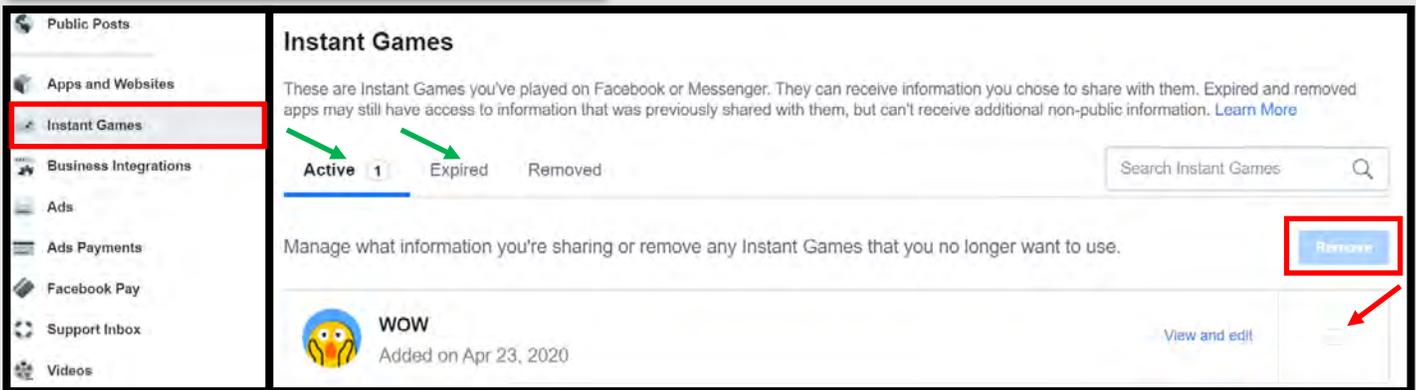
Never give up too much information, drawing out your family members on Facebook could help an Identity Thief answer security questions about you. #themoreyouknow



Next scroll down to the “Preferences” section on the same page. Here you can control how “Apps, Websites, and Games” are able to interact with your Facebook account.

We recommend that you keep the “Old Version of Facebook for Mobile” in a setting set to “Only Me” so that it is not viewable to any one else.

Now click on the “Instant Games” tab in the “Settings” menu. Review any games you may have allowed access to your account, the type of data they are collecting, and whether or not you want them to remain. If you choose to, you can delete any of the games, much like you just did in the “Apps and Websites” section. (see below)



Let’s look at “Your ad preferences”. Select “Ads” on the “Settings” menu (not shown), and see the page “Your ads preferences”. Under each tab you can review your information by clicking on the down arrow in the right hand corner of each category. Under “Your Interest” and “Advertisers you’ve interacted with”, you can remove any of the selections by clicking the “x” at the right of each tile.

1

*Some users are so overwhelmed by the curiosity that they tend to ignore some of the risks involved, and inadvertently give the app access to sensitive data.*

References:

1. <https://www.thequint.com/tech-and-auto/tech-news/sharing-data-with-facebook-apps-and-games-can-have-serious-consequences>

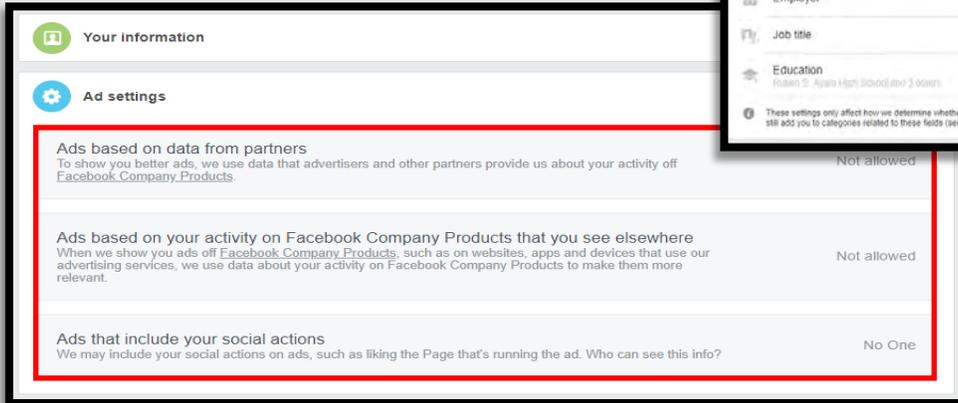
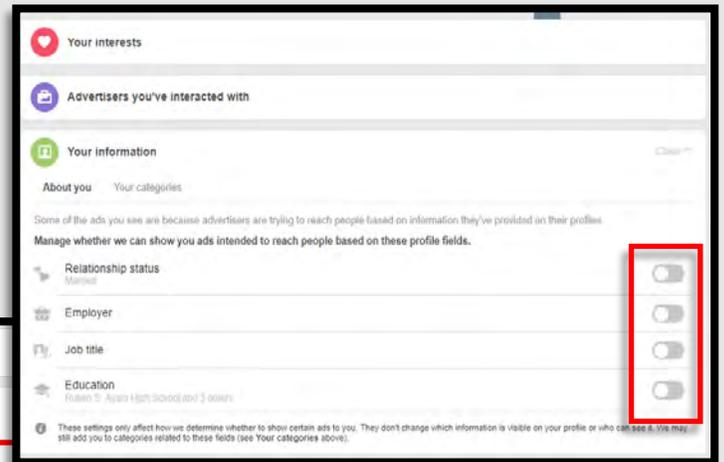
# FACEBOOK SMART CARD



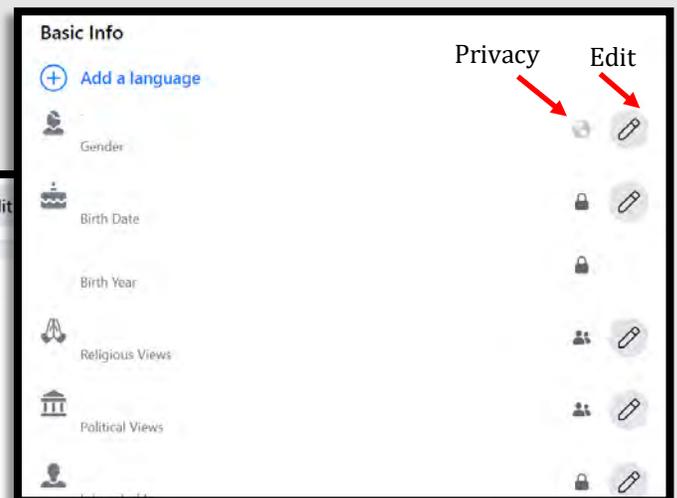
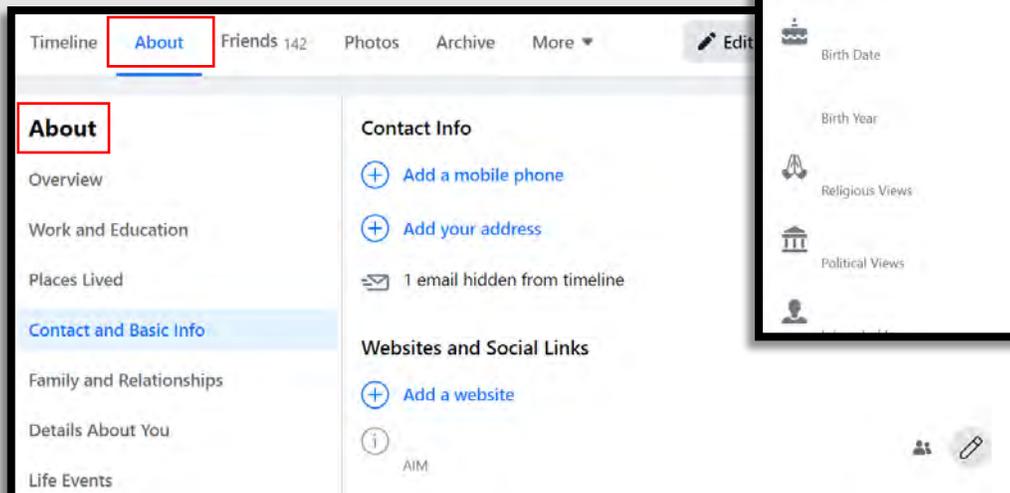
## Personal Computer (PC) Version

Under the “Your Information” tab, ensure all the sliders are off (greyed out) so that none of your information is provided by Facebook to advertisers. It is important to limit the information advertisers have access to about you. This will help to ensure your information doesn’t show up on advertisements and will limit unwanted ads on your timeline.

Under “Ad Settings”, it is recommended that you select “Not Allowed” or “No One” for each category.



Now that you have completed the “Settings” sections, let’s move on to secure your personal profile information. First, from the “Home” screen, select your “Profile Picture” or “Username”. Next, select “About” on your personal “Profile Page”. You should go through each selection in the “About” section and make sure the privacy settings are as secure as possible. You will see 2 update opportunities for each item: 1) privacy, and 2) edit. We recommend you choose “Only Me” as much as possible, and “Friends” as a second choice for who each piece of information is presented to. When “editing”, remember to include the least amount of information possible — wherever you can, leave your inputs blank, and where you provide information, keep it vague.



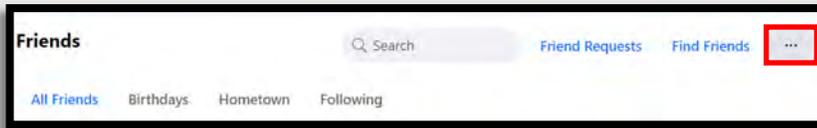
How much information does a criminal have to make you think you know them and can therefore trust them? #lockitdown

# FACEBOOK SMART CARD

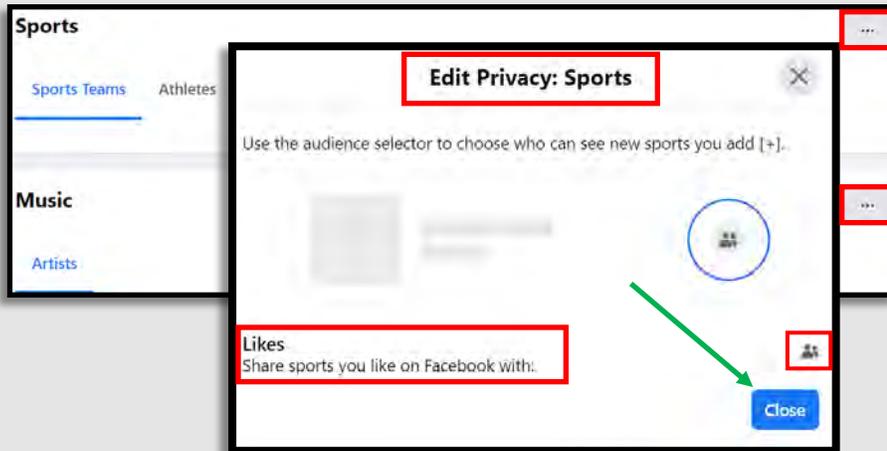
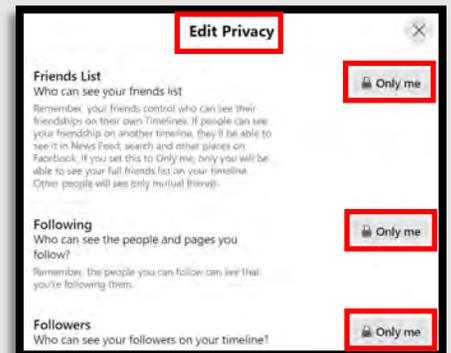


## Personal Computer (PC) Version

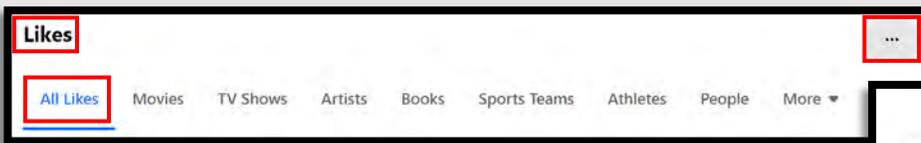
How many "Friends" do you have on Facebook? Would you recognize them if they were standing right in front of you? #FBpurge #whoareyourfbfriends



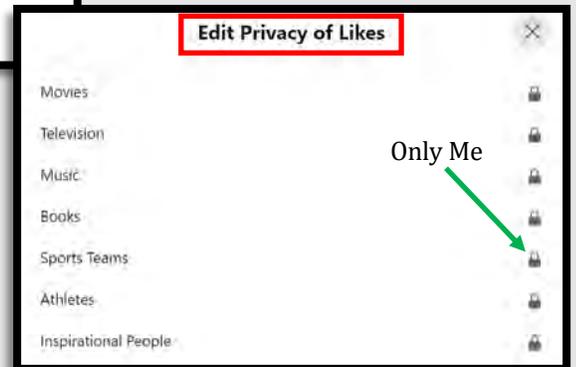
Below this, see your "Friends" section. Here, select the "Options", or "... " button in the upper right corner of the section. Select "Edit Privacy" (not shown, but only option), then adjust the settings in the pop-up box (see right). We recommend setting all three options to "Only Me".



The things you "Like" on Facebook can be analyzed in order to create a pretty accurate profile of you. This information can be a lot more dangerous than you might imagine. In the "About" section, you can control who sees your "Likes" by selecting the "... " button to the right of each interest category (eg: sports, music), then select "Edit Privacy", and set your "Likes Privacy" icon to "Only Me" or "Friends" on each section. "Only Me" is the most secure choice, and recommended whenever possible.



Although you have enhanced the security of your "Likes" above, you will need to repeat the process in one additional section. Beneath all the categories of your interests on your "About" page (under "Books"), you will see a "Likes" section. You will want to control the presentation of "Likes" here as well. Select the "... " button, then "Edit the privacy of your likes", then select "Only Me" on each category.



**Think**  
once before you act  
twice before you speak  
and three times  
before you post  
on Facebook

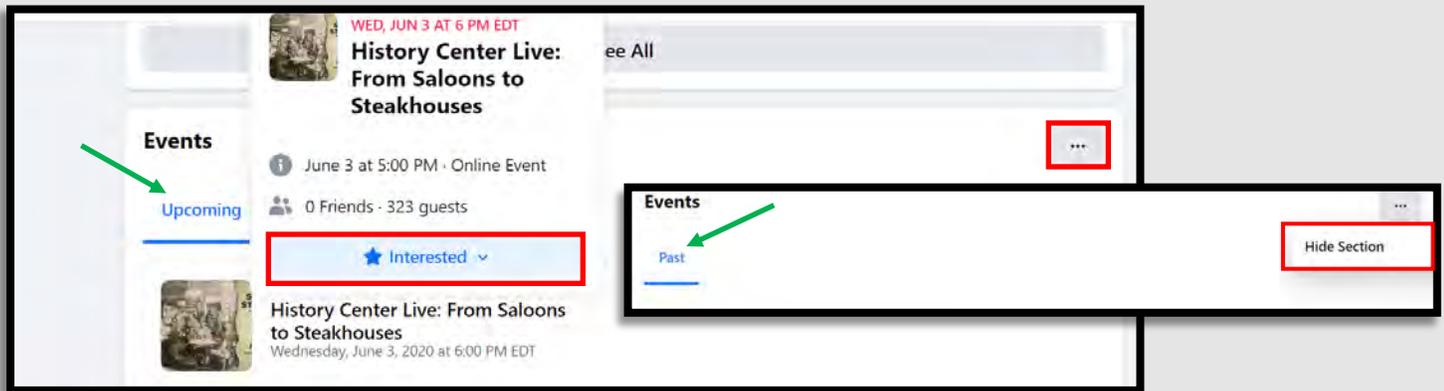
\*Social Engineers or Human Hackers are more likely to convince you that they know you if they have access to personal information about you. This information can be in the form of your likes/hobbies, friends, events you will or have been to or what schools you have previously attended. They can even review past posts you may have open to the public for some additional insight. Once they have convinced you that you are "old friends" there is significant danger. They could convince you to meet in person, lend them money, steal your identity, or get close to your children. The best defense is to limit who can see this information about you to "Only Me" or "Friends".

# FACEBOOK SMART CARD

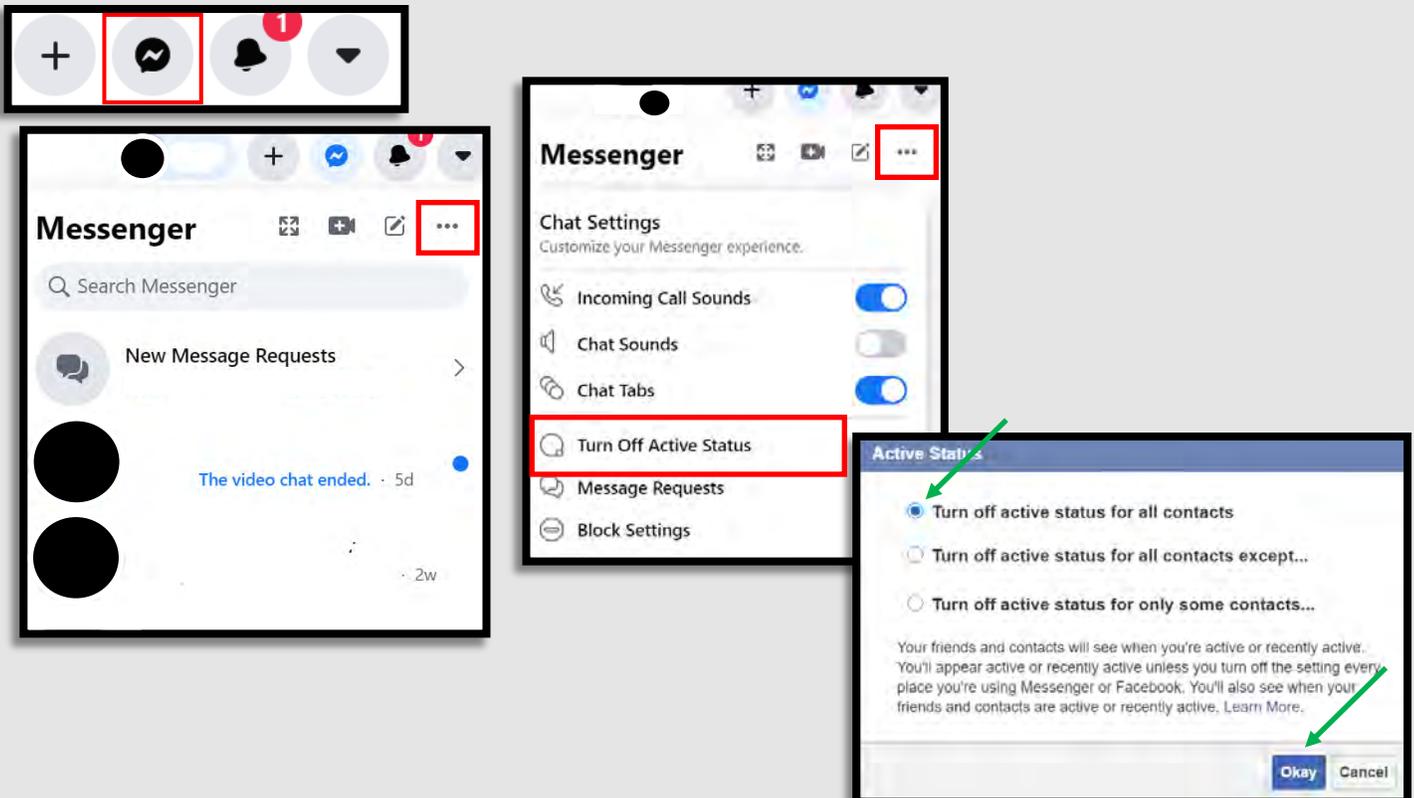


## Personal Computer (PC) Version

Next, as you continue to scroll down the page, you may want to go through all your “Events” to see if there are any you can delete. Also, make sure all your events are set to “Only Me” by hovering over the event title, clicking the “Going” button, and looking to the bottom line of the pop-up for “Visible to the Hosts and Only Me” (not shown). If you have an upcoming “Event” or an “Event” that you are “interested in” that is not set to “Only Me”, be aware that anyone will be able to see that you will be attending that event. You also have the option of hiding the entire ‘Events” section. Go to the “. . .” button at the top right corner of the “Events” section, select “Hide Section”. This is the quickest and easiest way to secure this information, and is what we recommend. Remember to do this in both “Upcoming” and “Past” sections. (see arrows above)



Next is the “Messenger” feature, there are a few things to cover in order to protect your privacy here. First, go to the top of the page to the “Messenger” icon, and see the “Messenger” dropdown menu. Here you will be able to turn “On” and “Off” your “Status” on “Messenger”. Select the “. . .” button, then select “Turn Off Active Status”. Choose one of the three options on the pop-up screen, and select “Okay”. In this way, you can control who, if anyone, can see that you are actively using Facebook at any given time.

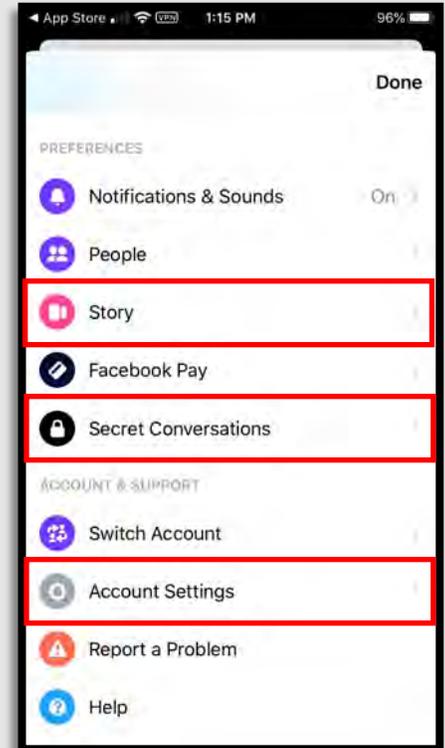
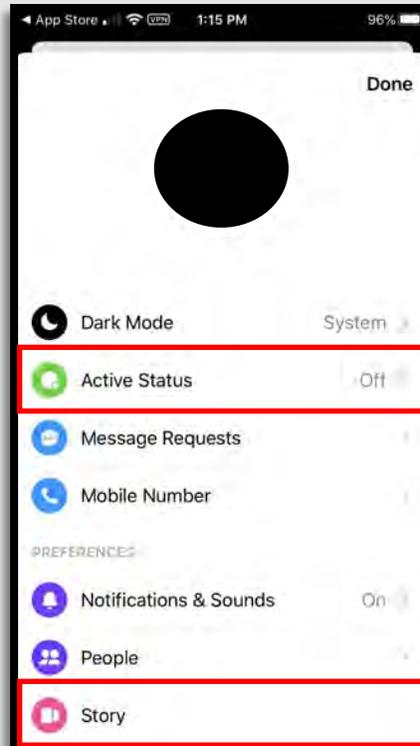
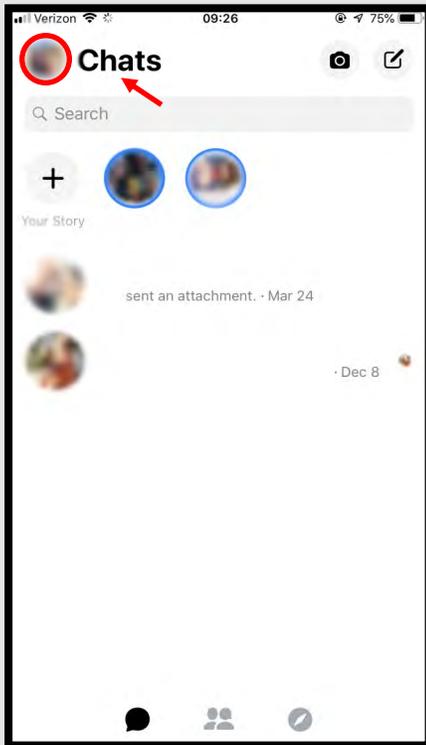


How many “Friends” do you have on Facebook? Would you recognize them if they were standing right in front of you? #FBpurge #whoareyourfbfriends

# FACEBOOK SMART CARD



## Mobile Device Version

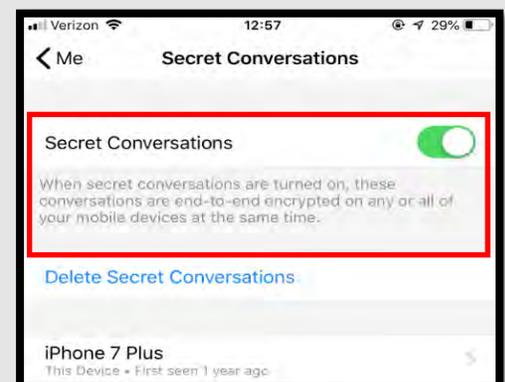


Remember, it is important to lock down your Facebook Messenger the same way you lock down the rest of your Facebook.

The final feature you may want to review your “Messenger” app, and this information may mainly apply to your mobile device. Facebook has launched a dedicated website interface, and separated its messaging functionality from the main Facebook app, allowing users to use the web interface or download one of the stand-alone apps. What this means for you is that you may be taken outside of Facebook sometimes, when you are trying to access Facebook “Messenger”. Also, your computer version of “Messenger” may look different from your mobile device version, and may he have more or less features. This page addresses Facebook “Messenger” on mobile device.

Once logged into Facebook “Messenger”, head to the top left of the screen, select your “Profile Picture” (highlighted above in red). Here you can review all of the additional settings “Messenger” has to offer. You can chose whether or not you want people to know when you are “Active” on “Messenger” by selecting the “Active Status” and turning it “Off.” You can also set your “Story” accesses the way you want—we recommend setting to “Custom”, by which you can select your audience manually, or “Friends”. You can also review your “Account Settings” (eg: personal info, privacy, ads).

Finally, Facebook “Messenger” has a feature called “Secret Conversations” where your conversations are encrypted end-to-end. To turn this feature “On”, select your “Profile Picture”, select “Secret Conversations” where you will then be able to turn the feature on. If you have children that use Facebook Messenger it is important to know about this feature so you can monitor it as you see fit.



# FACEBOOK SMART CARD

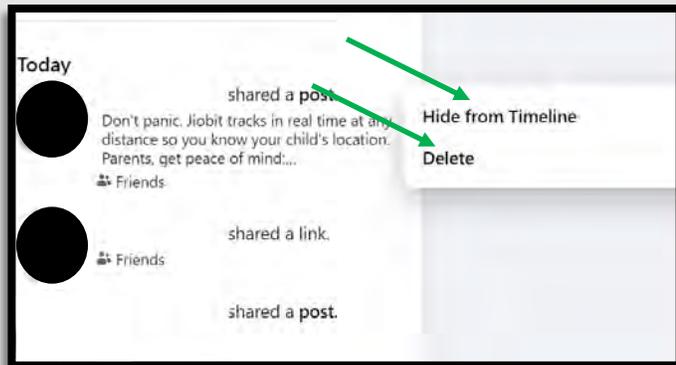
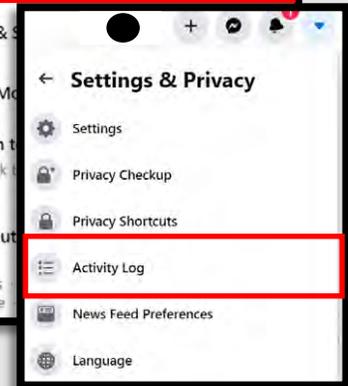
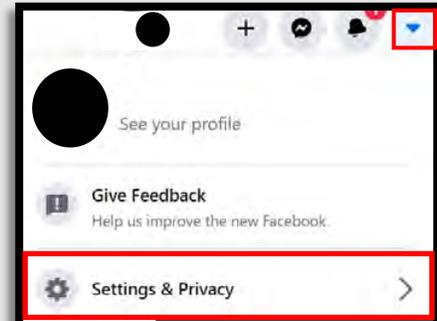


## Personal Computer (PC) Version

Finally, lets go back to Facebook’s “Activity Log”, accessed from the “Settings & Privacy” option under the “Down Arrow” in the right upper corner of the “Home Page”. The “Activity Log” allows you to review any click of the button (photos, comments, Likes, posts, etc.) or tag that has ever occurred and been associated with your profile. This is the central location for cleaning up your Facebook profile.

More specifically, from the “Activity Log” you can review information by date, all the way from the creation of the profile to the present. You can also see if a post is viewable to the public or just to friends, as well as review any posts you have been “Tagged” in. Finally, the “Activity Log” allows you to remove any actions you have taken on Facebook as well as any “Tags” that someone else may have posted.

From the “Activity Log” page, select “Timeline Review” first. A list of “Filters” appears, and you can go through each one. You can go through each post, photo and tag on your account, and hide or delete them as you decide.



Just select the “. . .” button that you will see when you hover to the right of the post, and select “Hide from Timeline” or “Delete”. Alternatively, you can click on the post and it will open in the box to the right of the page, where you can select the “. . .” button and choose from several additional options, including “Edit post” and “Edit audience”.

You can limit each post’s visibility by setting every one to “Only Me” or “Friends”. Remember if you “Like” or “Comment” on someone’s post whose privacy settings are set to “Public”, your comment will also be “Public”. You can only set your own privacy settings for your profile, and once you reach outside of your profile, you have no control over privacy.



Correcting posts might be tempting, but think about what correcting that post says about you and the information you have access to. #staysafeonfb

# FACEBOOK SMART CARD

## Personal Computer (PC) Version



Don't think you can hide your FB profile by using a different name. Better to assume people can find you and set your privacy/security settings accordingly. #bettersafethansorry

Finally, let's address "Tags", which are a feature of Facebook by which other people can call attention to your name by "Tagging" a photo that you may or may not be in, or "Mentioning" you in a "Post" or "Comment". People can do this without your permission if you don't have the "Tagging" options selected as we have done in this Card. When you are "Tagged" in a photo, that photo is viewable by the "Public", while also drawing attention to your name. Here is what you can do about it.

First, in "Activity Log", select "Tag Review", then select "Activity You're Tagged In". All the "Posts", "Comments", and photos you are tagged in appear in the left column. Select the "Post" you want to view and "Untag". The post will open in the box to the right of the screen. Select the "... " in the right upper corner of the post, and select "Remove Tag" on the drop-down.

**Note:** If you remove a "Tag" of yourself, it will NOT notify the individual who owns the post/picture that you have removed the tag.

Remember: Although the photo is "Untagged" and no longer on your profile, the photo has **not** been deleted from Facebook. It will remain on the profile of the individual who originally posted the photo. *Backdoor avenues* used in finding your profile may still exist (e.g. via a tagged photo of you on your spouse's profile or simply finding your name in the comments of the picture/post).

If you'd like for the photo to be removed, the best way is to ask the individual to delete the photo/post.

***I think it is important to fortify ourselves online the same way we would fortify our homes if we knew we were under attack.***

-II MEF Commanding General LtGen Hedelund's response when asked for his take on social media and force protection.

# FACEBOOK SMART CARD



## Indicators of Possible Account Compromise:

**Do you think your account may have been compromised or hacked? Have you noticed any of the following:**

- \* Unexpected posts posted by your account
- \* Any Direct Messages sent from your account that you did not initiate
- \* Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- \* A notification from Facebook stating that your account may be compromised
- \* A notification from Facebook stating that your account information (bio, name, etc.) has changed
- \* Your password is no longer working or you are being prompted to reset it. \*If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above, it is advised you take the following actions:

- ◆ Delete any unwanted posts that were posted while your account was compromised
- ◆ Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- ◆ Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- ◆ Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Facebook account
- ◆ Be sure to check that your email is secure. It may be worth changing the password to both your Facebook account and the email associated with your Facebook account. \*If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.

If you need to report **Spam/Harassment**: Go to [https://www.facebook.com/help/968185709965912/?helpref=hc\\_fnav](https://www.facebook.com/help/968185709965912/?helpref=hc_fnav)

If your account was hacked: <https://www.facebook.com/help/hacked>

Also, if you find that someone is impersonating you Facebook: <https://www.facebook.com/help/hacked> then scroll down to the "Impersonation Accounts" section and follow the directions. If you do not have a Facebook account and want to report an impersonating account go to: <https://www.facebook.com/help/contact/295309487309948>

To find additional "Security Features and Tips go to: [https://www.facebook.com/help/379220725465972?helpref=faq\\_content](https://www.facebook.com/help/379220725465972?helpref=faq_content)

If you still need help or have questions, you can always contact Facebook by: <https://www.facebook.com/facebookapp> where you can message a Bot Facebook created to help answer questions while they work on building a live customer support capability.

If someone is threatening to share information (ex: messages or photos) on Facebook of your child that they do not want shared you should report it to the local law enforcement. Facebook also says you can do the following: Report the incident to Facebook <https://www.facebook.com/help/contact/567360146613371>, then make sure that this person is blocked so they no longer have access to your child. It is important to talk to your children about this possibility before they begin to use social media so that they know what to do should this happen to them.

Con artists are more sophisticated than ever, targeting unsuspecting consumers with fake online listings and money-payment scams. Make sure to protect your information #privacymatters

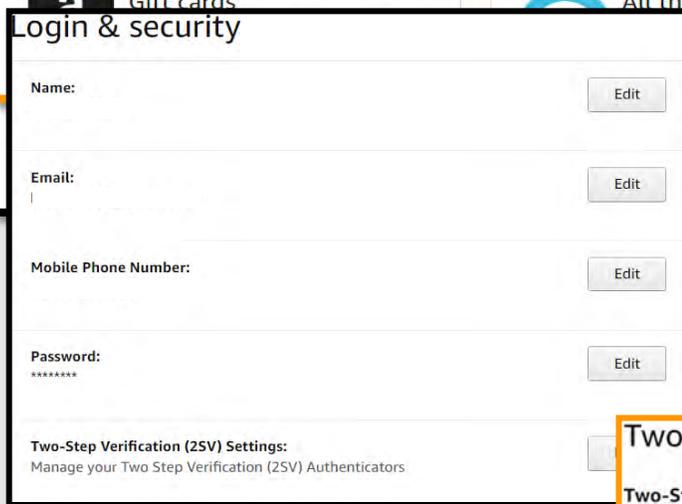
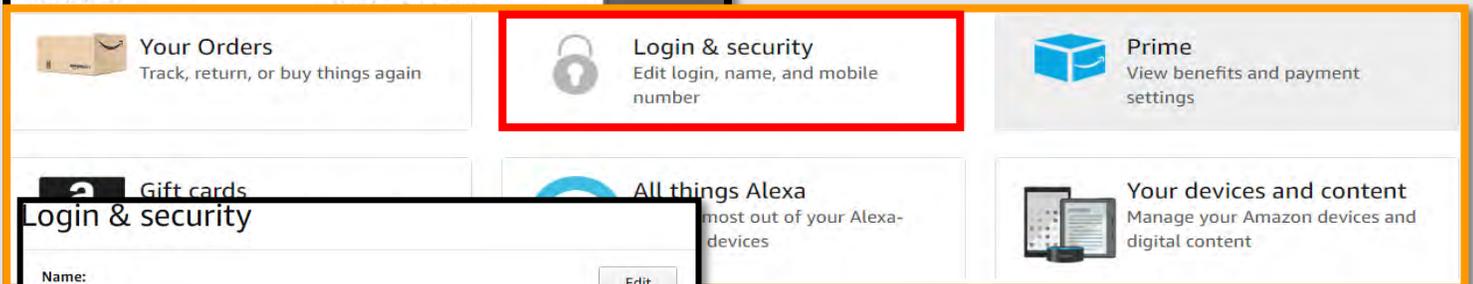
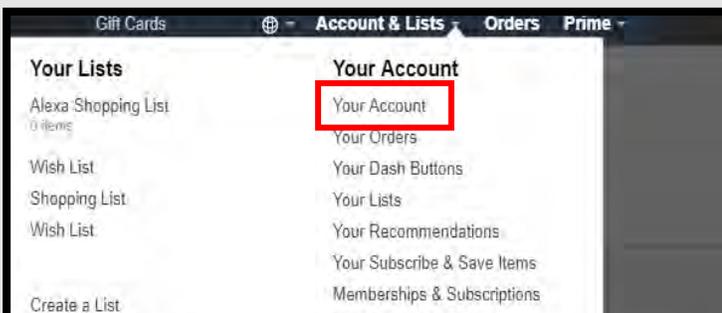
# LOCKING DOWN amazon

## Do's and Don'ts

- ◆ Do take time to clean up old credit cards from your account.
- ◆ Do use Two-Factor Authentication to protect all your information on Amazon. With all the information that Amazon captures it is important to make sure it is protected by every means available.
- ◆ Do frequently update your password for Amazon.
- ◆ Do not link any other accounts to your Amazon account. This will limit what outsiders can find out about you, to include your pattern of life and hobbies.
- ◆ Do not fall for scams on Amazon or from emails that appear to be from Amazon.
- ◆ Do not buy from international sellers. Avoiding this will help protect you from identity theft and scams.

## Account Security

In order to lock down your Amazon account you will need to access "Your Account," located on the upper right side of your screen. From the "Account & Lists" option, select the down arrow to expand the menu. From this list, select "Your Account." Let's look at the "Login & Security" settings first.



The "Login & Security" settings are located at the top of the "Your Account" page (shown above highlighted in red). First, review the general login information provided to ensure its accuracy. Next, head down to the "Two-Step Verification (2SV) Settings" section and select "Edit." Here, you can set up "Two-Step Verification" for your account. This is the most important thing you can do to help prevent hacking of your account.

To set-up "Two-Step Authentication" simply select "Get Started" (highlighted in red to the right) and follow the steps provided. Because Amazon retains some of your most sensitive information, like your credit cards and address, this feature is really important to help secure your account.

### Two-Step Verification (2SV) Settings

**Two-Step Verification**  
Require a password and an OTP to Sign-In to your account

**Get Started**

**Why do I need this?**  
Passwords can get stolen - especially if you use the same password for multiple sites. Adding Two-Step Verification means that even if your password gets stolen, your Amazon account will remain secure.

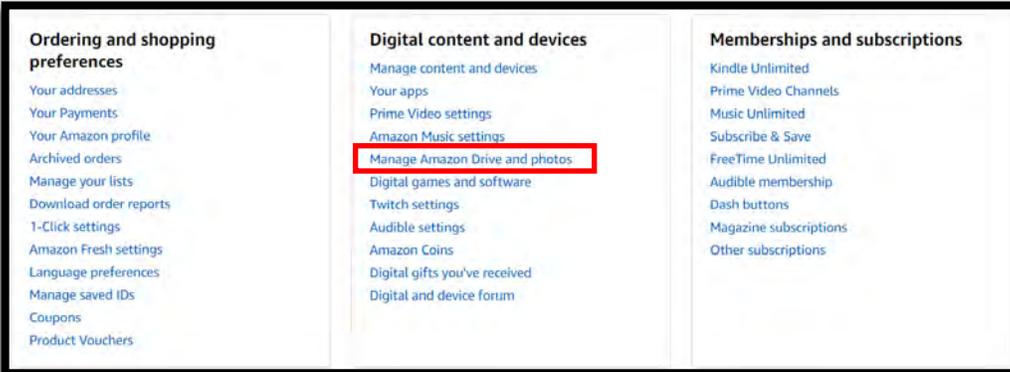
**How does it work?**  
After you turn on Two-Step Verification for your account, signing in will be a little different:

1. You'll enter your password, as usual.
2. We'll send you a One Time Password (OTP).
3. You'll enter the OTP, and complete your Sign-In.

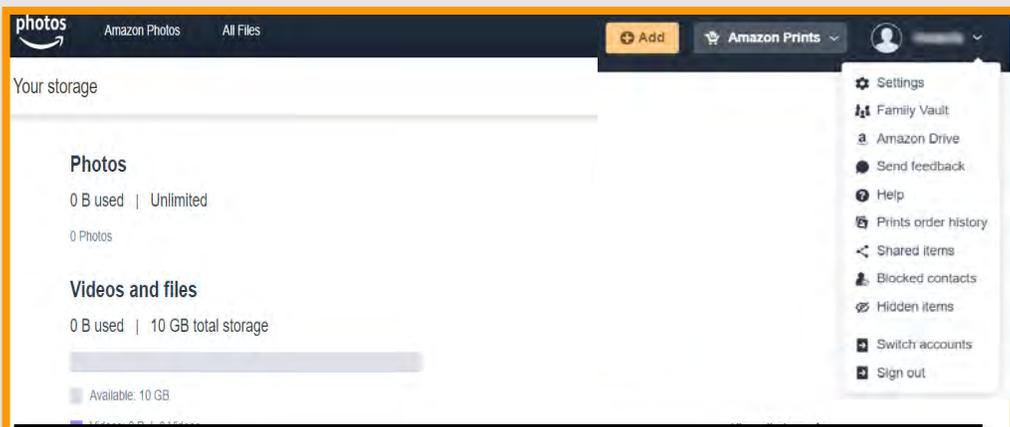
Don't assume every email you receive is trustworthy. Messages may appear to be coming from a legitimate retailer and could include a request for account information. #BeatIdentityTheft

# LOCKING DOWN amazon

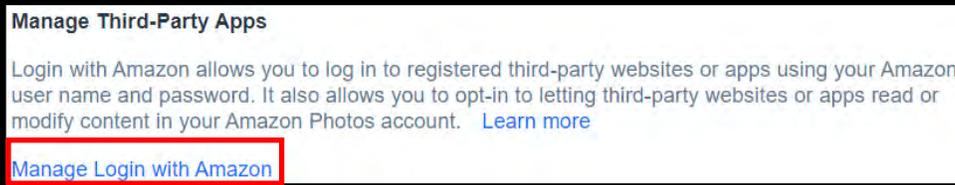
## Digital Content & Device Security & Privacy



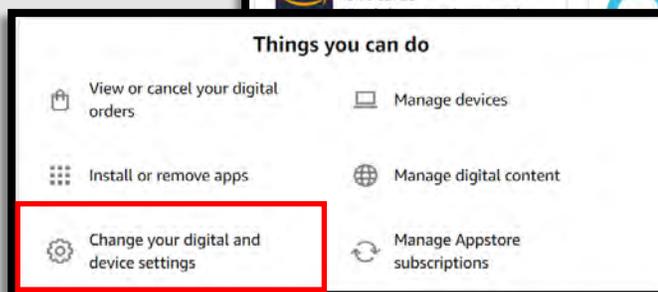
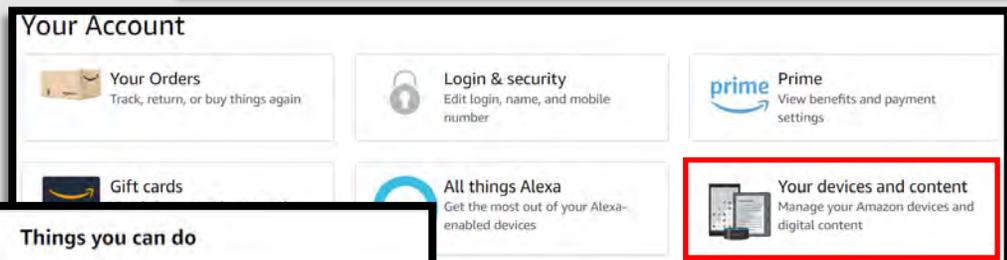
What is Amazon Drive? Amazon Drive is a secure online storage service for your photos, videos and files. Every Amazon customer gets 5 GB of free storage to save, organize, share and access all your files on desktop, mobile and tablet.



With each Amazon account comes an “Amazon Drive”. In order to lock down your “Amazon Drive,” go back to the “Your Account” section (shown on page one), and select “Manage Amazon Drive and Photos.” On the top right of the screen, select the profile picture to open the “Drive” menu. Next, select “Settings” and scroll down to the “Manage Third-Party Apps” section. Once there, select “Manage Login with Amazon.” Here you can review any apps you may have logged on to through your Amazon account and if need-be, remove accounts you no longer use.



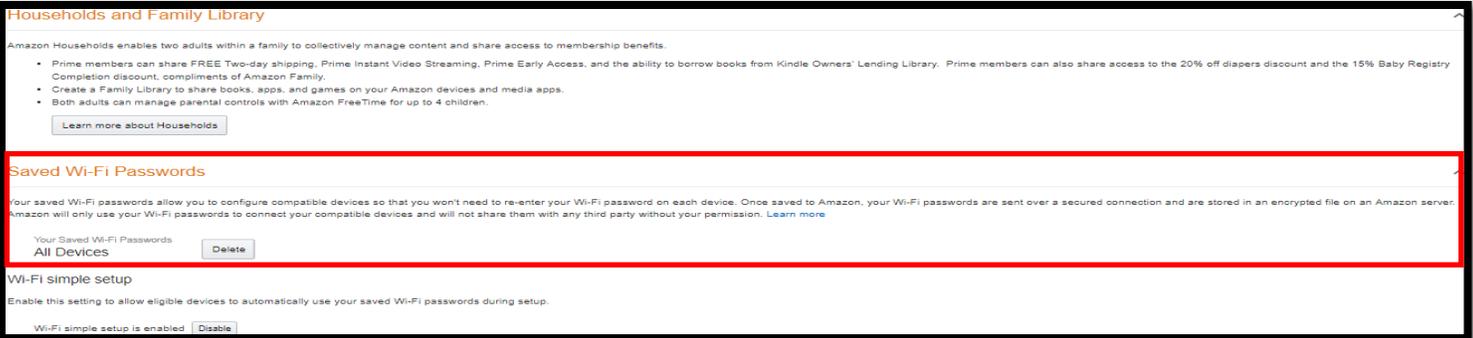
Now, let's go back to “Your Account” and select “Your devices and content”, then select “Change your digital and device settings”. You may want to review the settings (next page) to make sure the content agrees with your needs. We recommend that you review “Saved Wi-Fi Passwords” to make sure there are no passwords saved that you do not want Amazon to retain.



You can call the customer service department and ask about suspicious emails to see if it's authentic. Whatever you do, don't try to get to Amazon through the suspicious email. #trustbutverify

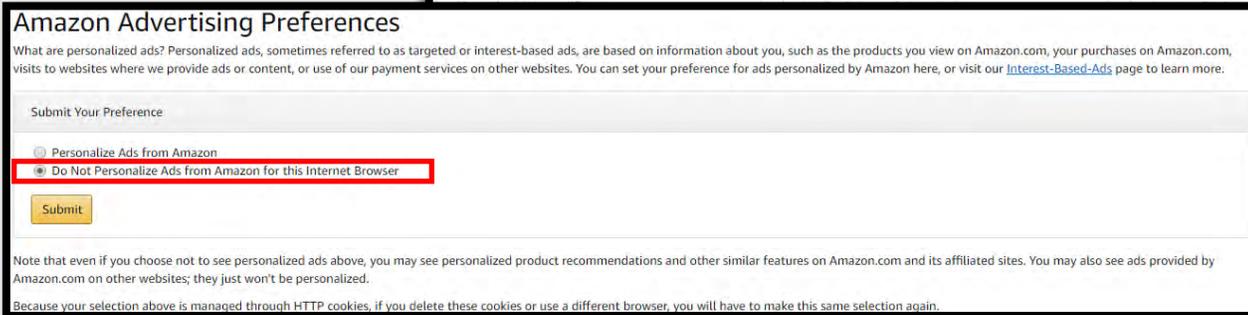
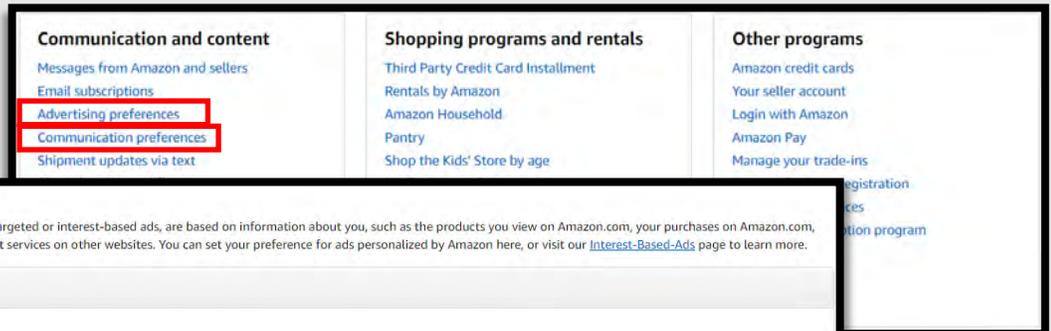
# LOCKING DOWN amazon

(... Image continued, last page)



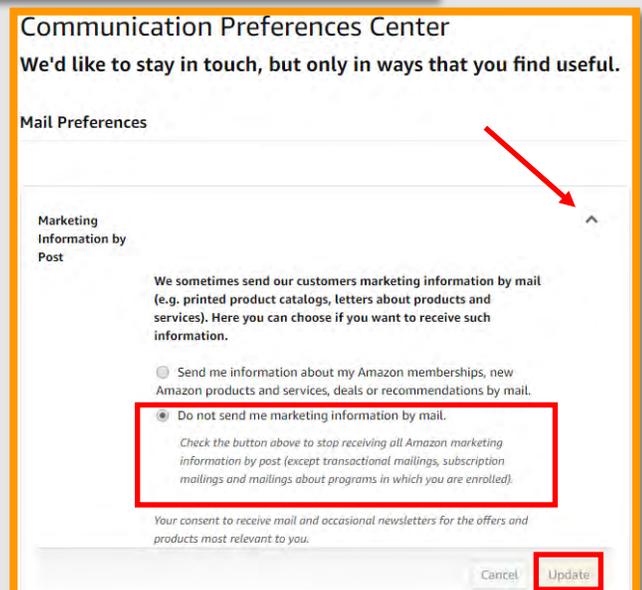
## Advertising & Communications Security

Now let's check the security and privacy settings regarding advertising and communications on your account. Go back to "Your Account" and in the "Communication and Content" section (see below), select "Advertising Preferences" so we can review what Amazon provides to you and to advertisers. Personalized ads, sometimes referred to as targeted or interest-based ads are based on information about you, such as the products you view, the purchases you make on Amazon, or websites you visit where Amazon might provide ads or content.



We recommend you select "Do Not Personalize Ads from Amazon for this Internet Browser." This does exactly what it says in the title, but for the current browser only. Amazon has been known to reset your privacy and other settings if it is opened from a browser different from the one used to lock it down originally. It will also reset your settings if you clear your cookies and delete your internet history. This means that you will need to go back into Amazon and make sure your settings are still intact any time you delete cookies or clear your browser history.

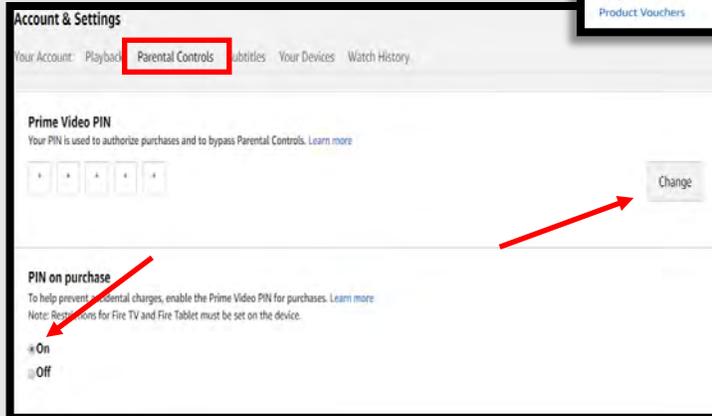
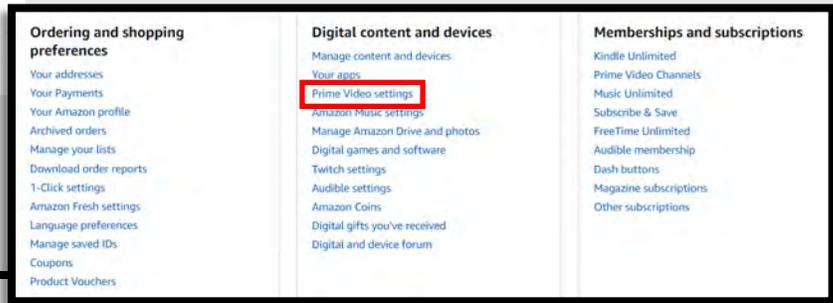
Now let's go back to "Your Account" and select "Communication Preferences" (see above). Select the down arrow to the right of "Marketing Information by Post", and select "Do not send me marketing information by mail" (highlighted in red to the right). This will help to eliminate spam and other marketing emails from cluttering your inbox. Be sure to select the "Update" button to save these changes.



If you need to contact Amazon's customer service make sure to find the number from the official Amazon site. Searching for it online could lead to you providing information to a fake call center.

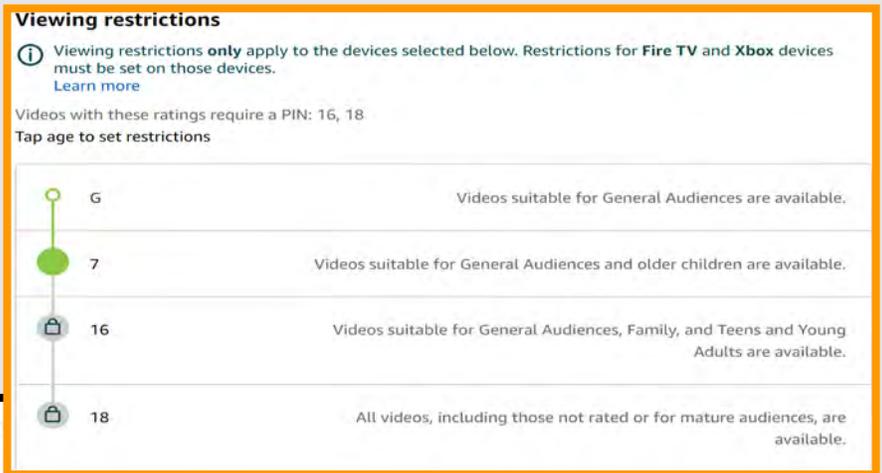
# LOCKING DOWN amazon

## Parental Controls



Let's take a look at the "Parental Controls" and settings located in the "Video" section of Amazon. To do that you will need to go back to "Your Account" and select "Prime Video Settings" under "Digital content and devices." At the top of the page select "Parental Controls". For parents, it is always important to monitor and protect our children from age inappropriate material on the internet and television screen. Amazon allows parents to set "Prime Video PINs" and "Viewing Restrictions". Setting the restrictions means that any time someone attempts to play a video or other content (depending on the device, i.e. the Amazon Fire Stick) they will be required to put in a PIN, which will be designated here by you.

If you scroll down on the "Video Settings" page, you will find the "Viewing Restrictions" section. Here you can select at what age rating you would like a PIN to be required. If you scroll even further down, Amazon lists other Amazon devices (as shown below) that require parental controls be set separately. These settings are inherent to, and accessed from, the devices themselves.



Prime Video parental controls work by requiring entry restrictions you've enabled.

**Important:** The following devices have their own parental controls settings to restrict access to content and purchasing, and you'll need to manage these settings directly on the device:

**Amazon Fire TV devices (Amazon Fire TV and Fire TV Stick)** – Amazon Fire TV devices have their own parental controls settings to block purchasing and access to titles in selected ratings categories. For more information, go to [Fire TV Help](#) and select your device.

**Fire tablets** – You can set purchasing restrictions for your Fire tablet from the Settings menu. To learn more, go to [Fire & Kindle Support](#) and select your device.

**Fire phone** - You can set purchasing restrictions for your Fire tablet from the Settings menu. To learn more, go to [Set Up Parental Controls on Fire Phone](#).

**Xbox 360** – Prime Video purchasing is not available on Xbox devices; and Xbox 360 consoles have their own parental controls settings you need to set directly on the device. For more information, go to [Xbox Support](#).

We recommend that you take time to review each device you own and set the parental controls according to your preferences. This is even more important for the Xbox and other gaming devices. These types of devices, if parental controls are not set, allow users to interact with others and purchase items using the credit card on file.

# LOCKING DOWN amazon

## Security & Privacy for Shopping

### Wish Lists

Next, let's review your security and privacy for some of your shopping features. Go back to "Your Account", select "Ordering and shopping preferences". We'll review "Manage your lists", but feel free to go through all items in this section.

#### Ordering and shopping preferences

- Your addresses
- Your Payments
- Your Amazon profile
- Archived orders
- Manage your lists**
- Download order reports
- T-Click settings
- Amazon Fresh settings
- Language preferences
- Manage saved IDs
- Coupons
- Product Vouchers

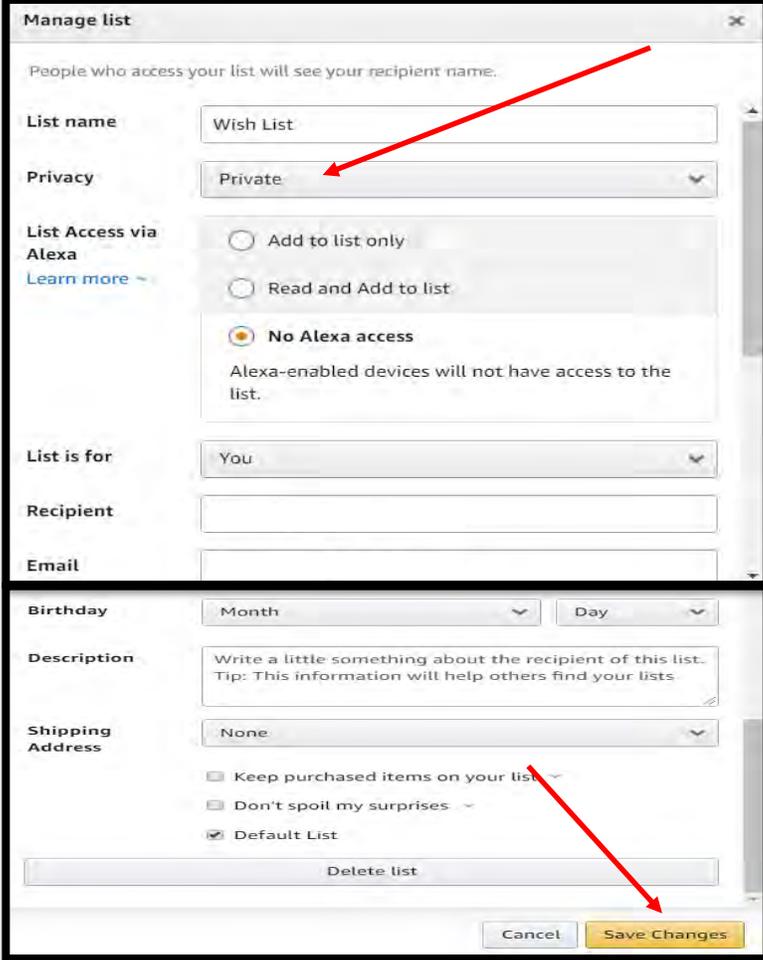
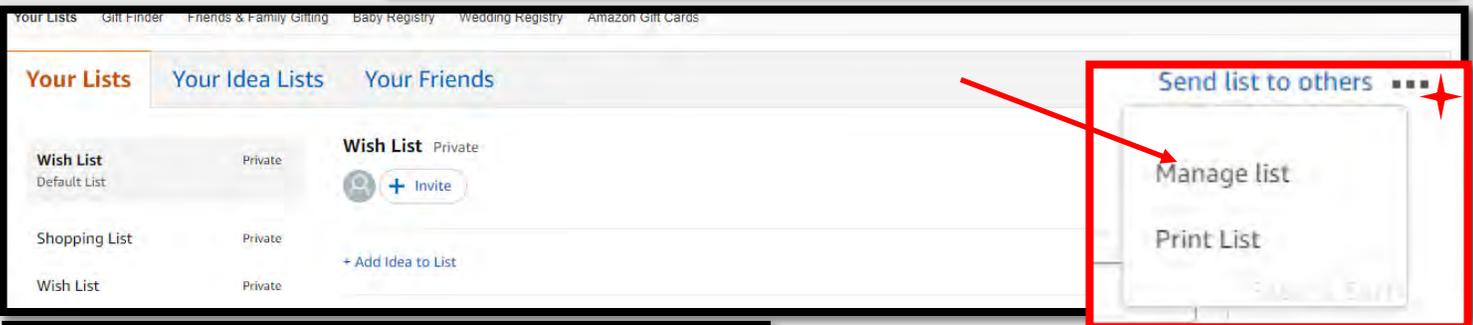
#### Digital content and devices

- Manage content and devices
- Your apps
- Prime Video settings
- Amazon Music settings
- Manage Amazon Drive and photos
- Digital games and software
- Twitch settings
- Audible settings
- Amazon Coins
- Digital gifts you've received
- Digital and device forum

#### Memberships and subscriptions

- Kindle Unlimited
- Prime Video Channels
- Music Unlimited
- Subscribe & Save
- FreeTime Unlimited
- Audible membership
- Dash buttons
- Magazine subscriptions
- Other subscriptions

If you see a product that is listed way below market value, don't hand over your credit card info right away. If it's too good to be true it very likely is. #themoreyouknow



One of the most public sections of Amazon is the "Wish Lists." If not made private, anyone can view your lists and gain information about who you are or who the people in your family are (how many, gender, age, etc.). People use "Lists" for making Christmas lists, birthday lists, or even grocery lists. The titles of these lists are revealing (i.e. a child's name for a birthday or Christmas list). These small tid-bits of information could be useful to a social engineer or identity thief when combined with other bits of data on you. Amazon has recently changed its privacy options for "Wish Lists", requiring users to enter an email address in order to access any "Wish List", so make sure that information is locked down. New to the "Wish List", is the option to provide Alexa with access to your "Lists". We do not recommend you provide such access but instead set each list to "Private".

Select "Manage your list" from "Ordering and Shopping Preferences" in order to begin the process of locking down your lists. Once there, your "Wish Lists" will be on the left hand side of the screen (see above). In order to review and change these settings, select the ellipse (as shown above in red), and select "Manage List." From there, select "Privacy" and select "Private" from the list. Be sure to select "Save Changes."

# LOCKING DOWN amazon

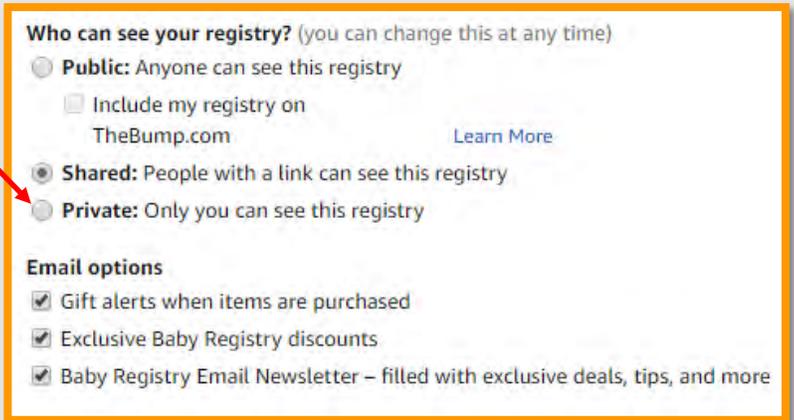
## Security & Privacy for Shopping, ctd.

### Registries



Much like a “Wish List”, your registries can also be displayed publicly unless you say otherwise. While still in your “Wish List”, go to the top menu and select “Baby Registry.” To create your “Baby Registry” select “Create a new Baby Registry” from the center of your page. Scroll down to “Who can see your registry” and select “Shared” or “Private” for the visibility of your registry. It is important to note that if you decide to make your registry “Public”, it may be shared on a third party website - TheBump - unless you “Unselect” that option.

If you have already created a baby registry, you simply need to go to the “Registry Settings” and change the privacy from there. It is also important to remember to delete your registries when you no longer need them.



Your “Wedding Registry” is equally important to lock down. Think about everything that goes into a wedding registry, what it might say about a couple, and how beneficial that information could be to an identity thief.



In order to lock down your “Wedding Registry”, go back to the “Wish List” menu, select “Wedding Registry” (see above). From there, scroll to the middle and select the appropriate privacy settings for your registry. We recommend setting your registry to “Private” until you are ready to use it and then only to “People with a link can see this registry” (found in your registry settings highlighted above). Once you no longer need the registry, be sure to delete it.

Like the “Baby Registry,” the “Wedding Registry” may be listed on a third party vendor - TheKnott.com. It is recommended that you **not** make your registry searchable on TheKnott.com, select the box to the left of this option in order to “Uncheck” it.

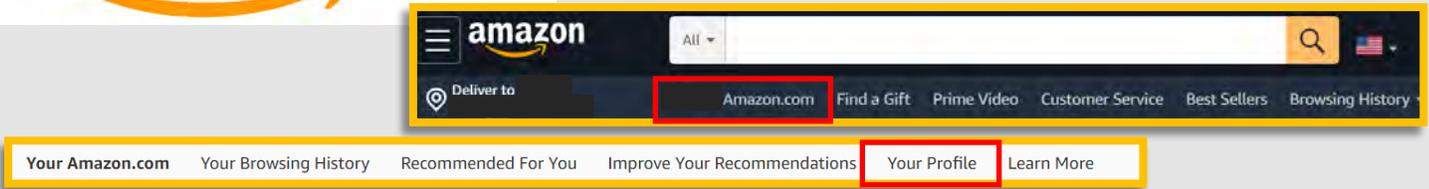


Keep all communication and transactions on Amazon, that way if you do happen to be scammed, Amazon can track the scam and all correspondences. #cyberfraud

# LOCKING DOWN amazon

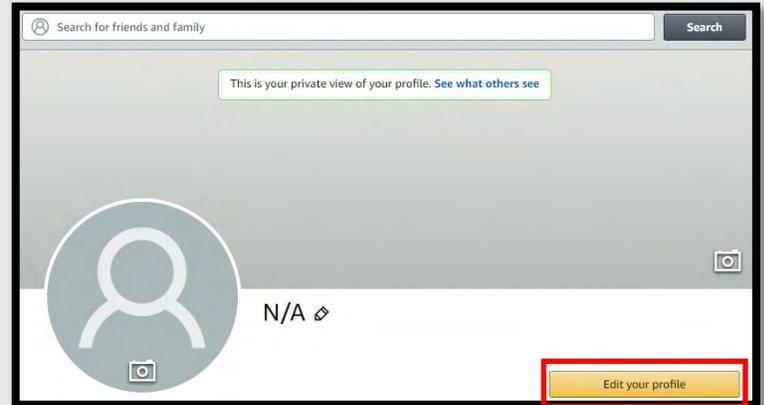
## Personal Profile Security & Privacy

"Ships from" and "sold by" [seller]: Third-party seller that ships an item from them directly to you. Amazon doesn't touch the item. This is where scammers thrive. #themokeyouknow

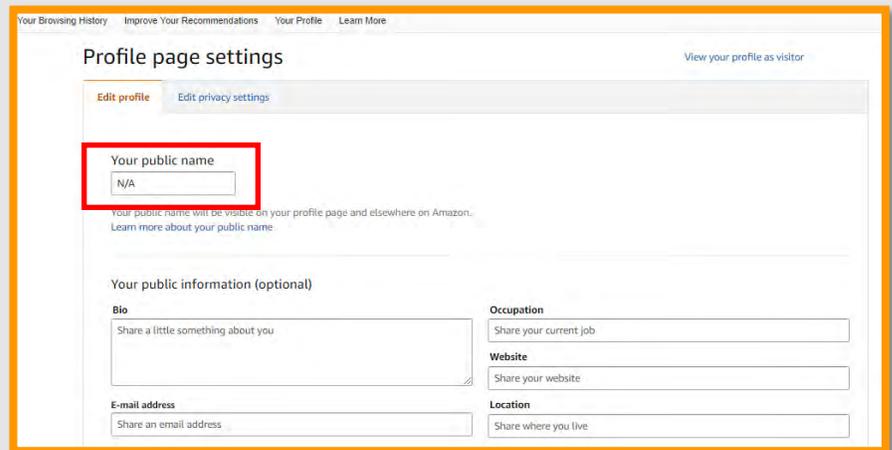


Most people do not realize that Amazon provides you with your own "Public Profile". This "Profile" and your entire "Amazon Account" can be linked to any of your social media accounts. It is therefore important to review your profile and its settings to ensure it is locked down, not linked to other social media accounts, and not searchable by the public.

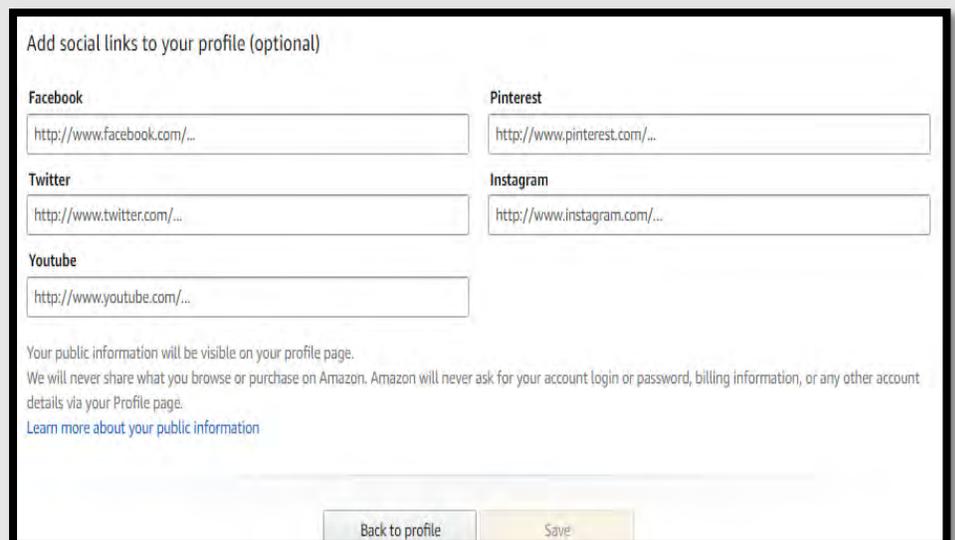
In order to lock down your Amazon account, go back to "Your Account", select "Your Name's Amazon.com", the second item on the second menu bar, then "Your Profile" on the third menu bar that appears (see above). From there, follow the steps below and on the remaining pages to best secure your profile.



Now let's begin the process of making sure your "Profile" is locked down. Select "Edit your profile" as shown above in red. In the "Profile page settings" review all of your information to make sure only information you want on public profile is filled in. We recommend you **not** display your full name in the "Your public name" section.



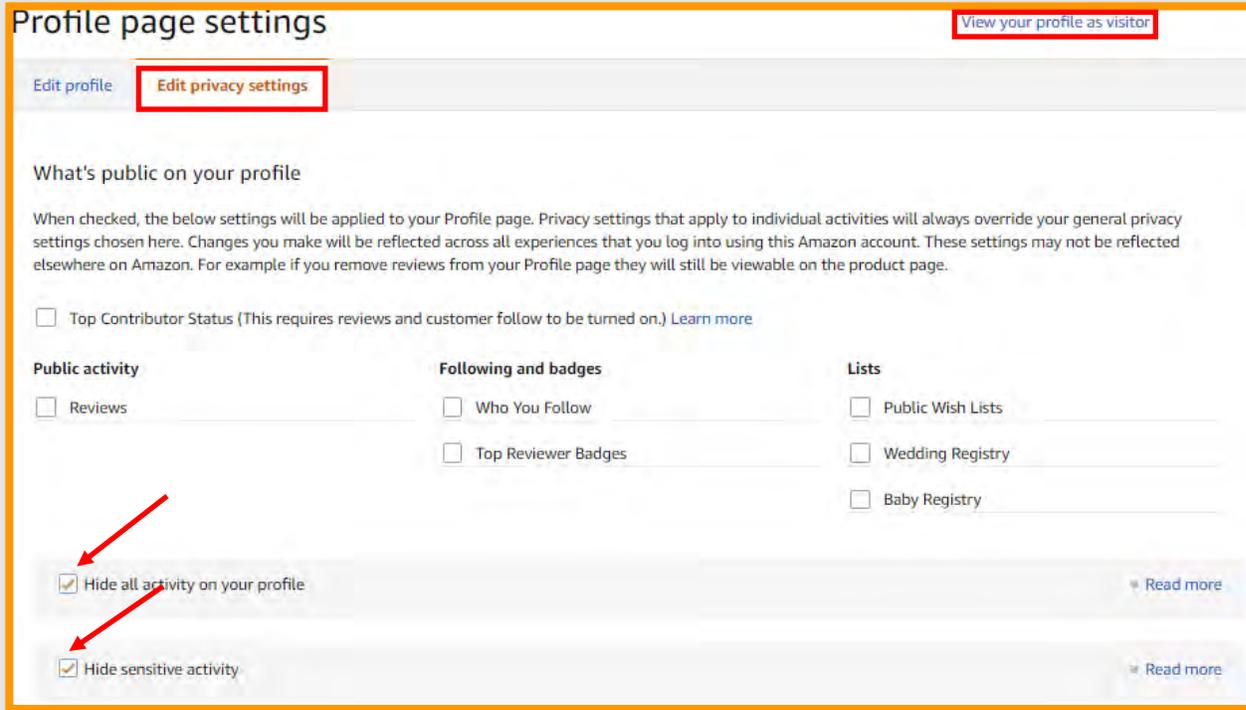
Scroll down on the page and find the "Add social links to your profile" section to make sure you have not linked any of your social media accounts to your Amazon account. Amazon is a great place to shop for just about anything, and as such it becomes a picture of who you are and who your family might be. This includes any product reviews you post on Amazon. It is recommended that if you do review products, that you do not put any personal information in your review.



"Sold by" [seller] and "Fulfilled by" Amazon: A third-party seller sends the product to Amazon's warehouse, then Amazon ships. These items can be "Prime" eligible, but are still third-party.

# LOCKING DOWN amazon

## Personal Profile Security & Privacy, cont.

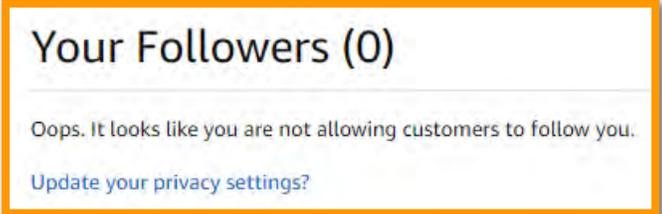


Now let's go to the "Edit privacy settings" to review and make sure they are set. Select "Edit privacy settings" (see above) to review how they are presently configured. We recommend that you select the box "Hide all activity on your profile" as well as "Hide sensitive activity." Users can view their "Profile" as a visitor, by selecting "View your profile as visitor" from the top right of the "Profile page settings." This capability allows users to ensure their profile is properly locked down so that information specific to the User is not readily available to anyone.

Next, scroll down to the bottom of the "Edit privacy settings" and make sure the box titled "Allow customers to follow you" is **not** checked. It is also important to click on the "See who is following you" link to make sure you have not allowed anyone to follow you up to this point (below).



If you have any followers, you can delete them from this link and then update your privacy settings as shown above to preclude any future followers. We recommend you do **not** let people follow you on Amazon, but especially if you do not know them.



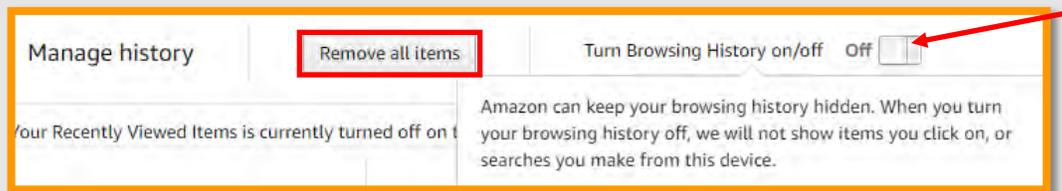
# LOCKING DOWN amazon

## Profiles Security & Privacy, ctd.

"Ships from" and "sold by" Amazon.com: This is the real deal and almost certainly not a scam of any kind. Choose this option whenever possible. #themoreyouknow #beatidentitytheft

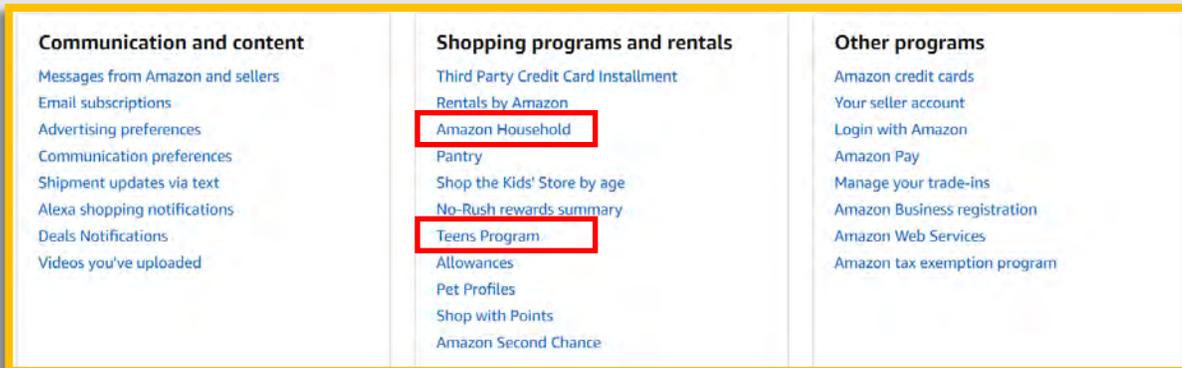


Now let's take a look at "Your Browsing History". Go to the top menu bar, from either the "Your Profile" section or the "Your followers" page, and select "Your Browsing History". From here, look at the right side of your screen and select the drop down arrow next to "Manage history." From here, it is recommend you remove all items and "Turn Browsing History" to "Off."



Amazon has different profiles to help you manage your account and any account you may want to create for your children. For instance, a teenager can have their own log in and purchase ability, while parents maintain control over purchases. Parents can also add any children under 12 to their accounts to help manage the content displayed on certain devices, such as the Fire TV. "Amazon Household" is an option if you want to share a profile with your whole family.

Explore these options by going to your "Account", then "Shopping programs and rentals", and "Amazon Household", "Teens Program", etc.



### What is an Amazon Household?

A Household allows you to connect and share Amazon benefits with the whole family. Two adults and up to four teens and four child profiles may link in a Household.

#### Adults (18 and up)

Two adults in a Household can share digital content and if they are Prime members, Prime benefits.

#### Teens (13-17 years old)

Teen logins allow teens to shop on their own and parents approve the order with a simple text. Teens may also access certain Prime benefits if their parents are a Prime member. [Learn more](#)

Teen logins are not currently supported on Kindle

#### Children (12 and under)

Parents can add children to a Household to manage parental controls on Fire tablets, Kindle e-readers and Fire TV through Kindle FreeTime. Personalize each child's experience by selecting what content they are able to see, and set educational goals and time limits. Children can access digital content that their parent allows on their child's device but are not enabled to shop.



# LOCKING DOWN



## Edit Profile & Account Settings

Since there aren't many privacy settings to manage on Pinterest, it is especially important to ensure the ones we have are locked down. In order to change your Pinterest settings look to the top right of your screen and select "Settings" (three horizontal ellipses, or a down arrow). Once you are on the "Settings" page you will be able to go through each of the settings provided by Pinterest. First, let's review the "Edit Profile" page, which provides your basic information on Pinterest. We recommend you avoid using your full name as your "Username", and instead use parts of your name or a nickname. We also recommend leaving the "Bio" and "Location" sections blank. This information is not required. Select "Done" if you make any changes.

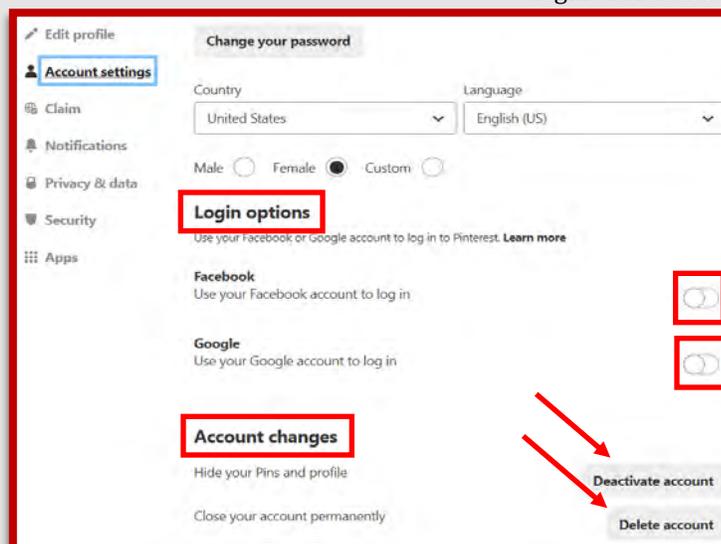
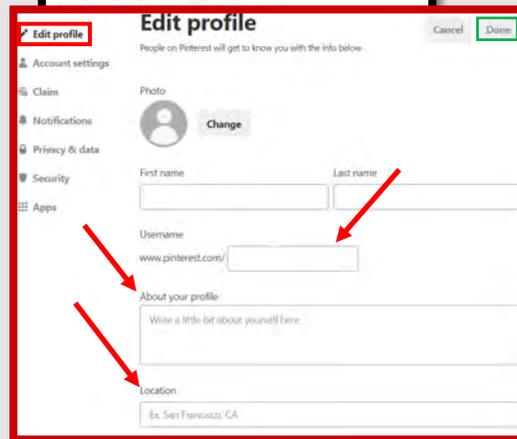
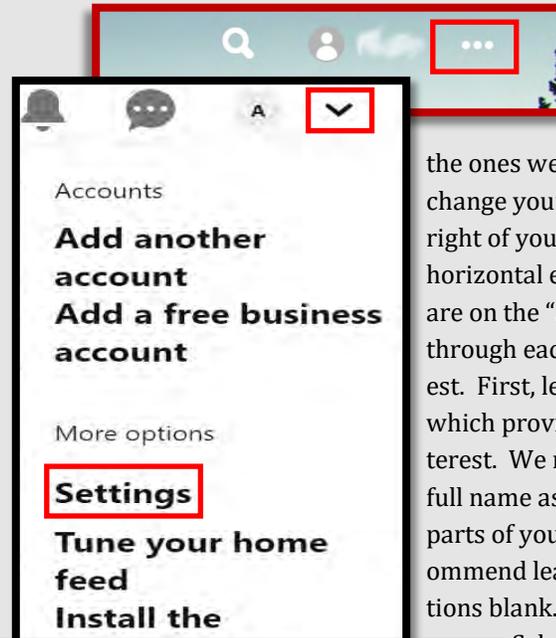
Next, let's review your "Account settings". Under "Account settings" you will find options to change your email address and password, set your login options, and delete or deactivate your account in the case you decide you no longer want to use Pinterest. We recommend you always log in with a unique password used only for Pinterest, and never log in via Facebook or Google. Ensure the

toggles next to these options are set to "Off". If you decide to deactivate your account for a period of time or delete it altogether, follow the prompts after selecting the correct option. Select "Done" at the top to save your changes.

## Personal Computer (PC) Version

### Do's and Don'ts

- ◆ **Do** use Two-Factor Authentication to protect all your information. Like all social media accounts, it is important to make sure your Pinterest is as secured as possible. Two-Factor Authentication is one of the best ways to control your information.
- ◆ **Do** make sure your email is up to date! If Pinterest suspects nefarious activity on your Pinterest account, they will lock your account down and send your new password to the email address on file.
- ◆ **Do** monitor what your children and teenagers are looking at on Pinterest. Pinterest does have inappropriate content that, if not specifically tagged as such, will not be flagged or removed by Pinterest.
- ◆ **Do** make your boards private once you create them so that they are not searchable by any and all Pinner.
- ◆ **Don't** put personal information on the title of your Pinterest boards. A lot of information can be obtained simply by reading a title (whether or not you have children, rent or own a home, marital status, etc.).



Check your credit report at least once a year. You may also want to check your credit report if you feel any of your social media accounts have been compromised. #beatidentitytheft

# LOCKING DOWN



## Personal Computer (PC) Version

Make sure your antivirus and antimalware software stays up to date. Keeping software up to date helps to prevent advanced malware and viruses from affecting your computer.

## Privacy & Security

The next few settings have to do with linking your other social media accounts to Pinterest. **As always, we recommend that you do not link any other social media accounts to Pinterest.** If someone gains access to one of your social media accounts, keeping them separate prevents an intruder from accessing all your other accounts.

First, see the “Claim” section. This option allows you to connect Instagram, Etsy, or YouTube accounts, with the purpose of gaining more popularity for your posts across all platforms. We recommend **not** claiming these accounts.

Next, continue down the screen to find “Privacy & data” and review the settings. First, you will see “@Mentions” which allows other Pinterest users to mention you in their comments and pins. It is recommended were feasible that this function be turned off or that “Only people you follow” be allowed to mention your name. Next you will see “Search Privacy”, which left unchecked, will allow your account to be searchable on Google. We recommend you make your account private by checking the box next to “Search Privacy”, as indicated above. Next look at “Personalization” and see the list beneath it. The purposes of these settings are for Pinterest to collect information about you in order to personalize ads and other content for you. We recommend leaving all boxes in this section “Unchecked”.

Now let’s visit the “Security” section, which allows you options for better account security. The first section is for “Two-factor Authentication”, which we strongly recommend you enable. Select the box next to “Require code at login”, and you will have the option of having a code sent to your mobile device that you will need to enter when you log in - a new code will be sent each time you log in. This is the highest level of security you can have for your account.

# LOCKING DOWN

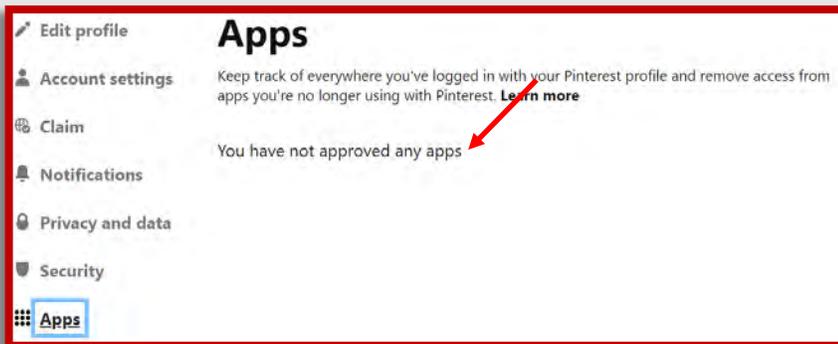
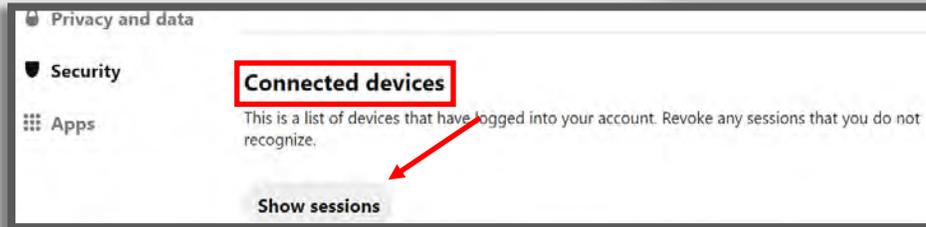
## Personal Computer (PC) Version



### Privacy & Security, etc.

Under “Two-factor Authentication”, you will see “Connected devices”. Select “Show sessions” in this section and you will be provided the opportunity to “End Activity” for all sessions that may seem suspicious or are not needed. If you suspect that your Pinterest account may have been compromised, the “Show Sessions” section may help you to identify a suspicious account and “End Activity” so that you can secure your account and change your password. It is a good idea to go through the “Show Sessions” section periodically and clean it up.

**Remove your last name.** A Pinterest profile is always open, everyone can see your profile picture and name. This is a severe privacy issue. For greater privacy, remove your last name and/or change your username (shown in the URL) to be something nonspecific to you. It is also recommended that users use an anonymous profile picture. Also remember **not** to link your Pinterest account with any other social media accounts.



Finally, the “Apps” section allows you to disconnect any third-party apps you might have linked to your account. Again, we recommend keeping all accounts separate for the best security. If you were to lose your mobile device or computer, you do not want someone to have full access to all of your accounts, including Pinterest. If there are any apps listed in this section, we recommend deleting them.

**Hide your profile from search engines.** The default Pinterest settings allow your profile to come up in search results when someone searches your name on a search engine. This gives access to your online activity to anyone who knows your name. Hide your profile by opening the “Settings” > “Privacy and data” > “Hide your profile from search engines”.



Remember if a “Pin” seems too good to be true it very likely is. Pinterest has many spam “pins” where a single click can lead to a third party site. #staysafeonline

# LOCKING DOWN

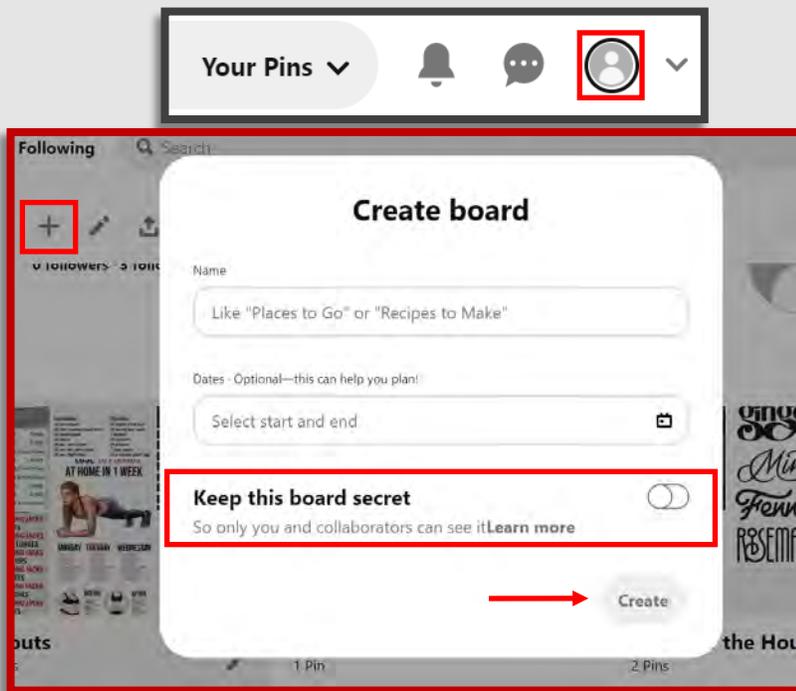
## Personal Computer (PC) Version



### Visible Content

What you display on your Pinterest account reveals a lot of information about you, so you have to be careful about what you “Pin”. Everything that you “Pin” is public. Not just your followers, but everyone can see your profile and what you pin. Pinterest has no means of limiting the visibility of your “Pins” or your “Comments” like there are on other social media platforms (unless you make them “Secret”, which is discussed next). Once a “Pin” or “Comment” is loaded, there is no taking it back.

Take a look at the titles of your “Boards”, and make sure they reveal no information about you or your family. For instance, do any of them have names of children, schools, churches, workplaces, etc? Also, take a look at your whole collection of “Boards” to see what kind of narrative it tells about you. Consider that all your “Boards” and “Pins” together paint a pretty illuminating picture of your interests, values and lifestyle.



There is only one way to ensure full control over your “Boards” and “Pins”, which is by setting them to “Secret”. When you use this feature, no one can see your content unless you specifically invite them to. We recommend you consider setting some or all of your “Boards” to “Secret” in order to limit the amount of information someone can gather about you.

To create a “Secret Board”, select your “Profile Icon” in the top right corner of the page. Then select the “+” icon to create a new “Board”, name the board, and set the toggle next to “Keep this board secret” to “On”. Select the “Create” button. Only the creator of the “Secret Board” has control over its features, and with whom content is shared. You must invite

“Collaborators” via email in order for them to see the content. When you “Pin” content to a “Secret Board”, the “Pins” are also private. Only the creator can make the board public, and when you do, all content is made public, including all “Pins” and “Comments”.



**Scam Pins:** Keep an eye out for “Scam Pins” that might be advertising “Amazing Weight-loss Techniques” or “Free Gift Cards”. These scams lead you to a scam website and ask you to fill out a survey with personal information, download malware, or share the “Pin” forward. To avoid “Scam Pins”, you should pay attention to the URL with every single pin. The URL is located at the bottom left of a pin. Avoid any pin that leads to an unofficial or fishy URL.

Everything you post on Pinterest can be seen by the “Public”. The ONLY way to maintain full control of your pins is to create a “Secret Board”.

# LOCKING DOWN

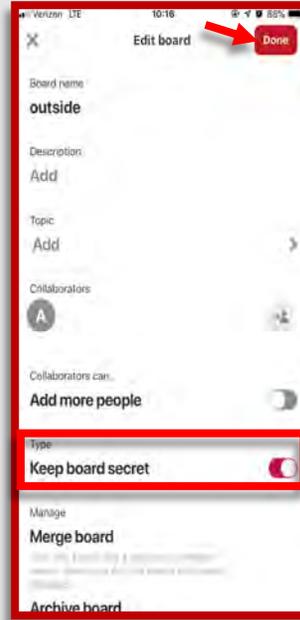
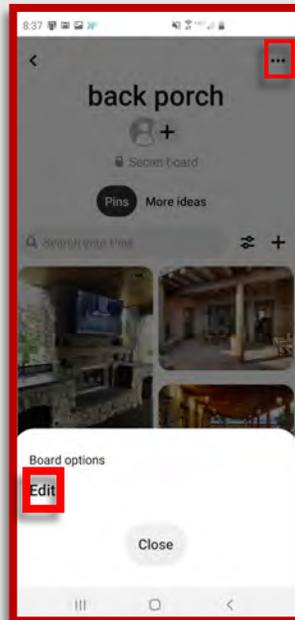
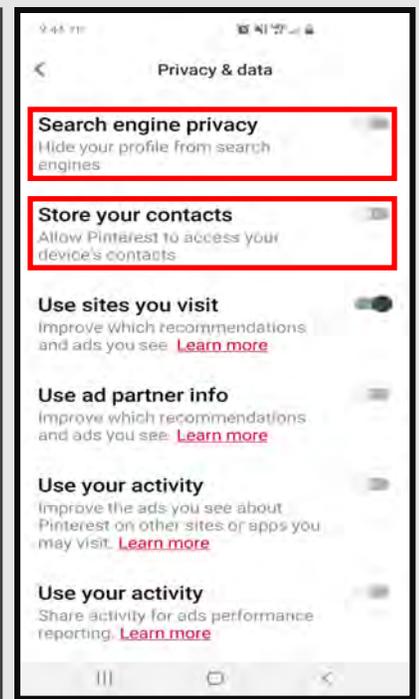
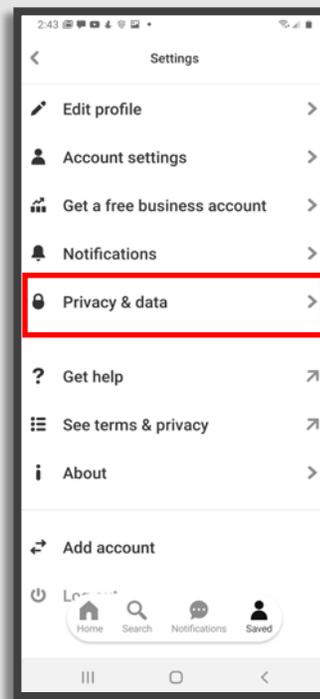


## Mobile Device Version

*\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Most images provided are of Android screens. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal - when they are significant, such differences are noted specifically.*

### Security & Privacy

On your mobile device, you will begin at your “Profile” screen by selecting the “Profile” icon at the bottom right of the screen, or locating your “Profile Picture” on the page. Then select the “Settings” icon at the top right. The “Edit profile” and “Account settings” are the same as the computer version. However, the “Privacy & data” section is a little different on the mobile version. If you select “Privacy & data”, then see “Store your contacts”, and ensure the toggle is set to “Off”. Additionally, make sure that all your privacy settings are set the way you want them, in case the settings you chose via computer did not transfer to the mobile app.



### Visible Content

To make a “Secret Board” on your mobile device, first go to your account by selecting the “Profile” icon at the bottom right of the screen. Select the “Board” you want to make private, then select the “Menu” icon, or “...” at the top right of the screen, select “Edit”, then scroll down to “Keep board secret”, and set the toggle to “On”. To save your changes, select the “Done” button at the top right of the screen.

While Pinterest is full of entertaining content, remember it is for all ages and as such its content can be “for Adults Only” and not what you want your children to see.

# LOCKING DOWN



## Indicators of Possible Account Compromise:

**Do you think your account may have been compromised or hacked? Have you noticed any of the following:**

- \* Unexpected posts posted by your account
- \* Direct Messages sent from your account that you did not initiate
- \* Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- \* A notification from Pinterest stating that your account may be compromised
- \* A notification from Pinterest stating that your account information (bio, name, etc.) has changed
- \* Your password is no longer working or you are being prompted to reset it. \*If this occurs it is highly recommended that you sign-in online and change your password immediately.

If you said "Yes" to any of the above , it is advised you take the following actions:

- ◆ Delete any unwanted pins that were posted while your account was compromised
- ◆ Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be pinned after you've changed your password
- ◆ Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- ◆ Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure that you and only you can access your Pinterest account
- ◆ Be sure to check that your email is secure. It may be worth changing the password to both your Pinterest account and the email associated with your Pinterest account. \*If you feel your email may have been compromised and need help finding the right contact information for your email provider please see page 21 of this smart book under the "blue box" at the bottom of the page.

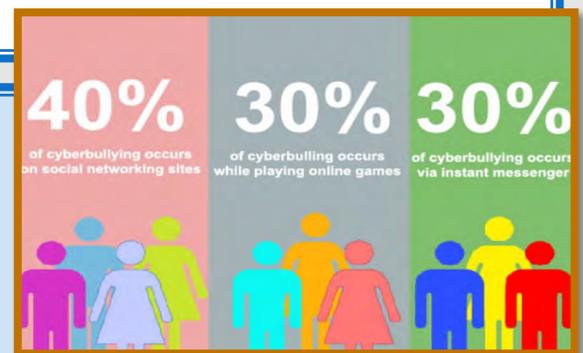
If you need report a pin, comment, or message: <https://help.pinterest.com/en/article/report-something-on-pinterest>

If your account was hacked: <https://help.pinterest.com/en/contact>, then go to "Account Access and Closure," "Login Issues," "Continue" and follow the steps to describe your specific situation.

If you find that you or someone else is being bullied or harassed go to: <https://help.pinterest.com/en/article/report-harassment-and-cyberbullying>

If you cannot log in to your email account, Twitter has provided links to each email account's "having trouble signing in" page for your convenience. <https://help.twitter.com/en/managing-your-account/cant-access-my-accounts-email-address>

If you still need help or have questions, you can always contact Pinterest by: [https://help.pinterest.com/en/contact?page=about\\_you\\_page](https://help.pinterest.com/en/contact?page=about_you_page)



If you do not have access to the email you originally signed up on Pinterest with or believe it may have been hacked, Pinterest will allow you to provide an alternate email for communication. This can be both good and bad for Users. While it can provide peace of mind if you need to regain access to your account, it does create its own vulnerability and Users should be aware of this.

# LOCKING DOWN YOUR SNAPCHAT



## Mobile Device Version

*\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

## Do's and Don'ts

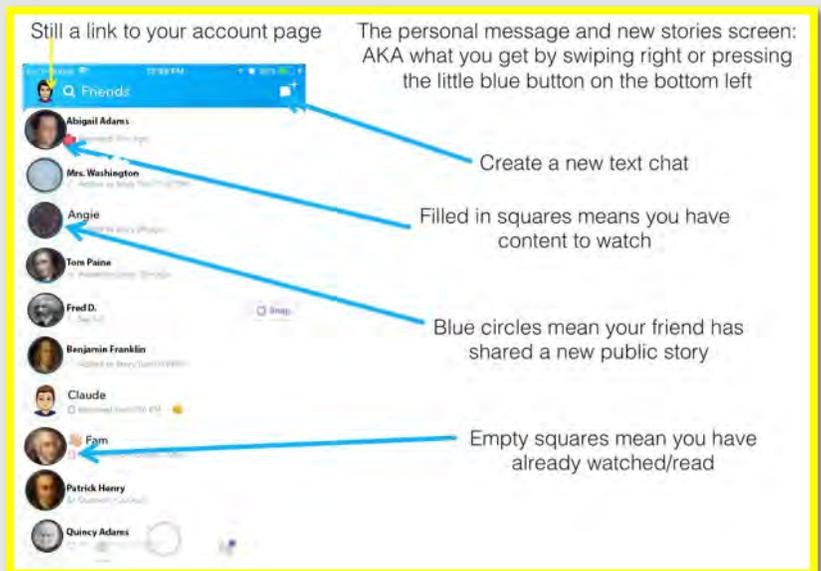
- ◆ Do set up privacy and security settings on your Snapchat and help your teenager to do the same.
- ◆ Do assume ALL information and images you share are publicly viewable, regardless of your settings.
- ◆ Do talk to your teenager about the dangers inherent to Snapchat. Make sure they know to come and tell you if someone they don't know tries to contact them or sends them inappropriate material.
- ◆ Do **not** add your birthdate, location, or other personal details to online profiles.
- ◆ Do **not** allow users you do not know personally to contact you via Snapchat.
- ◆ Do **not** believe that all pictures and videos are automatically deleted. There are ways to save and share content despite Snapchat's efforts to make all communications disappear.

Shown to the right is an overview of the "Chat" feature of Snapchat. Select the "Chat" icon on the lower left corner of the screen (above in red). Here you can see if someone has sent you a message, posted a story, or reviewed your posts. You can also start a "Chat". For now, let's select your "Profile" icon at the top left and head to your Snapchat stats and "Settings" section.

Snapchat is an image and video messaging app that allows users to share multimedia messages that will "self destruct" in up to 10 seconds. It's communication style is meant to mirror real life face-to-face interactions that are temporary, and not stored anywhere. Content is designed to delete automatically, but most users are aware that content can be saved using screen shots or other software.



The best way to begin understanding and locking down Snapchat's capabilities is to familiarize yourself with Snapchat basics. In the box above you can look over the main icons and functions located in Snapchat. Your "Home Screen" is shown above. You know you are there when you have a "Camera View". One of the main features of the app is making "Snaps", via photos, which you would do from this screen, then share with your "Friends". Next, identify your "Profile" picture at the top left of the box (highlighted in red), this icon will take you to your Snapchat statistics and the "Settings" icon.



As of March 2020, there are an estimated 229 million Snapchat users. Make sure you know who your children are talking to. #keepourkidssafe

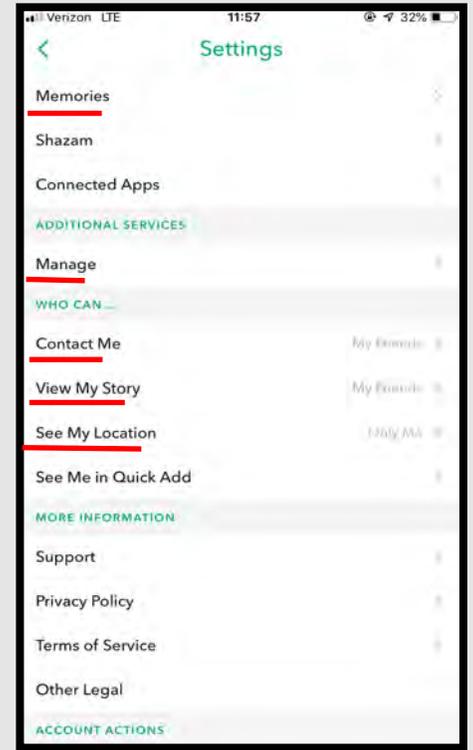
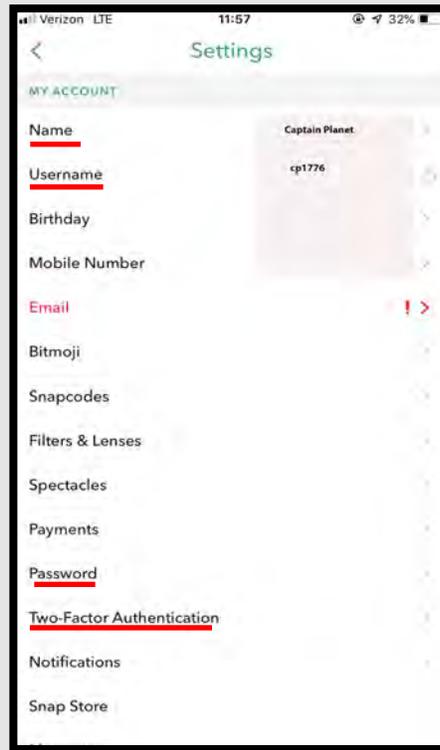
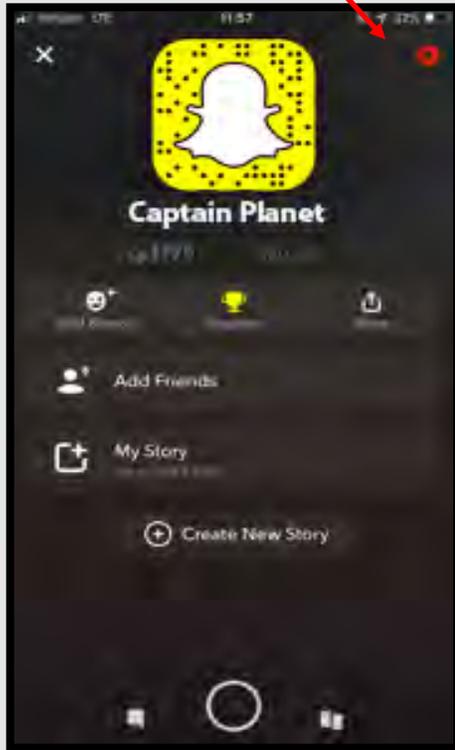
# LOCKING DOWN YOUR SNAPCHAT



## Mobile Device Version

*\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android yellow.*

The Pew Internet and American Life Project found 15% of teenagers ages 12 to 17 acknowledge they received a "sex" from someone they know.



After reviewing the different sections on page one of this Card, let us begin locking down your account.

Begin by selecting your "Profile" picture at the top left of the screen on your "Home Page". Next select the "Settings" icon from the top right corner of the screen (shown above in **red**).

From here we can review all of the settings offered by Snapchat:

The "Settings" screens on iPhone and Android have a few differences on Snapchat. Throughout this Card, you will find iPhone screenshots outlined in **black**, and Android screenshots in **yellow**.

First, check out your "Name" and "Username", and make sure they don't give too much information about you. We recommend you use a nickname or a mixture of names instead of using your full name, and never add birthdays or other significant information to your name. You do not need to put your real birthday on your account, and should consider using an inaccurate one.

Next, we recommend using a "Password" that is unique to Snapchat. As with all of your social media accounts, reusing passwords creates an unnecessary vulnerability, and you should use unique passwords for each account.

On the next page, we will go through the underlined menu items from the above 2 screenshots.

**Geo-filters:** location-specific elements that can only be unlocked by visiting a specific place. If the Geo-filters are shared, especially by teenagers, any individual could find or track them, to include predators. For all "Locations" It is recommended that this function be set to "Only Me" Additionally, Snapchat will now direct users together more precisely if "location" is turned on, by providing step by step direction.

**Snapcash:** like PayPal or Venmo, Snapcash lets users transfer money to each other.

**Memories:** Users can store snaps to appear as memories for later use, however this this is not recommended.

# LOCKING DOWN YOUR SNAPCHAT



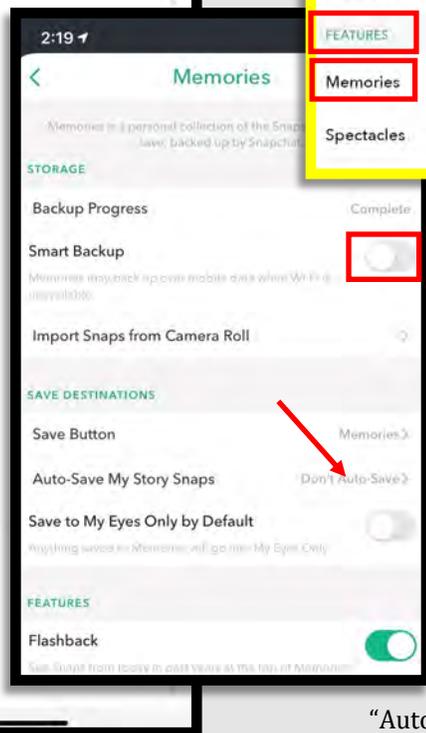
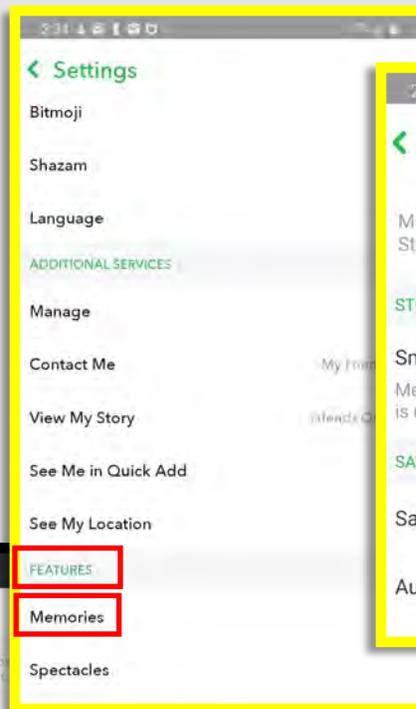
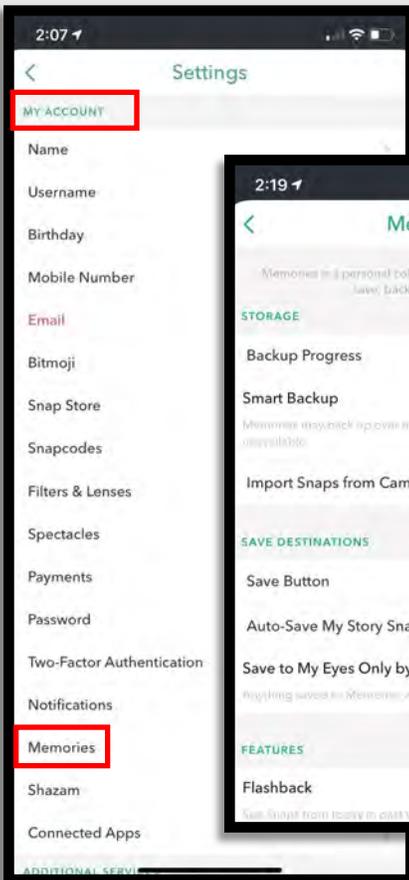
## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android yellow.**

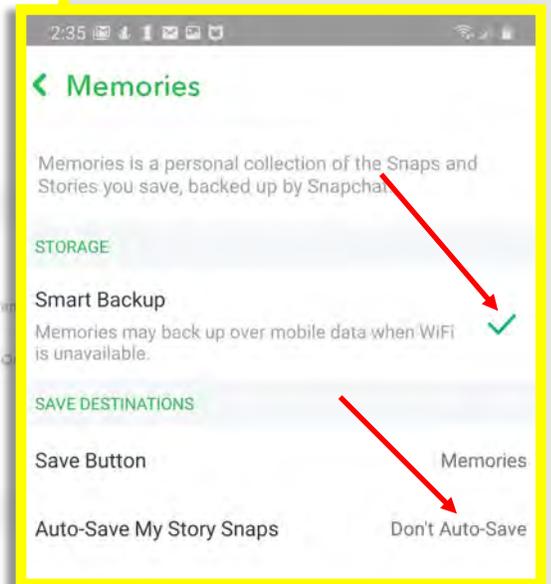
90% of Snapchat users are 13-24 years old, and 69% of U.S. teens say they use Snapchat. Talk to your child about acceptable behavior on Snapchat.

## Two-Factor Authentication

“Two-Factor Authentication” is the most secure option you have for Snapchat security and privacy. To enable it, select “Two-Factor Authentication” from the “Settings” menu, under the first section titled “My Account” (shown on page 2 of this card) and follow the prompts to complete the process. Also referred to as “Login Verification”, this feature requires you to enter **both** your password and a verification code that is sent to your phone, each time you log in on a new device.



## Memories



Next, let’s look at “Memories”, which is Snapchat’s storage function. Snaps are saved on Snapchat’s servers, but are searchable and visible only to you. We recommend you **not** allow Snapchat to store your photos, and instead choose manually when you want a “Snap” saved to your “Memories” as needed. It is important to know that snaps of all kinds do not truly delete on Snapchat.

**On iPhone:** go back to “Settings” and select “Memories” under “My Account”. We recommend setting the “Smart Backup” toggle to “Off” and select “Don’t Auto-Save” next to “Auto-Save My Story Settings”. (left)

**On Android:** go back to “Settings”, scroll down to “Features”, then “Memories”, and “Uncheck” the “Smart Backup” option. Also, ensure “Auto-Save My Story Snaps” is set to “Don’t Auto-Save”. (above)

# LOCKING DOWN YOUR SNAPCHAT



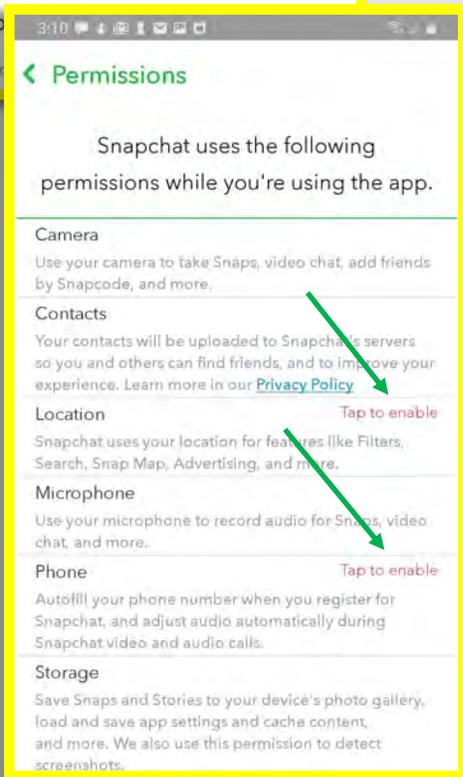
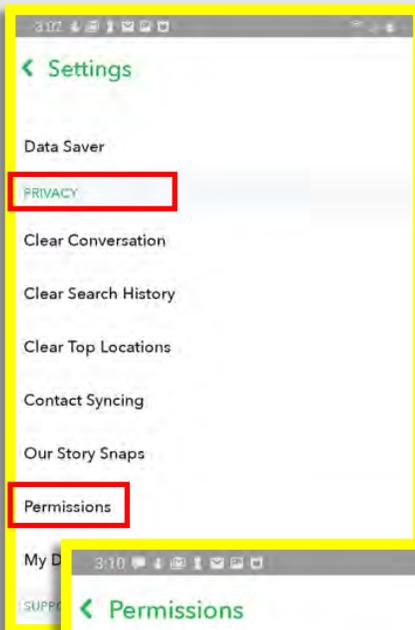
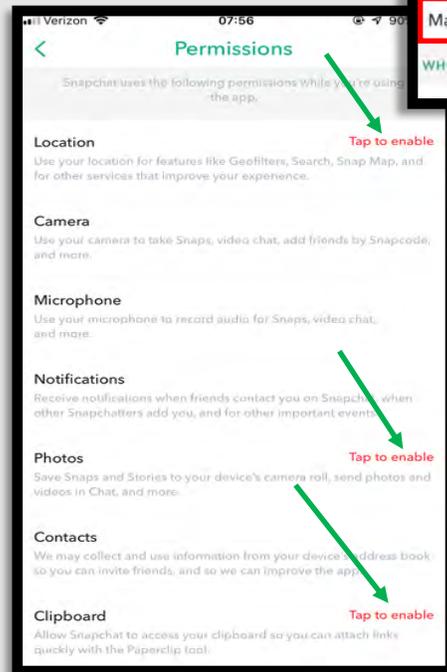
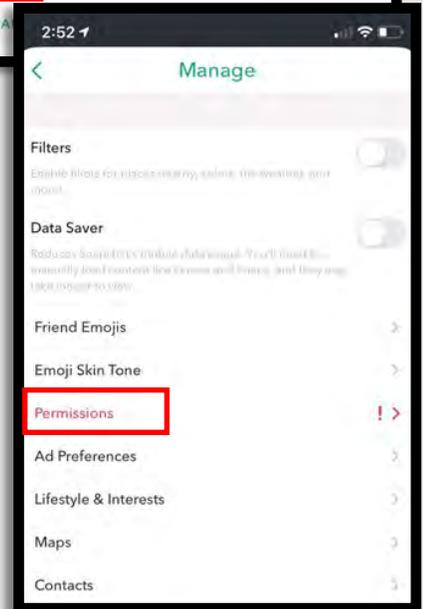
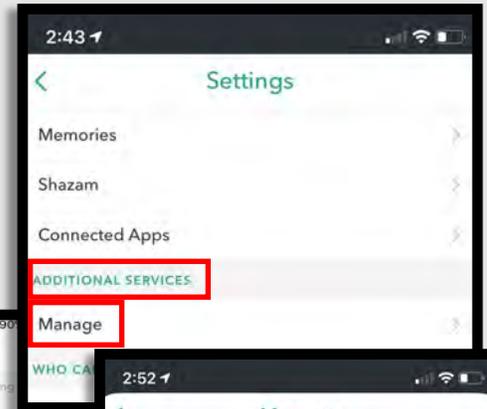
## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android yellow.**

### Manage Permissions

Next, let's go to the "Additional Services" section (both iPhone and Android), and locate the "Manage" option.

**On iPhone:** select "Manage", then "Permissions", and ensure "Location", "Photos" and "Clipboard" are **not** enabled. Each of these features allows Snapchat to capture and store information from your mobile device in some way.



**On Android (left):** under "Settings", scroll down to the section titled "Privacy", then select "Permissions". You can adjust "Location" and "Phone". We recommend you leave them "Disabled", as seen here to the left.

**What is "Scanning"?** "Scan" lets you identify things like products, songs, barcodes, and more. To power this feature, Snap partners with third-parties like Amazon and Shazam. This means that if / when you "Scan", certain information may be sent to these partners. For example, Snap may send images captured by your camera to Amazon, who will send back search results if they find a matching product. Snap may send audio hashes captured by your microphone to Shazam, who will send back matching songs. The data is maintained for a minimal period of time and is not connected to your Snapchat account. Still, we do **not** recommend using the "Scan" feature.

Hackers have been known to publish thousands of snaps mainly of 13 to 17 year old's. Talk to your teenagers about who they are connecting with.

# LOCKING DOWN YOUR SNAPCHAT



According to TeenSafe.com 47 percent of users admit to using screenshots and 52 percent note that others have used screenshots of their messages. #Staysafeonline

## Mobile Device Version

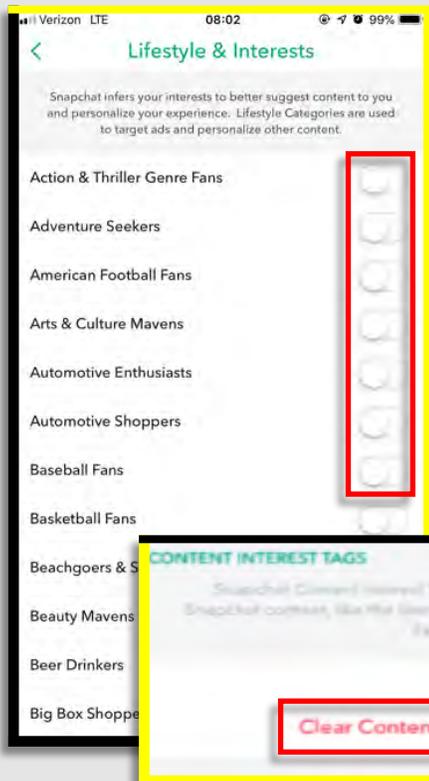
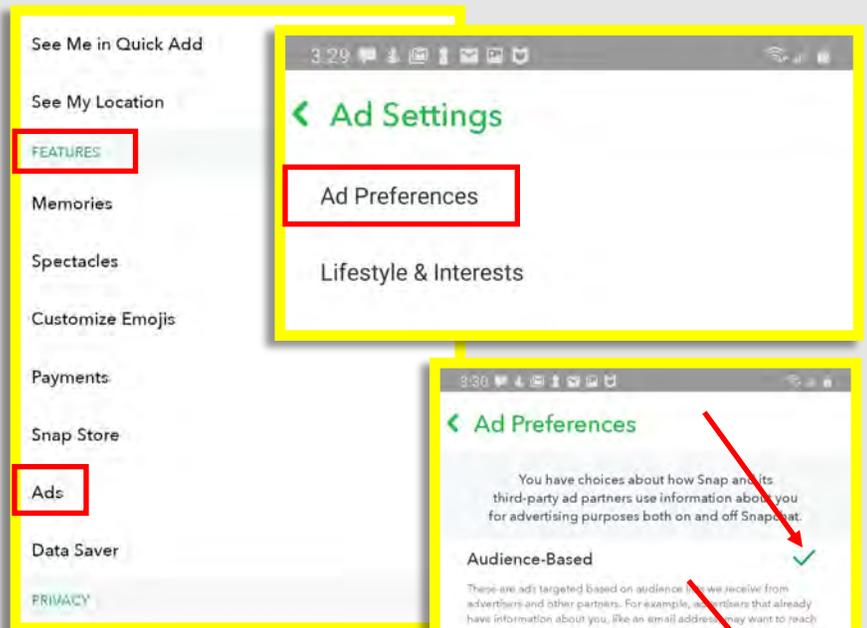
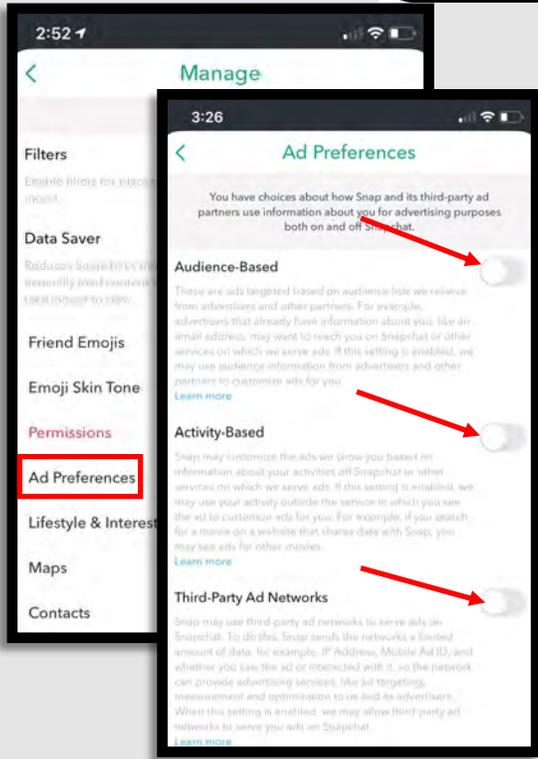
*\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

## Manage Advertising

Next, let's lock down what kinds of information Snapchat can capture from you in order to support advertising.

**On iPhone:** go back to the "Manage" section, select "Ad Preferences", ensure all three toggles are set to "Off"

**On Android:** under "Settings", scroll down to the section titled "Features", then select "Ads". Select "Ad Preferences" on the next screen, then ensure "Audience-Based", "Activity-Based", and "Third-Party Ad Networks" are all "Unchecked".



Next, go back to the "Manage" section ("Ad Settings" on Android) and select "Lifestyle & Interests," its recommended that you unselect any section that is enabled. You can also periodically clear any tags that may have specified your interests by selecting "Clear Content Interests Tag" located at the very bottom of the "Lifestyle & Interests" screen.

If you ever want to leave Snapchat for good, you can close your account on [accounts.snapchat.com](https://accounts.snapchat.com).

# LOCKING DOWN YOUR SNAPCHAT



## Mobile Device Version

*\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

### Manage Maps and Contacts

We want to make sure Snapchat cannot view your "Location" or the "Contacts" on your mobile device. First, we recommend you hide your location whenever possible.

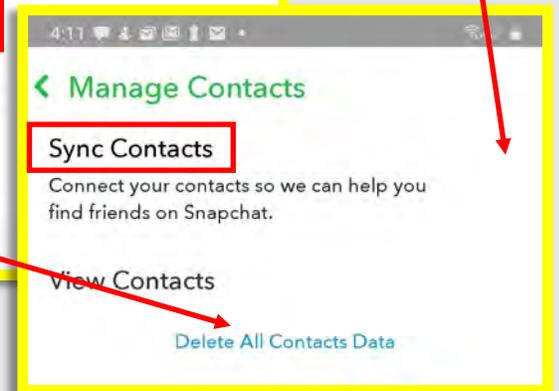
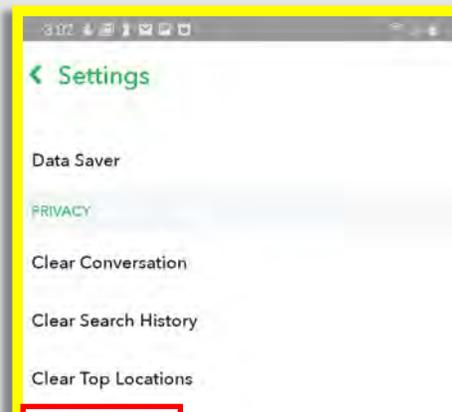
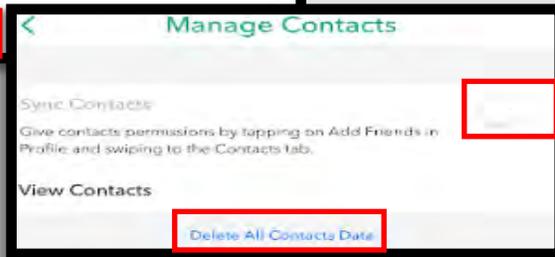
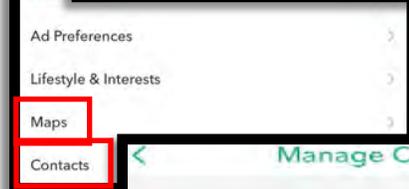
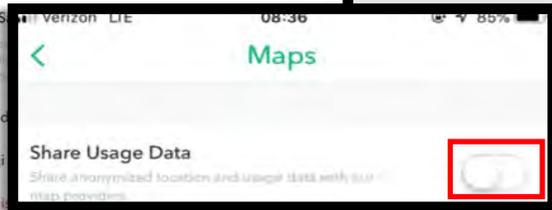
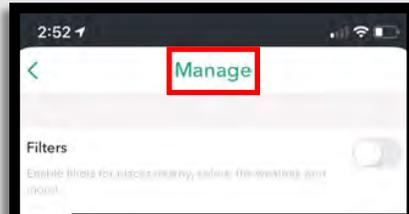
**On iPhone:** go back to "Manage", then "Maps". Set the toggle next to "Share Usage Data" to "Off".

**On Android:** go to "Settings", then scroll down to "Privacy", and go through all options listed, including "Clear Conversation", "Clear Search History", and "Clear Top Locations", and select "Clear" on the pop-up. This will clear location and other tracking data for you.

Next, we recommend forbidding Snapchat access to your "Contacts".

**On iPhone:** under "Manage", select "Contacts", then set toggle to "Off", and "Delete All Contacts Data" (see left).

**On Android:** under "Settings", scroll down again to "Privacy", select "Contact Syncing". Ensure this feature is "Disabled" by identifying the space to the right of "Sync Contacts", and see that there is "No Checkmark" visible. Also, select "Delete All Contact Data" below "View Contacts" as well.



**When does Snapchat delete "Snaps"?** Snapchat servers are designed to automatically delete all "Snaps" (on their servers) after they have been viewed by all recipients. All unopened "Snaps" are deleted after 30 days.



61% of Snapchat users are female and 38% of users are male. This is opposite of Facebook and TikTok, which have majority male users. #Staysafeonline

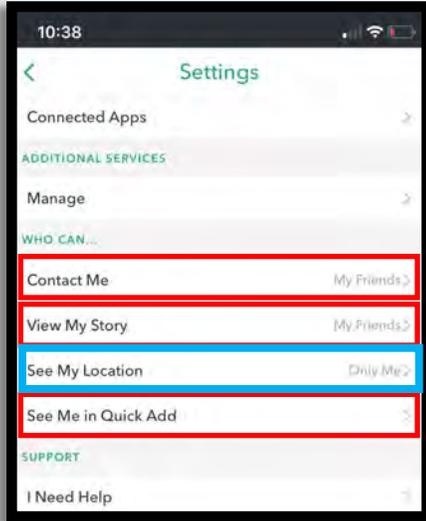
# LOCKING DOWN YOUR SNAPCHAT



## Mobile Device Version

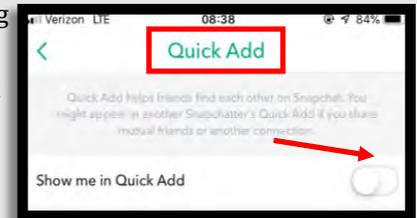
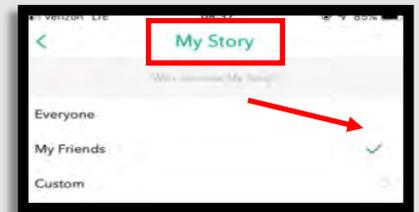
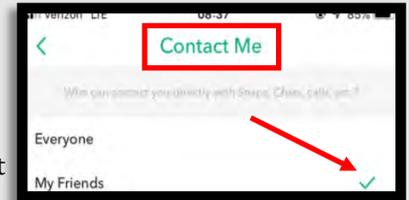
*\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

### Manage Privacy Settings



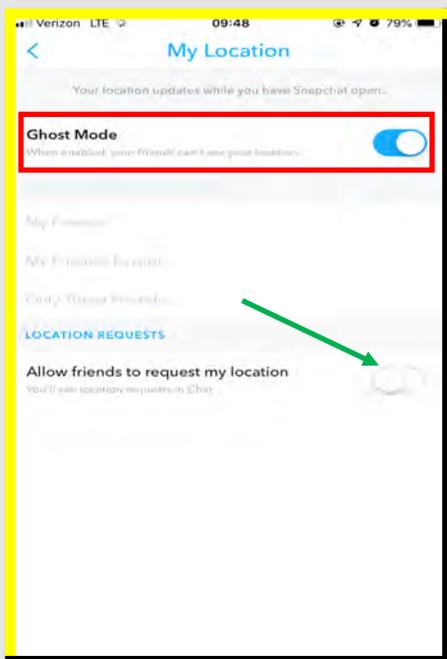
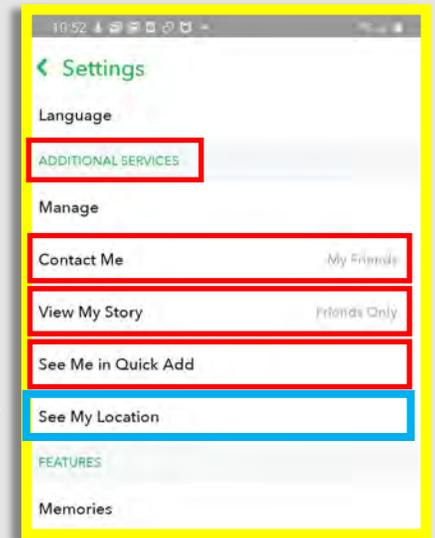
Next it is important to set your privacy settings in order to control who can see your “Snaps” and contact you.

**On iPhone:** go back to “Settings” and select “Contact Me” under the “Who Can...” section. It is recommended here that only “My Friends” are able to contact you, in order to help keep you and your children safer while using this App. Under the same “Who Can...” section select “View My Story” where it is also recommended that “My Friends” be enabled to ensure that your videos and pictures are not available to the public. Depending on your level of involvement (or your child’s) with this App, you may also want to lock down



the “See Me in Quick Add” section (shown to the right). Making sure this is **not** enabled will prevent your profile from showing up in other peoples’ profiles as a suggested contact.

**On Android:** go back to “Settings”, scroll down to “Additional Services”, and see “Contact Me”, “View My Story”, and “See Me in Quick Add”, and set them to the same as noted above. (see right)



Heading back to the “Settings” section, lets review the “See My Location”, under the “Who Can” section on iPhone, and the “Additional Services” section on Android (see **blue** boxes above left and to the right). Snapchat allows users to use “Ghost Mode” to prevent even their “Friends” from viewing their location. We recommend you enable “Ghost Mode” in order to prevent anyone from viewing your precise location on the Snapchat “Map”. We also recommend that you **not** enable “Allow friends to request my location.”

**What is “Snap Map”?** “Snap Map” lets you see where your “Friends” are and what is going on around them. To open “Snap Map”, pinch your fingers on the “Camera” screen, “Friends” screen, or “Discover” screen.

You won’t appear on “Snap Map” until you open it for the first time and choose to share your location.

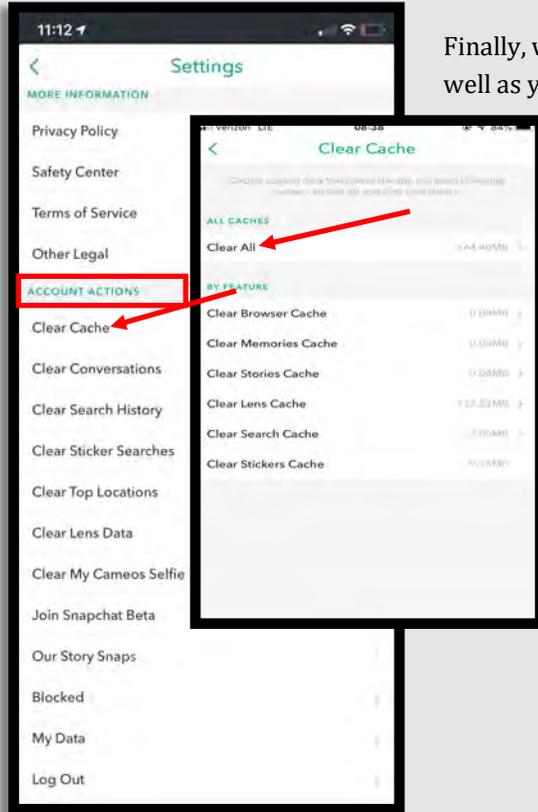
# LOCKING DOWN YOUR SNAPCHAT



## Mobile Device Version

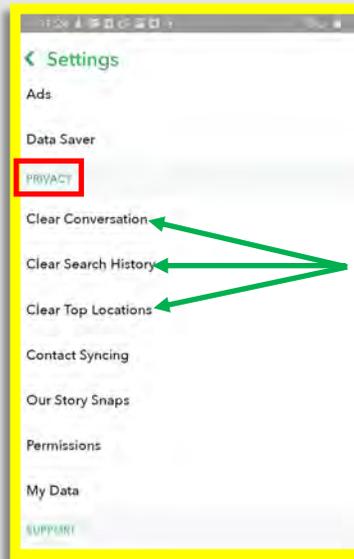
*\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are significant for some features, and in these cases iPhone images are outlined **black** and Android **yellow**.*

Because Snaps and messages disappear, it is impossible to monitor your child's behavior on Snapchat. Are they sexting peers? Are they bullying or being bullied?



Finally, we recommend clearing out old data periodically on your Snapchat account, as well as your other social media accounts, whenever this feature is available. Snapchat provides you the capability to “Clear Cache”, “Clear Conversations”, Clear Search History, and “Clear Top Locations” (in addition to others on iPhone). You will clear these and the other options listed, the same way you would clear your Internet browser cache.

**On iPhone:** go back to “Settings”, scroll down to “Account Actions”, and choose which caches you want to clear. Alternatively we recommend “Clear Cache”, then “Clear All”, which will clear all caches under “Account Actions”.



**On Android:** go back to “Settings” then “Privacy”. Select each, “Clear Conversation”, “Clear Search History”, and “Clear Top Locations”, and choose to “Clear” them. Each of these must be one separately and the options are fewer than offered on the iPhone.

**Clear Chats:** You can now unsend a sent message regardless of whether a recipient has seen it. This feature is different from “Clear Conversation”, which only deletes content from your end. “Clear Chats” works in group chats or in one-on-one conversations, and applies to text, stickers, audio, or pictures and videos sent from your “Memories” section — not content you just took though. Note that the person in the conversation is alerted that a message was deleted. The purposes of the function are to clean up a typo and prevent unintentional messaging.

In order to delete a chat you already sent: 1) hold down the chat, and then 2) select “Delete”. Once selected, Snapchat will provide another message box to confirm that you would like to delete the chat you have just selected, and to remind you that, although the message is being deleted, your friends will still be able to see that something was deleted, if not the deleted content itself.

# TikTok SMART CARD



## Do's and Don'ts

- ◆ **Do** opt out of personalized data. TikTok is owned by a company based in China, opting out helps prevent your data from being gathered and redistributed without your knowledge.
- ◆ **Do** ensure family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- ◆ **Do** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- ◆ **Do not** provide any identifiable information (e.g. name, hobbies, job title, etc.) on your profile or in your videos.
- ◆ **Do not** link your TikTok account to any third party applications such as Facebook, LinkedIn, Instagram or Twitter.
- ◆ **Do not** use default settings on TikTok. All default settings are set to allow "Everyone" to be able to view and comment on your videos.
- ◆ **Do not** use identifiable locations, backgrounds or relatable images, when posting videos. It is important to be aware of your surroundings when posting images.

TikTok can loosely be described as a social network for amateur videos, teenagers and young people are the primary users of the app. It is easy for random people to reach out to users, especially teens, for nefarious reason. Recently TikTok has attempted to fix this issue by updating it's privacy settings, as noted throughout this card. Understand that TikTok is owned by a Chinese-based company, and it is thus important to limit what personal information you include on your account, videos and posts.

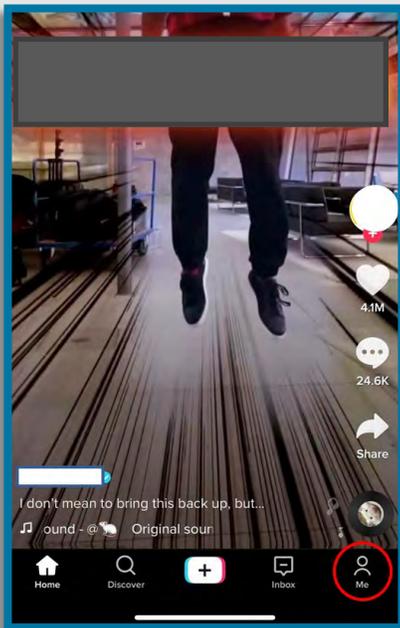
\*\* This information describes how to make your TikTok account secure on Android and iPhone mobile devices. Most images provided are of Android screens. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal - when they are significant, such differences are noted specifically.

TikTok is a video-sharing social networking service owned by ByteDance, a Beijing-based company.

## Edit Profile

When opening a new application, the first thing you want to do is set up your privacy settings in order to protect your personally identifiable information (PII). Default settings in Tik Tok are set to allow everyone to view, comment and access the information you post.

To begin locking down your account, look to the lower right hand corner and select "Me" to go to your profile settings (highlighted to the left in red). Click on the "Edit Profile" button. We recommend you do not use personal images or photos of yourself or your family. We also recommend you leave your "Bio" information blank or put as little personal information there as possible.



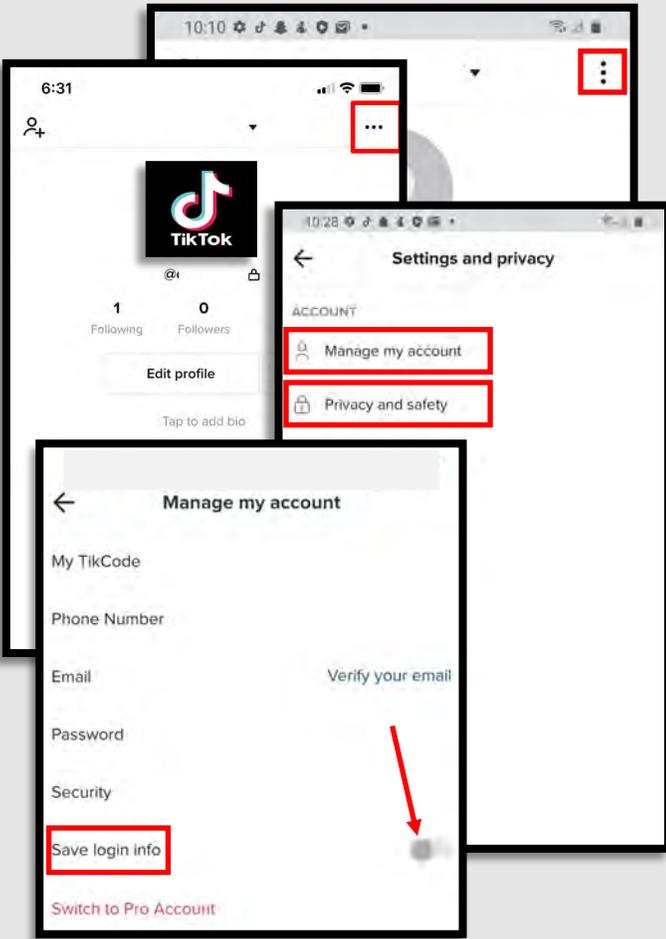
**Shut Off Direct Messaging** so that strangers cannot attempt to message you (or your children). Select the "Settings" icon, select "Privacy and safety", select "Who can send me messages", select either "Friends" or "Off".

We recommend you do **not** link your account to any other social media platform (e.g. Twitter, Instagram, Facebook), as TikTok will pull in your personally identifiable information and pictures from the other platforms. We also recommend you avoid using any Personally Identifiable Information (PII) anywhere on your profile. You are not required to put any personal or biographical information into your profile, and it is recommended you leave this section blank. PII is often used as a means to gain access to certain accounts (e.g. banks, credit cards, schools). Providing even just your birthday could help an identity thief steal your identity.

# TikTok SMART CARD



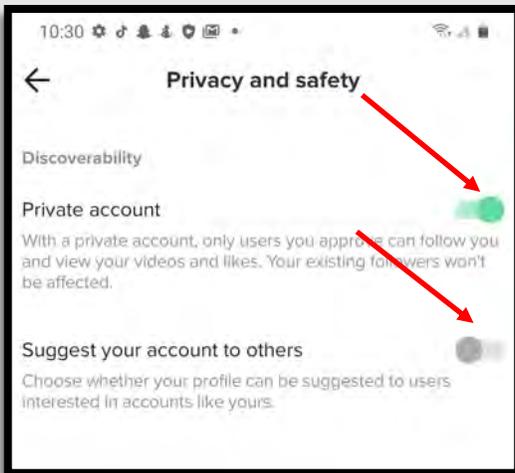
Talk with your children about what kinds of videos are okay to share, and with whom. Remember they are driven by "likes" and "reactions". #TikTokFamous



## Account Privacy & Login Information

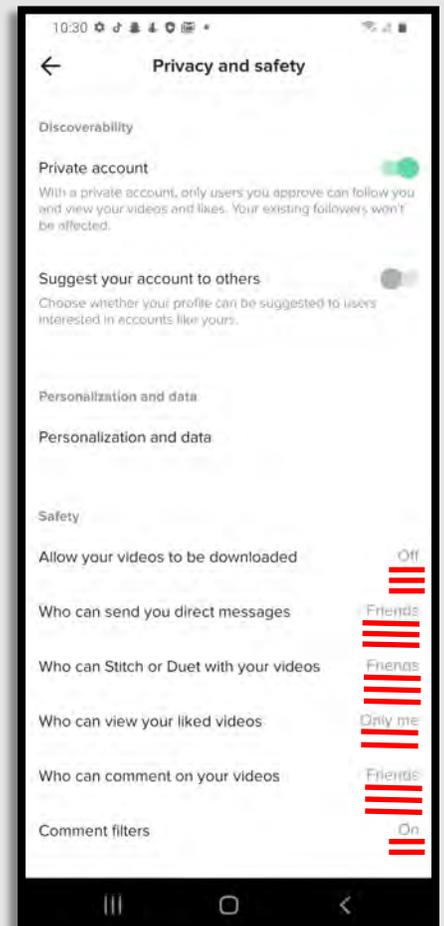
First, you will need to lock down your login information and set your account privacy. In order to access the "Settings and Privacy" tab go back to your "Profile" page and select the "Menu" button, (three horizontal lines on iPhone, 3 vertical lines on Android) in the upper right hand corner of your "Profile" screen (highlighted to the left). Under "Account", select "Manage my account". We recommend you set the "Save login info" toggle to "Off" in order to ensure that, should you lose your mobile device, no one has access to your TikTok account.

Next, let's look at how your posts appear to the cyber world. By default, all accounts are set to "Public", which means anyone can see what you post on Tik Tok. We recommend you set your account to "Private account", which will ensure that all videos can only be seen by the creator and no one else on the platform. With a "Private account" you can approve or deny users and limit incoming messages to "Friends" only. Note that even with a "Private account", your "Photo", Username" and "Bio" are still visible to all users of the platform. We recommend you set "Suggest your account to others" to "Off", which will allow you more agency in choosing and accepting your followers more proactively.



Go to "Privacy and safety", under "Settings and Privacy", then set "Private account" toggle to "On", and "Suggest your account to others" toggle to "Off" (see left).

Next, under "Safety", we recommend setting the toggles as they are seen to the right. It is most important that none of the options are set to "Everyone", as this allows all users to see your content.



Parents: Keep in mind that children may be tempted to take risks to get more of a following or get "likes" on a video, so it's important to talk with them about what they share and with whom. Also, users can "like" or "react" to a video, follow an account, or send messages to each other. This means that there is a risk that strangers will be able to directly contact children on the app.

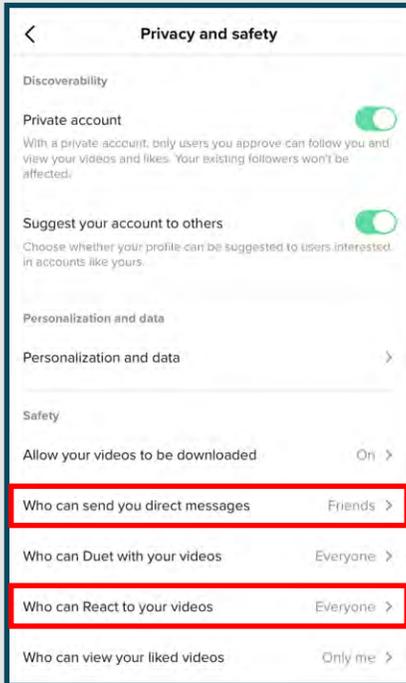
# TikTok SMART CARD

## Account Privacy, ctd.

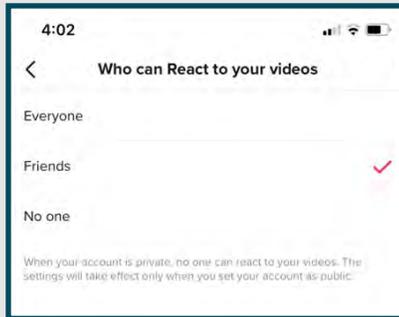


Following your child's TikTok account and paying close attention to your personal account is important not only for updates to policy and content, but to ensure account parameters. Help ensure your family is not vulnerable to anyone who can see what they are posting, liking and following.

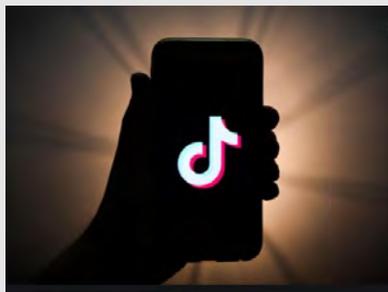
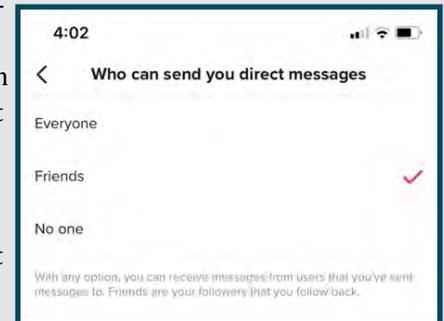
If your account is locked down, you're doing GREAT! If you allow your videos to be downloaded, you run the risk of compromising personal information.



We recommend that you control who will be able to react to the videos you or you child post to TikTok. Again, under "Settings and privacy" and "Privacy and safety", you are able to set some of the security settings to filter and protect your account, but more importantly your data, privacy and information. Highlighted to the left you see how to limit who can react to videos you post to TikTok. It is highly recommended you limit those who can react to your videos, to only "Friends."

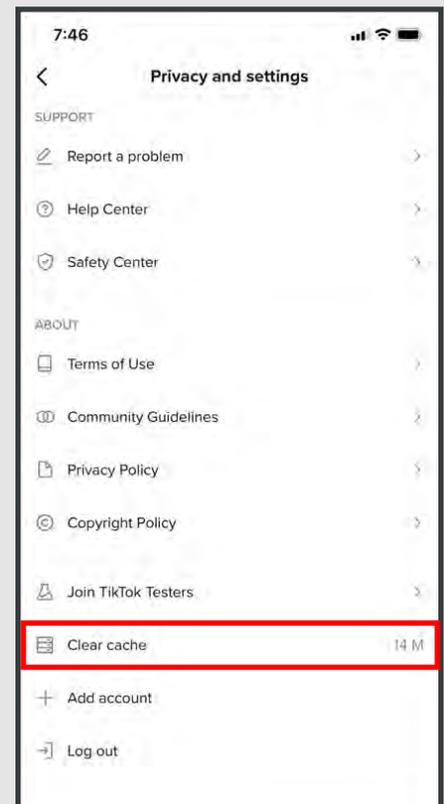


We also recommend you lock down "Who can send you direct messages", found in the same section. It is important you limit the people who can reach out and send a "Direct Message" to you (and your children). This will not only protect your safety, but also will protect you and your children from being "Messaged" by potential scammers or online predators.



Duets can be a fun way to create videos with another user, but you must be in control - TikTok gives you the option to **decide who can make duets with you** (everyone, no one, or just friends). We recommend you choose "Friends".

It is a good idea to clear your browser cache (highlighted to the right) because it will prevent you from using old forms, protect your personal information and help applications run better on your computer or phone. We recommend you clear your cache when you are done with every TikTok session in order to protect your information and remove potentially harmful data from your electronic device. In order to clear your TikTok cache, go to your "Profile" page, select the "Menu" icon in the top right of your profile screen. Select "Settings and Privacy, scroll to the bottom of the "Settings and Privacy" page and click on "Clear Cache."



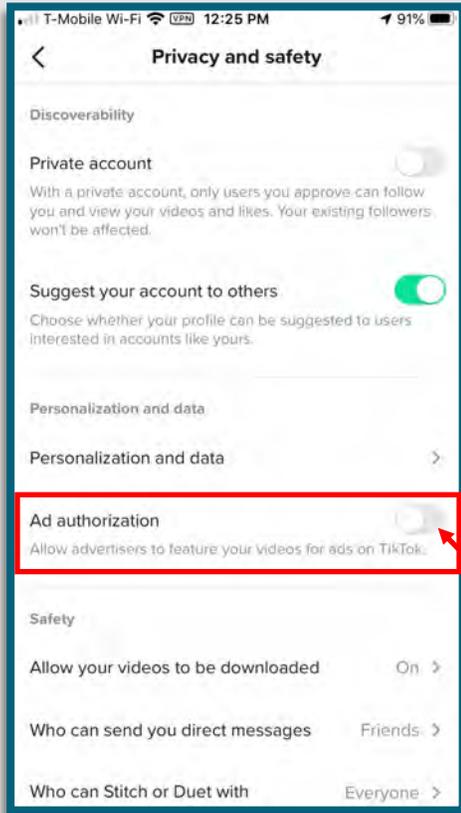
With a "Private account", only users you've approved as followers can see your content, but you can also choose to **make a specific video private**. Private videos are visible only to you, and you can select this setting when you originally upload the video - or by later making an uploaded video private. If you've already uploaded the video, tap the "Share" icon, then "Who Can View This Video" > "Private". If you're about to post, tap "Who Can View This Video" > "Private".

# TikTok SMART CARD



## Personalized Advertising

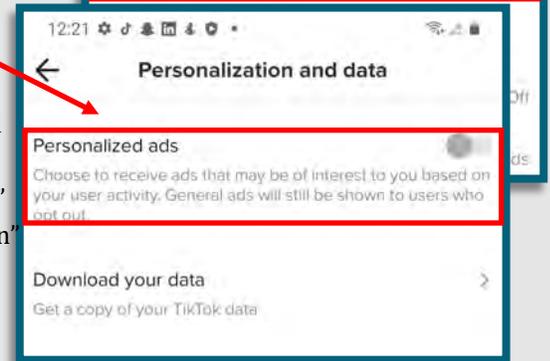
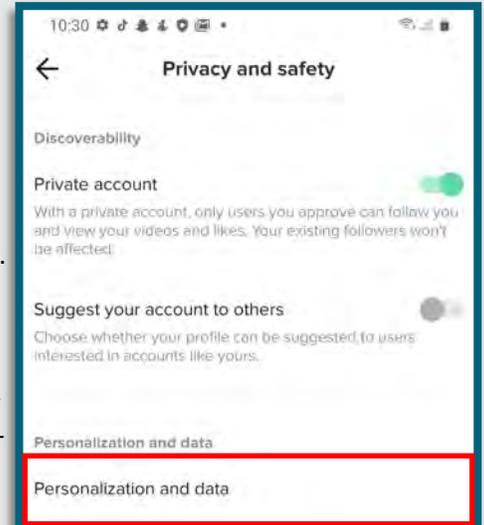
Parents have expressed concern about the inappropriate language and content of some videos posted on Tik Tok, which may make it less suitable for younger children.



Also in the “Settings and Privacy” section, you have the ability to control advertising data on your account. It is important to lock this kind of information down because, in order to personalize advertising for you, the app must access a lot of personal information and data on your device. It is best to disable this feature.

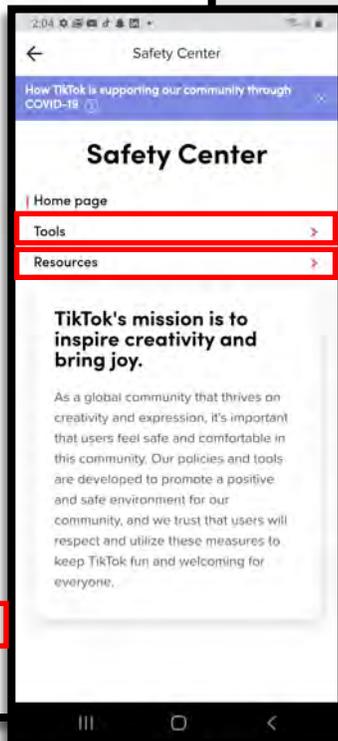
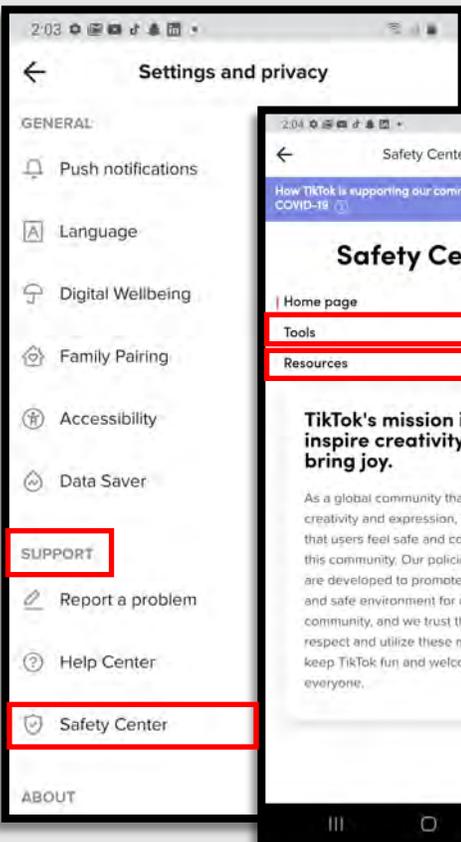
On your **Android**, under “Settings and privacy”, then “Privacy and safety”, in the second section select “Personalization and data”, then ensure the “Personalized ads” toggle is set to “Off”.

On your **iPhone**, select “Settings and Privacy”, then “Privacy and safety”, under the “Personalization and data” section. Ensure the “Ad authorization” option is toggled to “Off”.



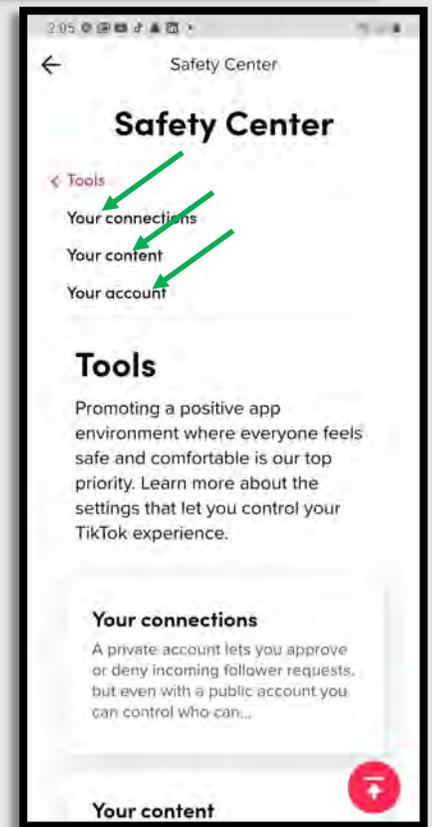
## Safety Center:

## Tools and Resources



Finally, let’s visit Tik Tok’s “Safety Center”, which is a useful resource hub that will help you learn how to use Tik Tok in the most safe and enjoyable way. In this section, you will find “Tools” and “Resources” that will help you further navigate your content, security, and privacy options. First, find the “Safety Center” by going to “Settings and privacy”, scroll to the middle of the menu and select “Safety Center” in the “Support” section.

Next, select “Tools”, and you will be given options to explore how to maximize your control over your “Connections”, your “Content”, and your “Account”.



# TikTok SMART CARD



## Safety Center: Tools and Resources, ctd.

Back under “Safety Center”, select “Resources” and see a list of various resources you will find useful. We recommend you check out “Safety Videos” (see right), and the “You’re in Control” video series, which are short educational TikTok videos on topics, many of which are presented in this SmartCard, such as “Choosing who can duet with you”, Reporting inappropriate behavior”, etc.

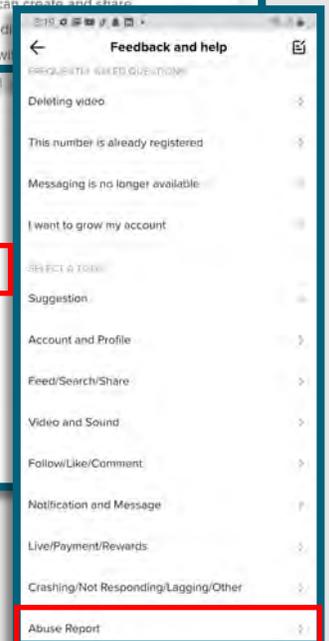
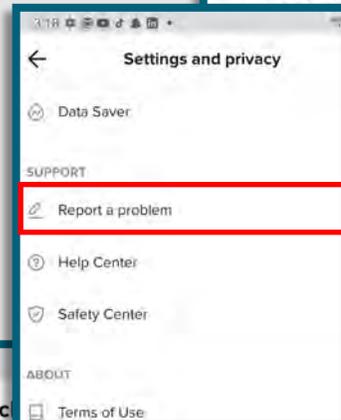
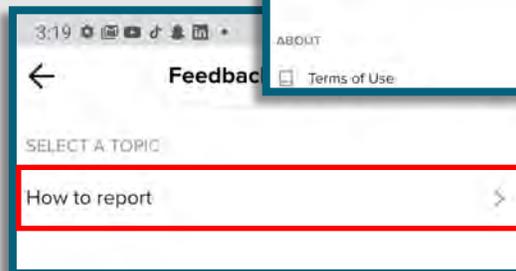
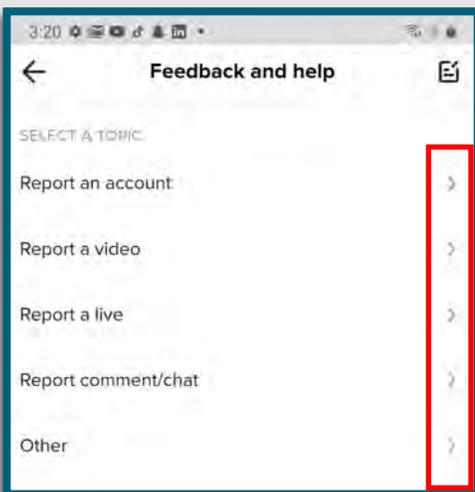
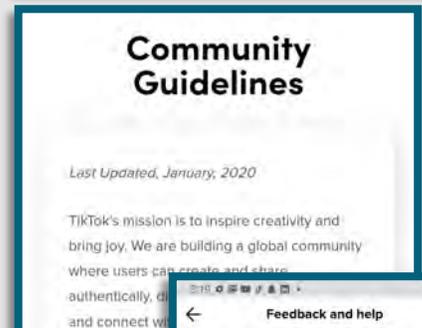
Also, check out the “Anti-Bullying” information, which explains what steps you can take to make sure you (or your child) are not receiving unwanted community interactions, as well as what you can do if you find yourself in a bullying situation.

Next, if you are a parent, do check out the “For Parents” link, which offers more explanation about what Tik Tok is meant to be and how to keep your child safe on Tik Tok. For instance, this section explains that Tik Tok is for children 13 years and older, but that in the U.S. children under 13 may register for a “Child Account”, which restricts posting and interactions on the platform. “Family pairing” and “Account Privacy” options are further explained as tools to help keep teens safe on Tik Tok. We recommend you visit the link and employ all recommendations suggested to keep you and your family safe.



## Report a Problem

Tik Tok has “Community Guidelines” that outline the types of behavior it considers counter to its values. Content that violates these guidelines can be reported, removed, and reported to legal authorities. You can access the “Community Guidelines” via the “Safety Center” on Tik Tok. But if you see content you think should be reported, you can do the following: under “Settings and privacy”, select “Report a problem”, then scroll to the bottom of the “Feedback and help” page that appears, and select “Abuse Report”. Select “How to report” and follow the rest of the prompts.



By changing all the safety settings for TikTok to “Friends” you are protecting your account from just anyone finding, commenting or contacting you or your child.

# TikTok SMART CARD



## Indicators of Possible Account Compromise:

Your TikTok account may have been hacked, if you experience following suspicious behavior:

- Change of your password, security email and associated phone number.
- Change of your username or nickname.
- Deleting / Posting videos without your permission.
- Sending messages you did not write.

If you suspect your account has been compromised, please follow the steps below to keep your account secure:

**Change Password:** In TikTok, a hacker will be automatically kicked out of your account after changing the password.

Check account information to determine if it is accurate: Select “Manage My Account” option under the TikTok settings, check if the associated account information is accurate. If you cannot change password by yourself, please contact TikTok via their In-app Feedback (App settings – Report a Problem). You may follow the steps shown below to change the password and verify account information.

- Tap on “...” for ‘Privacy & Settings’
- Go to ‘Manage My Account’
- Select password to change and other account information to verify

If you need to report **Spam/Fake Accounts/Harassment:** Go to <https://support.tiktok.com/en>

If your account was hacked: <https://www.tiktok.com/safety/resources/hacked-account?lang=en&appLaunch=web> and reach out to TikTok and notify them of your hacked account at <https://www.tiktok.com/about/contact?lang=en>

Also, if you find any bullying or inappropriate behavior TikTok has information at site <https://www.tiktok.com/safety/resources/anti-bully?lang=en&appLaunch=web>

If you cannot log in to your email account, Twitter has provided links to each email accounts “having trouble signing in” page for your convenience. <https://help.twitter.com/en/managing-your-account/cant-access-my-accounts-email-address>

### Important Message from TikTok:

If you have a public profile, anyone signed into TikTok can view your public videos. However, only approved followers can send you a message. Whether you choose to have a public or a private account, you can always: block another from contacting you at any time; save a video privately so content will not be viewable by any other user; filter comments; “manage” your duets.

### Tips to keep your account safe:

1. Never trust 3rd-party websites that promise to give away free likes, fans, crowns, coins, or other incentives as they may be able to take your login info.
2. Select a secure password that contains at least one number and one special character.



Make sure your options for “Who can download my video” are set to “Nobody”. Otherwise other users can download and share your videos. #lockitdown

# LOCKING DOWN



## Personal Computer (PC) Version

### Do's and Don'ts

- ◆ Do monitor the videos that your children are watching, even if they are in "Restricted Mode."
- ◆ Do use Two-Factor Authentication to protect all your information. Enable this function via your Google Account.
- ◆ Do set all your videos to "Unlisted" or "Private" so that you maintain full control over who can see them.
- ◆ Do **not** allow your children to post "Public" videos to their YouTube account. Posting public videos allows "subscribers" (strangers) to follow your children on YouTube.
- ◆ Do **not** ignore the "Comments" and feedback on your published videos. Review them to make sure they don't reveal any personal information about you.

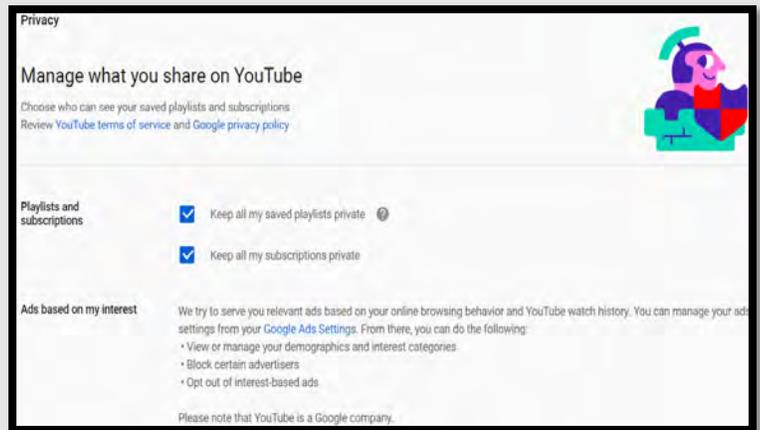
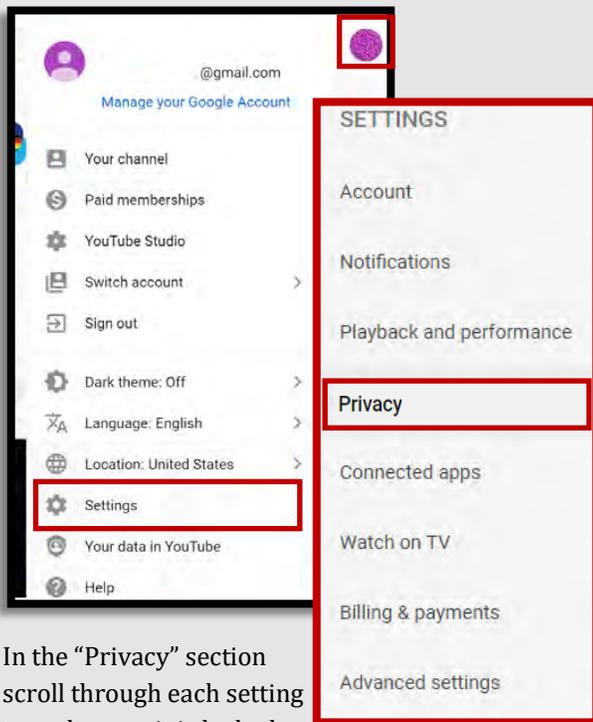
YouTube is a video sharing service with which users can create their own profile, upload videos, watch, react to, and comment on other videos. Created in 2005, YouTube is now one of the most popular sites on the Internet.

\*\* This SmartCard provides guidance on how to secure your YouTube account on personal computer (PC) and mobile devices, both iPhone and Android. PC instructions are followed by mobile device instructions below.

YouTube looks like it refreshes after that last step, but you'll still see the same content as you did before if you don't refresh your screen. #themoreyouknow

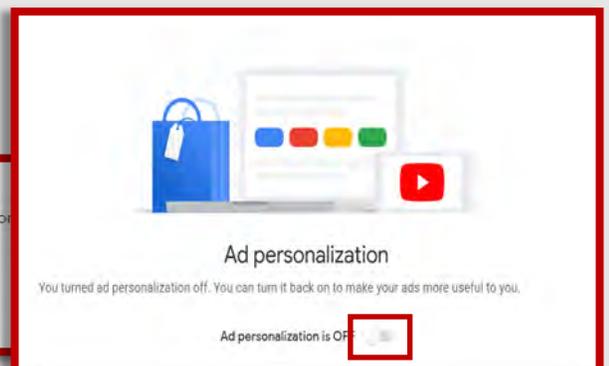
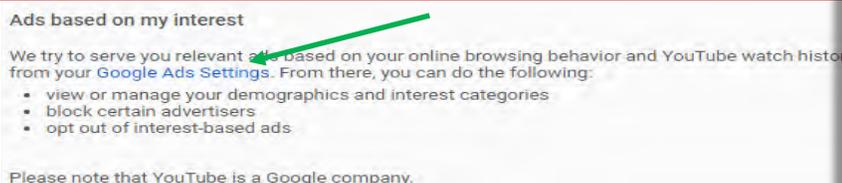
### Privacy Settings

Your "YouTube Account" (if you have one) is connected to your "Google Account", meaning your Google email and password are used to sign into YouTube. To set your security and privacy settings on YouTube, let's begin with "Settings". Look to the top right of your screen and select your "Google Profile" picture (see left). From the dropdown menu, select "Settings", and the "Settings" menu will appear. Select "Privacy".



In the "Privacy" section scroll through each setting to make sure it is locked

down. We recommend you keep all sections in "Manage what you share on YouTube" private, set the toggles to "On" or "Check" the boxes. In the section "Ads based on my interest", we recommend turning this feature off, as in order for it to function it must collect data from you. Disable the "Google Ads Settings" by selecting "Google Ads Settings", then set the toggle to "Off" as seen below.



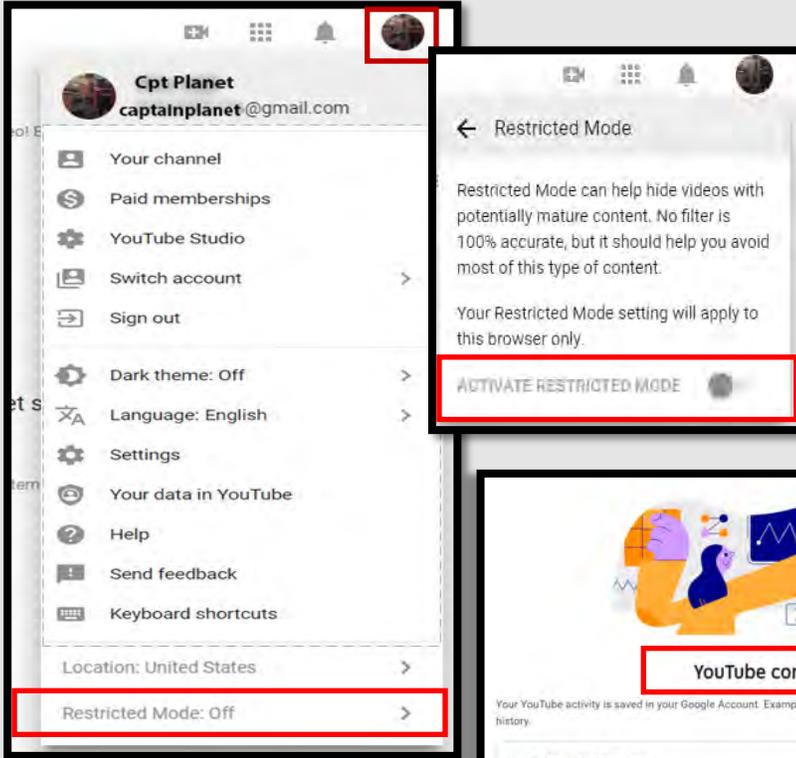
# LOCKING DOWN



## Personal Computer (PC) Version

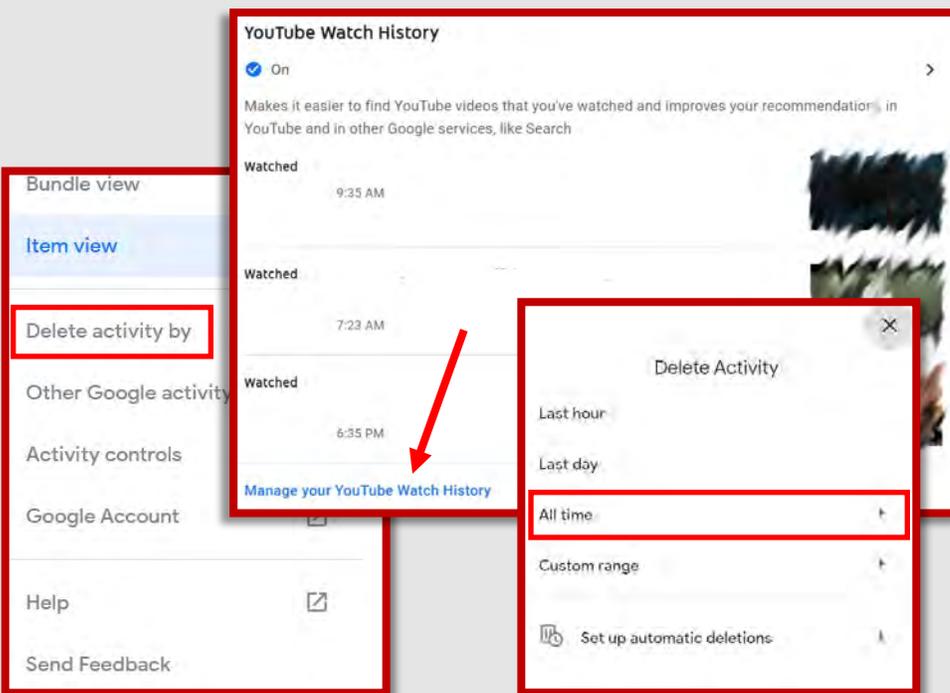
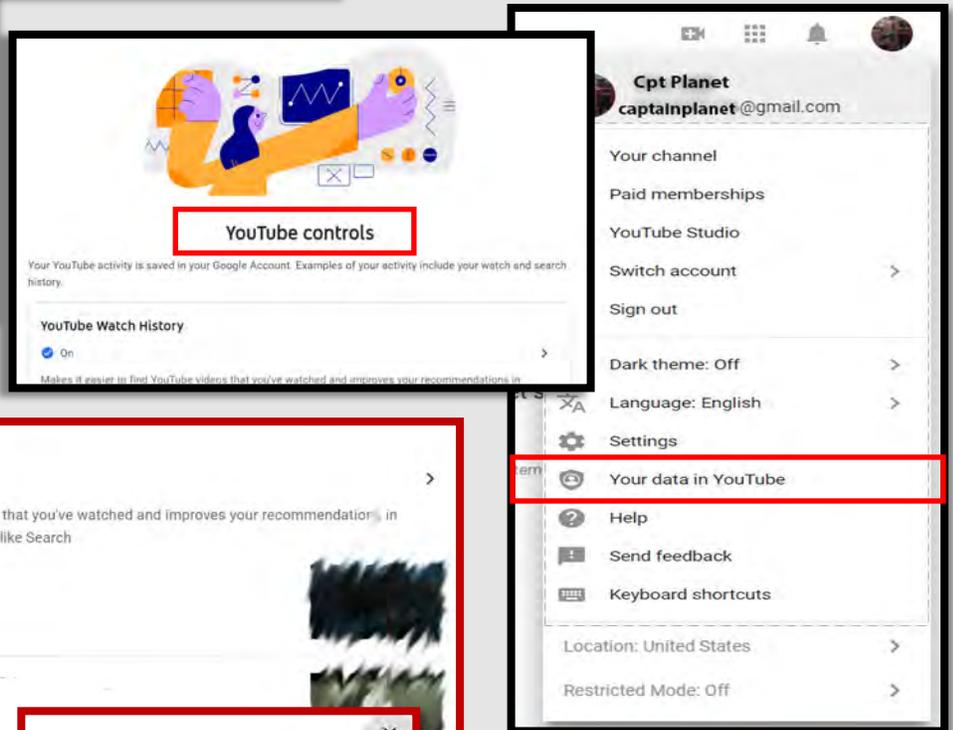
### Restrict Mature Content

Parents, are you concerned with what your children are watching on YouTube? "Restricted Mode" can help you ensure they are not being presented mature content. To enable this feature, select your "Google Profile" icon again. On the dropdown, you will need to scroll to the very bottom, select "Restricted Mode", set the toggle to "On".



### Delete History

Another important feature located at the bottom of your "Account Menu" (from your "Google Profile" icon) is the "Your data in YouTube" tab. Just as it is important to clear your browser history on your search engines, it is important to manage and clear your history on your YouTube account. Select "Your data in YouTube". On the next page, scroll down to "YouTube Controls", select "Manage your YouTube Watch History". (see below, green arrow)



From "Manage your YouTube Watch History" a new page will load (see left). Look to the left of your screen to see a menu of available options to manage and delete your history. We recommend you select "Delete activity by", then select "All time", which will delete your entire history. You can also set up automatic deletions and YouTube will delete your history according to the schedule you designate.

Set up automatic deletions to have YouTube delete your watch and search histories automatically, or delete manually. #themoreyouknow

# LOCKING DOWN

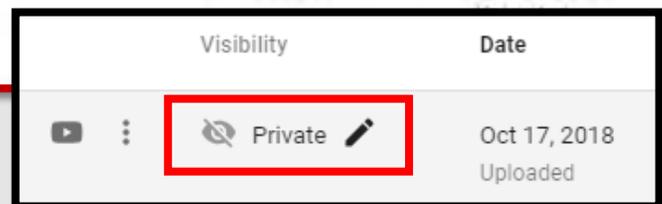
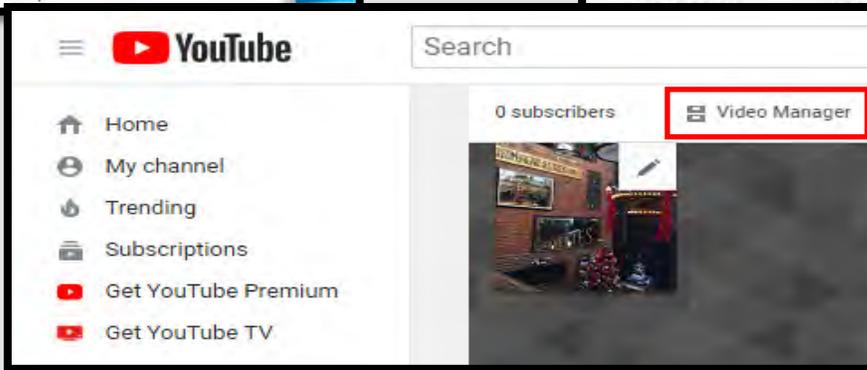
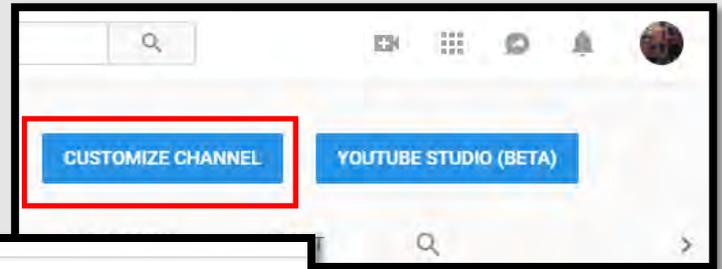
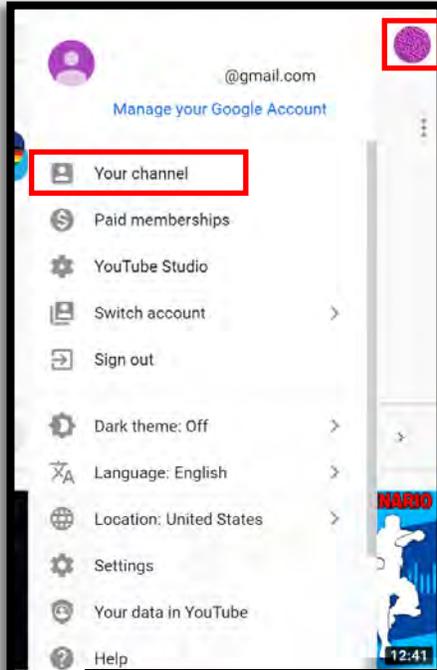


## Personal Computer (PC) Version

### Who can see your videos?

One of the main uses for YouTube is of course uploading and watching videos. In order to upload your videos and create privacy settings you must first locate your "Video Manager." Select the "Google Profile" icon, and on the dropdown menu select "Your Channel." Then press the blue "Customize Channel" button. Next, select "Video Manager" at the upper middle part of the page. Here you will be able to upload and edit videos. In order to edit the "Visibility" of a video, or who can see the video, simply hover over the "Visibility" column next to the video and select the "Down Arrow" or the "Edit" icon. From the popup menu that appears, you can choose "Private", "Unlisted", or "Public" - we recommend you select "Unlisted".

Restricted Mode doesn't catch everything, and it's easy to disable. It is important to check on your children and even teenagers while they are using YouTube.



The "Unlisted" privacy setting on YouTube means that your video is only visible to viewers who have a link to the video. "Private" means only you can view the video. And "Public" means anyone can search for the video and view it, react to it, and comment on it. Once a video is uploaded to YouTube and made "Public" there is no real way to pull back the video - it can be shared, liked, and commented on, and you lose control of it.

# LOCKING DOWN

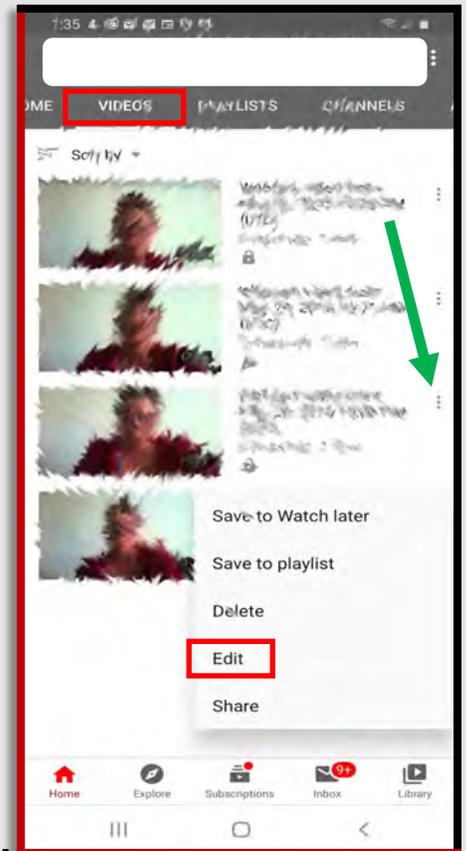
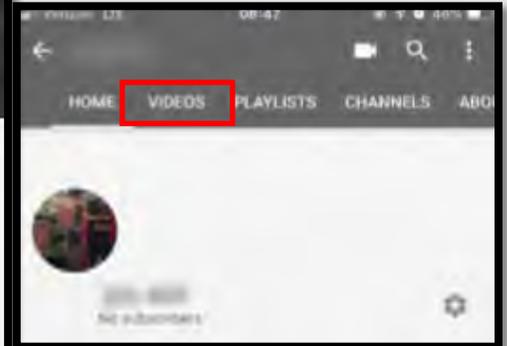
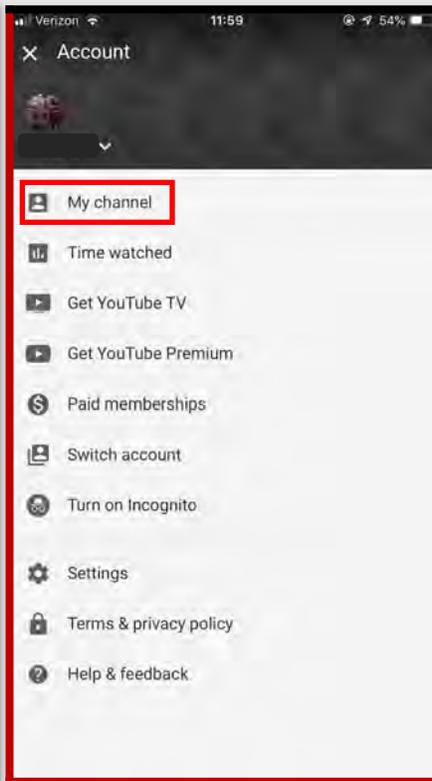


## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **black** and Android **red**.**

## Who can see your videos?

Unlike any other social networks, YouTube doesn't require you to create an account before you or your child can search for content or view videos.



In order to access uploaded videos and change their privacy settings via your smart devices, follow these steps.. From the “YouTube App”, select your “Google Profile” picture / icon, then select “My Channel.” Next head to the top menu and select “Videos” to take you to the video upload and settings section. The videos you have uploaded appear here, and you can edit them from this page by selecting the three ellipses to the right of each video, then select “Edit”, and then select “Privacy” and choose your privacy setting - we recommend “Private” or “Unlisted”.

The “Unlisted” privacy setting on YouTube means that your video is only visible to viewers who have a link to the video. “Private” means only you can view the video. And “Public” means anyone can search for the video and view it, react to it, and comment on it. Once a video is uploaded to YouTube and made “Public” there is no real way to pull back the video - it can be shared, liked, and commented on, and you lose control of it.

FYI - YouTube allows users to be in “Incognito Mode”. Simply select the “Turn on Incognito” from your “Google Profile Settings” menu (see above).

# LOCKING DOWN

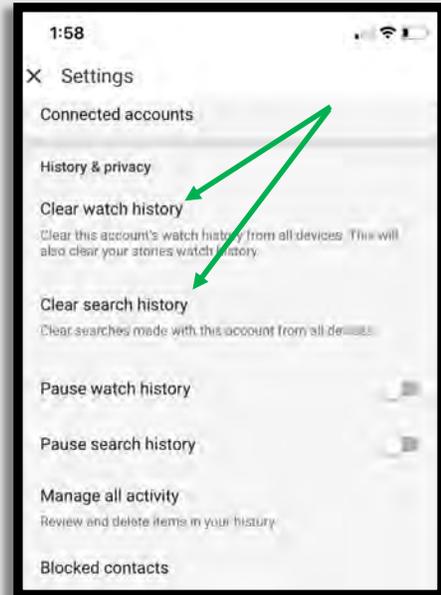
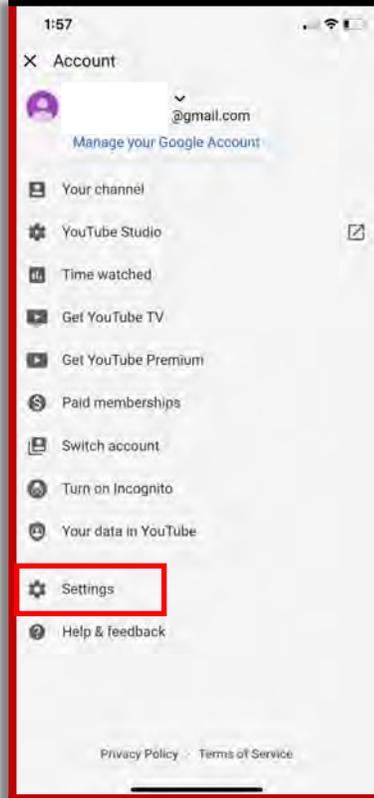
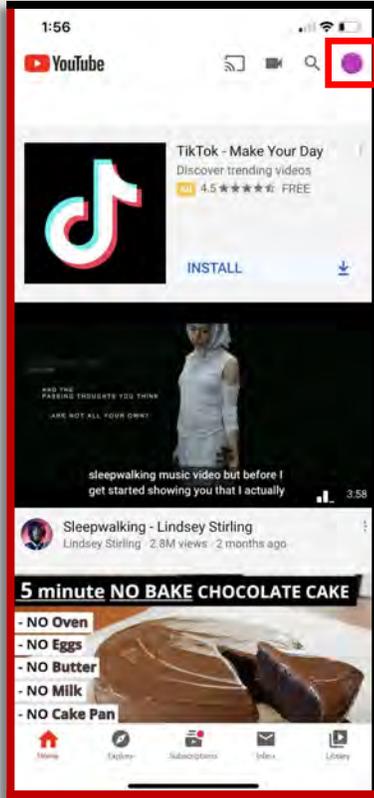


## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **black** and Android **red**.**

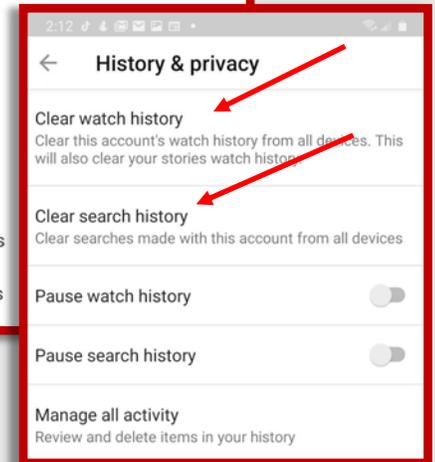
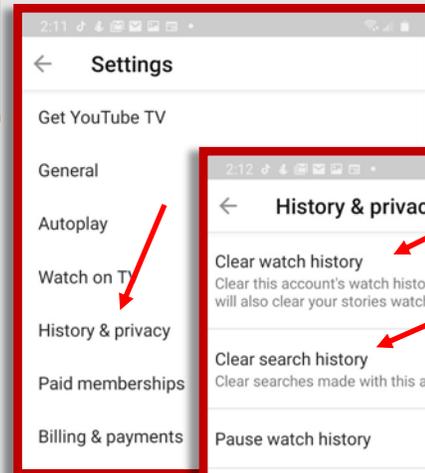
Your phone is your ultimate endpoint. You likely carry it everywhere and it holds your most sensitive information. Make sure to check for updates quarterly. #Staysafeonline

## Clear History

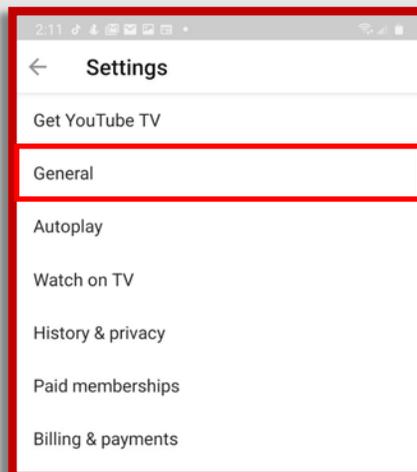
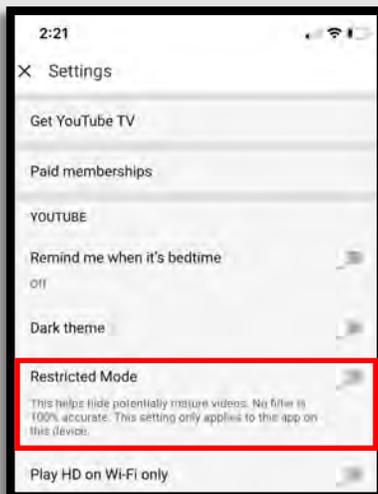


**On iPhone** (images outlined black): select your “Google Profile” icon, then select “Settings”, scroll down to “History & Privacy”. Follow prompts for “Clear watch history” and “Clear search history”.

**On Android** (images outlined red): select your “Google Profile” icon, then select “Settings”, then “History & privacy”. Follow the prompts to “Clear watch history” and “Clear search history”.



## Restrict Mature Content



**On iPhone:** go back to “Settings”, then set the “Restricted Mode” toggle to “On”

**On Android:** under “Settings”, select “General”, scroll down to “Restricted Mode” and set the toggle to “On”.

Remember this is a good idea if you have children that use your YouTube account.

# LINKEDIN SMART CARD

## Personal Computer (PC) Version

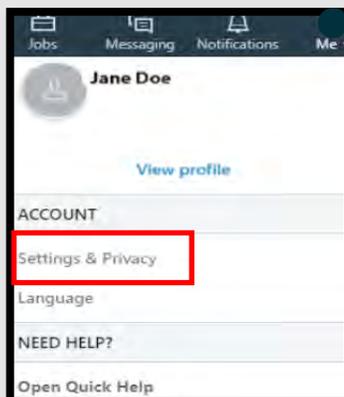


### Do's and Don'ts

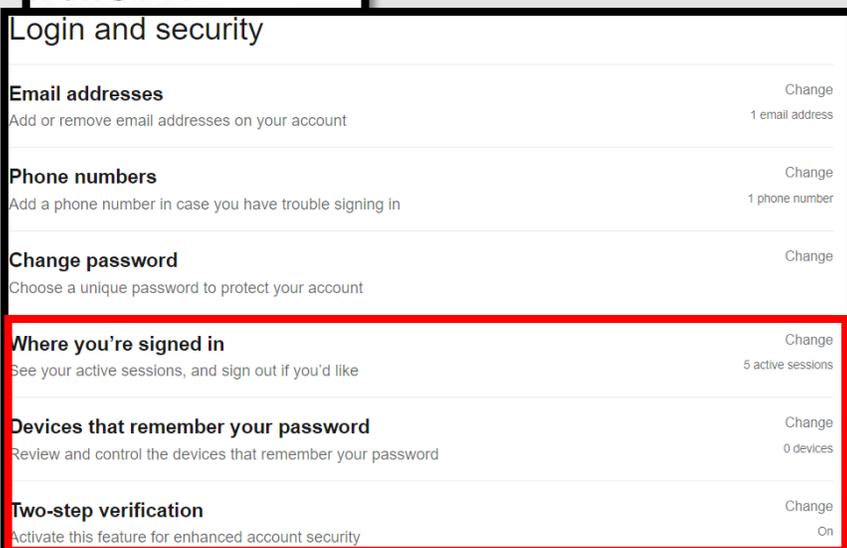
- **Do not** use an email account that is associated with your banking, finances, or other important contacts. Instead, consider creating an email account specific to this site.
- **Do not** establish connections with people you do not know and trust, not everyone is who they say they are.
- **Do not** register, log in, or link third party sites (e.g. Facebook, Twitter, etc.) using your LinkedIn account. Third party sites may aggregate and misuse your personal information and data.
- **Do** review your connections often to ensure that ensure they are current and that you are not providing your information to individuals who no longer need it.
- **Do** consider your profile picture. Posting a profile picture is optional, and we recommend that if you decide to post a picture, you dress in professional business attire.
- **Do** ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.

LinkedIn is the largest professional network on the Internet. It is used to find the right job, connect and strengthen professional networks, and learn professional skills. But a lot of sensitive personal information is uploaded to this site. See how to protect yours using the guidance below.

### Location and Two-Factor Authentication



The privacy settings for LinkedIn can be found in the “Me” section on the top right corner of the website (shown above). From the drop down menu, select “Settings & Privacy” (highlighted in red to the left). A new screen will appear with a header like the one shown below. The first section we are going to review is the “Account” settings.



First, on the “Login and Security” menu, see the “Where you’re signed in” section. In this section you can review any “Active” session you have on your account and where each session is located. If you see an active session or location that does not look familiar, we recommend you close it and change your password. Next, at the bottom of the “Login and Security” section, see the “Two-step verification” feature. This is a powerful security feature we recommend you enable. You will be asked to add your phone number, and then each time you log into your LinkedIn account, you will receive a text message with a code that you will enter upon login, kind of as a second password. This feature will protect you if your password is compromised in a security breach, and otherwise adds an additional layer of security to your account.

Sign out of your accounts after you use a publicly shared computer or your home computer. #stophackers #keepyouraccounts safe

# LINKEDIN SMART CARD



## Personal Computer (PC) Version

### Account Information

Account	Privacy	Ads	Communications
---------	---------	-----	----------------

#### Site preferences

---

**LinkedIn language**  
Select the language you use on LinkedIn Change

---

**Content language**  
Select a language for translation Change

---

**Autoplay videos**  
Choose if you want videos to autoplay on your browser Change

---

**Showing profile photos** ← Change  
Choose whether to show or hide profile photos of other members Only you

---

**Feed preferences**  
Make your feed your own Change

---

**Name, location, and industry** ← Change  
Choose how your name and other profile fields appear to other members

Next, under “Account” scroll down to the “Site Preferences” section. Here it is recommended that you make sure to review and update the “Showing profile photos” and “Name, location, and industry” sections to ensure each are locked down to your specifications. It is recommended here that you lock both down to “Connects” or “Only Me.” You can also check your “Feed Preferences” here to make sure you aren’t following or have inadvertently allowed someone to follow you that you aren’t familiar with or do not trust.

#### Subscriptions and payments

---

**Try Premium for Free** Change  
Unlock the power of LinkedIn

---

**View purchase history** ← Change  
See your previous purchases and transactions on LinkedIn

---

#### Partners and services

---

**Microsoft** Change  
View Microsoft accounts you’ve connected to your LinkedIn account 0 connected accounts

---

**Permitted Services** Change  
View services you’ve authorized and manage data sharing 0 connected apps

---

**Twitter settings** Change  
Manage your Twitter info and activity on your LinkedIn account Not connected

Next, if you continue scrolling in the “Account” section you will come to your “Subscriptions and payments” and “Partners and services” sections. It is important to review this section for a few reasons. First, you should know where the “View purchase history” section is just in case you find unknown LinkedIn purchases on your credit card — you can quickly review the accuracy of the purchases here. Second, under “Partners and services” you can confirm that you have not linked your LinkedIn account with any other service such as Microsoft or Twitter.

Manage your account information and privacy settings from your Settings & Privacy page. Remember to update update update! #privacymatters.

# LINKEDIN SMART CARD

## Personal Computer (PC) Version



Account **Privacy** Ads Communications

### How others see your profile and network information

<b>Edit your public profile</b> Choose how your profile appears to non-logged in members via search engines or permitted services	Change
<b>Who can see your email address</b> Choose who can see your email address on your profile	Change Only you
<b>Who can see your connections</b> Choose who can see your list of connections	Change Connections
<b>Viewers of this profile also viewed</b> Choose whether or not this feature appears when people view your profile	Change No
<b>Who can see your last name</b> Choose how you want your name to appear	Change Full
<b>Representing your organization and interests</b> Choose if we mention you with content about your employers or other content you publicly expressed an interest in	Change No
<b>Profile visibility off LinkedIn</b> Choose how your profile appears via partners' and other permitted services	Change No
<b>Microsoft Word</b> Choose whether work experience descriptions from your LinkedIn profile can be shown in Resume Assistant, a feature within Microsoft Word.	Change No

Next, go to the menu at the top of the “Settings & Privacy” section and select “Privacy” (shown above in red). Choose the “Edit your public profile” link in order to change the visibility of the LinkedIn profile so that search engines will not display the profile when the account name is searched. The purpose is to ensure you do **not** have a public profile.

### Edit Visibility

You control your profile's appearance for viewers who are not logged-in members. Limits you set here affect how your profile appears on search engines, profile badges, and permitted services like Outlook.

[Learn more](#)

Your profile's public visibility Off

The “How others see your LinkedIn activity” settings can be seen on the left of the page. In this section, you can change the “Profile viewing options,” which informs other LinkedIn users if you have reviewed their profile (as seen to the right). To remain anonymous when viewing other profiles select the “Private Mode”, button.

### Profile viewing options

Choose whether you're visible or viewing in private mode

Select what others see when you've viewed their profile

Your name and headline

IT Advisory  
Philadelphia, Pennsylvania | Information Technology and Services

Private profile characteristics

Information Technology Generalist in the Information Technology and Services Industry from Greater Philadelphia Area

Private mode

Anonymous LinkedIn Member

Note: Selecting this option will disable **Profile Stats**. Whenever you switch to anonymous, your viewer history gets erased.

### How others see your LinkedIn activity

<b>Profile viewing options</b> Choose whether you're visible or viewing in private mode	Change Characteristics
<b>Story viewing options</b> Choose whether you're visible or viewing in private mode	Change
<b>Manage active status</b> Choose who can see when you are on LinkedIn	Change
<b>Share job changes, education changes, and work anniversaries from profile</b> Choose whether your network is notified	Change No
<b>Notifying connections when you're in the news</b> Choose whether we notify people in your network that you've been mentioned in an article or blog post	Change No
<b>Mentions or tags by others</b> Choose whether other members can mention or tag you	Change No

As you scroll down in the “Privacy” section, notice a section called “Mentions by others”. This function controls whether or not other members can tag you in a post or photo. We recommend you turn this function off by toggling the switch to “No”. If working with an already established profile, page four of the LinkedIn card will explain how to find and remove older “Mentions”.

### How LinkedIn uses your data

<b>Manage your data and activity</b> Review the data that you've provided, and make changes if you'd like	Change
<b>Getting a copy of your data</b> See your options for accessing a copy of your account, data, connections, and more	Change
<b>Manage who can discover your profile from your email address</b> Choose who can discover your profile if they are not connected to you but have your email address	Change Full
<b>Manage who can discover your profile from your phone number</b> Choose who can discover your profile if they have your phone number	Change Full
<b>Sync contacts</b> Manage or sync contacts to connect with people you know directly from your address book	Change
<b>Sync calendar</b> Manage or sync calendar to get timely updates about who you'll be meeting with	Change
<b>Salary data on LinkedIn</b> See and delete your salary data	Change
<b>Search history</b> Clear all previous searches performed on LinkedIn	Change
<b>Personal demographic information</b> Choose what details you provide about your personal demographics	Change
<b>Social, economic and workplace research</b> Choose whether we can make some of your data available to trusted services for policy and academic research	Change

### Blocking and hiding

Followers Change  
Choose who can follow you and see your public updates

Finally, at the bottom of the “Privacy” section under “Blocking and hiding,” you can turn off the ability of others to “Follow” you, especially those not in your “Connections.” From the drop down menu, change “Everyone on LinkedIn” to “Your Connections”.

Be sure to verify accounts and users that are trying to connect with you on LinkedIn. If a company or user profile looks too empty it may be a fake account.

# LINKEDIN SMART CARD

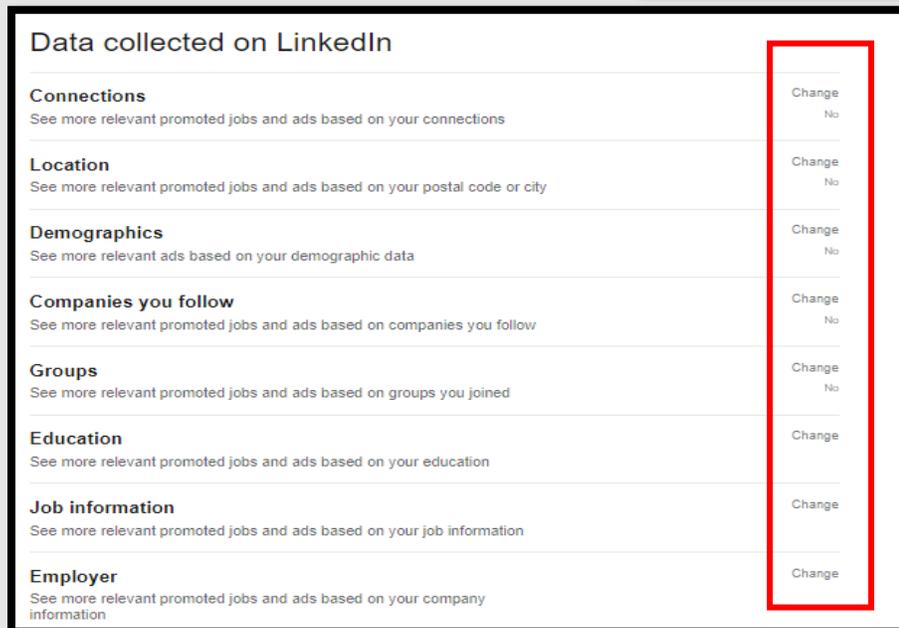
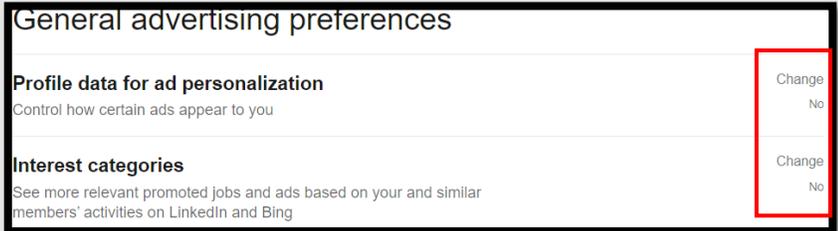


## Personal Computer (PC) Version

### Advertising

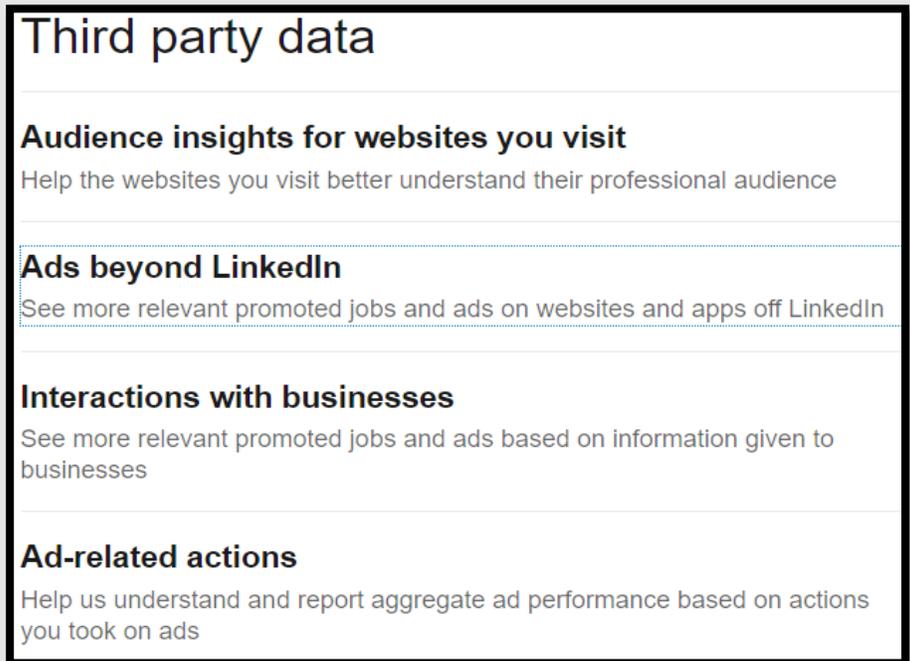


Next let's consider how LinkedIn uses your data to support its advertising. Select "Ads" from the top of the "Settings and Privacy" menu. It is recommended you limit the amount of information that LinkedIn is allowed to share with other third party apps as much as possible. Under "General advertising preferences" we recommend setting both options to "No" (see right).



Under the "Data collected on LinkedIn" settings, you will find our recommendations pictured to the left. Sharing this kind of information with LinkedIn will leave you vulnerable even if your account is otherwise locked down. Because LinkedIn shares your information with third parties, we recommend you disable all the functions in this section. If you choose to enable any of them, we recommend you read all available information regarding how your data is used, including the "Learn more" options within these features. It is important you understand what LinkedIn does with your data. And again, we recommend disabling all these options.

To the right you will find "Third party data" options that will help to eliminate unwanted ads, marketers collecting your information, and even spam in your emails! Simply review each section and begin controlling your data today.



FYI - If you are a LinkedIn member but logged out of your account on a browser, LinkedIn may still continue to log your interaction with their services on that browser for up to 30 days. LinkedIn does this in order to generate usage analytics for their services, and they may share in aggregate form with their advertising customers.<sup>1</sup> #manageyourdata

Reference: 1. <https://www.linkedin.com/legal/cookie-policy>

Even LinkedIn recommends not putting your email address, home address, or phone number in your profile summary. #staysafeonline

# LINKEDIN SMART CARD

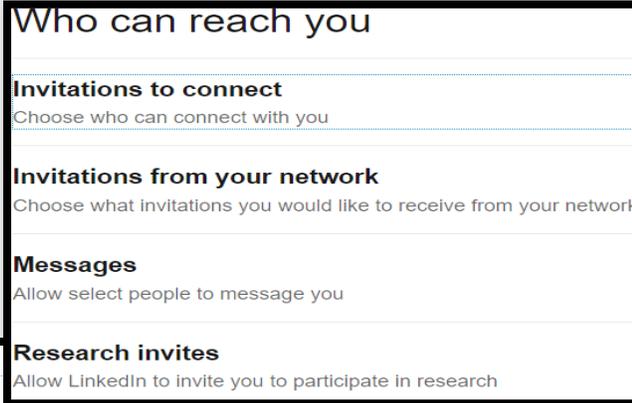


## Personal Computer (PC) Version

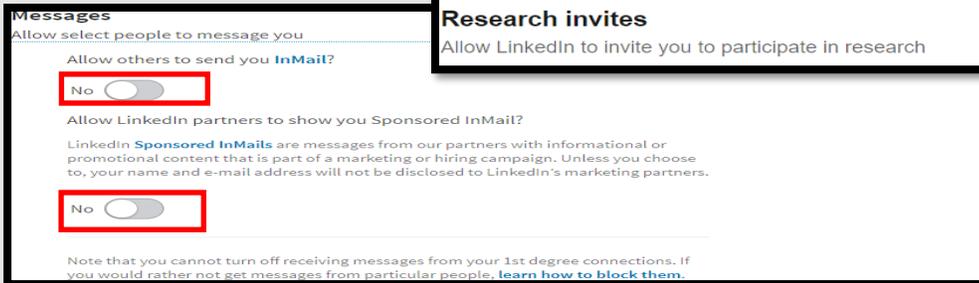
### Who can communicate with you?



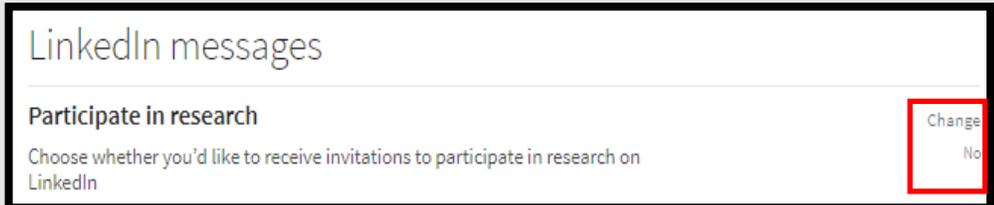
Finally, let's look at "Communications", which manages notifications, who can communicate with you, and messaging. Under "Communications" it is important to review each of the options under "Who can reach you" because here is where you decide who can attempt to "Connect" with you.



When reviewing your "Communications" on LinkedIn, it is important to consider why you are using LinkedIn...what are your main objectives? Are you hoping to find a job? Are you trying to connect with certain people or certain types of people? Consider your intent for using LinkedIn, and use this guide to lock down as much information as you can while still achieving the benefits you seek. Once you have achieved your goals using LinkedIn (for instance, you have found a great job), we recommend you go back and lock down the rest of your information.

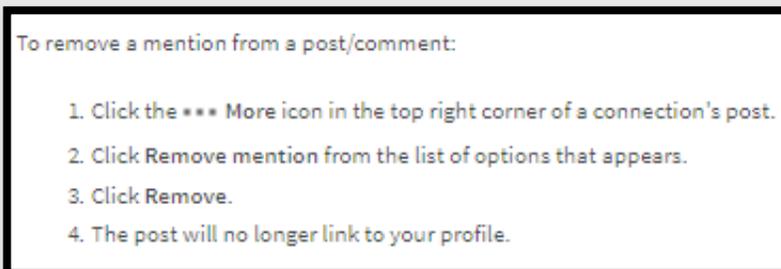


To review (and when ready, lock down) these settings, select the "Communications" tab at the top of the "Settings and Privacy" section. Review each setting to determine what best suits your desired purpose for using LinkedIn. Recommended settings are highlighted in red above.



Under the "LinkedIn message" section of the "Communications" tab – we recommend you choose not to "Participate in research" that LinkedIn conducts. "Participating in research events" could mean giving information about yourself that you wouldn't otherwise provide to third parties.

### Mentions



If you happen to be "Mentioned" in a post on LinkedIn, you can easily remove yourself from the tag following a few steps as noted above. It is important to manage "Mentions" because they link you to people, places, things, and ideas, thereby offering valuable information about you to people you may not have authorized - it is your "Connects" who give you "Mentions", and you cannot control their security settings.



#PHISHINGALERT: Messages containing bad spelling, grammar, and that aren't addressed to you personally, or asking you to act immediately, are major red flags.

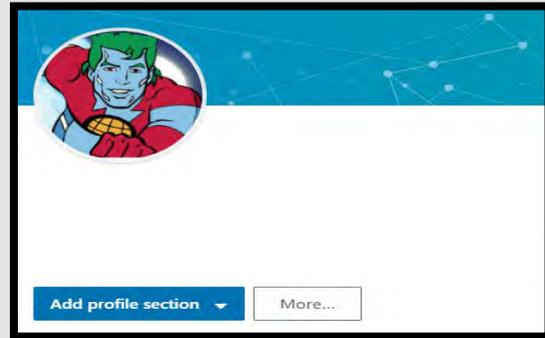
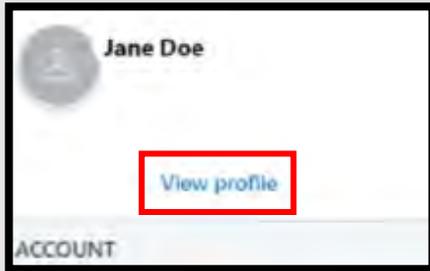
# LINKEDIN SMART CARD



## Personal Computer (PC) Version

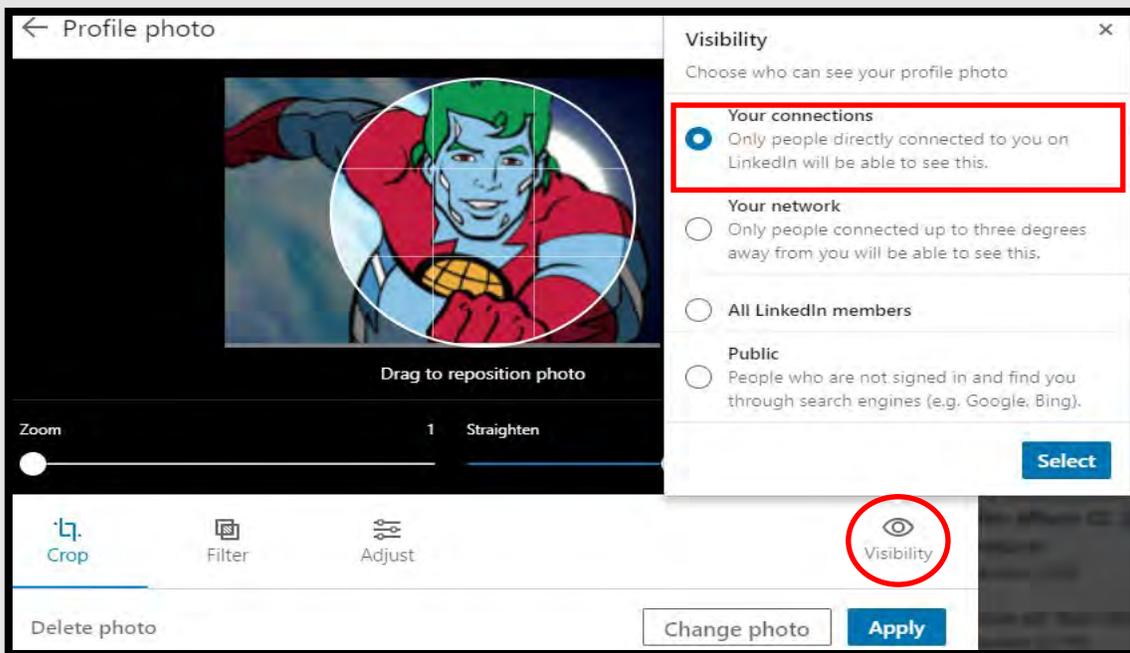
### Profile Picture

In addition to the “Security and Privacy” settings, it is important to look at your LinkedIn “Profile” and consider what kinds of information it is divulging about you. We recommend keeping profile data as general as possible, while still allowing it to serve your purposes for the account.



We recommend that you do **not** use photos of yourself for your profile or header photo. These are viewable to the public and so present an unnecessary vulnerability. If you decide to upload a profile picture, ensure that it is visible only to your “Connections”. Try to hide any obvious identifying marks that could make you more easily identified on another website or in person.

To add a picture to your profile, simply select the “View Profile” link in the “Me” dropdown on the top of your screen. Once there, select the “Picture” icon, then navigate to and upload your preferred picture. When complete, look down at the bottom of the window (shown below in the red circle) and select “Visibility”. Here you can decide who on LinkedIn is able to view your profile photo - we recommend “Your connections.”



Stop. Think. Act - If anyone (a “Connection” or not) sends you a message with an attachment, will you open it? Does your action depend on whether or not you know and trust the sender? Even if someone you know sends you an attachment, it is a good idea to verify with that person over the phone or face-to-face that they are the sender before opening it. You may not know immediately if you’ve been hacked, and by the time you find out, it could be too late.

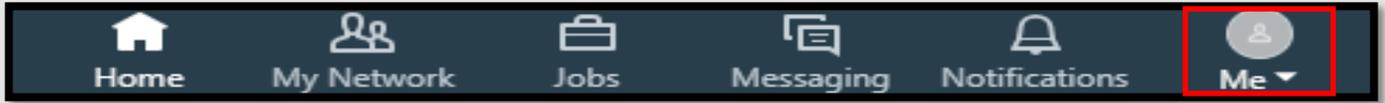
Private mode with a basic LinkedIn account will not allow you to see other users who have viewed your profile. #knowwhatyoudon'tknow

# LINKEDIN SMART CARD



## Personal Computer (PC) Version

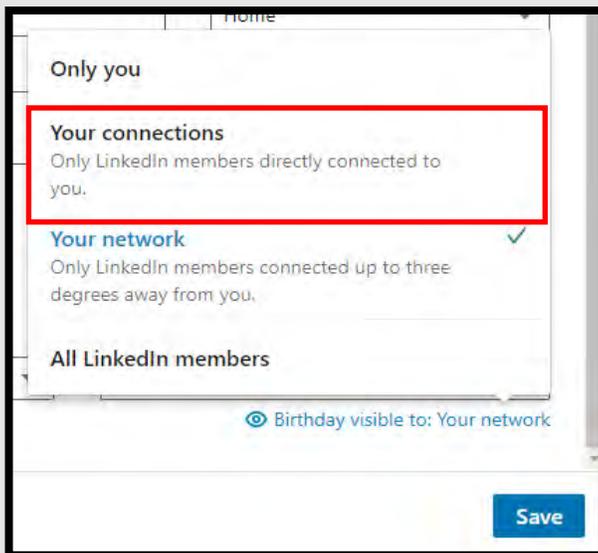
### Date of Birth & Contact Info



To further protect your information you will need to check whether your “Date of Birth” is displayed on your profile page. In order to do this, click the “Me” tab at the top right of the page (usually with your picture in it), then select the “View Profile” link. This will take you to your “Profile” page.



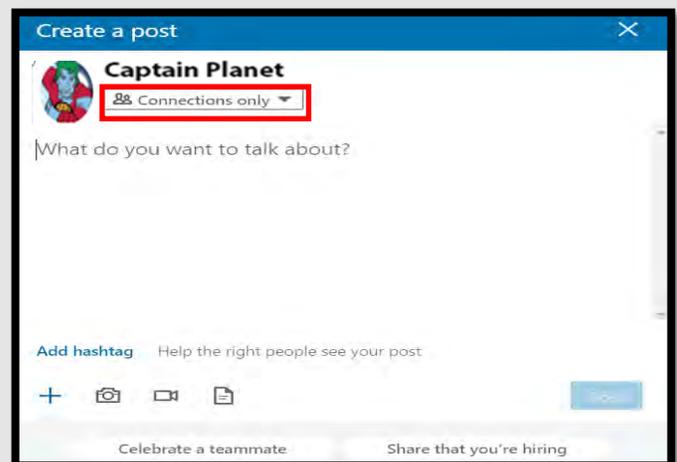
On your “Profile” page, locate the “Contact Info” function, as shown above. Select the “Edit” or “Pencil” icon located to the upper right of the window. From there review the information shown and edit as necessary. Keep in mind that this is information that appears on your profile for others to see.



Ensure the information listed in the “Profile” section is not displaying identifiable information to the public. We recommend you do **not** add a phone number, birthdate, or address in this section, and they are not required.

If it is important to you to display your birthdate, ensure that it is only visible to “Your Connections”. Do this by selecting the “Birthday visible to” link at the bottom of the screen (shown here to the left highlighted in **red**). Ensure that “Only you” or “Your Connections” is selected. Select the “Save” button before you exit out of this screen to keep selected settings.

### Creating and Managing Posts



If you decide to create a post on LinkedIn, be sure to set the privacy settings of the posts containing personal information so those posts do not appear to the public. As shown in the box to the right, posts made “Public” on LinkedIn can be viewed by anyone.

In order to change the privacy settings for your post, simply locate the “Post Settings” drop down menu located on the post itself (highlighted right in **red**). From there select the appropriate audience for your post, we recommend “Connections only”.

https://www.linkedin.com/help/linkedin will provide you with additional and continuously up to date information on how LinkedIn is changing.

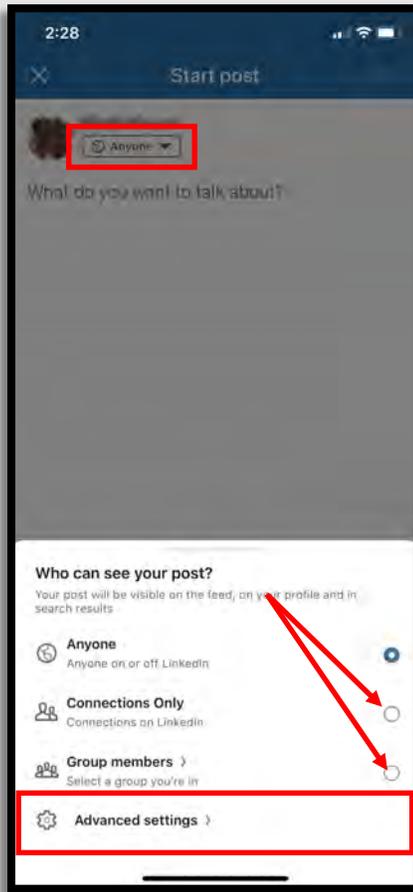
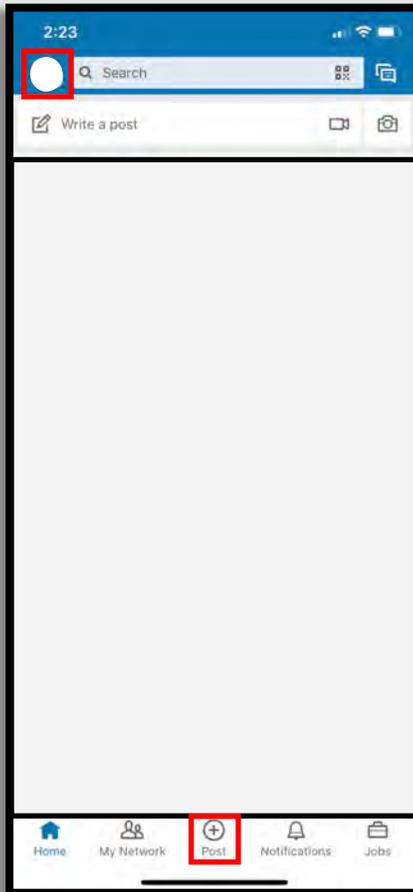
# LINKEDIN SMART CARD



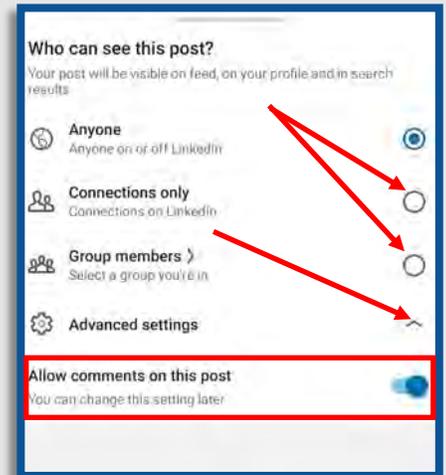
## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **black** and Android **blue**.**

**On iPhone:** Select “Create Post” at the bottom center of the screen, then under your name select “Anyone”, or the default. From the pop-up menu, select who you want to be able to see your post - we recommend “Connections only” or “Group members”. You can also select “Advanced Settings” to “Disable comments on the post”.



**On Android:** the process of locking down who can see your posts on Android is the same as on iPhone, except the “Advanced Settings”. When you select “Advanced Settings”, you will set the toggle to “Off” in order to disable comments for your post. (see below)



## Helpful Extra Hints

### iOS/Android

To access your “**Privacy Settings**” page from your mobile device simply follow these steps:

1. Tap your “Profile” picture.
2. Tap the “Settings” function located under your name.
3. Navigate through the four tabs to adjust settings for “Account”, “Privacy”, “Ads”, or “Communications”.

### In order to **delete a post from your feed** from your browser (**PC Version**):

1. Locate the post you want to delete in your LinkedIn homepage feed.
2. Click the “More” icon in the top right corner of the post. ...
3. Click “Delete Post” from the dropdown.
4. Click “Delete” to confirm.

### iOS/Android

To **delete a post** from your feed:

1. Locate the post you want to delete in your LinkedIn homepage feed.
2. Tap the “More” icon in the top right corner of the post.
3. Tap “Delete Post”.
4. Tap “Delete” to confirm.

To strengthen your password, try substituting numbers for letters that look similar. For example, substitute "0" for "o" or "3" for "E". #updateyourpassword

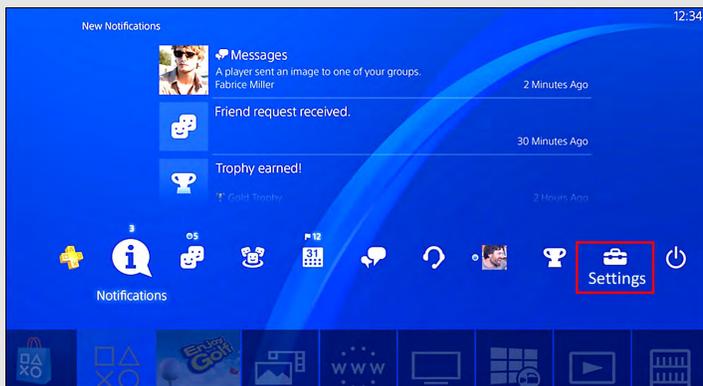
# PLAYSTATION SMART CARD



## Do's and Don'ts

- ◆ **Do** use caution when sharing Gameplay when messages, video, audio, and personal data may be available to other users participating in your game experience.
- ◆ **Do** select “Friends Only” for all available settings options. Ensure family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.
- ◆ **Do** use parental controls to restrict access to questionable content and features for children using the PS4.
- ◆ **Do** refer to privacy policies / user agreements of individual games and third party applications to see if they use the PS4 camera, and to understand other privacy information.
- ◆ **Don't** forget to update your PS4 system to the latest version of the system software.
- ◆ **Don't** use pictures of yourself for your profile photos. Instead, use avatars or photos of something else. Profile photos are potentially viewable to other users and the public depending on your privacy settings.
- ◆ **Don't** discard or transfer ownership of your PlayStation without using “Initialization”. Initialization sets your PS4 back to factory mode and erases the system data.
- ◆ **Don't** establish connections with individuals you do not know and trust. Understand that not everyone is who they say they are.

PlayStation allows you to manage a host of settings in order to take ownership of your system security and privacy, and determine what information other users can see. You must first access the “Settings” button from the “Dashboard Menu”, highlighted below in red. From there, go to “Account Management”.



**Two-Factor Authentication:** To enhance the security of your PlayStation, we recommend you set up two-factor verification. Follow the detailed steps below, along with the graphical depiction of the steps on page two. From the “Account Management” screen, select “Account Information”. Click on “Security”. Next go to “2-Step Verification”. Select “Set Up Now”. Enter the phone number you want to set up to your account. A code will be sent to your mobile device. Verify your identity by entering the code sent to your mobile phone. This verifies you entered your phone number correctly. “Activate” the two-factor authentication. This adds an extra step to your basic log-in procedure, but can significantly help protect your system from being compromised later.



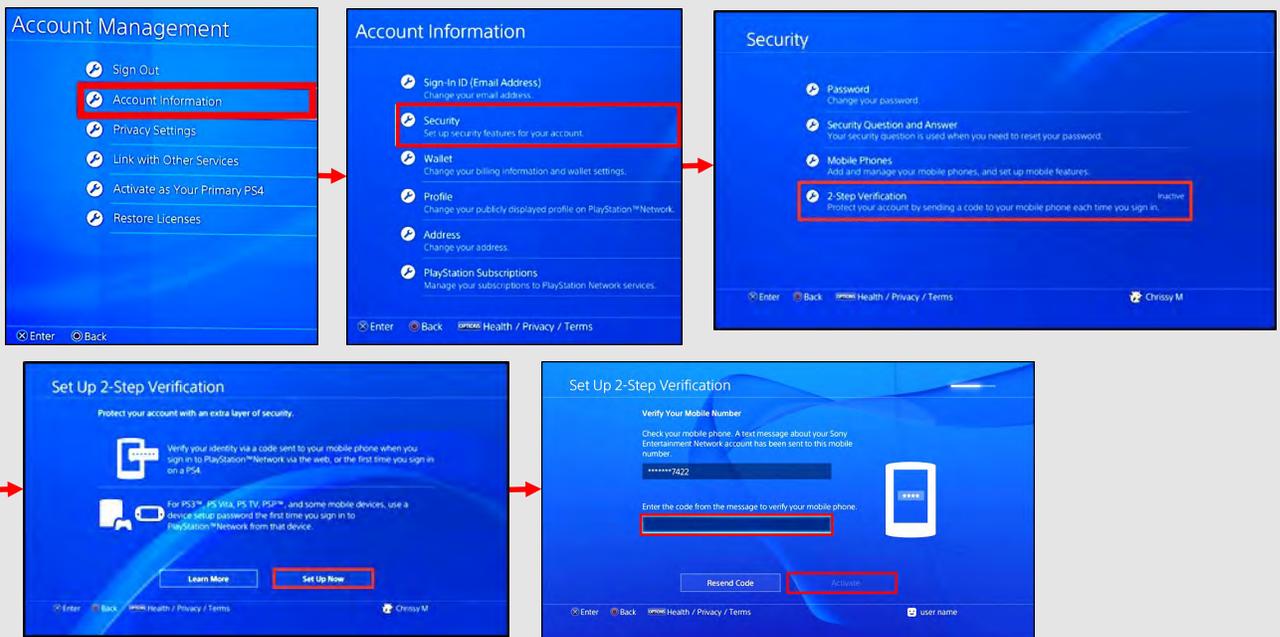
PlayStation's two-factor authentication is an added layer of security to ensure only authorized individuals have access to the system, accounts, and privacy information.

# PLAYSTATION SMART CARD



It is good to understand PlayStation's privacy policies; however, users grant third party applications access to privacy information and these apps that have their own privacy policies.

## 2-Step Verification Graphics



## Privacy Settings

Next, let's take a look at privacy settings. From the "Account Management" screen, select "Privacy Settings" as seen on the right highlighted in red. The "Gaming | Media" subcategory allows you to determine which activities are viewable by others. The "Friends | Connections" subcategory allows you to decide which status of individuals (e.g. friends, followers, etc) can view established connections. The "Personal Info | Messaging" subcategory allows you to choose who can see your real name and who can communicate with you. View the picture on the bottom right to see the privacy setting subcategories.

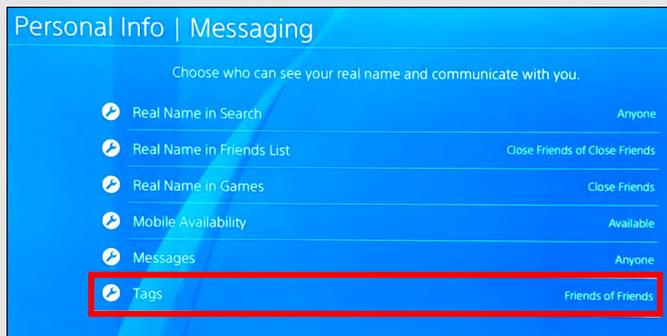
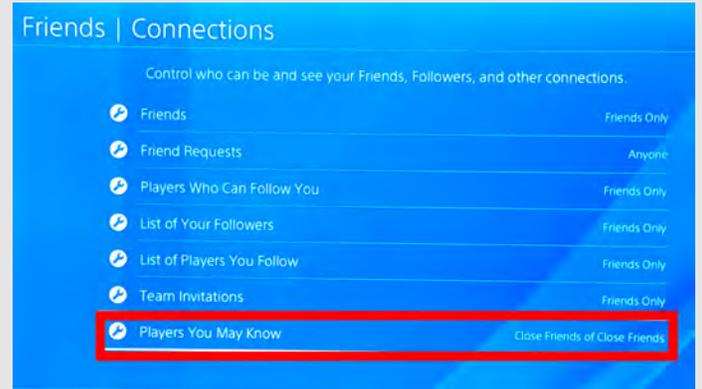


# PLAYSTATION SMART CARD

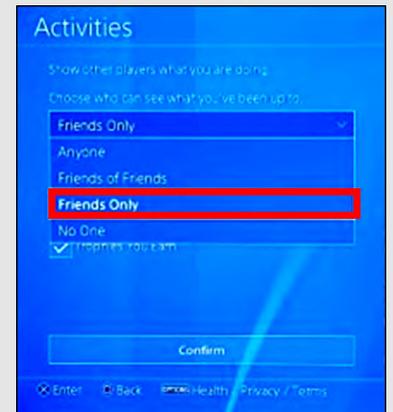


## Privacy Setting Recommendations

We recommend that you set your privacy settings to “Friends Only” for most sections, in order to prevent the general public from seeing information pertaining to the user. See “Recommended Privacy Settings” on the privacy settings graphics for “Gaming | Media”, “Friends | Connections”, and the “Personal Info | Messaging” subcategories. We recommend the primary user and family members be mindful of who they become friends with and connect to on the system. It is important to remember not everyone on your family and friends “Friends List,” should be trusted. Parents, it is important to know not all users have good intentions, and are accurately portraying themselves online. For this reason, we recommend that you review your child’s “friends” periodically. Other users on the system may utilize gaming systems to connect with potential victims or use social engineering against other users. If you do not know someone, we recommend you **not** add them to your “Friends List”.



After going through “Gaming | Media”, the “Activities” box shows different setting options you can choose from for privacy. We recommend that you select the “Friends Only” option as shown here in the example picture on the right, highlighted in red.



## Parental Controls

PlayStation allows you to manage numerous parental control settings with the ability to limit playing time, restrict user account creation, set maturity levels for games, and change systems passcodes. To get to “Parental Controls/Family Management” settings, select the “Settings” tab on the front “Dashboard Menu” and scroll down to “Parental Controls”. The subcategories are “PS4 System Restrictions” and “Family Management”.



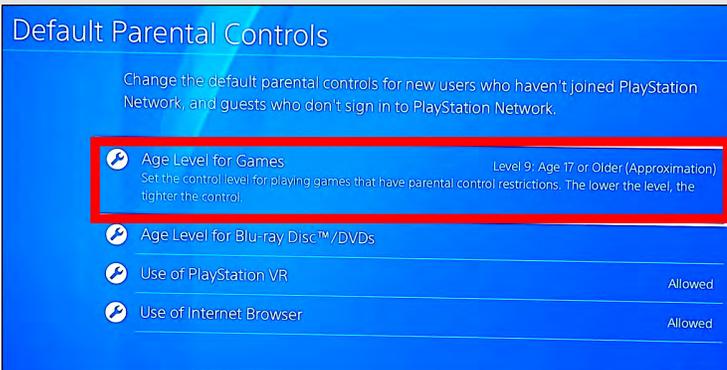
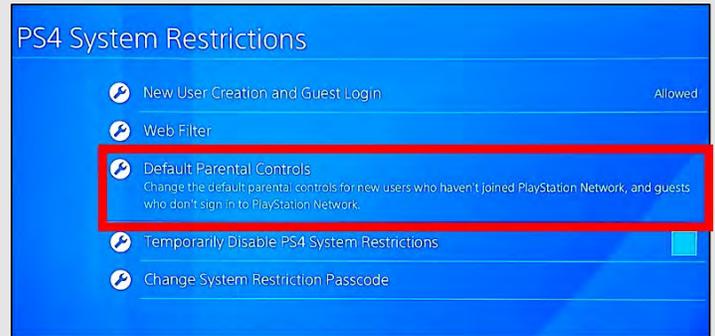
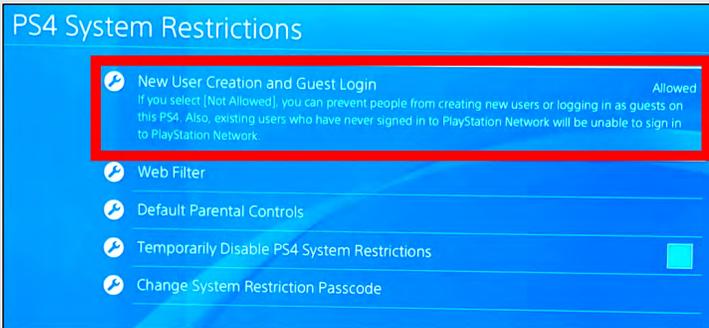
PlayStation provides a login feature that utilizes facial recognition technology. The photos and derived data are stored on the system but are not shared with third parties.

# PLAYSTATION SMART CARD



From the “PS4 System Restrictions” section, you can select “New User Creation and Guest Login” to restrict who can log into the PlayStation and whether guests can access the system. From the “PS4 System Restrictions” section, you can click “Default Parental Controls” for the purpose of setting age and maturity restrictions for your users. See the graphics below highlighted in red for the pathways of these features within the settings. Parents are recommended to implement the various system restrictions and the age appropriate parental controls.

Parental controls are a means to protect children from online predators and prevent children from accessing content that is not appropriate for their age levels.

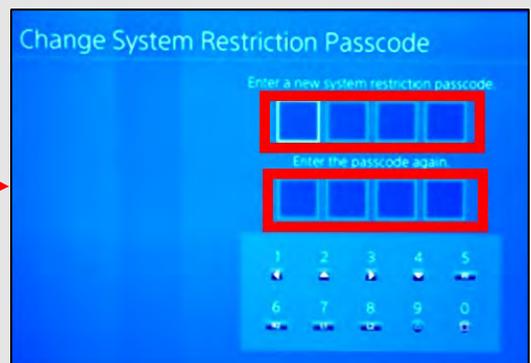
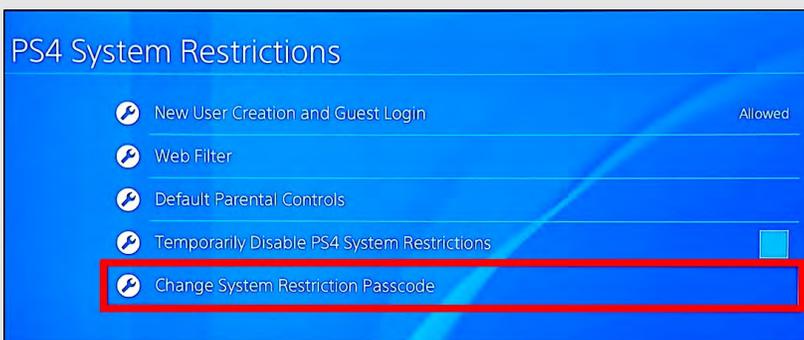


See below for the approximate user ages that match up to the parental control levels available in the user settings.

Parental control level	1	2	3	4	5	6	7	8	9
Approximate age of user	0	3	6	10	12	-	15	17	18
North America/Central America and South America*1									
					*2				*3

## Passcode

The PlayStation Passcode is defaulted to “0000”. We recommend you change the system passcode to enhance the security of your device. To change the passcode, go to the “PS4 System Restrictions” section, and select “Change System Restriction Passcode” as illustrated in the bottom left graphic below, highlighted in red. Next, type in a new system restriction passcode. Verify the passcode by entering it twice.



# PLAYSTATION SMART CARD



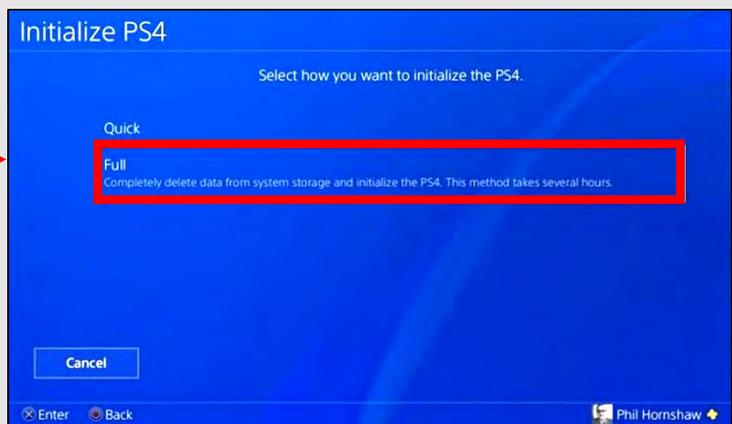
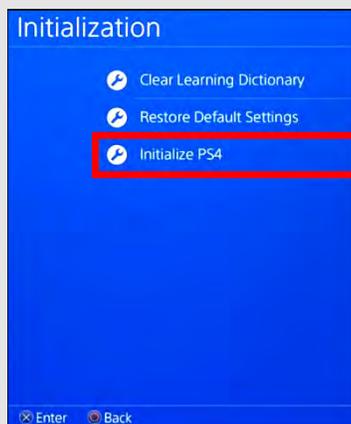
## Family Management

Go to the “Parental Controls/Family Management” section. On the PS4, select “Family Management” (as seen on the right, highlighted in red) and click “Set Up Now” (as seen below, highlighted in red). Within the “Family Management” area, parents can identify all the family members that will use the PlayStation system, manage play time limits, and set restrictions for children. A parent, guardian, or family manager can set the parental controls.



## Initialization

Next, we recommend you use the “Initialization” feature whenever you are discarding or transferring the PlayStation system to another person. Initialization of your PS4 system restores system settings to default values. It deletes data saved on system storage and deletes all users and their data from the system. When you initialize the system software, all settings and information saved on your PS4 system are deleted. This cannot be undone, so make sure you do not delete any important data by mistake. Deleted data cannot be restored. Initialization helps ensure the removal of your privacy information after you are done with the system. In order to “Initialize” the PS4, first go to “Settings”, then “Initialization” as seen to the right, highlighted in red. Next, select “Initialize PS4” as illustrated on the bottom left, highlighted in red. Finally, click “Full”, as depicted on the bottom right graphic, highlighted in red. Selecting “Full” completely initializes the system. If the “Quick” feature is selected, the system will not be completely restored to a default system - some data will still remain on the PS4. Be sure you are doing a “Full” initialization.



Users should never discard systems or devices that still have personal information retained on the device. When possible, always return the device back to factory settings.

# PLAYSTATION SMART CARD



## Potential System Compromise:

**Do you think your account may have been compromised or hacked? Have you noticed any of the following:**

- \* Unexpected charges from financial institutions tied to your PlayStation accounts.
- \* Primary email and password have been changed without your authorization.
- \* Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.).
- \* Primary console changed to another device without your consent.
- \* Receive a special character in a private message, immediately followed by the system crashing or frequent glitches.

If you said "Yes" to any of the above, you are recommended to take the following actions:

- ◆ Change your password immediately and use strong/complex passwords.
- ◆ Enable two-factor verification.
- ◆ Notify the financial institutions about fraudulent purchases resulting from the hack.
- ◆ Set your "Messages" privacy setting to "Private" and adjust other privacy settings as well.
- ◆ Restrict who has access to create new accounts and logins.
- ◆ Contact PlayStation Support or the Sony Customer Service line immediately.

If you need to report **Spam/Fake Accounts/Harassment**: Contact the PlayStation Support Site at 1-800-345-7669 or the Sony Customer Service Line.

Also, you can report that your account has been hacked by going to <https://support.playstation.com>.

If you have additional questions about responding to system compromise, contact <https://twitter.com/AskPlayStation/>.



**Important Message on PlayStation:** you are responsible for all activities on your PlayStation Network, so it's very important you do your best to ensure you are the only person using it.

The PlayStation System is an entertainment system that enables users to enjoy multiplayer online gaming, stream live TV, provides a social and messaging network for friends to connect, allows for video streaming services such as Netflix, Amazon Video, Hulu, YouTube, HBO Now, NBA TV, and more. Each application has its own privacy concerns and is susceptible to being breached or hacked.

Contact US – PlayStation Customer Support Service | Contact PR | Jobs  
 Contact PlayStation customer support service for hardware, software and account management solutions.  
 Contact PR team for media inquiries. Contact HR for Job related queries.

[PlayStation Support Site](https://support.playstation.com)

Contact Phone: 1-800-345-7669



# Hidden Phone Apps



## What are Hidden Apps?

“Hidden” apps, “Vault” apps and “Ghost” apps, are apps that look innocuous, perhaps like a calculator, but are actually used to hide pictures, videos and messages on a smart device. Teens often use these apps because they want to hide their activity from their parents. Most times, these apps require a password to be entered in order to gain entry into the hidden area of the app. Some Vault apps go a step further and if the password is entered incorrectly, a picture of the individual attempting to gain access will be taken.

### Android Hidden Apps (some examples)

	<b>1 Gallery Vault</b> - hide pictures & videos, strong encryption
	<b>LockMyPix</b> - hide photos, videos, AES encryption
	<b>Vaulty</b> - hide pictures and videos
	<b>Keepsafe Photo Vault</b> - hide private photos and videos
	<b>Vault</b> - ide pics and video

### iPhone Hidden Apps (some examples)

	<b>Fake Calculator App</b> - hide photos and videos (many versions)
	<b>Private Photo Vault</b> - picture safe
	<b>Secret Calculator Fake Vault</b>
	<b>Keepsafe Photo Vault</b> - hide private photos and videos
	<b>Secret Vault Hide Photos</b> - private picture safe

## Do's and Don'ts

- ◆ **Do** periodically check your child's smart devices to make sure they have not downloaded anything you have not approved.
- ◆ **Do** think about using a monitoring service (as discussed in the Keeping Children Safe Online Smart card) for your child/teens smart devices, especially if you have given them the ability to download apps themselves.
- ◆ **Do** talk to your teens about the dangers of taking and sending nude photos or videos on their smart devices and make sure they understand the serious consequences.
- ◆ Do **not** give your child/teen the password or authorization to download apps in their respective “App Store”. Having them ask you for the password allows you to re-view any app they might want to put on their device.
- ◆ Do **not** allow your child to use “Messaging Apps” that instantly delete the content they hold. Allowing such apps will take away from your ability to help your kids navigate through smart device social norms.
- ◆ Do **not** allow children to set private passwords without sharing them with you. Always ensure that you can access your child/teen's phone at any time.

# Hidden Phone Apps



## How to find “Hidden Apps”

- ◆ One of the easiest ways to search for hidden apps on a smart device is to visit the devices respective App store (Apple or Google Play Store).
  - ◆ **Android device-** In the “Google Play Store” select “Menu” (3 vertical lines in the “Search” box), then select “My apps & games.” Next, select the “Installed” tab in the middle of your screen. Here you can review all the apps that have been downloaded to the device. Additionally, from your “Account” (under the same “Menu”) you can review “Purchase History” which will provide you an overview of all purchased apps.
  - ◆ **iPhone device-** In the “App Store” find and select the “Account” icon, or “Profile Picture” at the top right of your screen. Then select “Purchased” and the account you want to review purchases from (if you have an “Apple Family Sharing Plan”, more than one account will appear).
- ◆ Another way to review purchase history on a smart device is to find the “App Store” and search for “Hidden Apps.” Once a list of available apps appears on the screen, you can scroll through the list. If any “Hidden Apps” are downloaded on the device, it will be noted to the left side of the screen. This method may return inaccurate results due to some apps being miscategorized.

### Red Flag Indicators

- I. If your child seems to have more than one of any kind of app it may indicate that one of those apps is not what it appears to be. Redundancy in apps may indicate that one is a “Hidden App”.
- II. If your child seems to try and hide his / her screen any time you enter the room, it may indicate he / she is trying to hide his / her phone activity from you.

### How to Prevent Your Child from Downloading Hidden Apps

- ◆ **On iPhone:** iOS has an “Apple Family Sharing Plan” that allows parents to turn on a feature called “Ask to Buy”. When this feature is enabled, your child will not be able to download any apps without your approval.
- ◆ **On iPhone:** iOS has a built in feature that can be controlled through the “Settings” of your iPhone. Simply go in to your “Settings” section and find “Screen Time”. Select “Turn On Screen Time” > “Continue” > “This is My Child’s iPhone” > “Not Now” > “Not Now”. From there you can go in and set “Content & Privacy Restrictions” as well as a “Use Screen Time Passcode” to make sure that your settings are not changed by anyone who doesn’t have a password.
- ◆ **On Android:** Android users can setup parental controls in the “Google Play Store” by creating a PIN and choosing the maturity levels you want to allow. Go to the “Google Play Store” > “Menu” > “Settings” > under “User Controls”, you will find “Parental Controls”, and other settings you can review to control what your children download. It is also important to note that where many of the “Hidden Apps” are concerned, “Google Play Store” rates them “E” for everyone.
- ◆ **On Android:** Android users can also create a password for authentication to authorize purchases. This feature is located in the “User Control” section of your “Google Play Store” “Settings”.

You can limit the amount of time your child spends on his/her device unsupervised, by ensuring he/she puts it in the kitchen or living room before bed.

# Pay Apps



## Do's and Don'ts

- ◆ **Do** review all privacy settings, and set them in accordance with your personal preference and acceptable risk level. Some mobile pay apps have a social side to them which may display your payment activity if not locked down.
- ◆ **Do** make sure you have an anti-malware app on your phone to protect your phone, and the information on your phone from getting into the wrong hands.
- ◆ **Do** make sure to periodically check transactions made on mobile pay apps. Make sure they are accurately showing up on the payment device you have linked to the app.
- ◆ Do **not** visit online banking or online shopping websites by clicking on a link you have received in an email or from a text message. Doing so may lead to fictitious websites and possible identity theft.
- ◆ Do **not** use unsecured Wi-Fi or public Wi-Fi networks while using mobile pay apps or for any online banking purposes.
- ◆ Do **not** download mobile pay apps from unofficial sites. It is recommended for all apps, not just mobile pay apps, that you use official stores such as the Apple and Google Pay stores.

Even if you rely solely on mobile pay apps to make your purchases, it is important to have some other form of payment handy in case you are unable to access your phone.

### DEFINITION

Mobile wallets utilize technology you already own— your smartphone, for example — to allow you to make in-store payments quickly and securely without having to use your credit or debit card. The term “digital wallet” may refer to either an electronic device that stores payment information (such as a smartphone) and the program or app used to make the payment, such as Apple Pay, Google Wallet, Samsung Pay, or PayPal.

#### Risks

Using mobile pay apps means that losing your phone essentially becomes that equivalent of losing your wallet. Whoever finds your phone holds the keys to your identity.

Using pay apps via your smart device means having to be on the alert for cyber criminals.

Using mobile pay apps means you may run the risk of malware infecting your phone and gaining access to payment and identity information.

#### Gains

Unlike your wallet, if your cell phone is stolen or even misplaced, there are levels of security that will limit or even prevent anyone from accessing the contents of your smartphone. Additionally, the user usually has the ability to “wipe” (delete all personal information) their phone if they feel it has been compromised or simply cannot be found, unlike a physical wallet which becomes immediately compromised.

Using physical debit or credit cards means you run the risk of having your card copied upon scanning it if the machine being used has been tampered with.



*The privacy policy for each “Pay App” states what agreements a user consents to when signing up for the application. While each app has different information that is stored and/or shared, they all have a common theme. Many applications collect your name, date of birth, email address, telephone number, name of financial institution, financial account numbers, additional information from consumer reporting agencies, people you invite to use the application, the operating system on the device, etc. The company may be able to keep your information for an indefinite period of time, depending on what the privacy policy states.*

# Pay Apps



Use any available password protection for your smart device - two-factor authentication, phone log on password - to ensure the protection of your data.

App	Apple Pay	Venmo	Facebook Messenger	Cash	Zelle	Xoom	Google Pay
<b>Security</b>	High	Low-Medium	Medium-High	Medium-High	High	Medium-High	High
<b>International Pay Feature</b>	Yes, User must manually turn this feature on	No	Yes, limited	No	No	Yes	Yes
<b>Linked to Bank Account</b>	Transfer to Bank account	Yes, through third party app	Yes, only through debit card	Yes	Yes	Yes	Yes
<b>Linked to Debit Card</b>	Yes	Yes	Yes	Yes	Yes	Yes	Yes
<b>Linked to Credit Card</b>	Yes + Fee	Yes +Fee	No	Yes + Fee	No	Yes	Yes
<b>Paying on the Web</b>	Yes if accepted and while using an Apple device.	Yes, if accepted and while using a smart device where App is loaded.	Payments can only go to other FB friends.	No	No	No	Yes if accepted
<b>In Store Payments</b>	Yes	Limited acceptance at retailers.	No	No	No	No	Yes

	Apple Pay	Venmo	Facebook Messenger	Cash	Zelle	Xoom	Google Pay
<b>Pros</b>	Rated most secured payment app. Most widely accepted.	User friendly. owned by PayPal	Secure payment method. User friendly.	Easy to use and friends do not need the app to receive money. Can purchase and sell Bitcoin.	Works directly with your bank app.	Offers a money back guarantee, pay bills and reload mobile phones. Powered by PayPal.	Widely accepted, easy to use.
<b>Cons</b>	Transfers can only be made to other Apple device users.	Default privacy setting shares your payment history with the world. Requires recipients to install app. Customer Service	Limited use. No ability to stop a payment on your end once you send it (however, receiver can reject it).	Not widely accepted. Customer service limited to messaging in app, no call center.	If money is sent to the wrong person or user becomes a victim of fraud or scam, Zelle will not reimburse you.	There is a minimum payment for use. Requires Gov. issued ID as well as a proof of residents. They may also require a bank statement.	In order to use Pay to Pay (pay a friend etc.) you have to download the Google Pay Send App separately.

# DATING SITE BEST PRACTICES

**#DATESAFE**

## Do's and Don'ts

- ◆ **Do** protect your information and set limits on what and when you provide information to people you meet on dating sites.
- ◆ **Do** provide your own transportation when meeting an individual for the first few times
- ◆ **Do** use more popular dating apps and stay away from less popular sites, which may have less security in place.
- ◆ **Do not** use dating app sites on any public Wi-Fi. It is important to always make sure you are connected through a secure internet connection.
- ◆ **Do not** synch your social media accounts with your dating accounts.
- ◆ **Do not** forget to trust your "gut". If something doesn't feel or seem right it very likely isn't.

- \* **Be Anonymous - Don't include your last name or any other identifying information in your profile or initial communications. Likewise, we recommend you *not* include your contact information - email address, home address, phone number - on your profile**
- \* **Create a unique email address and Username for Dating Apps**
- \* **Keep your financial information private!**
- \* **Do *not* meet at your house or place of work**
- \* **Do *not* ask or allow a lot of personal questions initially. Save that for the date, this will help to prevent you from giving away too much information, too early.**
- \* **Do avoid drinking too much during your first several dates. Wait to loosen up until you get to know your date a little better.**
- \* **Try to do a search of your date on the internet before meeting up (see Self Assessment Smart-Card).**
- \* **Online dating scams are known to run as long as six months before you notice anything suspicious. Always be on the lookout for unusual conversations and behavior, such as your date requesting money or suddenly needing a ride somewhere.**

### *Things to watch out for:*

- ◆ An early request for photographs or videos
- ◆ A request for money or donations
- ◆ Minors using the platform!
- ◆ Users sending harassing or offensive messages
- ◆ Users behaving inappropriately after meeting in person
- ◆ Fraudulent profiles - if a profile looks incomplete or too good to be true, it probably is.



If someone immediately directs you to a different website from the one you are already on, you could be dealing with a scammer. #themoreyouknow

# DATING SITE BEST PRACTICES

## HOOKUP APPS: Tinder, Happn, HUD, Bumble

A hookup app is one that accepts and encourages casual sexual encounters or “hookups”, including one-night stands and other related activity, without promising or requiring emotional bonding or long-term commitments. These types of sites pose serious dangers to their members because they usually involve meeting up with strangers. A lot of trust is expected in such a situation, where no justification is provided.

If you choose to use a “hookup app”, it is important to let someone you trust know where you are going and with whom, whenever you decide to “meet up” with someone you don’t know well. These apps may not be intended to be used only for “hooking up” and can also be used to develop meaningful relationships. In reality however, that is not their primary function.

## CASUAL DATING SITES: Match, Zoosk, Plenty of Fish, OkCupid

Online dating services such as these allow users to become “members” by creating a profile and uploading personal information including (but not limited to) age, gender, sexual orientation, location, likes and dislikes. Most of these services offer digital messaging, as well as online chat, telephone chat (VOIP), and message boards. Members can constrain their interactions to the online space, or they can arrange a date to meet in person. These dating sites usually attract people looking for something a bit more long term than a “hookup”, and have more chance of leading to a relationship. In fact many of these sites allow you to declare your dating and commitment intentions.

These sites target specific demographics based on features like shared interests, location, religion, or relationship type. Most are completely free and depend on advertising for revenue. Others offer a free registration and use, with optional paid premium services.

## Larger Dating Apps: eHarmony, Christian Mingle, Farmers Only

Online dating services such as these tend to be more methodical in their matching of partners. They usually have a signature questionnaire that helps to match people based on compatibility of shared interests, and further, in terms of emotional and relationship values. These sites offer more nuanced compatibility ratings than the “hookup” and “casual dating” apps, and are targeted towards clients looking for longer term relationships.

These apps offer more services than the others. For instance, the app may guide you through the initial stages of your relationship by helping you to pace communication with your matches so that each of you remains comfortable, and things don’t move too quickly.

These sites usually require a form of payment and a membership for access to full content. Generally, these are sites people use when they are seeking a deeper connection and long term relationship or marriage.

**“Millions of Americans use dating sites, social networking sites, and chat rooms to meet people. And many forge successful relationships. But scammers also use these sites to meet potential victims. They create fake profiles to build online relationships, and eventually convince people to send money in the name of love. Some even make wedding plans before disappearing with the money.**

**An online love interest who asks for money is almost certainly a scam artist.”**

**-Federal Trade Commission**

# Fitness Apps



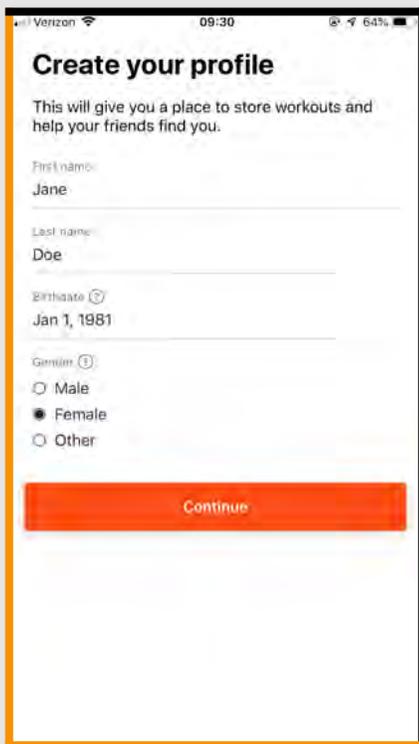
## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined orange and Android black.**

## Do's and Don'ts

- **Do** make sure that your profile is not set to “public”. Also, limit what information you put on your profile even if it is set to “private”.
- **Do** keep your fitness app *activity* set to “private” by default, so that your routes cannot be tracked online.
- **Do** ensure that family members take similar precautions with their accounts.
- **Do** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- Do **not** link your fitness app to any of your social media accounts. Doing so allows your routes and the times you exercise to be published to your social media accounts for others to see.
- Do **not** track exercises that begin at your own home, work place, or school.
- Do **not** chose the same route every time you go for a run or walk. It is important to mix it up so that any potential stalker won't be able to track your whereabouts.

Always go back and check the privacy settings in your fitness app after an update has taken place to ensure they remained intact.



## Strava Activity Tracker

Strava is a fitness tracker as well as a social network, its key feature is that its members can locate the most popular bike and running paths in their areas, follow their friends' routes, and log group exercises. For these key features to work, an optimal number if members must continuously be sharing location data. In other words, if you want to get the most out of Strava, you need to share your location data, but this comes with a big privacy trade-off.

Late last year Strava's heat map came under fire for posting its users' locations publicly online. If you leave your location data for people to see, you become vulnerable to victimization, for instance of physical attack, stalking, or theft of your belongings when you are away from your home. The following describes the best way to create an account on Strava, while maintaining the utmost privacy to ensure your safety.

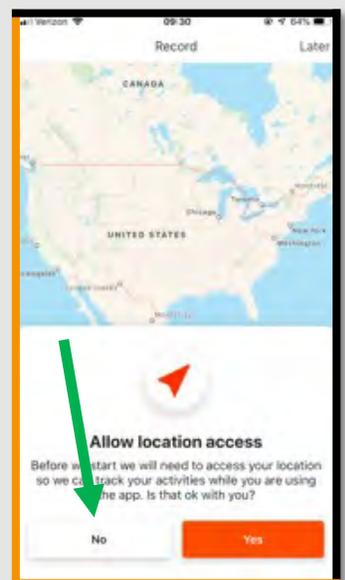
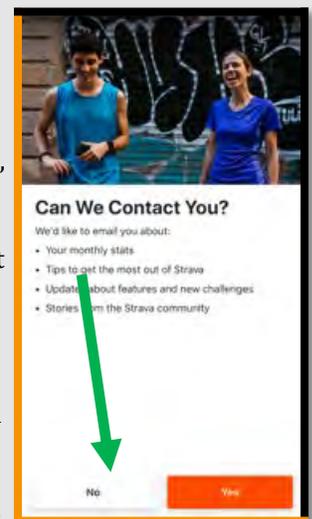
## Create Your Profile

Start by creating your account, only putting in the minimum personal information required to create your log on (shown here to the left). Later you will have the option to build upon your "Profile" by adding additional information about yourself, but we recommend keeping as little personal information on your profile as you can..

Next (shown on the top right), you are asked if you would like Strava to push monthly reports to your email. We recommend you decline this option because it is possible for Strava to then share additional information with you, or about you to others. Select the “No” option.

The next screen asks if you will allow Strava to access your location. Although this is a big part of the app, we strongly recommend you **not** allow Strava to have access to your location.

You will also be asked several times to synch your contacts to the Strava app during set up. We recommend, anytime you are asked, that you **not** synch your contacts to this app.



# Fitness Apps



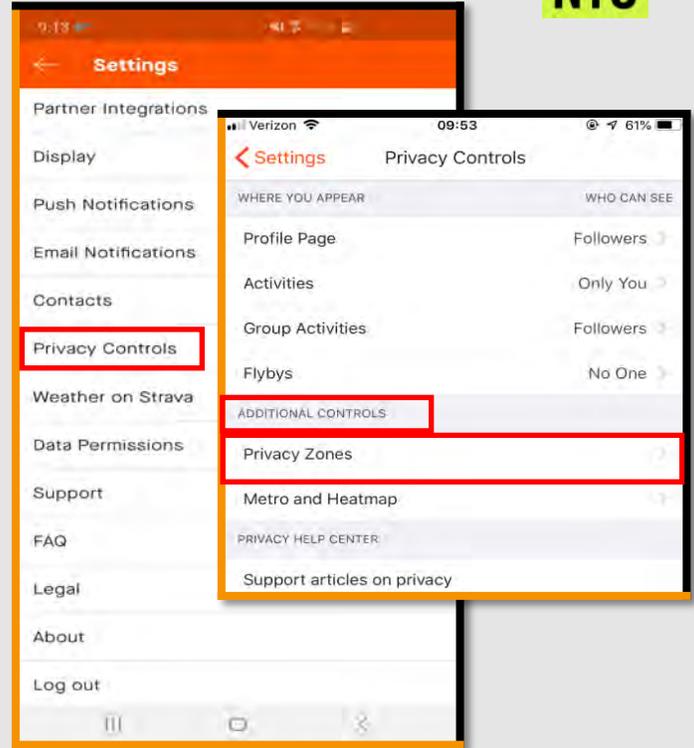
## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined orange and Android (and when both are same) black.**

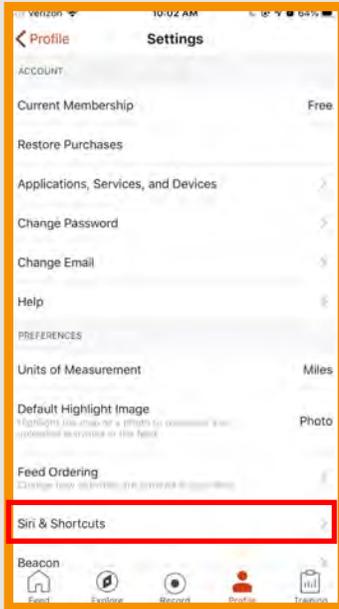
### Who can see your routes?

Once you have completed the set-up process, there are several settings that must be set in order to protect your privacy. From the “Home” screen, look to the bottom of the page and select “Profile” then select the “Settings” icon (looks like a wheel) at the top right of your screen. In the “Settings” section scroll down and select “Privacy Controls” (see right). Under “Privacy Controls” it is recommended that you change all of the tabs under “Where You Appear” from “Public” to either “Followers” or “Only You” to maximize your privacy.

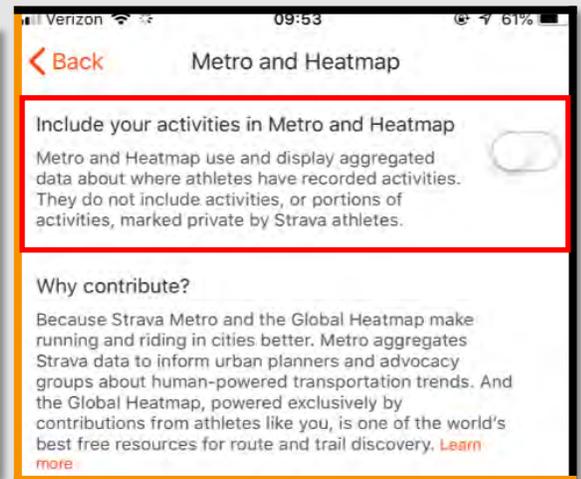
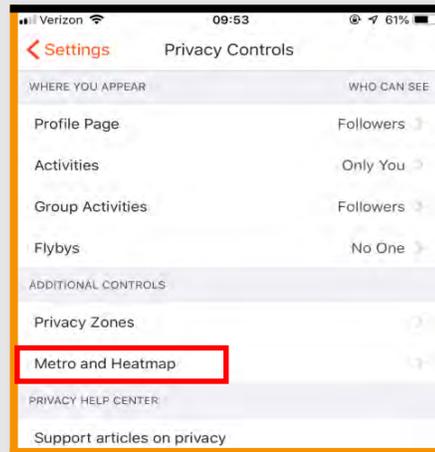
The “Privacy Zones” function, under “Privacy Controls” > “Additional Controls”, allows you to draw a privacy circle around a certain area such as your house or work. When you run in that circle you are automatically hidden from all other users. The downside is that if you step outside of that designated circle, that data will become public automatically.



Even with phone apps, it is important to make sure you keep a strong password to prevent anyone from accessing your account.



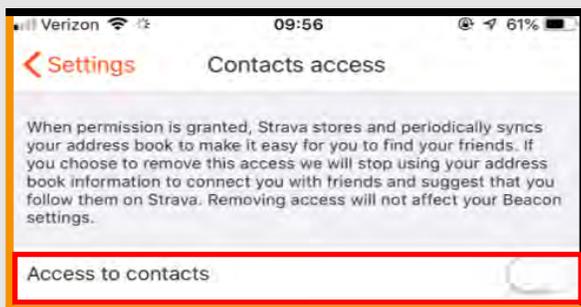
**On iPhone:** we recommend you scroll to the “Siri & Shortcuts” tab, under “Settings” (see left) and review the current settings there. Ensure your “Siri” function is off.



Next, we recommend you turn the “Metro and Heatmap” function off. This feature allows Strava to collect data and recordings from your device. First, under “Privacy Controls”, go to “Metro and Heatmap”, then next to “Include your activities in Metro and Heatmap”, set the toggle to “Off”, as seen above.

### Contacts

Finally, we recommend you turn off the function that allows Strava to have access to your “Contacts” - the default for this function is set to “On”. Go back to “Settings”, scroll to the middle of the menu, select “Contacts”. Set the toggle to “Off”.



# Fitness Apps

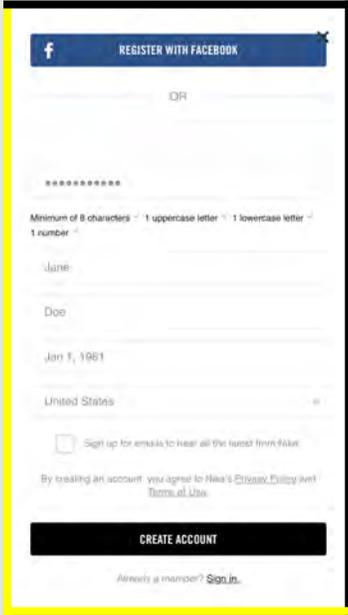
## Mobile Device Version



**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **yellow** and Android **black**.**

### Nike Run Club

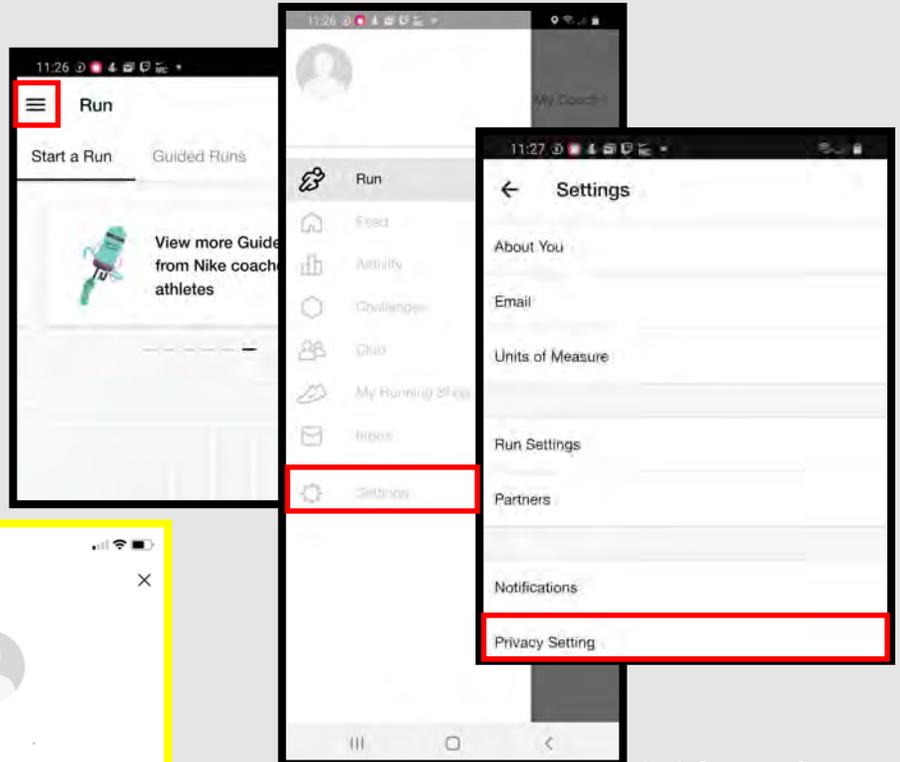
The “Nike Run Club” App is one of the most popular activity tracking apps available. One of the things it does is publish your completed runs and fitness activities and stats directly to your social media accounts when you finish - this includes your running routes, which creates vulnerabilities. We recommend that as you create your Nike Run Club account, you provide the minimum amount of personal information possible. First, you will enter your “Basic Information”. Remember, never allow one app to have access to another - so do not log in via Facebook or another social media account. Instead, use an email and password unique to this account. Also, we recommend you **not** allow this app to access your location.



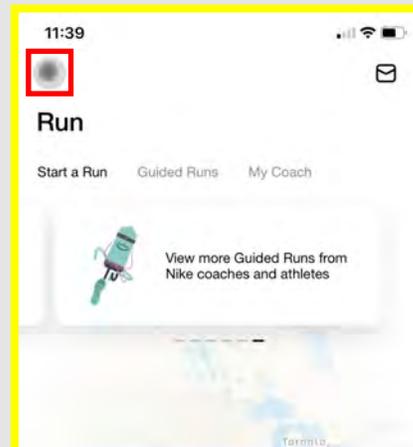
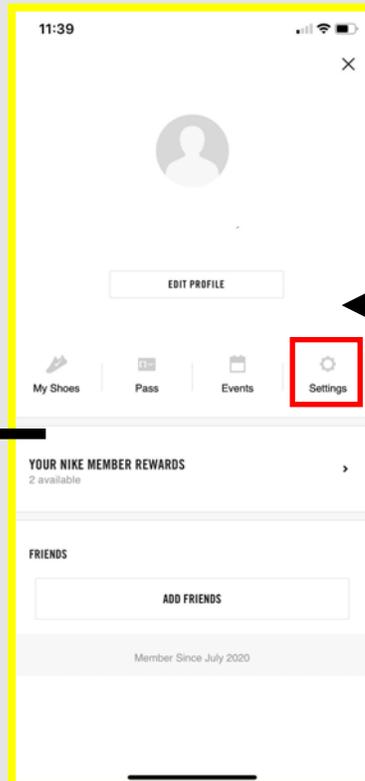
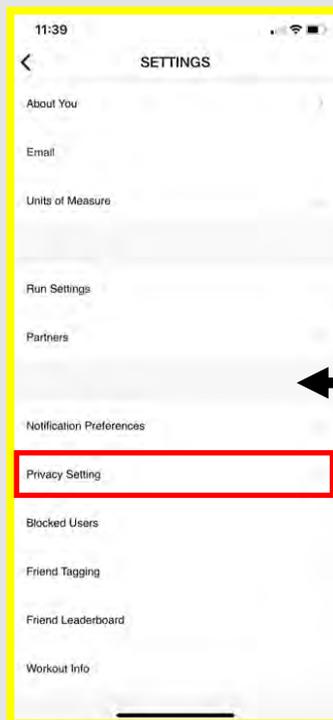
### Who can see my info?

First, let’s go to the “Settings” and establish your “Privacy” settings.

**On Android:** select the “Menu” option at the top left of the screen, then select “Settings” at the bottom of the list. (see right)



If you allow other third party apps to connect to your fitness app be sure to check both apps for up-to-date privacy settings.



**On iPhone:** select your “Profile Picture” at the top left of the screen, then select “Settings”, toward the middle right of the screen. (see right)

Next, on both Android and iPhone, select the “Privacy Setting” option from the menu, and we recommend setting to “Only Me” or “Friends.”

# Fitness Apps



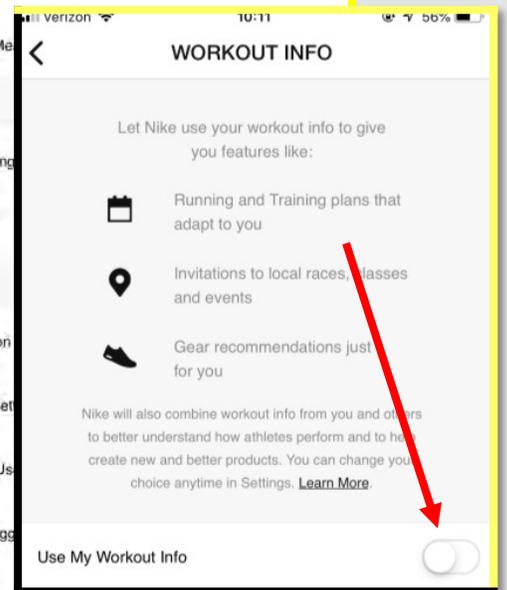
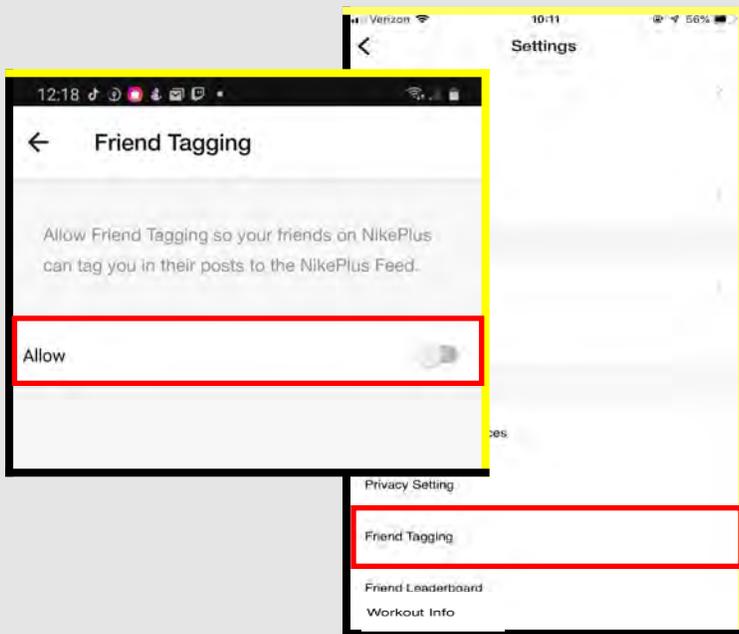
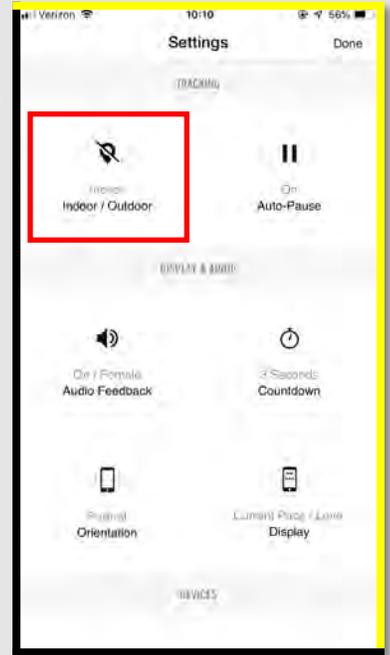
## Mobile Device Version

\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined **yellow** and Android **black**.

### Nike Run Club

Next, go back to “Settings” and visit “Run Settings”. We recommend you set the “Tracking” function to “Indoor” so that the app cannot track your outdoor routes.

We recommend you **not** allow “Friends” to “Tag” you in their posts, this is one way you really lose control over your information. Go to “Settings”, then “Friend Tagging”, then next to “Allow”, set the toggle to “Off”.



What personal data does Nike Run Club collect? Nike Run Club collects the following data in order to provide you with its products and services - unless you lock down your account:

- contact details including name, email, telephone number, address
- login and account information
- personal details like gender, hometown, birthday
- credit card information

Finally, let’s visit the “Workout Info” function, below “Privacy Settings”, which also must access your location and other personal data in order to work optimally. We recommend you set the toggle to “Off” in order to secure your data and personal information.

Fitness trackers have gained popularity. Strava has 42 million users and FitBit has 27 million. Neither has had a major data breach yet, but Under Armour did in 2018.

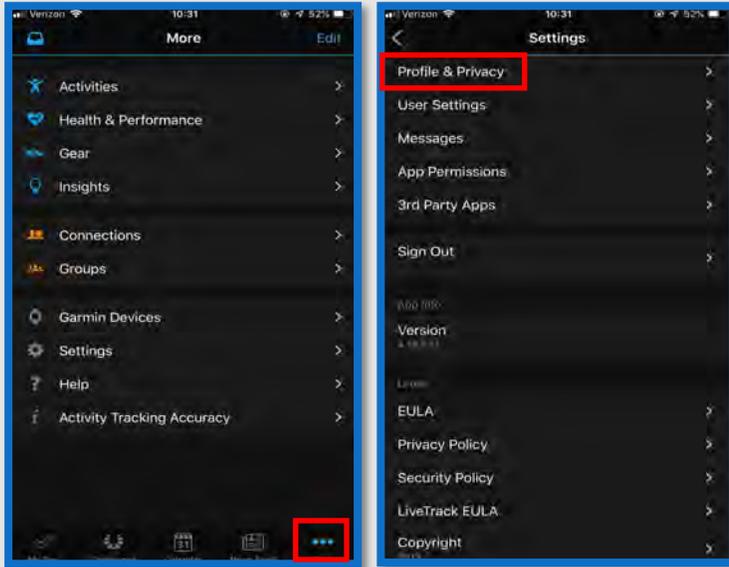
# Fitness Apps



## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined blue and Android black**

### Garmin

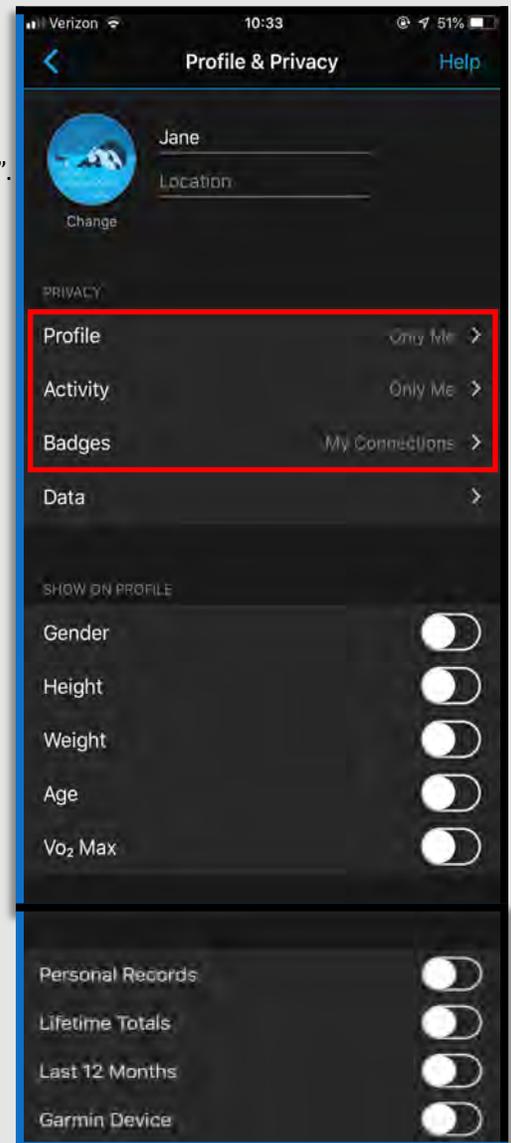
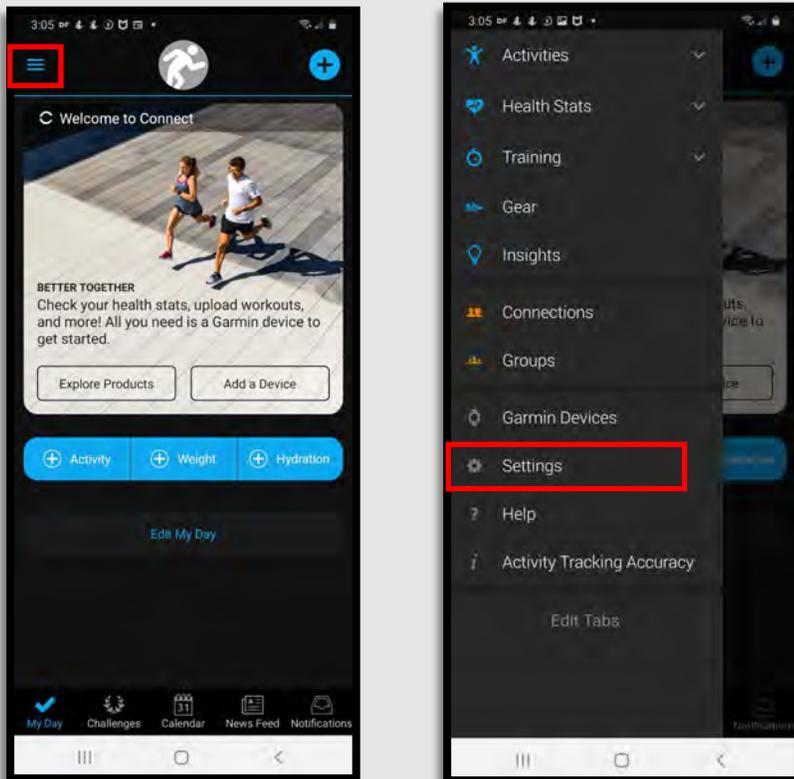


The “Garmin Connect” fitness app is another popular exercise tracker that is capable of sharing a lot of personal information you may not be aware of. If the settings are not set correctly, Garmin will automatically share your information with the public.

First, let’s lock down your “Profile” so that you limit which people can see what kinds of information about you.

**On iPhone:** from the “Home” screen, select “More” tab, then select “Settings”, then “Profile & Privacy”. (see left)

**On Android:** from the “Home” screen, select the “Menu” tab in the top left corner, then select “Settings” toward the bottom of the menu list, select “Profile & Privacy”.



Once in the “Profile & Privacy” section, look through all the privacy settings (see right). We recommend that the tabs in this section be set to “Only Me” or “My Connections.” Here you can also choose what personal information you want published on your profile for others to see.

Connecting with friends on fitness apps means that you must be concerned with their privacy settings as well as yours.

# Fitness Apps

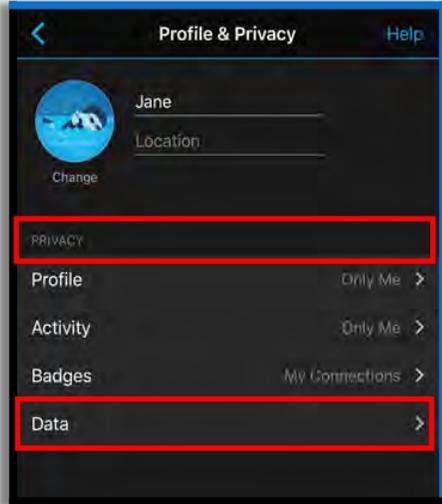


## Mobile Device Version

**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined blue and Android black.**

U.S. health privacy law, known as HIPPA, does not apply to info customers collect for their own use. Therefore, fitness apps don't fall under HIPPA regulations.

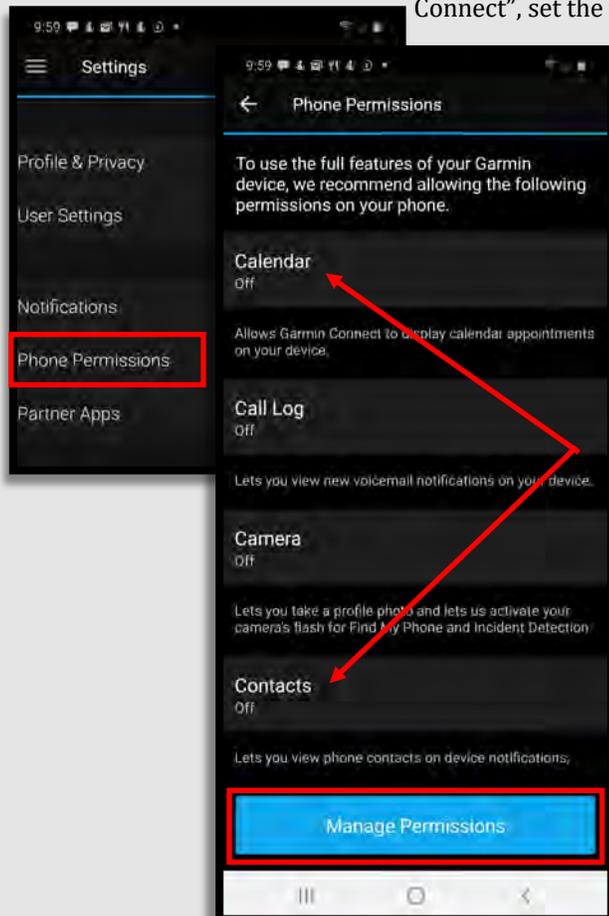
### Garmin



Also, in the “Profile & Privacy” section, let’s look at the “Data” section. It is located in the subsection labeled “Privacy” (see left). On the next screen, you will see a list including “Data Upload”, “Insights”, and “Popularity Routing”. First, select “Popularity Routing”. This function allows Garmin to collect data from your account and device in order to build and reinforce data-bases that hold popular routes. We recommend you turn this function off by setting the toggle to “Off”. Next,

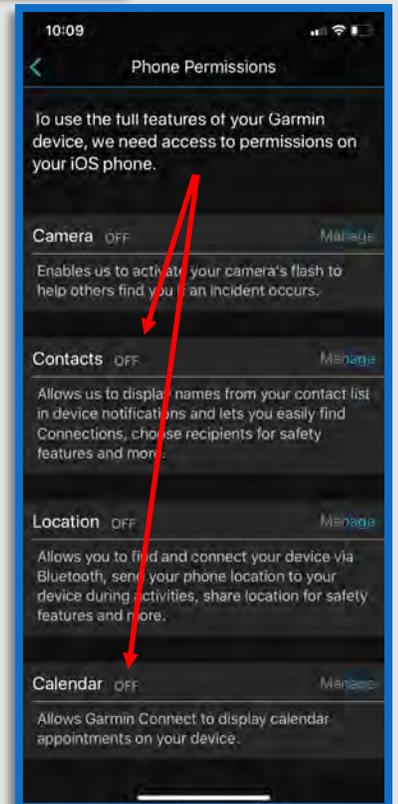
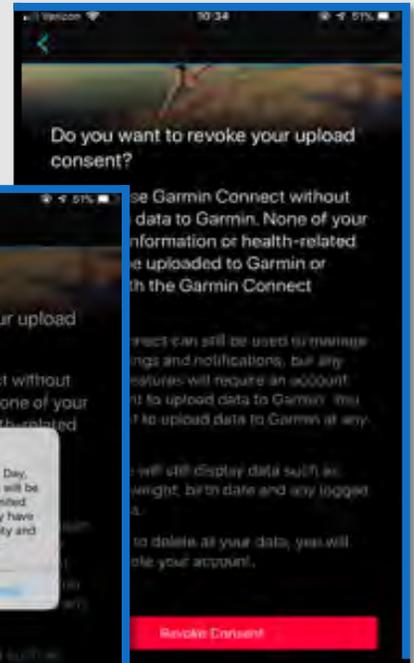
select “Insights” and read through the consent policy provided before you decide if you want to “Agree” or “Do Not Agree”, this is your choice. Finally, select “Device Upload” and decide whether you want to Garmin to connect your Garmin devices to “Garmin

Connect”, set the toggle to “On” or “Off” based on your preference here.



Finally, let’s look at what other features of your phone you are letting Garmin have access to. Go back to “Settings”, select “Phone “Permissions” and review which device features Garmin is connected to. We recommend you set both “Contacts” and “Calendar” to “Off”, and we suggest you consider doing the same for “Camera” and “Location”. (see left for Android, and right for iPhone).

**On Android:** Note that “Location” is further down the list, reference screen shot left.



# Fitness Apps

## Mobile Device Version

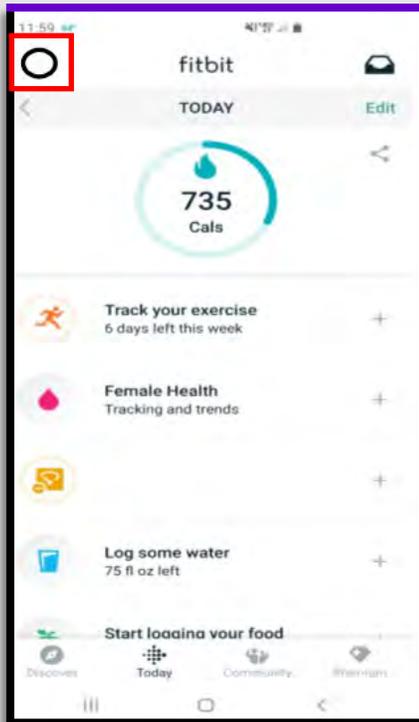


\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined purple and Android black

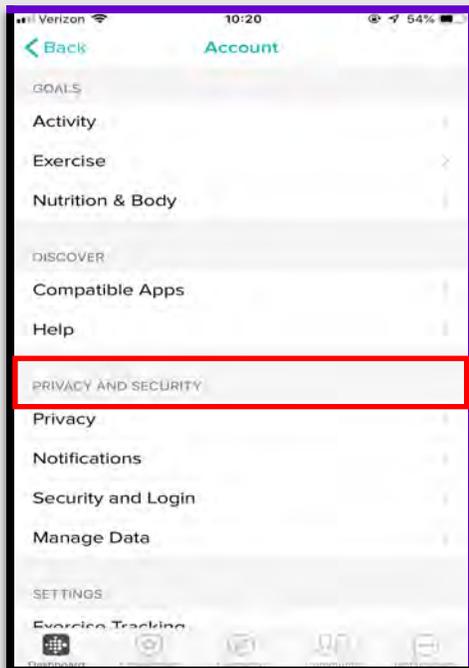
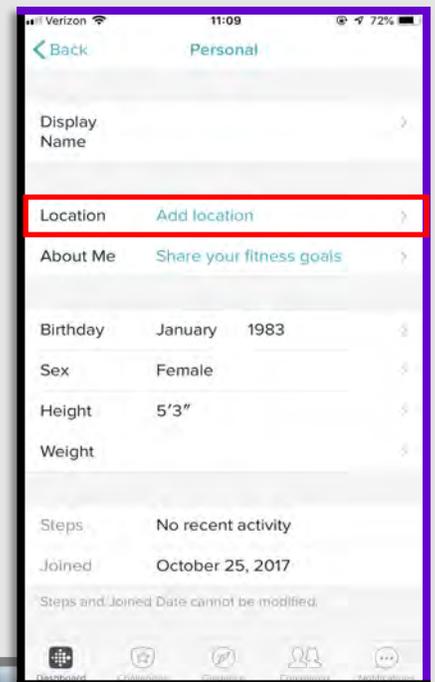
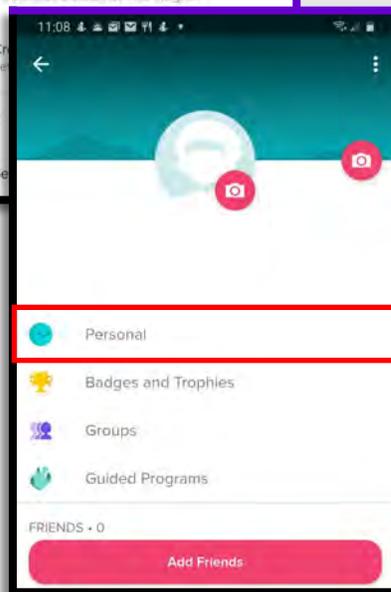
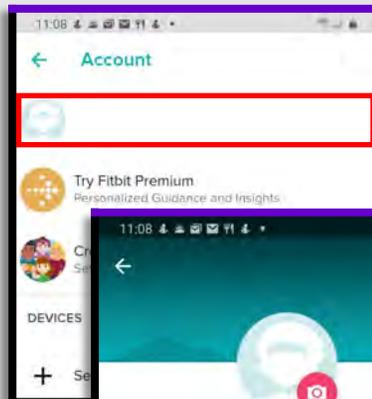
## Fitbit

FitBit is another popular activity tracker, and one of the first of its kind. Older versions of FitBit were designed to automatically publish workout statistics and information to the public, but newer versions have changed default settings to keep this information private. Therefore, unless you configure it otherwise, your privacy setting *should* be set by default to “Private”. Nevertheless, we recommend you always confirm settings yourself.

Anytime your fitness app has an update it is a good idea to use this time to also update your password.



First, let’s review your “Profile” information. From your “Home” screen (see left), select your “Profile Picture” icon in the top left corner. Then select your “Account”, noted by your name, and your “Profile Page” will appear, select “Personal” and ensure that “Location” is not turned on. Also review the personal data you have provided to Fitbit on this page. Next, go back to the “Account” section (where you selected your “Account” by name earlier). Here you can review each of your FitBit settings and then head to the “Privacy and Security” section where you will want to pay special attention to each setting.



# Fitness Apps

## Mobile Device Version



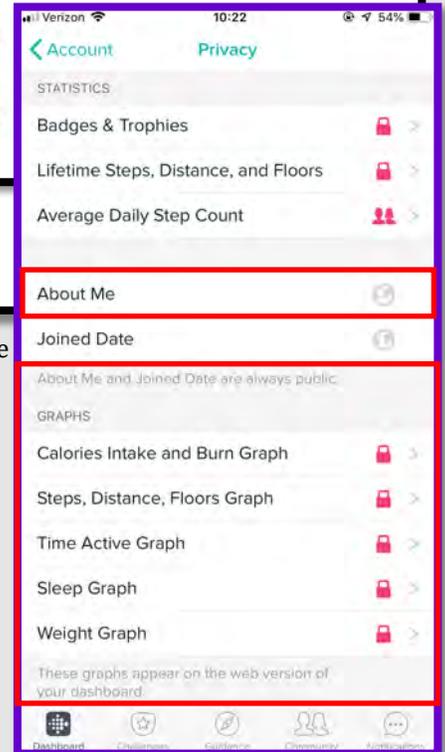
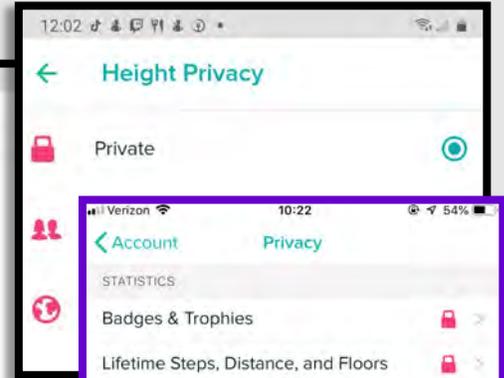
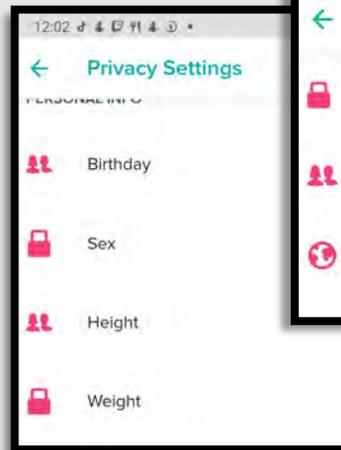
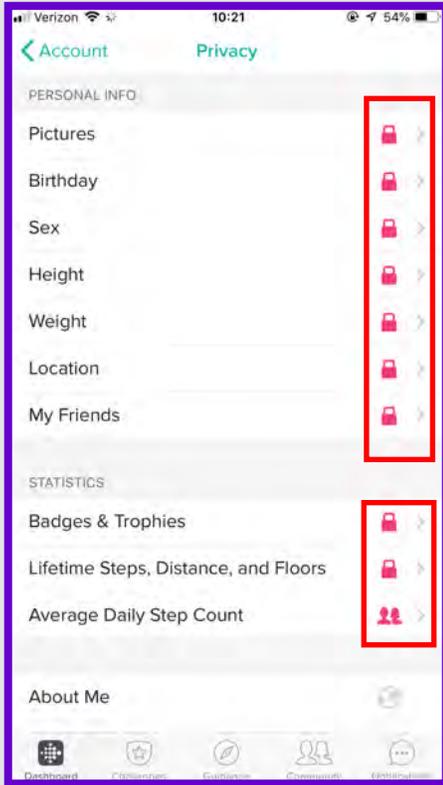
**\*\* This information describes how to make your account secure on Android and iPhone mobile devices. Differences between iPhone Operating System (iOS) and Android Operating System (AOS) are minimal, in such cases iPhone images are outlined purple and Android black.**

### Who can see my information?

In the “Account” section, under the “Privacy & Security” section, select “Privacy”. We recommend that you avoid sharing any information that would be considered “Personally Identifiable Information”, or PII. This is any information connected with your personal identity, including your name, birthday, social security number, etc. To change the setting:

**On iPhone:** (see left) select the icon to the right of the category, for instance the “Private” icon is a padlock, “Friends” is an image of two people, and “Public” is represented by a globe. Select the icon and make the change, then select “Save” in the upper right corner of the screen.

**On Android:** select the category itself, make the change, and select the back arrow. The change is automatically saved.



**Important Note:** The “About Me” section, located toward the bottom of the “Privacy” page, is always set to “Public”. You cannot control this feature, as indicated by its greyed out appearance. You write your “About Me” information in your “Profile” section. The image to the right is for iPhone only, and this section is not available on Android.

Finally, go back to the “Account” section and review the “Manage Data” section where you can delete or limit what third party apps have access to your Fitbit and vice versa. (not shown)

### Polar Flow

Polar is a company that produces fitness tracking watches and hardware, all of which connect to its popular app, Polar Flow. According to a recent investigation, the app's tracking map exposed the home addresses of thousands of users. This is in part because people often turn their fitness trackers “On” or “Off” when they're close to home, unintentionally revealing where they live.

To keep your data private on Polar Flow:

- Go to “Settings” and then “Privacy”, and set the default to “Private”
- Change the privacy of each of your past runs individually, set them each to “Private”
- Set your “Profile” to “Private”



Don't just set the settings within the fitness app, make sure you go into your phone settings and update what you allow for each app from your phone.

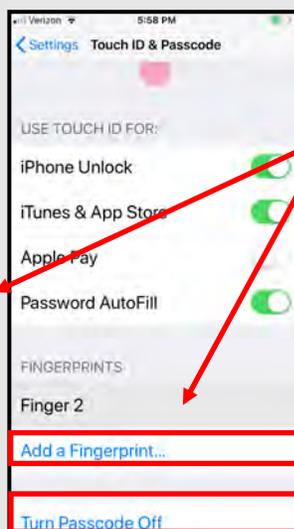
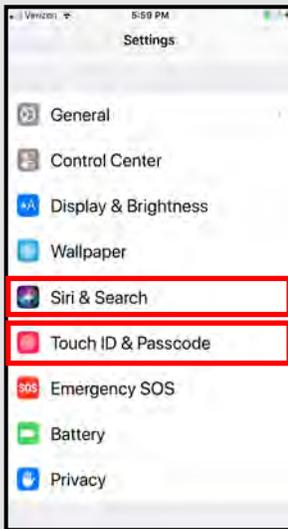
# iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD



## “Best Practices”

- ◆ Smartphones and tablets are not impenetrable. Secure your smartphone with a password, and use apps such as “Find My iPhone” to locate lost or stolen devices.
- ◆ All smartphones and tablets have cameras and microphones that can be remotely activated. Caution should be used when device is near anything of personal importance.
- ◆ Bluetooth and wireless capable devices are convenient but easily exploitable by hackers. Use a VPN if possible and avoid public wireless networks. It is advisable to turn these services off if not immediately needed.
- ◆ Prior to downloading apps on your device, read the developers permissions. Many apps require permission to access your camera, microphone, text messages, and contacts.
- ◆ Turn off location services until they are actually needed. Otherwise, your daily movements may be tracked by various apps and vendors. Whether turned on or off, location services are always available to 911 and first responders.

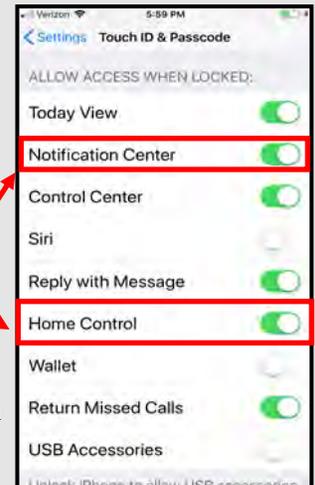
## “Physical Security”



Under “Settings” and “Touch ID & Passcode,” select “Add a Fingerprint” and “Turn Passcode On”. Be sure to use at least a 6 digit passcode. Alpha-numeric passcodes are even better options.

**Note:** iPhone 11 has taken off the feature “Touch ID” and replaced it with “Face ID”. Follow directions to create a Face ID, and we recommend under “Use Face ID For”, the same settings as “Use Touch ID For” (left)

Additionally, we recommend that you turn off “Siri” due to its listening capabilities and bugs associated with accessing your phone through Siri without a password.

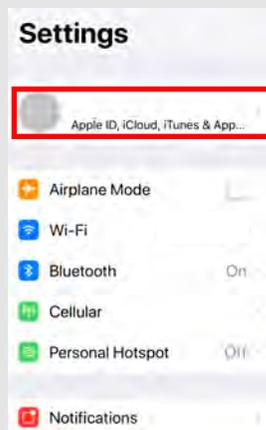


Finally, scroll further down in this section, and

we recommend setting the functions under “Allow Access When Locked”, as seen here (above right), in order to limit access.

## “Find My iPhone”

Next go to “Settings” and select your account at the top (highlighted in red to the right). From there, select “Find My,” then select “Find My iPhone” and ensure it is turned “On”. This way if you lose your phone, you can access your account online and geo-locate where it is.



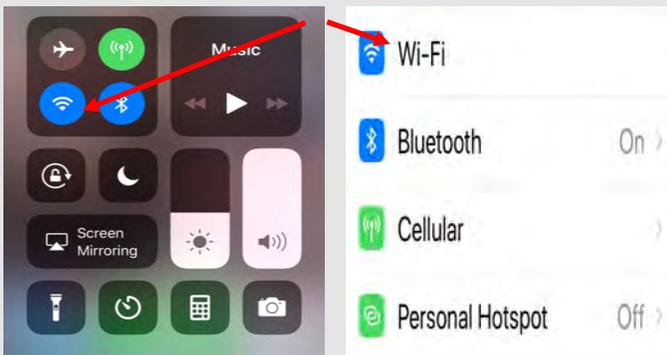
Smartphones contain extremely sensitive personal data and therefore should be treated with extra security precautions #protectyourdata



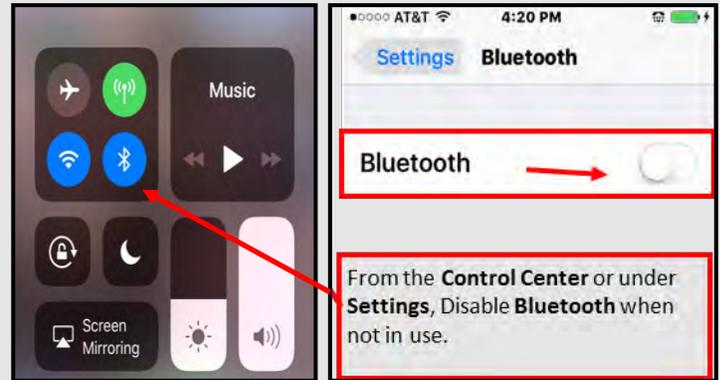
# iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD

## “Wireless Networks”

Where possible, public WIFI networks should be avoided due to the vulnerabilities they present to your personal data. If public networks must be used, avoid logging into accounts that require passwords and always use a VPN client to encrypt on-line transactions. There are two ways to turn off WIFI: 1) Scroll up from the bottom of your phone and tap the icon on the control screen; or 2) In “Settings”, Select “WIFI”, and it turn off.



## “Bluetooth”

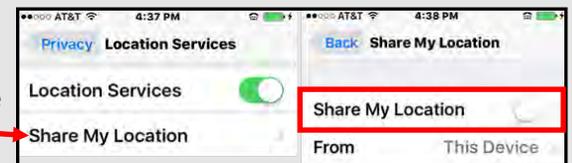
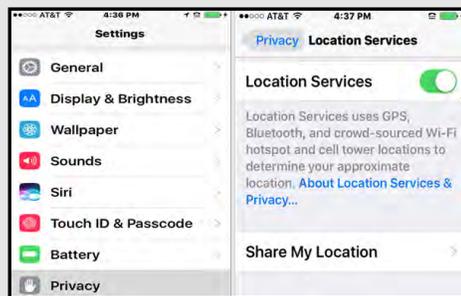


Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your iPhone or tablet, hackers can gain access to your device and obtain contacts, messages, calendars, photos, and notes without your knowledge. It is therefore recommended that you only use Bluetooth when necessary, like in your car, and that you turn it off after you are done using it each time.

## “Location Services”

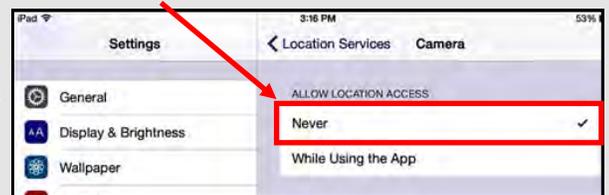
Whenever you take a photo, your phone records the location and saves that information inside the photo’s EXIF data. When you send that photo to someone else, they may be able to see where you took it, in some cases, down to a specific street. If you post a picture taken from your home, anyone who can view the EXIF data could figure out where you live and more. It is important to remove the EXIF data, or better yet prevent your devices from including it in pictures. Please refer to the “EXIF” Smartcard in this book for information on how to do this.

To disable your location from being shared in “Message “and “Find my Friends”, open the “Settings” app and navigate to “Privacy” > “Location Services.” Then navigate to “Share My Location” and tap on the toggle to disable “Share My Location.”



Note: If you turn off “Location Services” in the “Privacy Setting “menu, you cannot use location services for things such as “Navigation” or “Find My iPhone” if lost or stolen. You can still wipe your phone, using the “Find My iPhone”, if “Location Services” are off. “Alternatively, you can leave “Location Services” on in “Privacy Settings” but turn it off for installed apps you don’t want to have access. Just scroll down to find which apps use your location.

Go back to “Location Services“ to disable your location from being saved with photos, and tap on “Camera“ to change this setting. Note: The “Location Services” toggle must be on to find the camera option. Perform the same steps to disable location services for other apps listed in the “Location Services” setting. Navigation and maps apps are examples of those that require “Location Services.”



Leaving location settings on can give someone a pattern of life for you and your family. #turnitoff

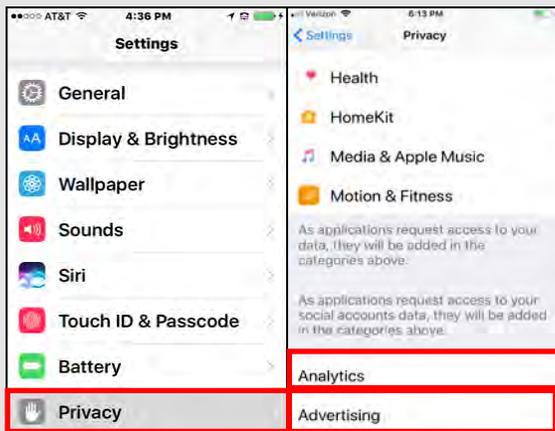
# iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD



## “Analytics Data and Ad Tracking”

“Analytics” enables a feature that gives Apple permission to track your activities. “Ad Tracking” allows vendors to send ads to you, targeted to your interests. Apple provides a setting to allow you to opt out of both of these features. It is recommended that you turn off “Ad Tracking.”

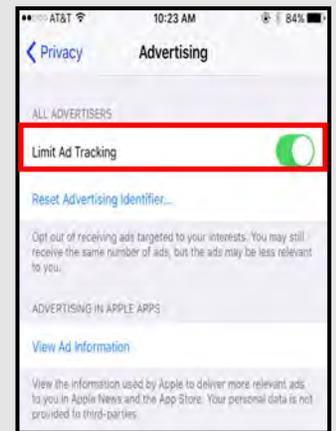
1) Open up the “Settings” app and navigate to “Privacy” then to “Analytics” and “Advertising”



2) Select “Analytics” and Then turn off “Share iPhone Analytics”



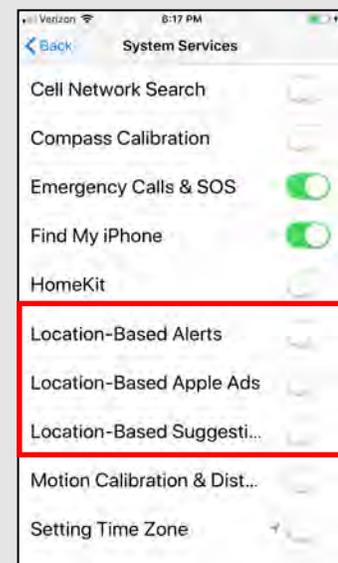
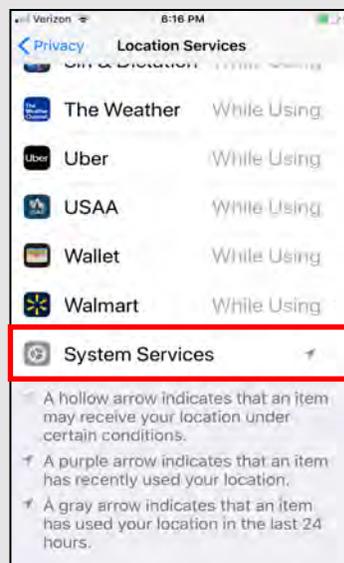
3) Then go back and select “Advertising” Turn ON “Limit Ad Tracking.”



## “Location-Based Apple Ads”

“Apple Ads” allow Apple to serve you with ads, based on your location. “Location-Based Ads” do not use your exact location and Apple does not give this information to advertisers. Here’s how to disable “Apple Ads”:

Open up “Settings” > “Privacy” > “Location Services” > “System Services.” You’ll see a list of location-based selections that can be toggled off.

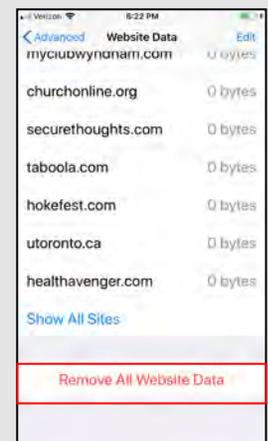
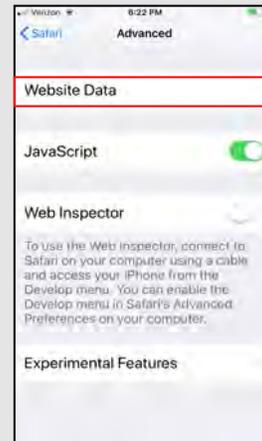
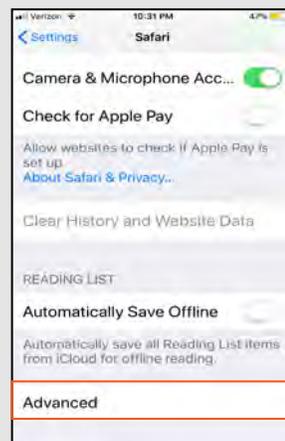
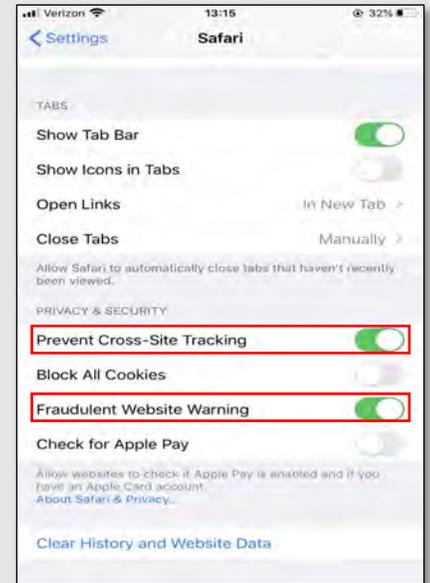
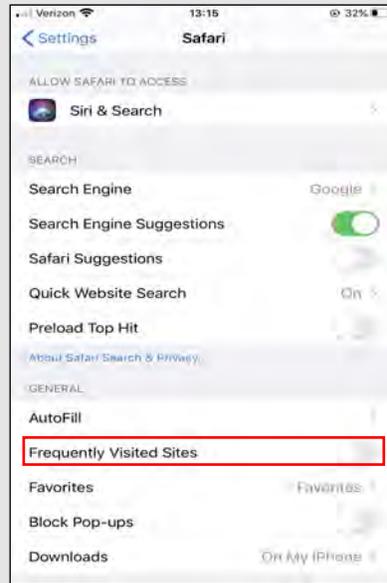
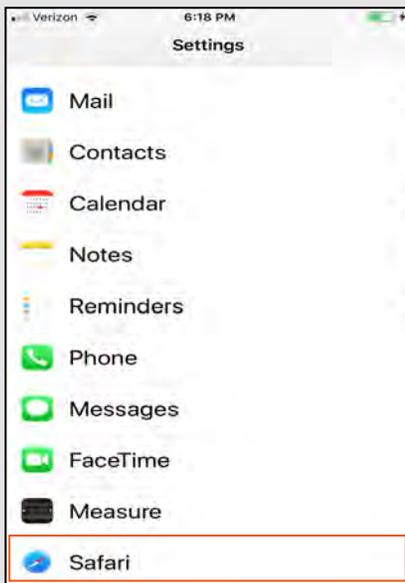


# iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD



## Safari's "Do Not Track"

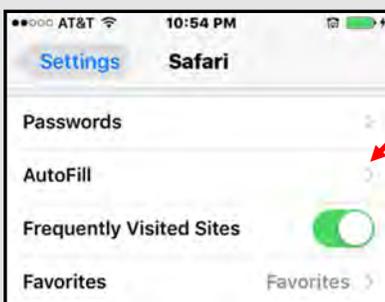
Safari's "Do Not Track" is a universal web tracking opt-out initiative that allows users to prevent advertisers from tracking your browsing habits. The Safari browser on iOS 13.0 allows users to opt-out to prevent advertisers from seeing users mobile web browsing history. To opt-out, open the "Settings" app, scroll down and select "Safari". There are several sections to look through and adjust the settings, but definitely turn off "Frequently Visited Sites" under the section titled "General". This prevents Safari from tracking sites you regularly visit. Next, under the "Privacy & Security" section on the "Safari" page, turn on "Prevent Cross-Site Tracking" and "Fraudulent Website Warning."



Google already tracks everything we do, so why let another search engine do it too? #saynototracking

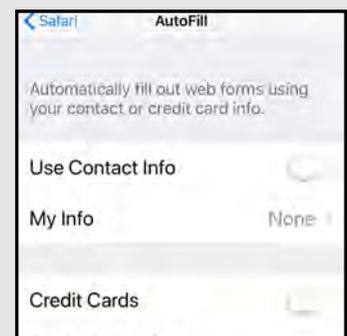
It is also a best practice to clear the browser history periodically. To do so, continue to scroll down in the Safari settings, at the very bottom select "Advanced" > "Website Data", then select "Remove All Website Data"

## "Passwords and AutoFill"



Clear the AutoFill to protect passwords and credit card information. To do so, open "Settings" > "Safari" and click on "AutoFill"

Next, select the following settings to disable "Use Contact Info", and "Credit Cards"



# iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD



## COVID 19 Contact Tracing

Apple and Google have partnered on offering a secure and private coronavirus contact tracing implementation on iOS and Android. Contact tracing is called “Exposure Notifications” on iPhone, and is default set to “Off”. You’ll have to download an app from your local health authority that will require your explicit permission to use anonymous Bluetooth data for it to work, upon rollout of the system in May 2020. Later in the year 2020, contact tracing software will allow it to work without a third-party health authority app.

In the meantime, you may be curious as to status of the “COVID 19 Exposure Logging” function on your iPhone. You can see whether yours is activated by going to “Settings” > “Privacy” > “Health” > “COVID-19 Exposure Logging”. When you see “Exposure Logging”, you will notice a toggle to the right that is probably “Off”. You can attempt to turn it “On”, and if you aren’t able to do so, then the tool is not yet active on your iPhone.



If you decide at any point that you want to disable the “COVID-19 Exposure Notifications Logging” tool on your iPhone, you can take the following steps. First, on iOS 13.5 and later, go to “Settings” on your iPhone. Next, swipe down and select “Privacy”, then choose “Health”, then “COVID-19 Exposure Logging” at the top. For now, you’ll need an authorized app before “Exposure Notifications” can be turned on, but when that happens you can tap the toggle to turn notifications “On” or “Off”. You can also delete the exposure logs manually at any time by going to the bottom of the “COVID-19 Exposure Logging” page and selecting “Delete Exposure Log”. (see above)

If you have opted-in to the “COVID-19 Exposure Logging” system, you may be interested to know who is trying to access your exposure information. To find out, select “Exposure Checks” on the “COVID-19 Exposure Logging” page. This is a record of all requests to check your “Exposure Log” from the past 14 days.

**Note:** The “COVID-19 Exposure Logging” toggle is disabled by default in iOS 13.5. It does not connect any data without you installing and authorizing a local health authority app, which will be available soon. Apple and Google’s exposure notification system will be completely opt-in.

The Covid-19 Exposure Tracking System will be opt-in on your iPhone. It will require an additional download from your local health system in order to work.

# ANDROID PRIVACY SETTINGS (ANDROID 10.0)



## Best Practices

- ◆ Smartphones and tablets are not impenetrable. Secure your smartphone with a password or biometrics, and utilize apps such as **Find My Device** or **Prey Anti Theft** to locate lost or stolen devices.
- ◆ All smartphones and tablets have cameras and microphones that can be remotely activated. Consider your device when you are in certain places or conversations.
- ◆ Bluetooth and wireless capable devices are convenient but easily exploitable by hackers. Use a VPN if possible, and always avoid public wireless networks.
- ◆ Prior to downloading apps on your device, read the developer's permissions. Many apps request permission to access your camera, microphone, text messages, and phone contacts.
- ◆ Keep location services turned off until they are actually needed. Otherwise, your daily movements are likely being tracked. Don't worry, location services are always available to 911 and first responders, even when turned off.
- ◆ If you have a google account, you can use your google credentials to login at [maps.google.com/locationhistory](https://maps.google.com/locationhistory) to see your device location history for the last year or more.

**\*NOTE:** Due to varying Android manufacturers, the instructions in this Smart Card may vary slightly depending on the device being used.\*

The most important thing you can do to keep your information secure is to keep your device up to date. In order to make sure your Android is up to date with the latest Android Version, first go to "Settings" then "System," scroll to the bottom and select "Advanced." From there you will see the "System Update" tab, select the tab. (On some versions, you may go to "Settings", then "Software update" toward the bottom of the "Settings" list).

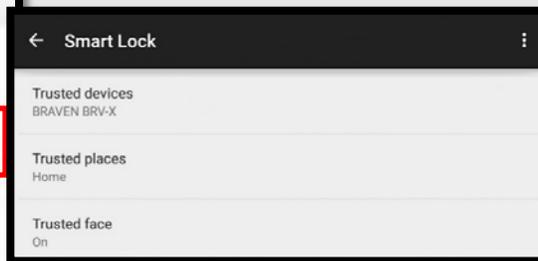
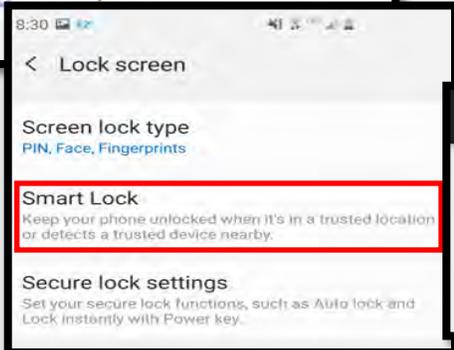
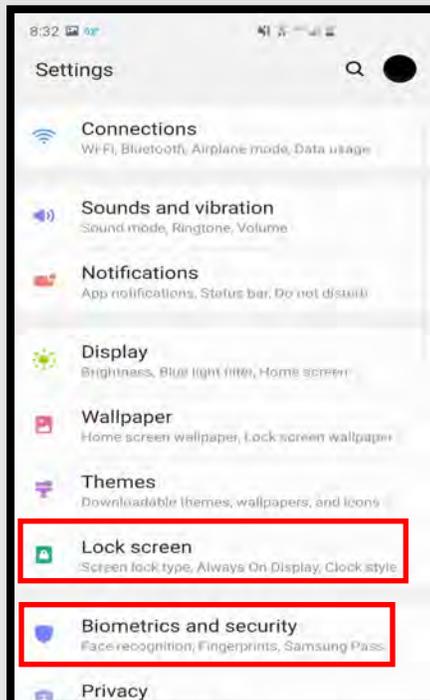
## Physical Security

The first line of defense in preventing unauthorized access to your device is to protect it with a "Passcode". In addition, Android 9.0 offers several enhanced security features, including "Fingerprints", "Facial Recognition", "Encryption", and "App-level Permissions".

Under "Settings", first select "Biometrics and security". Here, you can set up your "Face recognition" and "Fingerprints" profiles. You will then go back to "Settings" and select "Lock Screen" in order to set your screen-lock preferences. Tap the "Settings" icon and then tap "Lock Screen." The options are Swipe, Pattern, PIN, Password, Face, Fingerprints. The most secure way to protect your phone is to use the **biometric** options, such as "Face Recognition" and "Fingerprints". A "Password" is the strongest backup solution.

Also under "Lock Screen", you will see the feature "Smart Lock", which allows you to set "Trusted Places" inside of which your device will unlock itself and remain unlocked. This feature can be set to recognize your face and "Trusted Devices" as well, all of which trigger your device to "Unlock" and remain unlocked. This feature is meant for your convenience, but presents obvious vulnerabilities. We recommend you do not enable any "Trusted Features".

Under the "Biometrics & Security" section, you may be able to select the option to "Encrypt Phone", which allows you to initiate the encryption of all data on your device. According to the instructions, this could take up to an hour and requires your device to be plugged into its charger. This process must not be interrupted, so be sure to start it when you are sure you will not need to use your device for that amount of time. You will only need to perform this once. Locking your device encrypts the data on your phone. Unlocking your encrypted device decrypts your data.



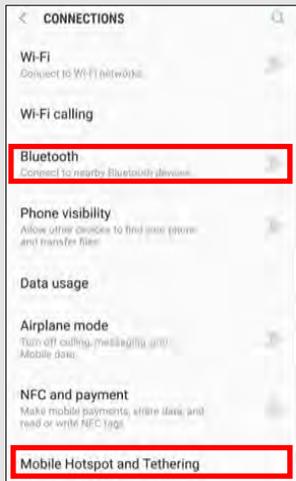
# ANDROID PRIVACY SETTINGS (ANDROID 10.0)



## Mobile Hotspot and Bluetooth

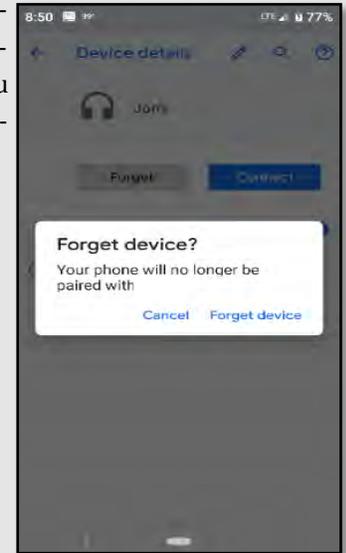
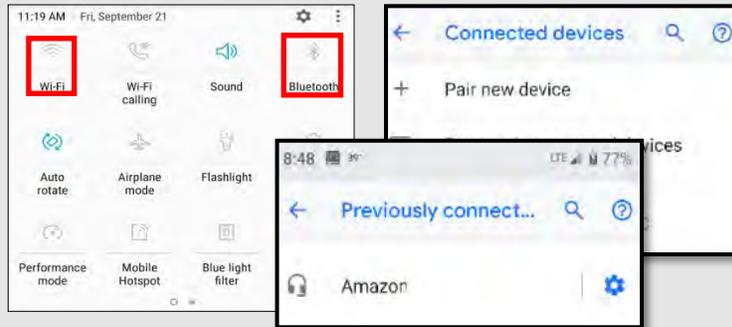
**Mobile hotspots** are areas away from your home where your internet company provides you with Wi-Fi. Alternatively, hotspot devices can be purchased and used for connecting to the internet remotely, but without connecting to public Wi-Fi, which we always discourage. Most Android Smartphones have a “hotspot” feature that allows you to connect to your internet (for instance on your laptop) remotely. By turning on this feature, your phone uses its cellular data to create a “Wi-Fi hotspot”. Then, you can connect to this hotspot with a computer or another device that does not have cellular data. You can turn this option on and off under “Settings” > “Wireless & Networks” or “Connections” > “Mobile Hotspot and Tethering”. **Bluetooth** is a wireless technology for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your device, hackers could gain entry to your device and obtain contacts, messages, calendars, photos, and notes, or install malware without you even knowing. To disable Bluetooth go to “Settings” > “Wireless & Networks” or “Connections”.

Google Maps will use your location history and travel times to notify you of traffic before you travel. #GoogleIsWatching



When Bluetooth is enabled on your device, hackers could gain entry to your device and obtain contacts, messages, calendars, photos, and notes, or install malware without you even knowing. To disable Bluetooth go to “Settings” > “Wireless & Networks” or “Connections”.

### Wireless Networks



Note: We always recommend avoiding public Wi-Fi networks because they are unsecured. If you must use one, avoid logging into accounts that require passwords and use a VPN client to encrypt on-line transactions.

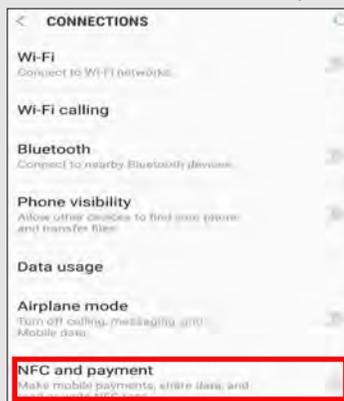
Note: In order to delete Bluetooth sessions you no longer need, go to “Bluetooth”, select “Previously Connected Devices” then select the “Settings” icon, select “Forget.”

Note: From the “Quick Settings” drag-down tray, tap and hold “Wi-Fi” to see available networks. Tap the “Wi-Fi” icon to turn Wi-Fi “off” when not in use.

### Near Field Communication (NFC)

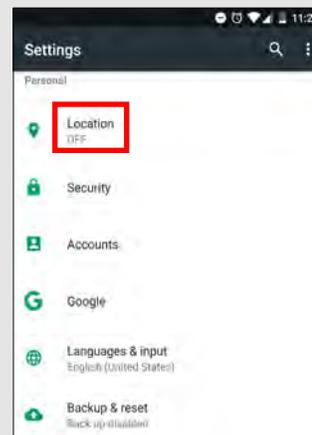
NFC is a set of short-range wireless technologies, typically requiring a distance of 4cm or less to initiate a connection. The technology allows you to “bump” your smartphone with other NFC devices to exchange information or pay for items using a Pay app. Although extremely close range, a malicious user can tamper with the data being transmitted between two NFC devices if they are within range. NFC risks include: data tampering, data interception, and mobile malware.

Turn off NFC when not in use by tapping “Settings” > “Wireless & Networks” or “Connections”. Then tap the toggle switch for “NFC and payment” so that it is in the “off” position.



### Location Services

Whenever you take a photo, data on your location is saved inside of the photo’s EXIF data. When you send that photo to someone or post it online, data on where you took the photo may be available to those who know how to view it. If you post a picture that you took from your home, anyone that can view it may be able to figure out where you live and more.



To disable your location from being shared, select “Settings” and scroll down to “Biometrics and security.” Disable your location services by switching the toggle to “off”.

\* Newer device “Location” function is separately under “Settings”, just below “Biometrics and security”.

# ANDROID PRIVACY SETTINGS (ANDROID 10.0)



## Lost/Stolen Phone

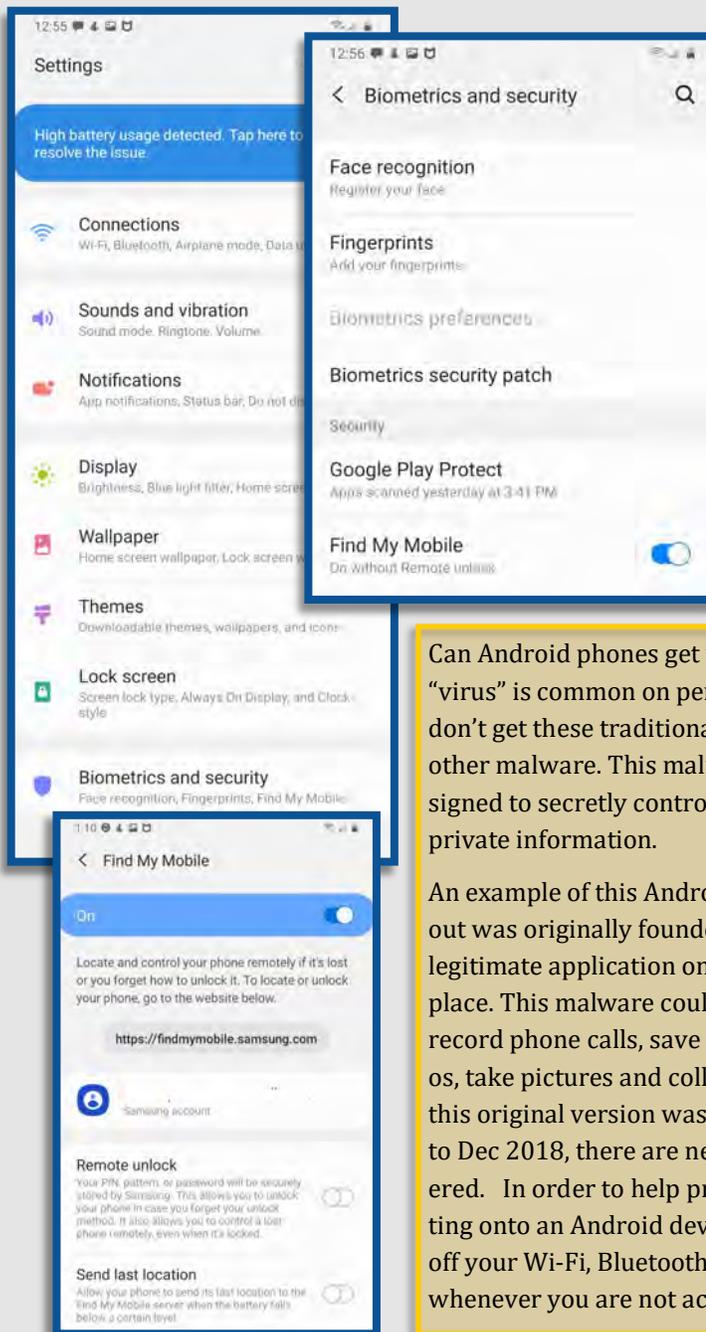
Over 100 cell phones are lost or stolen in the U.S. every minute, which shows how necessary it is to keep your device secure and locked with biometrics or a passcode. All Android phones work by syncing a phone to a google account, so if you lose your device, you can go to [android.com/find](https://android.com/find) in order to locate it. This is the native “Find My Device” tool for Android, and is automatically enabled on your Android Smartphone. Alternatively, you can download the “Find My Device” app from Google Play Store.



- ◆ Locate Android devices associated with your Google account.
- ◆ Reset your device's screen lock PIN.
- ◆ Erase all data on the phone.

Note: If you turn off “Location Services” in the “Location Setting” menu, you cannot use “Location Services” for apps that locate lost or stolen devices. You can still wipe your phone if the “Location Services” are “off”. If you wish to use some “Location Services”, be sure to go into each app and set the “Location Settings” as desired rather than turn off the main “Location Services” setting.

Although saving your passwords is convenient, it poses a huge threat to your security should your device be stolen.



What should you do if your device is lost or stolen? Google can help you locate it. Let's enable the settings on your device so that in case you need to, you can locate your lost phone.

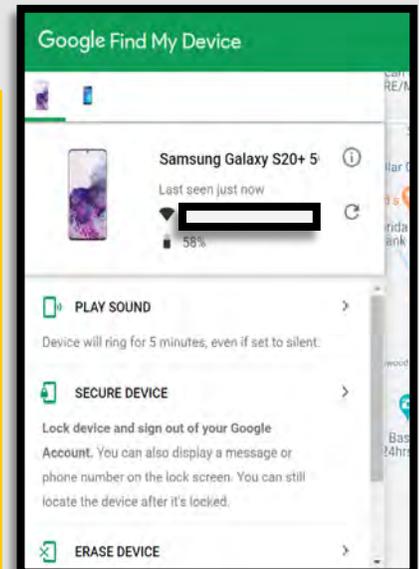
Go into “Settings” > “Biometrics and security” > “Find My Mobile”. Ensure the Toggle is set to “On”

If your device is lost or stolen, you can then go to “Google Find My Device” page and see where your phone was located last. You can make the ([android.com/find](https://android.com/find)) device ring at full volume to help you find it or remotely lock or erase all data on it.

In order to test this feature, let's go to [android.com/find](https://android.com/find) and see if it works.

Can Android phones get viruses? The traditional “virus” is common on personal computers, Androids don't get these traditional viruses, but they do get other malware. This malicious software can be designed to secretly control the device or even steal private information.

An example of this Android malware is Triout. Triout was originally founded in 2018, bundled with a legitimate application on the Google Play marketplace. This malware could hide on your Android and record phone calls, save text messages, record videos, take pictures and collect your location. Although this original version was only active from May 2018 to Dec 2018, there are new variations being discovered. In order to help prevent malware from getting onto an Android device it is important to turn off your Wi-Fi, Bluetooth, and sharing capabilities whenever you are not actively using them.



# ANDROID PRIVACY SETTINGS (ANDROID 10.0)



## Lost or Stolen Android Device

### Ad Tracking

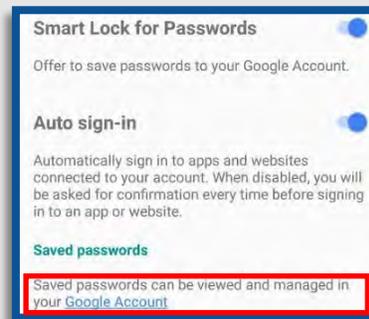
Ads can track everything you do. Not all Android devices and OS versions have settings to turn Ad tracking off. If your device does not have this setting, you can download ad blocking / privacy-oriented browsers or browser add-ons. Here are just a few examples:



### Smart Lock for Passwords

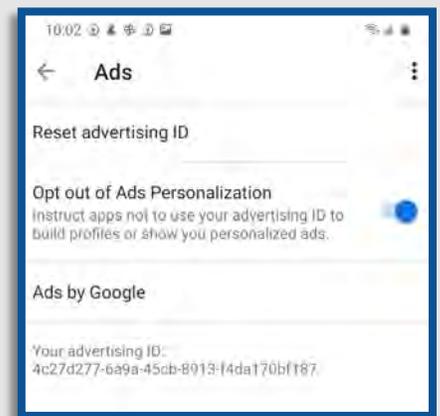
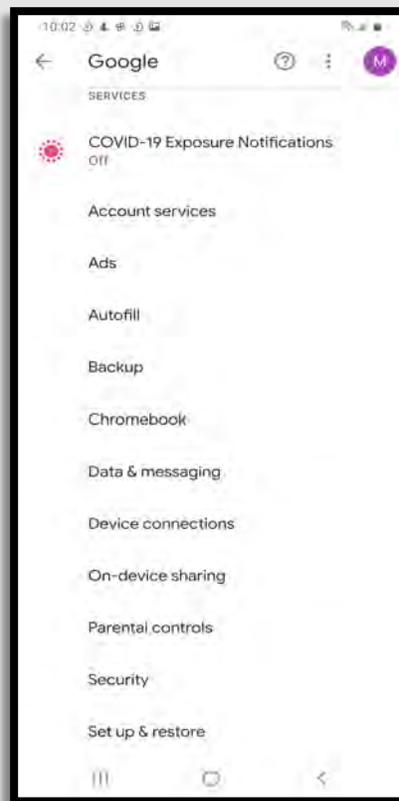
From the same Google Settings section, select “Smart Lock for Passwords”. You will then see the screen where you can turn off the options to save your passwords and automatically sign-in to web pages and other account-oriented sites. You can also add apps for which you don’t want passwords to be saved.

Alternately, you can select specific accounts and delete the saved password by tapping the “Google Account” hyperlink. All saved passwords are encrypted and stored in the Google



cloud storage that comes with your account. Although it is recommended that you turn off the above options, only you can balance your security with the convenience of saved passwords.

If your device has the option to control advertisements, the following directions show you how to disable the feature: Go to “Settings” > “Google” > “Ads”. Tap the toggle switch to the “On” position for “Opt out of Ads Personalization”.



Safe Browsing: Android devices have a “safe browsing” mode that is built into them and enabled by default. While using Google Chrome, this feature will give warnings before entering a suspicious site. As long as your Chrome and Android are updated to the most recent versions, this feature should work to protect you from malicious sites.

Google Play Protect is Android’s native built-in security feature. Ensure that it is on, “Settings” > “Biometrics and security” > “Google Play Protect”.

# ANDROID PRIVACY SETTINGS (ANDROID 10.0)



## Internet Privacy Settings

Browser history and cookies are tracked when browsing the web from your mobile devices. To ensure privacy, open your browser (Chrome) and tap the three dots in the upper right-hand corner. Tap “History” then “Clear Browsing Data” at the bottom (or top) of the screen. On the next screen, select the applicable boxes (use the below screen shot as an example) and tap the blue “Clear Data” button.

Pay attention to user agreements when downloading new apps. Understand what kinds of information the app wants to access from your device.

You have the option here to tap the drop-down arrow and select a date range of data to be deleted. If you get in the habit of clearing your browser history, cookies, and cache then taking this step will become less important.

## Application Manager

The applications you load access different capabilities on your device, regardless of whether they are active or working in the background. You can see, and to some degree control, what access each application has in the “Application Manager”.

Go to “Settings” > “Apps” and tap the app you want to view.

Then tap “Permissions”.

This will show you what permissions are granted when you accept the user agreement to download the app. In most instances these permissions can be controlled individually.

This only works with apps designed for use specifically with Android. Permissions for older apps or those without full Android functionality can still be disabled, but this could make the app function unreliably.

# ZOOM SMART CARD

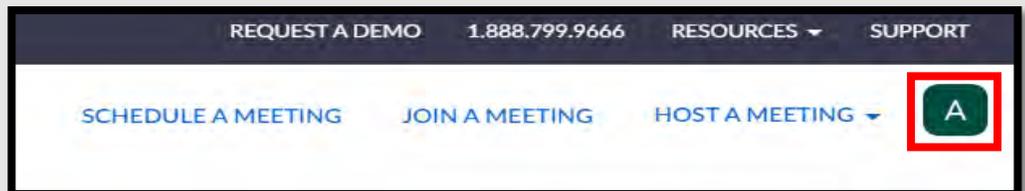
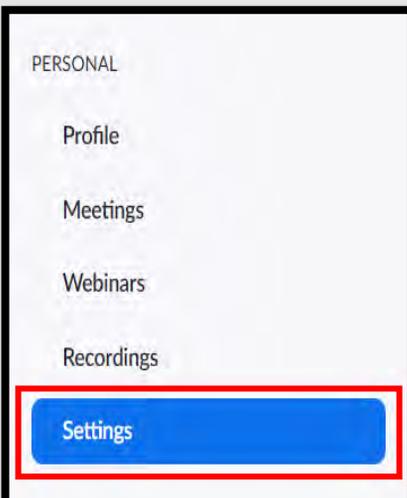


## Do's and Don'ts

- **Do** require a password for all meetings and webinars conducted in Zoom. This will help to minimize intruders from gaining access to your conferences.
- **Do** make sure to control screen sharing capabilities within Zoom. We recommend you never give up control of your personal screen to anyone you are in a meeting with.
- **Do** have all attendees register prior to meeting on Zoom in order to dissuade Zoombombers from entering your meetings.
- **Do** discuss potential security and privacy concerns with your participants or company prior to using Zoom.
- **Do** review updated security notes posted by Zoom.
- Do **not** use video call if it is not required. When possible, it is recommended to refrain from using video conferencing in Zoom. Instead, simply dial into meetings, which limits the information you are required to provide.
- Do **not** allow participants to share their screen during any of your meetings.
- Do **not** forget to lock your meeting once you have confirmed all known participants have entered your meeting domain. Doing so will prevent intruders from gaining access during your meeting.
- Do **not** engage a Zoombomber. It is recommended you lock your meeting to prevent intruders.

Zoom is a U.S. based remote conferencing service utilized by businesses, schools and individuals all over the world. It provides a remote conferencing service that combines video conferencing, online meetings, and a messaging feature. Zoom has recently come under scrutiny for its inadequate privacy and security protocols, most notably its lack of encryption and accidental routing of calls through China. While we do not recommend using Zoom for conferencing, the next several pages show recommended ways to manage the security and privacy settings for Zoom, in case you find yourself needing to use it.

When using video conferencing it is important to remember to check and secure your network connections. #updateandbesafe.



The following steps are for the computer web based application, followed by the Android and iPhone.

Once you are signed into your Zoom account, look to the left of your screen and below "Personal", select "Settings" (shown here highlighted in red to the left). On the screen you will see three tabs; "Meeting", "Recording" and "Telephone". In the "Meetings" tab scroll down until you see the section shown below. We recommend you always authenticate users and require a password when scheduling any meeting.



In response to criticisms of weak security and privacy, Zoom has modified passcode options. Zoom has pre-selected and locked user ability to toggle "Off" passcode options, thus making it more secure for users. We recommend you still verify these options are toggled "On", as shown to the left. The last portion, "Only authenticated users can join meetings from Web client" allows users the option to toggle "On" or "Off". We recommend you keep it toggled "On".

# ZOOM SMART CARD



It is important to think about what people can see and hear when using Zoom. Encourage the use of virtual backgrounds so attendees' personal environments are not shown.

**Require a passcode for Personal Meeting ID (PMI)** 

Only meetings with Join Before Host enabled

All meetings using PMI

**Embed passcode in invite link for one-click join** 

Meeting passcode will be encrypted and included in the invite link to allow participants to join with just one click without having to enter the passcode.

To the left you will see a continuation of the password requirements and recommendations located in "Meeting." We recommend you require meeting attendees to input the provided password and **not** to embed the password into the meeting link. We also recommend you use a "Pre-meeting Password" and not your "Personal Meeting ID".

**Require Encryption for 3rd Party Endpoints (H323/SIP)** 

Zoom requires encryption for all data between the Zoom cloud, Zoom client, and Zoom Room. Require encryption for 3rd party endpoints (H323/SIP).

**Chat** 

Allow meeting participants to send a message visible to all participants

Prevent participants from saving chat 

**Private chat** 

Allow meeting participants to send a private 1:1 message to another participant.

**Auto saving chats** 

Automatically save all in-meeting chats so that hosts do not need to manually save the text of the chat after the meeting starts.

Also, we recommend you use end-to-end encryption whenever possible when using any device that holds your personal information, Zoom is no different.

Note: Zoom's encryption capabilities have been called into question on several occasions. Therefore, we recommend you watch what is documented on Zoom when in a meeting, as the meeting host's encryption may not keep your information secure.

While using chat features on Zoom, we recommend you not allow other attendees to save chats. In order to do this, scroll down until you see "Chat" (shown here to the left). All configurations to the left are recommended for the "Chat" section.

**File transfer** 

Hosts and participants can send files through the in-meeting chat. 

Only allow specified file types 

Scrolling past "Chat" you will find "File transfer" next in your "Meeting" tab. Due to Zoom's lack of acceptable encryption and recent security issues, we recommend you **not** send files of any kind on Zoom.

**Screen sharing** 

Allow host and participants to share their screen or content during meetings

**Disable desktop/screen share for users** 

Disable desktop or screen share in a meeting and only allow sharing of selected applications. 

Next, scroll down to "Screen sharing". We recommend you **not** allow the ability to screen share when in a meeting on Zoom. If you must allow screen sharing, we recommend that users control who can share screens and who can take control of those screens.

# ZOOM SMART CARD



As you continue to scroll down, we recommend you disable the sections “Whiteboard” and “Remote control” (highlighted here in red). It is never recommended that Users give up control of their own computer to any other individual, whether it is a personal computer or company computer.

**Whiteboard**  
Allow participants to share whiteboard during a meeting

**Remote control**  
During screen sharing, the person who is sharing can allow others to control the shared content

**Remote support**  
Allow meeting host to provide 1:1 remote support to another participant.

**Closed captioning**  
Allow host to type closed captions or assign a participant/third party device to add closed captions.

**Save Captions**  
Allow participants to save fully closed captions or transcripts.

**Far end camera control**  
Allow another user to take control of your camera during a meeting.

**Virtual background**  
Allow users to replace their background with any selected image. Choose or upload an image in the Zoom Desktop application settings.

**Identify guest participants in the meeting/webinar**  
Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar. The Participants list indicates which attendees are guests. The guests themselves do not see that they are listed as guests.

Once you have set the above recommendations, continue to scroll down until you find the “In Meetings (Advanced)” section. Here you will find a series of settings that need to be updated/checked to ensure they meet your specific security requirements. However, we recommend meeting attendees **not** participate in any third party activities while on Zoom. We also recommend users **not** allow other users to take control of their camera while using Zoom. Even if you know the individual to whom you are considering giving access, you should **not** allow them control. When setting up a meeting or webinar, it is important to ensure you are able to see “guests” who might be participating for both you and your contacts. If you scroll down, still in “In Meetings (Advanced),” you can enable the “Identify guest participants in the meeting/webinar” (shown to the left).

Now, scroll back to the very top of the screen and select “Recording” from the menu option (shown to the right, selected in blue). Though there are not very many selections to go through, it is still very important to review all your settings here and enable or disable any features you see fit. We recommend you disable most, and preferably all, features located in the “Recording” section. The only exception here would be the very last feature, which is more of a personal preference than a security issue. We recommend you **not** allow anyone to record your meetings.

Meeting **Recording** Telephone

**Recording**

**Local recording**  
Allow hosts and participants to record the meeting to a local file.

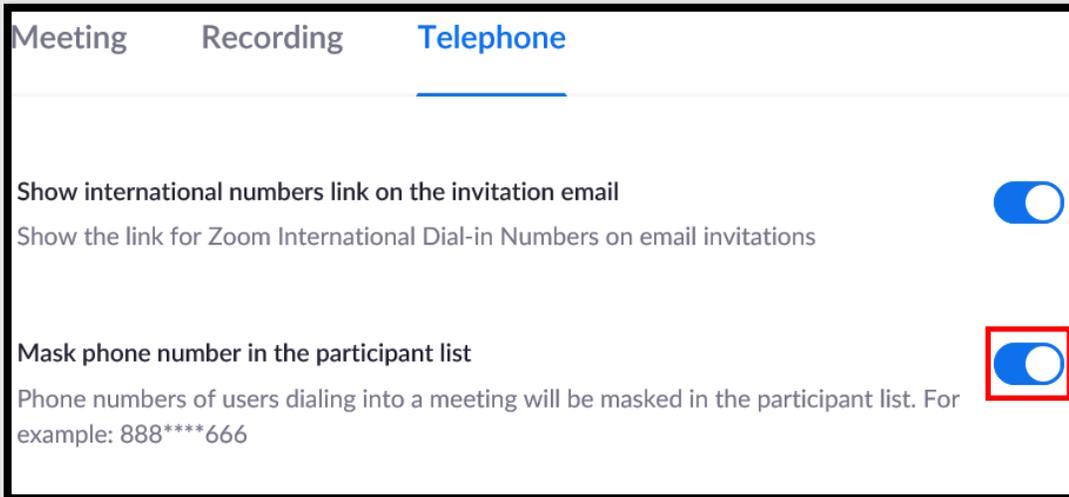
**Automatic recording**  
Record meetings automatically as they start.

**Recording disclaimer**  
Show a customizable disclaimer to participants before a recording starts.

**Multiple audio notifications of recorded meeting**  
Play notification messages to participants who join the meeting audio. These messages play each time the recording starts or restarts, informing participants that the meeting is being recorded. If participants join the audio from telephone, even if this option is disabled, users will hear one notification message per meeting.

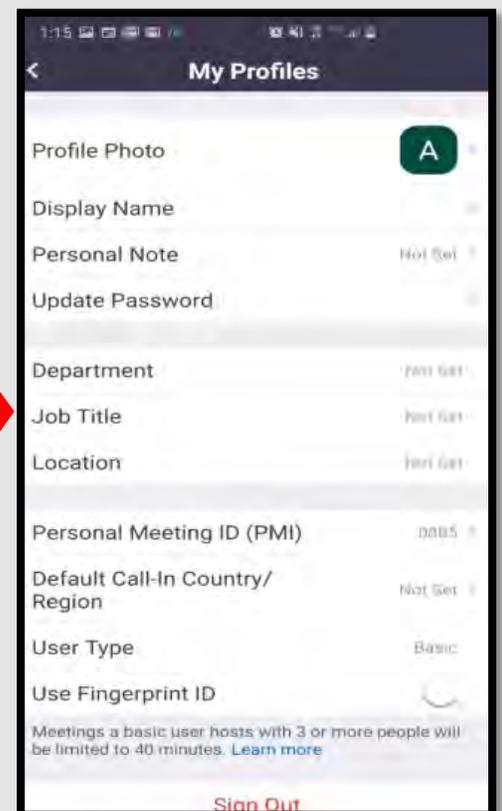
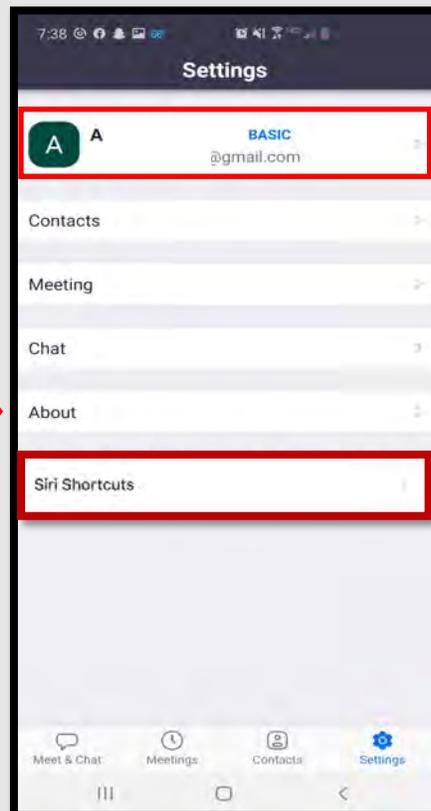
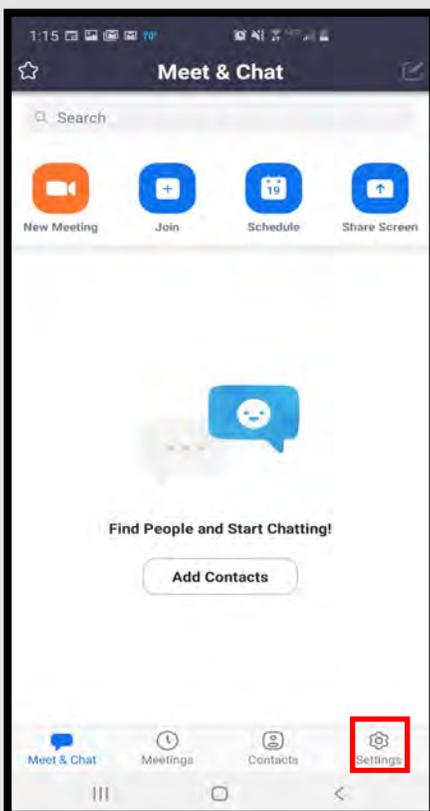
When possible use a Co-Host or an Alternate Host to help monitor activity during your meeting.

# ZOOM SMART CARD



Finally, head back up to the menu and select “Telephone” to review the final settings here. First, we recommend that you mask meeting attendees’ phone numbers. In order to do this, simply toggle the “Mask phone number in the participant list” to enable (shown here to the left highlighted in red).

When using Zoom on your smartphone there are a few security and privacy settings that should be considered for safe use. Though it is not recommended for use on your smart phone, should you chose, there are a few settings to consider here. On both the Android and iPhone, look to the lower right of your screen and select “Settings” (shown below to the left in red). Next, select your name/email from the top of the screen to take you to your profile page. NOTE: iPhone Users, before selecting your name/email you can look to the lower portion of your screen to “Enable” or (recommended) “Disable” any “Siri Shortcuts” related to this application. In your “My Profiles” section, review each individual section and ensure no personal information has been provided. It is recommended you use initials for your “Display Name,” write no “Personal Notes” about yourself and not fill in any other personal information about yourself or the company you are affiliated with unless otherwise directed.



Holding participants in a “waiting room” and approving the connection of each individual gives the host control over who is in the meeting.

# ZOOM SMART CARD



**Do you think your account may have been compromised or hacked? Have you noticed any of the following:**

- ◆ Unexpected calls or messages made or received from your account
- ◆ Any Direct Messages sent from your account you did not initiate
- ◆ Other account behaviors you didn't perform or approve (like following, unfollowing, blocking, etc.)
- ◆ A notification from Zoom stating your account may be compromised
- ◆ A notification from Zoom stating your account information (bio, name, etc.) has changed
- ◆ Your password is no longer working or you are being prompted to reset it. \*If this occurs it is highly recommended you sign-in online and change your password immediately

If you said "Yes" to any of the above, it is recommended you immediately do the following actions:

- ◆ Delete any unwanted messages that were posted while your account was compromised
- ◆ Scan your computers for viruses and malware, especially if unauthorized account behaviors continue to be posted after you've changed your password
- ◆ Make sure to change your password. Always use a strong password you haven't used elsewhere and would be difficult to guess
- ◆ Consider using login verification (if you haven't done so already), instead of relying on just a password. Login verification introduces a second check to make sure you and only you can access your Zoom account. Note: Two Factor Authentication for Zoom ONLY works on the web based app and only if you are an admin or if the admin has set it up for you.
- ◆ Be sure to check your email is secure. It may be worth changing the password to both your Zoom account and the email associated with your Zoom account.

If you need to report a violation of Zoom's Terms of Services follow this link:  
<https://support.zoom.us/hc/en-us/articles/200613919-Report-Terms-Of-Use-Violation>

If you would like to terminate your account follow this link: <https://zoom.us/account>

If you cannot log in to your email account, **Twitter** has provided links to each email account "having trouble signing in" page for your convenience. Please see the **Twitter** smart card for this information.

If you still need help or have questions, you can always contact Zoom using their Support site at: <https://support.zoom.us/hc/en-us/articles/201362003>



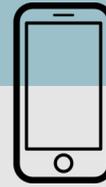
PASSWORD LENGTH	POSSIBLE COMBINATIONS	TIME TO CRACK	
		S - SECONDS M - MINUTES	H - HOURS Y - YEARS
4	45697	< 1	S
5	11881376	< 1	S
6	308915776	< 1	S
7	8031810176	~ 4	S
8	208827064576	~ 1.5	M
9	5429503678976	~ 45	M
10	1411677095653376	~ 19	H
11	3670344486987780	~ 1	Y
*12	95428956661682200	~ 1.5	Y
13	248115287320374E4	~ 39.3	Y
14	645099747032972E5	~ 1,022.8	Y
15	167725934228573E7	~ 26,592.8	Y
16	436087428994289E8	~ 691,412.1	Y
17	113382731538515E10	~ 17,976,714	Y
18	2947951020001390E10	~ 467,394,568	Y

**Important Information Regarding Zoom:**

If your Zoom meeting gets "Zoombombed" there are a few things that can be done. First you can lock them out by going to the "Participants List" in the navigation bar and select "more." Next click "Lock Meeting" to prevent any additional intruders from entering your meeting, which will also allow you to remove individuals without them being able to regain access.

If you are less worried about the intruder and more worried about the disruption follow the same path but to the "Participants List" and scroll down to select "Mute All Controls." This option is not recommended for privacy and security concerns.

# TRAVELING SAFELY WITH SMARTPHONES



## Do's and Don'ts

- ◆ **Do** enable password and fingerprint locks on your device. Also, protect “Settings” changes on your phone by requiring a password.
- ◆ **Do** assume that all information on your device can be accessed remotely. Don't store passwords and sensitive information on your phone
- ◆ **Do** always use complex passwords, the stronger and longer the password the more difficult it will be for someone to hack into.
- ◆ **Do** delete emails that are old or no longer needed prior to travel. Remember emails contain a lot of personal information. Think about what a hacker might gain if they were able to access your email?
- ◆ **Don't** become stagnant upon returning from your travels. Examine your smartphone as soon as you return to your home. If it is acting up or repeatedly making you put your password in there may be malware on your device and you may want to take it in or consider getting a new device.
- ◆ **Don't** link apps and social media accounts together (i.e. using one SM account to login to another). Remember if someone hacks into one of your accounts, it is better if they only get access to that one. Linking accounts together makes all of them vulnerable.
- ◆ **Don't** leave GPS, Bluetooth, and Wi-Fi turned on when traveling. Any of these left on could allow a hacker to connect to your phone if they were able to get within a certain distance from you.

## Wi-Fi Safety Tip

Avoid Public Wi-Fi at all costs, hackers will name the network the same thing as the hotel or other public network. Hackers in Europe have been caught making Public Wi-Fi networks to resemble the public network name. Do not assume all networks are secure, just because it says the name of a company does not mean it is a legitimate network, check with the company to be sure. Also, be sure to turn your Wi-Fi off when you are not using it in order to prevent tracking or hacking of your phone.

## Precautionary Tips

- ◆ Be aware that your phone may be scanned forensically when entering a foreign country.
- ◆ Set your phone to lock automatically and make sure you have a complex password or fingerprint enabled while traveling. This will help to limit an intruders ability to break into your phone if you happen to misplace it.
- ◆ Consider installing a VPN to ensure more secure online activity.
- ◆ Turn off Wi-Fi and Bluetooth when traveling. Only turn these capabilities on when absolutely necessary, then turn them off when done.
- ◆ Purchase SIM Cards for international travel in the U.S. prior to departure. This will ensure not only your security but functionality with your device. If you do decide to use a SIM card make sure to turn off “Auto Sync” to conserve your battery and data plan.
- ◆ Make sure all the software is updated on your phone, this will in turn ensure the most up to date security patches are installed on your device.
- ◆ Make sure to backup all your data before traveling, so that if your phone or data is lost you can easily restore the information and won't be without important contacts and travel information.
- ◆ When feasible, recommend purchasing a pay-as-you-go phone for travel, especially travel overseas. This is probably the single best way to prevent any of your personal information from getting into the wrong hands should you lose the phone.

Traveling internationally can present new problems, ensure you prepare yourself *before* you travel not once you are there.

# IDENTITY THEFT SMART CARD



## Identity Theft Scams On The Rise

**Utility Bill Scam:** As of September 2018, the Federal Trade Commission (FTC) reported an increase in local utility scams. The consumer receives a call from someone posing as a local utility company claiming the consumer has a past due bill. The caller is very convincing, even to a consumer who may have just paid their bill. Oftentimes the caller will threaten to cut off service, hoping this threat is enough to get the consumer to provide personal and financial information, thereby falling for the scam. If you feel a call from someone claiming to be a bill collector is suspicious in any way do NOT settle the bill at that time. You have the right to call the utility company yourself but remember do not use the phone number they provided you, look up the number yourself. Also, report this suspicious activity to the FTC.

*“Do you know what an overdue bill could do to your credit?”*

**Imposter Scams:** Reports of IRS impostors have surfaced during the 2018 tax season. Consumers receive a call from an individual claiming to be an “IRS Officer,” who will then inform the consumer that they owe a large amount of money and if they don’t pay an agreed upon amount immediately local law enforcement will issue a warrant for their arrest. They will often try to “negotiate” a smaller amount to make the consumer feel as if they are getting a deal. Instead of paying with a check or money order, these scammers instruct their victims to buy gift cards and read the numbers to the fake agent over the phone for verification. Remember, no legitimate organization will ever ask for payment in gift cards! Also, report all scams involving taxes or the IRS to the IRS fraud department.

*“Just pay with Amazon gift cards or I will send the police to your house tonight!”*

*“Your Social Security Number was just used in a crime, we can help you”*

**Suspended Social Security Number:** Consumers are reporting a new “government related scam.” The consumer receives a call and is told that their SSN was used in criminal activity. The caller will claim that the SSN has been suspended and they can help the vic-

tim get the situation cleared up. The Social Security Administration does NOT suspend SSNs, ever! Do not give personal information out to callers. If you feel you’ve been scammed, report it to the FTC immediately. Also, personally look up the number of and call the agency the scammer(s) claim to represent. Make a detailed record of the interaction and be prepared to provide as much information as possible.

**Mobile Phone Scams:** This scam was identified when a consumer received an email from their mobile phone provider. The email stated, “Your new mobile phone is on its way” and listed a delivery address that didn’t belong to the consumer, it was actually the address of a local hotel. Further investigation revealed that someone had used a fake identity to obtain the consumers account information and ordered the additional phone on the consumer’s account.

**Report fraud & identity theft scams to the FTC at 1-877-FTC-HELP (1-877-382-4357) or online: [ftc.gov/complaint](https://www.ftc.gov/complaint)**

## 12 Practices to Avoid Identity Theft

1. Do not disclose your full nine-digit Social Security number
2. Avoid paper billing by requesting secure electronic statements instead, or have them mailed to a Commercial Mail Receiving Agency (CMRA)
3. Lock your mailbox
4. Keep your information safe, both online and offline, by shredding documents containing personal information and passwords and protecting sensitive computer files
5. Use unique, hard-to-guess passwords that include a combination of letters, numbers, and symbols
6. Avoid using the same password across multiple accounts
7. Install and update antivirus, anti-malware, and security programs on all computers, tablets, smartphones and operating systems
8. Don’t disclose information commonly used to verify your identity on social network sites such as; date of birth, city of birth, mother’s maiden name, and name of high school
9. Avoid making purchases, paying bills, or sending sensitive information over unsecured WiFi networks
10. Disable Bluetooth on devices when not in use
11. Watch out for “phishing” scams; do not trust unsolicited offers and ads
12. Fight “skimmers” by touching ATMs to see if all the parts are solid and not add-ons, cover the keypad/screen with your hand while typing the password, and always look for suspicious holes or cameras

Phone Scammers will say anything to get you to disclose personal information; always offer to call back on your own

# IDENTITY THEFT SMART CARD



## Preventing Other IRS Scams and Fraud

It is very common for criminals to file IRS Tax returns using stolen identities. The fraudsters will typically file early and claim their tax refunds before the victim is aware. It is only when the victim attempts to file their own, valid tax forms that they are informed a refund has already been issued. Victims of identity theft can request a PIN to prove their identity when they file their tax return.

According to the FTC, identity theft was the top complaint received for the past 15 years, increasing 47% from 2014 to 2015 as a result of a massive rise in tax-related identity theft (see "FTC Releases Annual Summary of Consumer Complaints," March 1, 2016).

## Children also Victims of Tax Fraud and Identity Theft

Increasingly children are becoming victims of identity theft and tax fraud. Criminals will obtain Social Security numbers or will attempt to obtain credit cards in the names of minor children. It is only when parents attempt to obtain legitimate cards for their children that they discover their children have been targeted. To prevent this, parents may place freezes on accounts for their children to ensure no new credit is issued until they are ready.

## What to Do if Your Identity is Stolen

The FTC has put together a great, step-by-step [guide](#) on what to do if you think your identity has been stolen (link below). Here's where to start: <https://www.identitytheft.gov/steps>

**Take action immediately! Keep records of your conversations and all correspondence.**

**Flag Your Credit Reports.** Contact the fraud department of the three major credit reporting agencies. Tell them you are an identity theft victim. Ask them to place a "fraud" alert in your file. An initial fraud alert is good for 90 days.

- ◆ Equifax 1-800-525-6285
- ◆ Experian 1-888-397-3742
- ◆ TransUnion 1-800-680-7289

**Order Your Credit Reports.** Each company's credit report about you is slightly different, so order a report from each company. They must give you a free copy of your report if it is inaccurate because of fraud. When you order, you must answer some questions to prove your identity. Read your reports carefully to see if the information is correct. If you see mistakes or signs of fraud, contact your creditors about any accounts that have been changed or opened fraudulently. Ask to speak with someone in the security or fraud department.

**Create an Identity Theft Report and Report it to the Local Police.** An Identity Theft Report can help you have fraudulent information removed from your credit report, stop a company from collecting debts caused by identity theft, and get information about accounts a thief opened in your name.

To create an Identity Theft Report:

- ◆ File a complaint with the FTC at [ftc.gov/complaint](http://ftc.gov/complaint) or 1-877-438-4338; TTY: 1-866-653-4261. Your completed complaint is called an FTC Affidavit.
- ◆ Take your FTC Affidavit to your local police, or to the police where the theft occurred, and file a police report. Get a copy of the police report.

For more information regarding identity theft, visit the following websites:

Federal Trade Commission (FTC) <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>

FTC Identity Theft Online Complaint Form <https://www.ftccomplaintassistant.gov/>

[www.fraud.org](http://www.fraud.org) (You can also call: 1-800-876-7060)

You can get free copies of your credit report once a year from each agency, get one every four months to monitor your credit

to protect them. Their smartphone is yours for the monitoring, after all who gets the bill? #keepourkidsafeonline

# KEEPING YOUR CHILDREN SAFE ONLINE



- ◆ An April 2015 Pew Research Center study revealed that 92% of teens report going online daily – including 24% who say they go online “almost constantly.” Most of the teens also have used or use a smartphone. A separate study showed that nearly 40% of 3–4 year olds and two thirds of 5-7 year olds go online.
- ◆ Cyber-bullying, malware, and predators are a few dangers that make the Internet an unsafe environment for unsuspecting children. In 2012, the FBI launched Safe Online Surfing (SOS), a challenging but fun and informative game that educates children about online safety. See more at <https://www.fbi.gov/fbi-kids>
- ◆ In half of all sex crimes against a minor involving a social networking site, the social networking site was used to initiate the relationship. 55% of teens have given out personal information to someone they don't know, including photos and physical descriptions. <https://www.guardchild.com/social-media-statistics-2/>
- ◆ 67% of teenagers say they know how to hide what they do online from their parents. 43% of teens say they would change their online behavior if they knew that their parents were watching them.

## Do's and Don'ts

- ◆ **Do** only connect with gamers and online profiles of people you know and trust. Review connections often.
- ◆ **Do** assume ALL information and images you share are publicly viewable, regardless of your settings.
- ◆ **Do** use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- ◆ **Do** tell kids to let parents or responsible adults know anything online makes them uncomfortable.
- ◆ **Do not** use location services.
- ◆ **Do not** add your birthdate, location, phone number, or other personal details to online profiles.
- ◆ **Do not** forget your children have online privacy rights as well. If you are unsure what those rights or laws are you can find them here: <https://www.ftc.gov/consumer-protection/childrens-privacy>

## CONTROL WHAT APPLICATIONS GET INSTALLED ON YOUR CHILD'S DEVICE

One of the best ways to help protect your child online is to monitor what applications they are using. For iOS users it is recommended that parents keep the Apple ID password and not provide it to the child using the device. Also, make sure that the iPhone requires the password before any downloads can take place. This can also be done on your Android devices as well.

### Extras to Help Parents:

Can you set age restrictions on Disney +? The answer is no. You can learn more about this topic here: <https://www.androidauthority.com/disney-plus-parental-controls-1108634/>

Setting up router controls for your kids: <https://kb.netgear.com/25687/How-do-I-set-up-Live-Parental-Controls-on-my-NETGEAR-router-using-the-genie-desktop-app>

Your child's "right to privacy" doesn't supersede your right



Now it is time to give this app another look. YouTube Kids has just pushed their parent-approved content, a control that lets you select every video and channel available to your child. It is available today on Android and coming soon to iOS. In the “Restricted mode”, kids are not able to search for content on their own.

Open settings and scroll down to the bottom just past your child's (or your) profile. Select “approved content only” or “Restricted Mode On.” Next, you may want to also Lock “Restricted Mode” on this browser. “Restricted Mode” lock prevents others from changing the “Restricted Mode” settings on this browser.

<https://www.youtube.com/yt/kids/>

# KEEPING YOUR CHILDREN SAFE ONLINE



## Security Applications

A variety of paid software packages are available for monitoring your child's online activities. The following packages are effective tools for monitoring or preventing access to certain online content.

### Blocksi Web Filter

Blocksi Web Filter is a web filter and parental control extension for Google Chrome. It can be configured to protect your family from inappropriate content on the Internet.



### Microsoft Family Safety

Microsoft family is a free service that helps families stay connected, and keep kids safer on Windows 10 and Xbox One devices, along with Android devices running Microsoft Launcher. You'll find settings like activity reporting, screen time limits, location sharing, and content restrictions on [account.microsoft.com/family](https://account.microsoft.com/family), where you can also track kids' spending and add money to their Microsoft accounts.

Google has its own Safety Center to help ensure your kids remain safe Online, stay up to date at [www.google.com/safetycenter/families/start/](https://www.google.com/safetycenter/families/start/) #themoreyouknow



**Net Nanny**

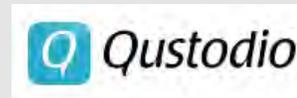
Net Nanny Social lets you keep track of all your children on social media including Facebook, Twitter, Google+, Instagram, Pinterest, and LinkedIn. Features include:

- Detects registered accounts any new accounts created
- Ability to identify cyberbullying, cyber-stalking, or grooming
- Access to view photos and videos child has published
- Alert Notifications
- Daily/Weekly Reports



Monitor your child's cell phone use, including call logs, texting, photos (MMS), web history, web filtering, time restrictions, sync contacts and block applications. Receive real time alerts when a stranger contacts your child. Must be installed on your child's phone.

- Monitor your child's cell phone use
- Includes Web filtering, time restrictions, app blocking, and more
- Get real time alerts when a stranger calls the child's phone
- Location Tracking! Track up to 99 locations and know exactly where your child is at any time.
- DailyWatch Summaries! A daily breakdown of your child's activity conveniently packaged and sent to your email.



Free parental control app that offers simple tools to manage kids' screen time, filter content and monitor or block apps kids use. Premium features include:

- SMS Messages & Call Tracking
- Location Tracking & Panic Button
- Ability to view social media activity including Facebook, Twitter, Instagram, and Whatsapp
- Block pornography
- Set multi-device time limits
- Control games and apps
- Browser-independent content filter that handles HTTPS traffic



### Family Premier

Includes support across Windows, Android and iOS devices (no MAC support):

- Web supervision that allows warnings, blocking, or monitoring of sites based on your own site category choices
- Video tracking
- Control SMS contacts on Android
- Email Alerts
- Online time limits
- Activity Tracker to view device Internet history
- Location tracking to know where your child is at any time

# PHOTO SHARING SERVICES CARD



## Do's and Don'ts:

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li>• Do share photos only with known and trustworthy people.</li> <li>• Do use caution when posting images and videos of you or your family. Be aware of your surroundings, to include identifiable locations and any other personal security vulnerabilities.</li> <li>• Do ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose personal data.</li> </ul> | <ul style="list-style-type: none"> <li>• Don't tag geolocations. The information in these tags can disclose location of where the photo was taken.</li> <li>• Don't give apps permissions to access the cellphone location services.</li> <li>• Don't post photos of others, especially children, without getting permission beforehand.</li> </ul> |
|---|---|

Choosing the right photo sharing service will depend on intent and audience. Key questions to ask:

- ◆ Are you sharing photos primarily for yourself, your friends and family, or for public consumption?
- ◆ Are your contacts and viewers already using a specific service?
- ◆ How much control and privacy do you want over your images? Is the retention of EXIF data problematic?

Although photo sharing services allow you to remove images, not all of them allow you to delete your account. Deleting content and/or account does not ensure removal from the internet or the service provider's systems. Those with access to the photos on a photo sharing service can acquire and redistribute photos as they please. You can find more detailed information on how to set privacy settings for these Services on the following pages.

## 6 Popular Photo Sharing Services

Service	Primary Use	Image Privacy Options	Retains EXIF	Geo-Location Options (non-EXIF)	Allows Reposting	Populates in Google Searches (Indexed)
Instagram	Share photos and videos from camera enabled mobile devices	<b>Public</b> ; Private (other users must request to follow you);	No	GPS-based device location and customizable location (both removable)	Yes, only with third party applications	Profiles are indexed, but not photos
snapchat	Share photos and videos that "disappear" after a certain number of views or a period of 24 hours.	<b>Public</b> ; Private (other users must request to follow you)	No	Snapchat Geofilters use location services on your mobile device. Using Geofilters is optional.	No. Please note that viewers can still screenshot your Snaps.	No
facebook	Social network	<b>Public</b> ; Only Me; Friends; Friends of Friends	No	Free-form text; location suggestions; map-based (removable)	Yes	Public profiles are indexed
Google Photos	Photo and video sharing and storage service	<b>Private</b> ; Shared Albums allow anyone with the unique web link to view your photos	Yes	GPS-based from camera and Google's Estimated Location (both can be disabled in the phone settings)	Yes, photos can be downloaded from a Shared Album.	Shared photos may possibly be open to public search in the future
flickr	Photo and video hosting site used for sharing and embedding on blogs and social media	<b>Public</b> ; Only You, Your Friends, Your Family	<b>Yes for original uploaded file (not for resized file)</b> ; You can also hide EXIF data	Editable location; map-based (both removable)	Yes	Public albums are indexed; Offers opt-out for 3rd party searches
photobucket	Photo and video hosting site used for sharing and embedding on blogs and social media	<b>Public</b> ; Private (optional password protection)	Yes for original uploaded file (not for resized file)	Location data is available unless you disable it	<b>Yes</b> ; No	Public albums are indexed

\*Default settings are in **bold**.

\*\*Converting a photo to PNG file format will remove EXIF data.

# PHOTO SHARING SERVICES CARD

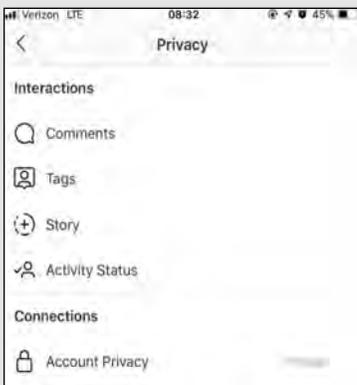


## EXIF Removal Tools

- ◆ **EXIF Wizard:** <https://itunes.apple.com/us/app/exif-wizard/id387652357?mt=8>
- ◆ **TrashEXIF:** <https://itunes.apple.com/us/app/trashexif-metadata-photo-remover/id585543219?mt=8>
- ◆ **ACDSee Photo Software:** <http://www.acdsee.com/>
- ◆ **Paint Shop Pro Photo Software:** <http://www.paintshoppro.com/en/>

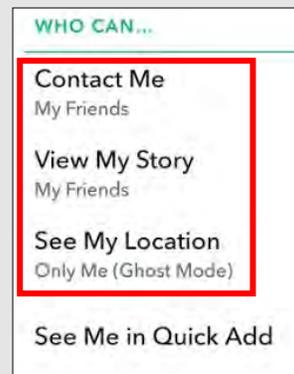
*For more information, please see the EXIF Data Smartcard*

## Privacy Settings

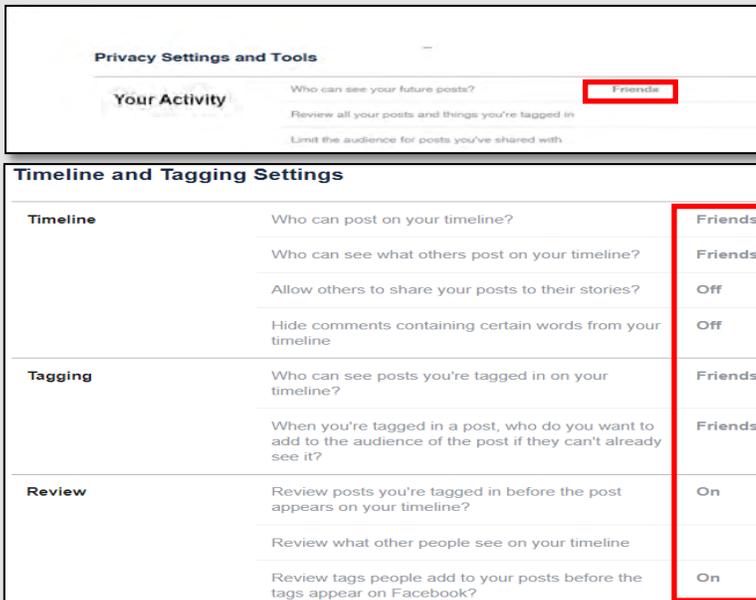


Tap on the bottom right. Then tap the menu icon at the top right. Tap at the bottom of the screen. Scroll to find "Privacy" and then "Account Privacy," make sure the toggle is on for "Private Account".

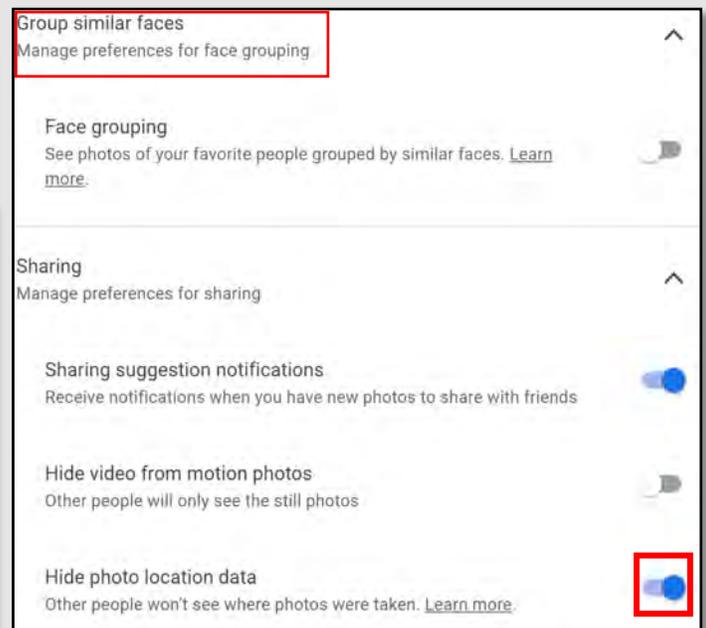
When your account is private, only people you approve can see your photos and videos.



Tap at the top. Tap to access Settings. Scroll down to the "Additional Services" section. Set each category except "See My Location" to "My Friends". Set "See My location" to "Only Me (Ghost Mode)".



From your smart phone, tap the at the top right corner. Select "Privacy" then "Settings". Navigate to "Privacy Settings and Tools" and "Timeline and Tagging Settings" to adjust who can see your posts and pictures.



At the top of the page select to select "Settings". Ensure that the toggle is *on* for "Hide photo location data" from the Share section. Ensure that the toggle switch is *off* for "Group similar faces".

Android devices typically automatically backup photos with your EXIF data, so be sure to check your settings! #KeepGoogleInCheck

# PHOTO SHARING SERVICES CARD



## Privacy Settings Continued



For a comprehensive Flickr security walkthrough, visit the following URL:  
<https://safety.yahoo.com/SafetyGuides/Flickr/index.htm>

Tap the  at the top right corner.  
 Tap "Settings".

Tap the "Privacy & Permissions" tab and use the image to the left as an example for your security settings.

Now tap on the "Sharing & Extending" tab.

Make sure you do not have any third party applications such as Twitter or Tumblr linked to your Flickr account. You should see a message like the one outlined in red below.



### Account Settings

[Personal Information](#)   [Privacy & Permissions](#)   [Emails & Notifications](#)   [Sharing & Extending](#)

#### Global settings

Who can download your images (including originals)?	Only you
Largest shared image size	Best display size
Allow others to share your stuff	No
Who can add you to a photo?	Only you
Allow your stuff to be added to a gallery [?]	No
Hide your EXIF data [?]	Yes
Hide your stuff from public searches [?]	Yes, on flickr.com and 3rd-party sites
Hide your profile from public searches	Yes
Who can see what on your profile	<ul style="list-style-type: none"> <li>Email address: Only you</li> <li>Real name: Your friends and family</li> <li>Current city: Your friends and family</li> </ul> <a href="#">Edit your IM names, real name, or current city</a>
Show autotags [?]	No

#### Defaults for new uploads

Who will be able to see, comment on, add notes, or add people	<ul style="list-style-type: none"> <li>View: Only you</li> <li>Comment on: Only you</li> <li>Add notes, tags, and people: Only you</li> </ul>
What license will your content have	All rights reserved ©
Who will be able to see your stuff on a map	Only you
Import EXIF location data [?]	No
What Safety Level and Content Type will your photostream have	<ul style="list-style-type: none"> <li>Safety level: Safe</li> <li>Content type: Photos</li> </ul>

#### Content filters

Search settings	<ul style="list-style-type: none"> <li>SafeSearch: On</li> <li>Content type: Photos / Videos</li> </ul>
-----------------	---

### Your account

[Personal Information](#)   [Privacy & Permissions](#)   [Emails & Notifications](#)   [Sharing & Extending](#)

Account links

You have no third-party applications linked to your account, but here are some you might like to try

With proper security settings Flickr is a great web-based photo storage service, with 1 TB of free storage. #SecureMemories

# PHOTO SHARING SERVICES CARD



## Privacy Settings Continued



Many photo sharing apps encourage you to link other social media accounts, but with convenience comes increased risk.

### Privacy

Personal
Albums
Privacy
Apps
Notifications
Mobile
Account

**Followers**

Allow others to follow me. You currently have no followers.

**Content Privacy**

Allow others to copy, download and/or print my photos & videos

Allow comments in my albums

Show where my photos were taken

When I upload, permanently remove information about where my photos were taken

**File Name Scrambling**

To protect your privacy, we recommend that you select the options to scramble both future and past upload file names. However, if you intend for your photos to be public or used for business purposes, we recognize that you may not want to scramble.

**For Future Uploads**

(Recommended) During upload, scramble file names to make links hard to guess

**For All Previous Uploads**

Scramble File Names

Scrambling file names changes links. You will need to re-establish published links once the scramble is complete.

Save Cancel

**Album Privacy**

Make All Public
 Make All Password Protected
 Make All Private

Tap the at the top right corner.

Tap "Settings".

Tap the "Privacy" tab and use the image to the left as an example for your security settings.

Then tap the "Apps" tab.

Make sure you do not have any third party applications such as Twitter or Facebook linked to your Photobucket account.

**Safety Fact:** Although it is possible to set Photobucket albums to "private," this does not prevent the photos within being accessed by someone who knows or can guess the URL. Internet programs, such as Fusers, have been created that can identify URL patterns and test for working photo URLs. This allows "private" photos on Photobucket being downloaded and distributed elsewhere on the Internet without the consent of their uploaders.

Photobucket monitors suspicious activity to prevent software from guessing URLs and downloading photos. It is recommended that Photobucket users scramble the links to photos and videos, and select the option to scramble the links of both past and future if there is no need to preserve the original file names.

### Applications

Personal
Albums
Privacy
Apps
Notifications
Mobile
Account

**Connected Services**

Connect your social profiles to Photobucket for quick sharing and for finding friends.

Facebook

Connect

Twitter

Connect

# SMARTPHONE EXIF REMOVAL SMART CARD



## EXIF Data

EXIF—Exchangeable Image File Format—is a standard format for capturing, storing and exchanging image metadata. Metadata is the description and context of files that allows computers to organize, find, and display information about a file. For example, when a music app displays the artist, year, album, and song name of an mp3 being played, it uses the mp3s metadata to display that information. Images and videos also contain metadata that can show time, date, camera settings, copyright information, and location. Some social networks and photo-sharing sites, such as Flickr, Google+, and Dropbox, have features that display EXIF data alongside images. Facebook, Instagram, Twitter and Reddit, do not share EXIF data publicly, but may use the information internally. EXIF metadata are listed as tags that store information that can be used to identify an individual. The chart below shows the tag categories, the metadata included in each category, and the potential security risks associated to each piece of metadata.

Tag Category	Important Tags	Security Implications
<b>Geo-location</b>	GPSLongitude, GPSLongitudeRef, GPSLatitude, GPSLatitudeRef, GPSDateStamp, GPSTimeStamp, GPSAltitude, GPSAltitudeRef, GPSProcessingMethod	Ability to reveal the exact location of private places, such as homes or offices. Some photosharing sites, including Google+ and Flickr, publicly display image GPS coordinates on a map.
<b>Timestamps</b>	ModifyDate, DateTimeOriginal, CreateDate	Creates a log of behavioral patterns and personal timelines.
<b>Camera</b>	Make, Model, Serial Number	A unique serial number identifies the particular device for an image or set of images.
<b>Authorship</b>	Artist, Owner Name, Copyright	Links images with a name or organization.
<b>Image Summary</b>	ImageDescription, UniqueImageID, UserComment	Potentially reveals identifying information about the content of the images, such as captured persons or locations.

### Do

- ◆ **Do** prevent your device(s) from capturing geo-location data when taking pictures. Remove EXIF metadata from images taken by smartphones or digital cameras.
- ◆ **Do** use privacy settings from the app to limit the audience to only yourself or close friends and family, before uploading pictures.
- ◆ **Do** assume that anyone can see, copy, or forward photos that are posted online. Even with no EXIF data, the content of images may contain identifying information, including people and locations.

### Don't

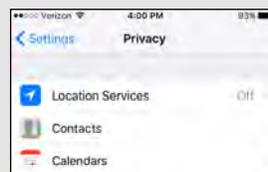
- ◆ **Don't** allow apps to automatically upload and share captured images (e.g. Instagram, Flickr).
- ◆ **Don't** assume that device settings remain the same after updates or over time. Verify the settings frequently.
- ◆ **Don't** upload pictures with landmarks, easily identifiable structures, or signs indicating location.
- ◆ **Don't** give apps used for sharing photos permission to access your device's location or other information.

## Prevent the Capture of Geolocation Data

### iOS

If iOS location services are turned off, images captured with the native iPhone camera app will not contain geo-location EXIF data.

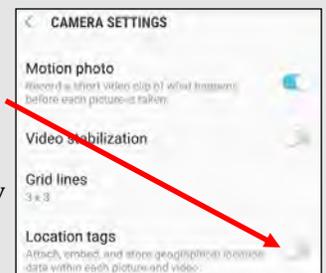
- 1 Select the "Settings" app. Click "Privacy" > "Location Services".
- 2 Turn off location services altogether or for the iPhone's camera applications.
- 3 Return to the "Settings" app. Click "Privacy" > "Photos".
- 4 Disable permissions for other apps to have access to the photos stored in the device's camera roll.



### Android

Turning off location storage in the Android camera application prevents captured images from containing EXIF data.

- 1 Open the camera app and go to "Settings" by tapping the gear icon. This varies from phone to phone since there is no standard camera app on Android devices.
- 2 After that, scroll down until you see 'location tags' and touch the toggle switch to disable geotagging of photos. The wording may vary slightly between devices.



Twitter doesn't share your EXIF data, but it will geo-tag your post if location services are enabled. #DisableLocationServices

# SMARTPHONE EXIF REMOVAL SMART CARD



## Prevent the Capture of Geolocation Data Continued

- ◆ Taking a screenshot of a photo on a device running iOS or Android will create a new image containing no EXIF data. To take a screenshot on an iOS device, simultaneously press the lock and home buttons or google how to take a screenshot on your specific android.
- ◆ Even photos taken in airplane mode contain geo-location data. It is recommended to turn off location services/storage on your smartphone camera application, as shown on the previous page.
- ◆ Remember that uploading or sharing a lower quality image will contain EXIF data. EXIF data and image quality have no correlation.
- ◆ It is important to not only lock down Apps such as Snapchat, Instagram and Twitter (see corresponding Smartcard), but to also remove the meta data from them as best as possible.

## EXIF Removal Apps and Programs

### Reviewing & Removing EXIF Data for iOS

- 1 Download the free US-based Photo Investigator app from the App Store.
- 2 Open the app and tap the gallery icon on the bottom left.
- 3 To view EXIF data, you can tap on the various icons below the image.
- 4 To remove EXIF data tap "Metadata" and then select "Remove".



An easy way to identify photos that have EXIF data with geolocations is to view your "Places" folder. Any images that appear in this folder have geolocation data, once you disable the geotagging feature and remove your EXIF data, this folder should be empty.

5

### Reviewing & Removing EXIF Data in macOS

Use the Image Optim (UK based) application (available at <http://imageoptim.com/>) to remove EXIF data on your OS X device.

- 1 Drag the photos for EXIF removal into the app window and wait for a green check mark to appear next to the file name.



- 2 Check that the EXIF data has been removed by right clicking the image and selecting "Get Info". EXIF data is listed under "More Info".

### Metadata Remover for Android

Metadata Remover is a free US-based app that deletes all EXIF data from image files stored on your Android device.

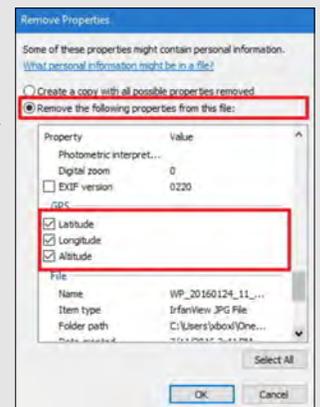
- 1 Download a Photo Exif Editor app from the Play Store.
- 2 Open the app and select an image.
- 3 The EXIF data will be removed.
- 4 Processed images will be saved separately from the original file.



### Reviewing & Removing EXIF Data in Windows

Use the Windows OS to verify EXIF data has been removed.

- 1 Navigate to an image in File Explorer. Right click the image and select "Properties".
- 2 Select the "Details" tab. You can examine EXIF metadata that is available.
- 3 Click "Remove Properties and Personal Information".
- 4 You can click "Create a copy with all possible properties removed" to remove all potential properties or select individual properties such as GPS information. Click "OK".



## Geo-localization

Even with EXIF metadata removed, images containing vegetation, addresses, business names, road markings, and landmarks allow someone to identify the location a photograph was taken. Geo-localization, the determination of a location of an image through visual information, is currently being developed. This will allow computers to compare a picture without EXIF metadata to millions of other picture found on the internet that do have location metadata. Once the computer discovers a close match between two pictures, it can apply the location metadata of one picture to its match that does not have location metadata.

# LOCK DOWN YOUR LAPTOP SMART CARD

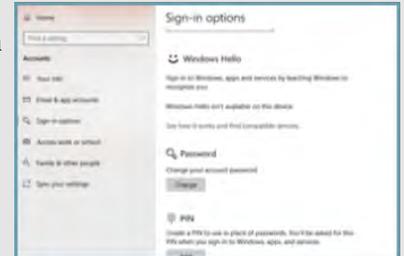


## Creating a Windows Log-in Password

Although a log-in password won't protect against a competent hacker, it can be enough to dissuade unsophisticated criminals from snooping through your personal files and accessing your online accounts. Protecting each account (Guest, Admin, and User) with different passwords helps prevent a hacker from getting access to everything on your computer should they gain access to any one account. It is recommended you create and use a "User" account, not the "Admin" account for all daily activity. This way hackers would be limited in the damage they can do to your computer.

Windows 10 offers a number of enhanced log-in and security features.

Navigate to **Start Button > Settings > Accounts > Sign-in Options** to setup your 'Sign-in Options'.



## Practical Password Tips

If you have files on your computer that you don't want anyone else to access, you can use password-protected file or folder encryption to keep them safe. However, encrypted files are only as secure as the strength of the password protecting them.

For this and the rest of your security measures to be maximally effective, make sure you follow these simple password rules:

- ✓ Use a password that's at least 12 characters long and includes a mix of lower and upper case letters, symbols, and numbers. Try not to use complete words, but if necessary avoid common words that can be found in a dictionary. Not all devices, systems, or accounts allow these combinations, but do what you can within the available options.
- ✓ Avoid sharing passwords across multiple platforms, especially for sensitive accounts like a Windows logon, bank account, and email account.
- ✓ Change your passwords frequently - every 6 months for important passwords, at a minimum.

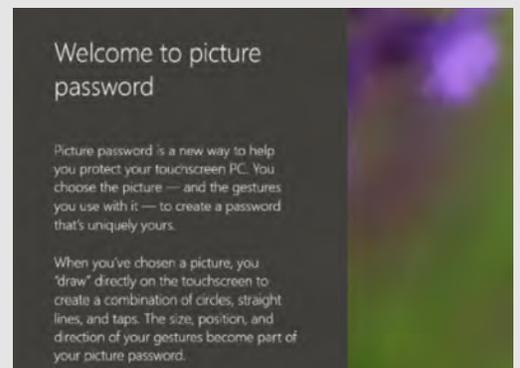
## Additional Security

Windows 10 also has a number of additional log-in security features. At the "Settings," "Accounts" and "Sign-in Options" menu you can select "Picture Password" to enable secure log-in based on your unique mouse movement responses.

**Note: You can use a PIN to sign into Windows, apps, and services. However, this option is not as secure as the "Picture Password."**

Windows 10 also has a feature which allows you to pair your laptop with a Bluetooth-enabled device and automatically lock your computer once the device is out of range. You can enable this feature from the "Settings," "Accounts" and "Sign-in Options" menu by pairing your laptop to a Bluetooth device with the "Dynamic Lock" slider.

For personal accounts you can also enable two-factor authentication (2FA). 2FA requires users to authenticate access through a supported device, i.e. a text to a phone number or an email to a backup address, before accessing an account.



## Encryption Basics

Some versions of Windows 10 allow users to easily encrypt file, folder and hard drive data with BitLocker protection. To access BitLocker, navigate to "Control Panel", "System and Security" and select the BitLocker slider or "Device Encryption" to secure your hard drive data. Some newer devices are encrypted by default, which may be the case if you are unable to locate a Bitlocker option on your device. If you'd rather use "on-the-fly" software to lock certain files or folders, you can also use a number of Freeware (Free Software) encryption services such as VeraCrypt, AxCrypt, GNU Privacy Guard, or 7-Zip. You can find these tools and other simple encryption tips at: [lifehacker.com/five-best-file-encryption-tools-5677725](http://lifehacker.com/five-best-file-encryption-tools-5677725)



# LOCK DOWN YOUR LAPTOP SMART CARD

## Virtual Private Network (VPN)

A Virtual Private Network (VPN) connection is the safest way to connect to the Internet and also safeguard your information.

Unsecured networks present a major threat to your personal information, especially when using your device on a public WIFI network. When connecting to public WIFI, we don't know who else is on the local network, which leaves our personal data vulnerable to snooping. Even when connecting to the wider web, our data is increasingly collected, inspected and exploited.

One sensible solution is to use a VPN. We recommend using a VPN whether you are connecting to the internet from home (even with a secure WIFI connection) or in public. This is simply the most secure way to access the Internet.

### VPN For Beginners

When you connect to a VPN, you access a site or service directly from your laptop, which acts as a secure launchpad into the World Wide Web. Once connected to the service, your data is encrypted and sent to a third-party server. There it is combined with other traffic before being integrated into the "normal" traffic flow on the World Wide Web. Since your information is jumbled up with other information, it becomes difficult to identify as *your* specific information, it is like a needle in a haystack.

### A Few VPN Perks

-  VPN services are cheap, with some starting around \$5 per month.
-  A VPN can help protect your data from identity theft and fraud.
-  VPN providers often allow users significantly increased privacy protections from advertisers and hackers alike.
-  VPN providers allow you to enjoy services that require connections from certain countries, regions or time zones.
-  If your Internet Service Provider blocks some applications, such as Skype or other VoIP (Voice over Internet Protocol) applications, use of a VPN may help.

### Where To Find VPN Services

Not all VPN services are created equal. Depending on your typical Web usage, you will want to shop around for a service that fits your profile. If you need a fast connection for rapid-fire browsing or streaming services and your VPN provider doesn't have enough servers, you may experience poor Internet speeds or be unable to make a connection at all. Others might offer some privacy protections but require you to give up some control of your anonymity.

Before subscribing to a VPN service, be sure to look at reviews. The VPN market is competitive and expanding which means VPN providers often offer free trial periods to new users.

For additional information on current VPN providers see: [www.pcmag.com/article2/0,2817,2403388,00.asp](http://www.pcmag.com/article2/0,2817,2403388,00.asp)

#### Sources

- <http://www.pcworld.com/article/2025897/a-road-warriors-guide-to-locking-down-your-laptop.html>
- <https://www.umass.edu/it/support/security/laptop-mobile-device-physical-security-dos-donts>
- <http://www.pcworld.com/article/2308725/encryption/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html>
- <http://www.lehman.edu/itr/documents/computer-security-dos-donts.pdf>
- [http://www.pcworld.com/article/223044/vpns\\_for\\_beginners\\_to\\_experts.html](http://www.pcworld.com/article/223044/vpns_for_beginners_to_experts.html)
- <https://laptop.ninja/5-dos-and-donts-for-laptop-owners/>
- <https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up>

# SECURING YOUR HOME WIRELESS NETWORK



## Best Practices

- ◆ Create passwords that are sufficiently long and complex to include; upper and lowercase letters, numbers, and symbols. Consider a multi-password phrase that does not consist of dictionary-based words. An example would be ILuvF00tb@77 from the phrase “I love football.”
- ◆ Use a cable to directly connect any stationary computers / devices to your home network to limit vulnerabilities presented by wirelessly connected devices
- ◆ Turn off your wireless network when you will not be using it for an extended period of time.
- ◆ If you have guest-access set up for your network, ensure that it is also password protected.
- ◆ If possible, turn on automatic updates for your network device’s firmware. If they are not offered, periodically check for firmware updates on the network devices’ website(s) and manually download and install them.
- ◆ If your router is compromised or if you cannot remember the password, you can restore it to the default factory settings by pressing the reset button usually located on the back of the router.
- ◆ Position the router away from windows and as far into the interior of your house as possible to limit the range of the WiFi signal outside your home.

## Glossary of Commonly Used Terms

<b>Wireless Router</b>	Physical hardware that allows users to connect their devices to a shared internet network.
<b>Service Set Identifier (SSID)</b>	Public name of a wireless network.
<b>Pre-Shared Key (PSK)</b>	Authentication mechanism that mandates a password. Adds additional security to wireless networks.
<b>Hypertext Transfer Protocol Secure (HTTPS)</b>	Uses various encryption protocols to add additional security to HTTP.
<b>Media Access Control (MAC) Address</b>	Unique, individual identifier assigned to computers and devices.

Wi-Fi Security Level	Level of Security	Explanation
WEP	Low/Risky	Old encryption protocol. No longer considered a standard. Highest risk next to an “open” network.
WPA	Low-Moderate	Older encryption protocol. Better than WEP but should not be used when more modern encryption (WPA2) is available.
WPA2	Moderate-high	WPA2-PSK (AES) is the most secure option which uses the latest Wi-Fi encryption.
WPA3	High	Approved and replacing WPA2 by the end of 2018, as the new and more secure option for Wi-Fi Security.

## Accessing Your Router

In order to change your WPA2 password you will need to access your router. In order to access your router, you must enter the appropriate IP address, username, and password. If you do not have this information, your Internet Provider should be able to provide it to you.

It is **important** to understand that when your internet is being set up by your Internet Provider, they are not required to set it up using WPA2 (see the chart to the left). Recommend you ensure they set it up for you and provide the IP address for the router’s settings. That way, once they leave you can change the user name and password.

When changing your username and password for the WIFI, it is important to consider the following: choose a username that does not include you or your family members’ names; create a password that is long and complex. Lastly, it is important to change any “Guest Account” password to something other than your “Admin/Family Account” password.

Passwords provided by your internet provider are general in use; it is a good idea to change the password after everything is set up. #keepyourhomeseecure

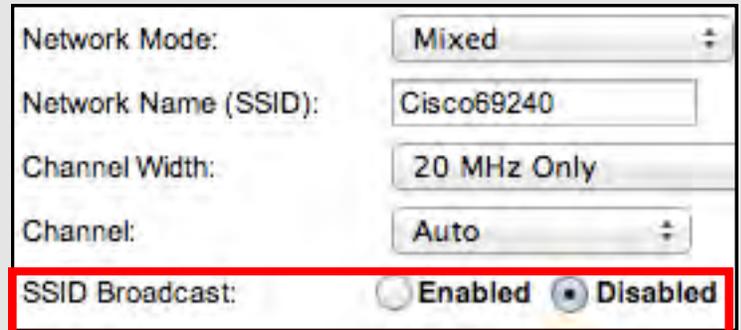
# SECURING YOUR HOME WIRELESS NETWORK



## Creating a Unique SSID



## Disabling the SSID Broadcast



When creating a name for your Wi-Fi (your SSID), it is important to consider who will be seeing it and what information it may give away about you and your family. For instance, if you decide to give it the family name (last name and perhaps number of family members), then anyone within range will be able to see your last name and likely piece together what the numbers represent. Alternatively, if you name your SSID “FBI Van,” that may call attention to your specific network and entice nefarious individuals into attempting to hack into it. It is recommended that you choose a name for your SSID that is generic in nature, providing no information about your family, address, date of birth, etc.

If you would like to hide your SSID so that it does not broadcast to the public, you can do so by scrolling down from where you created your SSID name till you find what’s pictured above. Note that, while it is nice to be able to disable the broadcasting of your SSID, it can be “unhidden” by any individual requesting “hidden Wi-Fi’s”.

**Children’s Learning Devices:** If you have smaller children in your home who have devices like the Leapfrog or Vtech games, and you disable your SSID broadcasting, these devices will not be able to locate your WIFI network and connect to the internet. In order for these devices to connect, you need to go back into your router settings and “Enable” the broadcasting of your SSID.

## Router Firewall

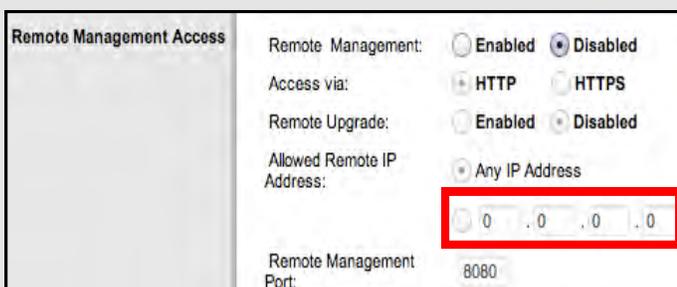


The next two settings are usually found in “Router Settings” but you may have to look around a bit to find them.

A “Firewall” is a layer of security between your home network and the Internet. Since a router is the main connection from a home network to the Internet, the firewall function is merged into the router. Every home network should have a firewall to protect its privacy.

A firewall does not secure against every kind of attack. For example, you still need to run a virus-checker on all your computers.

## Remote Access



Check that the Remote Management IP Address is set to **0.0.0.0** to ensure that remote access is disabled. This will help to ensure that others cannot access your router remotely and without your permission.

Even if you have set up WPA2-PSK on your Wi-Fi it is still very important to have a virus and malware protection for your computer. #cybersecurity

# SECURING YOUR HOME WIRELESS NETWORK



Routers need to be updated. We tend to take our Wi-Fi for granted, but just like taking the car in for an oil change we need to patch routers routinely. #themoreyouknow

## Enabling HTTPS

HTTPS is a variant of the standard web transfer protocol (HTTP) that adds a layer of security on the data in transit. HTTPS enables encrypted communication and secure connection while on the internet. It is used by websites to provide enhanced security for customers OR financial transactions OR where personally identifiable information (PII) is shared. Enabling HTTPS on your servers is a critical step in providing security for your web pages. It is recommended that you enable HTTPS in order to further protect you and your family while navigating the internet.

## Wireless MAC Filtering

MAC address filtering allows you to define a list of devices' MAC addresses so that only those devices can access your Wi-Fi. In order to do so, follow the steps below:

Add the MAC address of each device you want to authorize access to your network (as highlighted above). Next, enter the MAC address and a brief description of the connected device for filtering. Finally, enable MAC address filtering to ensure that only approved computers and devices can connect to your router (as highlighted in the box to the right). Click the 'Add' button when done entering authorized devices.

Wireless Client List			
MAC 01:	00:00:00:00:00:00	MAC 17:	00:00:00:00:00:00
MAC 02:	00:00:00:00:00:00	MAC 18:	00:00:00:00:00:00

## Encryption

Between the optional WEP, WPA, WPA-PSK, WP2, and WPA2-PSK algorithms, you should select WPA2-PSK and also AES (a cryptographic cipher that is responsible for a large amount of the information security that you enjoy on a daily basis) for encryption. The PSK password should be long and complex, but different from the administrative router-access password.

## Useful Links

### Practically Networked

[www.practicallynetworked.com/support/wireless\\_secure.htm](http://www.practicallynetworked.com/support/wireless_secure.htm)

### Wi-Fi.org

[www.wi-fi.org/discover-wi-fi/security](http://www.wi-fi.org/discover-wi-fi/security)

# DELETE BROWSER ARTIFACTS SMART CARD

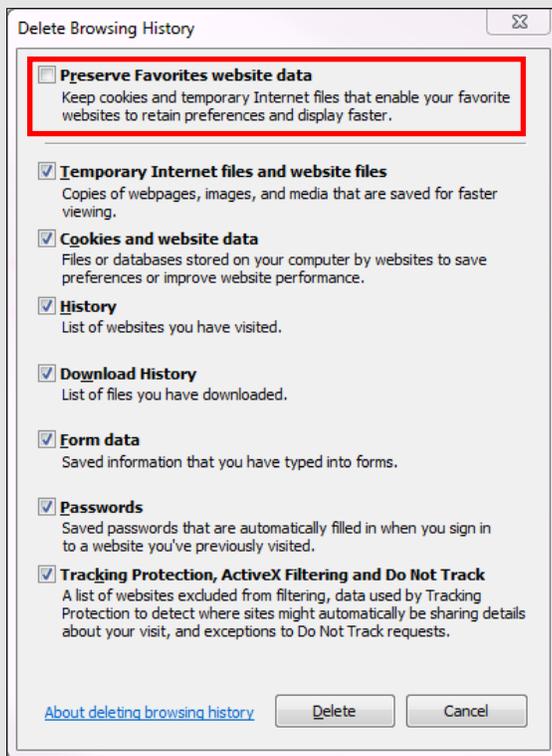


## Browser Artifacts—Cookies, Cache & History

Information such as browsing history, cache, and cookies are saved on your computer while you surf the Web. They are used in various ways to improve your browsing experience. These private data components, while resulting in conveniences such as faster load times and auto-populated fields, can be used by nefarious actors. Whether it be the password for your email account or your credit card number and address, much of the data left behind at the end of your browsing session could be dangerous in the wrong hands. In order to protect yourself, we recommend you delete these artifacts on a regular basis.



### Deleting Internet Explorer Web Browser Artifacts



Make sure you are using the latest version of Internet Explorer (IE), IE 11.

Click the Settings  button on the top right.

Click “Internet Options”.

Under the “General” tab, locate the “Browsing History” section.

Click “Delete”.

You will see the window to the left. (A useful keyboard shortcut to access this window is “*Ctrl-Shift-Delete*”).

Deselect “Preserve Favorites website data”.

Select the boxes next to the history you want to remove and click “Delete”.

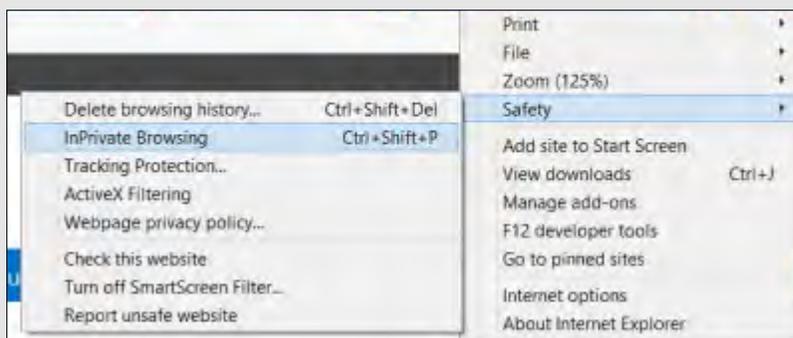
Exit/quit all browser windows and re-open the browser.

**Note:** Internet Explorer is no longer supported on any mobile device.

As of March 2017, Microsoft announced that Microsoft Edge would replace Internet Explorer as the default browser on its Windows 10 devices. As of February 2020, IE version 10 is no longer in support. If you are still using IE be sure to upgrade to IE 11.



### Using Internet Explorer InPrivate Browser



To activate “InPrivate”, click the Settings  button on the top right.

Click “Safety”.

Click “InPrivate Browsing”.

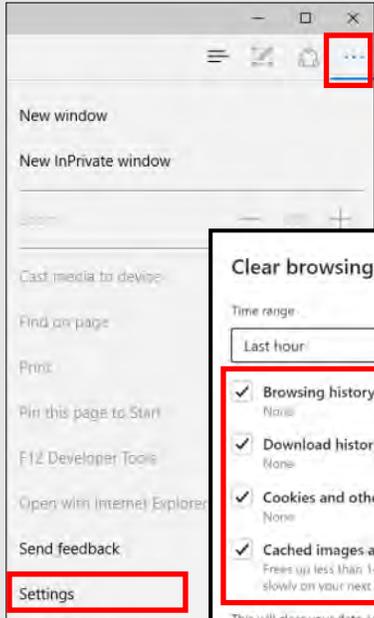
(Alternatively, after opening Internet Explorer you can use the shortcut “*Ctrl-Shift-P*”).

An internet cookie is a small piece of data sent from a website and stored on a user's computer while the user is browsing.

# DELETE BROWSER ARTIFACTS SMART CARD



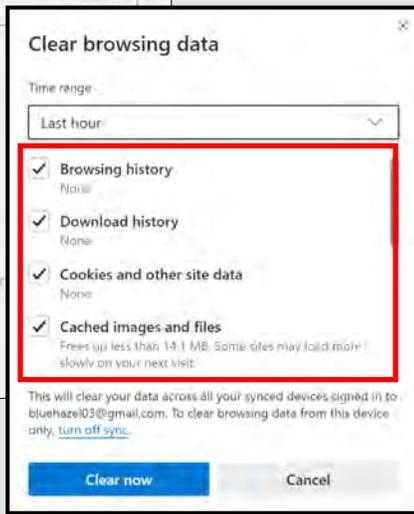
## Deleting Microsoft Edge Web Browser Artifacts



Be sure to delete the browser artifacts regularly.

Click the three dots at the top right corner.

Click "Settings" followed by the

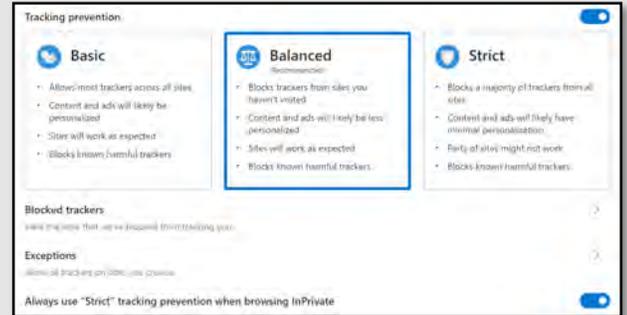


"Privacy & security" tab.

Select "Tracking prevention," recommend selecting the "Balanced" tracking selection.

Then click "Choose what to clear" under "Clear Browser Data".

Select the boxes next to the history you want to remove and





### Mobile Browser

Open the Edge browser.

Tap the menu button  on the top right.

Tap to  view history.

Tap to  clear all history.

Choose the types of data to remove from your phone and tap "Clear".

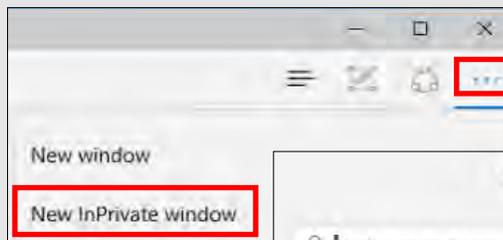
## Using Microsoft Edge InPrivate Browsing

Edge is Microsoft's new browser that comes with Windows 10. It is meant to eventually replace IE.

Edge comes with an option called "InPrivate", which is the browser's private mode that does *not* record your activities.

To activate "InPrivate", click the three dots in the browser's upper right corner.

Click "New InPrivate window".

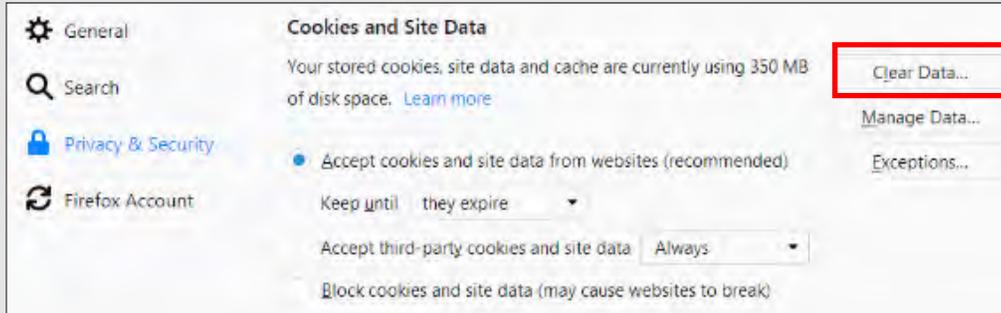


An internet cookie is a small piece of data sent from a website and stored on a user's computer while the user is browsing.

# DELETE BROWSER ARTIFACTS SMART CARD



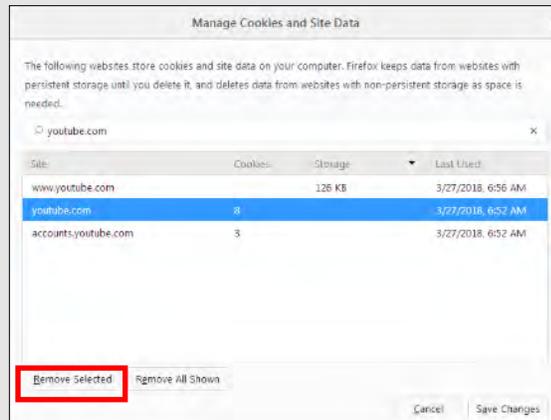
## Deleting Firefox Web Browser Artifacts



Click the menu button at the top right and click "Options".  
 Click "Privacy & Security" on the left.  
 Then click "Clear Data".

### Individual Cookies

You can also remove individual cookies.  
 From the "Privacy & Security" screen, click "Manage Data".  
 Select the site(s) you wish to clear data for.  
 Then click "Remove Selected".

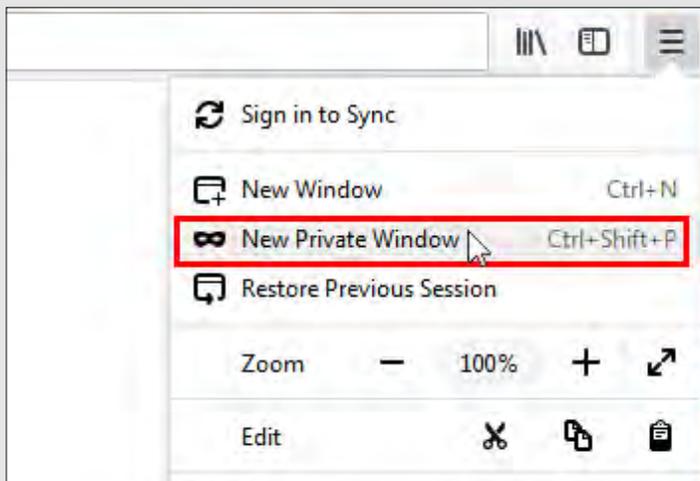


### Mobile Browser

Tap the Menu icon on the top right.  
 Tap "Settings". Scroll down to "Clear Private Data" and tap it.  
 Selected data to be cleared. Tap "Clear Data."  
 To manage how your data is shared and tracked, tap "Privacy" then tap "Tracking Protection" from the Settings menu.  
 "Enabled In Private Browsing" will inform sites that you do not want your browsing behavior tracked, but honoring this is voluntary.  
 Cookies can also be disabled from this screen.



## Using Firefox Private Browsing Mode



To open a new Private Window, click the menu button on the top right.  
 Click "New Private Window".  
 Alternatively, after opening Firefox you can use the shortcut "Ctrl-Shift-P".

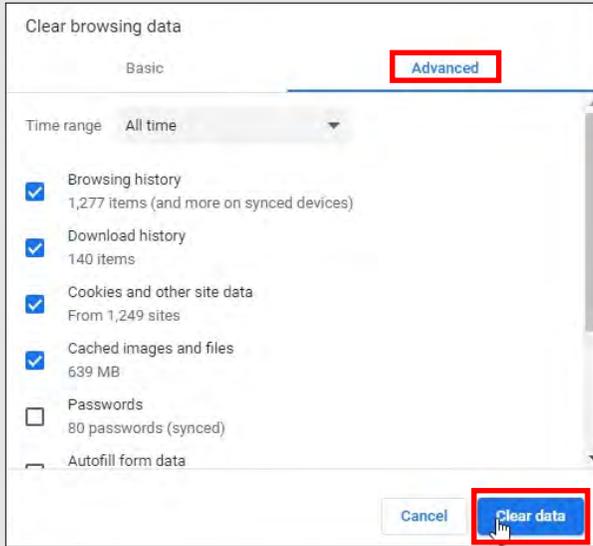
**Important:** Private Browsing doesn't make you anonymous on the Internet. Your Internet service provider, employer, or the sites themselves can still track what pages you visit. Private Browsing also doesn't protect you from keyloggers or spyware that may be installed on your computer.

Private Browsing also includes Tracking Protection, which prevents companies from tracking your browsing history across multiple sites.

# DELETE BROWSER ARTIFACTS SMART CARD



## Delete Google Chrome Browser Artifacts



Click the  icon at the upper right corner.

Click "History" or hold *Ctrl-H*.

Click "History" again on the menu on the upper left hand side.

Click "Clear Browsing Data". You can also hold *Ctrl-Shift-Delete*.

Click the "Advanced" tab in the pop-up window.

Select the Time range you desire.

Select the boxes next to the history you want to remove and click "Clear Browsing Data".

Exit/quit all browser windows and re-open the browser.



### Mobile Browser

Tap the menu  icon.

Then tap "Settings".

Tap "Privacy".

Tap "Clear Browsing Data".

Select the boxes next to the history you want to remove and tap "Clear Data".

### Individual Cookies

You can also remove individual cookies.

Click the  icon at the upper right corner.

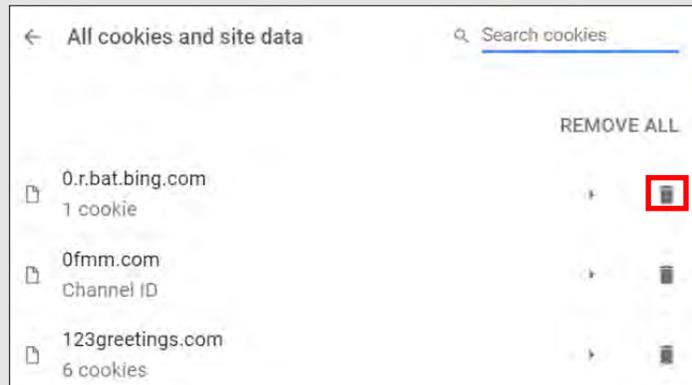
Click "Settings".

Click the "Advanced" button on the left hand side.

Under the "Privacy & Security" section, click the "Site Settings".

Click "Cookies and site data" and then "See all cookies and Data".

Click  for the sites you wish to clear.



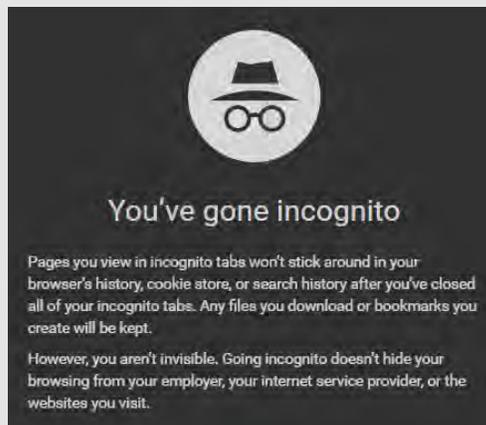
## Using Google Chrome Incognito Mode

Chrome's Incognito mode will *not* save a record of what you visited or downloaded.

Be aware that Incognito is not available if you are using Window 10's "Family Mode."

Click the  icon at the upper right. Select "New Incognito Window".

You can also use Incognito via the Chrome app on your iOS or Android device. Follow the same steps as above with the app.



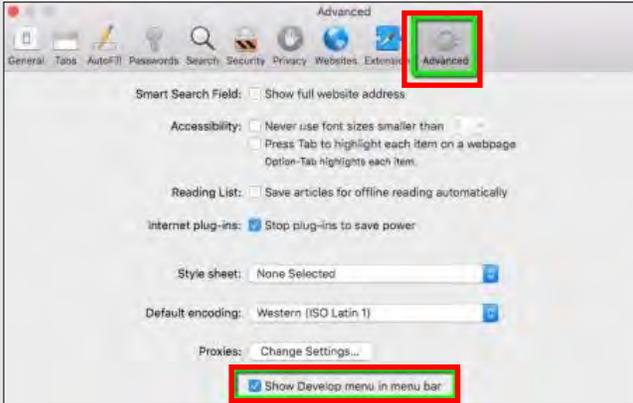
Like Microsoft Edge's InPrivate Browser, Chrome's Incognito will require you to constantly type in your password for logins. So you may prefer to use the regular Google Chrome browser out of convenience.

Chrome doesn't have control over third party websites or their privacy practices, so be cautious when accessing websites.

# DELETE BROWSER ARTIFACTS SMART CARD



## Deleting Safari Browser Artifacts



Click the “Safari” menu on the top left.

Click “Preferences”.

Click the “Advanced” tab.

Check the box at the bottom for “Show Develop menu in menu bar” and close the window.

Click the “Develop” menu at the top and click “Empty Caches”.

Then click the “History” menu at the top and click “Clear History”.

Right click on the Safari icon in your App tray and select “Quit”.



### Mobile Browser

Open your iOS Settings app.



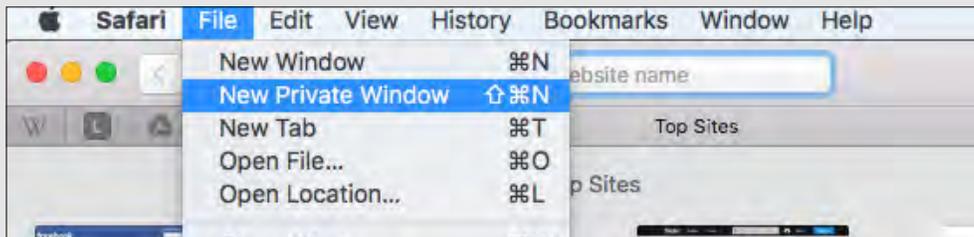
Scroll down and tap “Safari”.

Tap the “Clear History and Website Data” link in blue.

Exit/quit all browser windows and re-open the browser.

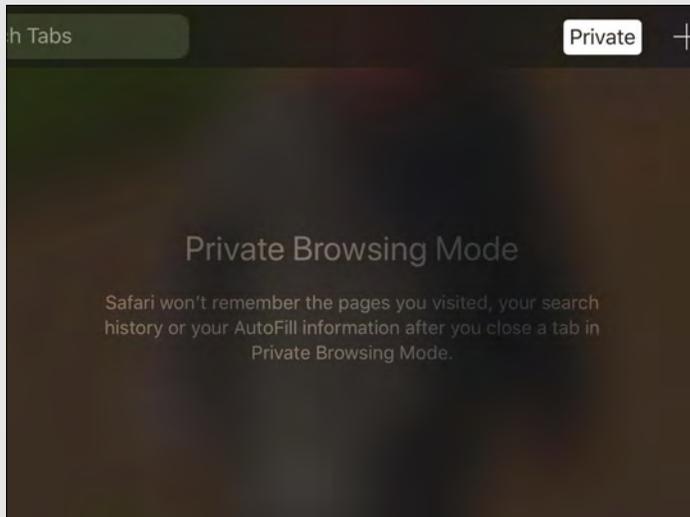


## Deleting Safari Browser Artifacts



To open a Private Window, click “File” on the top left.

Click “New Private Window”.



Enabling Private Browsing limits Safari in three important ways: It prevents the browser from creating a history of the pages you visit, it stops AutoFill information like website usernames and passwords from being remembered, and any tabs you open won't be stored in iCloud.

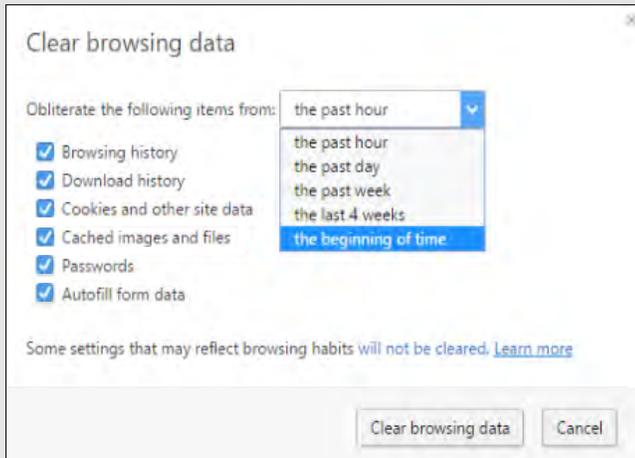
Safari automatically prevents cross-site tracking, and requests that sites and third-party content providers don't track you as a rule. Additionally, the privacy mode stops sites from modifying any information stored on your iOS device, and deletes cookies when you close the associated tab.

When you are on a website that uses Apple Pay, the site can automatically check if you have Apple Pay set up if you haven't disabled this feature.

# DELETE BROWSER ARTIFACTS SMART CARD



## Deleting Opera Browser Artifacts



Click the “Menu” button on the top left.

Click “History”.

Click “Clear Browsing Data”.

Select the Time frame and the boxes next to the history you want to remove and click “Clear Browsing Data.” Selecting “Advanced” will provide the user with more options to clear.

Exit/quit all browser windows and re-open the browser.



**Mobile Browser**

Tap on the “Menu” button.  
Tap “History”.  
Tap “Clear All”.  
Tap “Yes” to confirm.



## Using a Private Tab in Opera Browser

Opera’s Private Tab browsing deletes browsing history, cache, cookies, and logins when you close the tab.

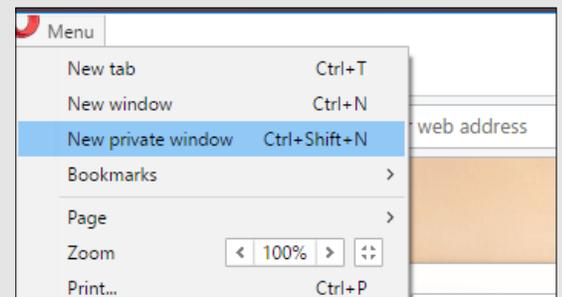
Please note that if you deliberately save data, such as a bookmark or a file, it will still be visible after the tab is closed.

You may prefer to use the regular Opera Browser window out of convenience. Be sure to delete browser artifacts regularly.

To create a Private Tab, click the “Menu” button on the top left corner.

Click “New Private Window”.

Private browsing is also available on Opera Mini mobile browser as well.



# DELETE BROWSER ARTIFACTS SMART CARD



## Privacy and Security-Related Browser Tools



**Ghostery** is a German-owned freeware browser extension that allows you to choose what to block, on a tracker-by-tracker or site-by-site basis, or a combination of the two.

The tool also offers tracker profiles so you can learn about the companies collecting data on you as you browse the web.

Ghostery looks at the HTML code on each web page you visit to see if there are “tags” or “trackers” placed by a company that works with the website. The tool can determine if the company is showing you ads, collecting data, or giving you added functionality on the page.

The extension is available for Firefox, Chrome, Safari, Internet Explorer, Microsoft Edge, and Opera. It is also accessible via a mobile application for Android, iOS, and Firefox for Android.



**Adblock Plus** is a German-based extension that blocks banner ads, pop-up ads, rollover ads, and more. It stops you from visiting known malware-hosting domains and disables third-party tracking cookies and scripts. It can even block video ads on Facebook and YouTube.

This extension works for Android, Chrome, Firefox, Internet Explorer, Opera, Safari, Microsoft Edge and Yandex.



**Blur** protects your passwords, payments, and privacy from cyber criminals.

The US-based tool masks your passwords, email addresses, credit card numbers, and address information. It also has the ability to create strong passwords for new and existing accounts.

Blur blocks hundreds of companies from collecting your data online and blocks tracking that doesn't rely on cookies.

Free and Premium versions are available. Masked credit card is only available with the Premium version which costs \$39/year (Basic), \$14.99/month (Unlimited), or \$99/year (Unlimited). This extension is available for Chrome, Firefox, Safari, Opera, Internet Explorer, Android, and iOS.



**Disconnect** is a smart filter that stops third-party sites from tracking you. The companies that are collecting your information are shown in real-time as pages load. You can even see how those sites may be linked to other sites that track information.

Disconnect encrypts the data you exchange with common sites and helps to prevent visiting sites that have malware.

The extension is available for Chrome, Firefox, Safari, and Opera.

# ADDITIONAL RESOURCES



**Free Annual Credit Report**

[www.annualcreditreport.com](http://www.annualcreditreport.com)

**USA.Gov**

<https://www.usa.gov/identity-theft>

**Stay Safe Online**

[www.staysafeonline.org](http://www.staysafeonline.org)

**On Guard Online**

[www.onguardonline.gov](http://www.onguardonline.gov)

**Equifax—ID Protection Kit**

[www.equifax.com/idtheftprotectionkit](http://www.equifax.com/idtheftprotectionkit)

**Child Identity Theft- Transunion**

<https://www.transunion.com/fraud-victim-resource/child-identity-theft>

**Opt Out Prescreen -**

<https://www.optoutprescreen.com/>

**Federal Trade Commission—ID Protection Tips**

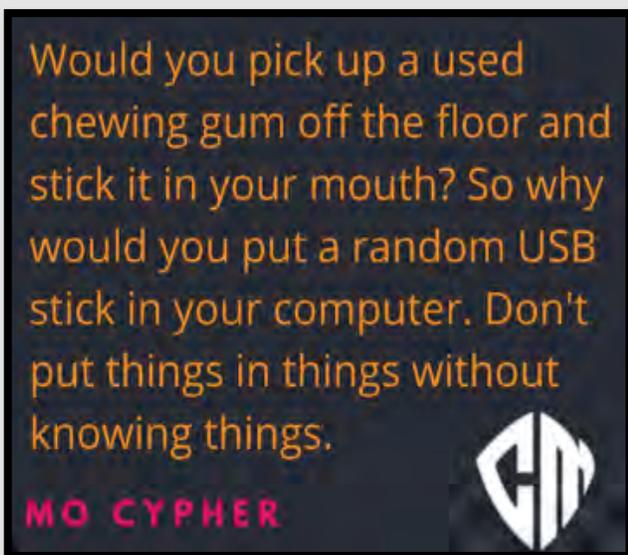
[www.consumer.ftc.gov/topics/protecting-your-identity](http://www.consumer.ftc.gov/topics/protecting-your-identity)

**IRS—ID Protection, Prevention, Detection and Victim Assistance**

[www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection)



Remember the more you know the easier it is to prevent something like Identity Theft from happening to you. #stopthinkpost #themoreyouknow



**Netsmartz Workshop for Parent & Guardians**

<https://www.missingkids.org/NetSmartz>

**Organization for Social Media Safety**

<https://www.ofsms.org/>

**FBI Parents Guide to Internet Safety**

[www.fbi.gov/stats-services/publications/parent-guide](http://www.fbi.gov/stats-services/publications/parent-guide)

**Kids Games**

<https://sos.fbi.gov/>

**Safety Reviews for Games, Websites, & Apps**

[www.common sense media.org](http://www.common sense media.org)

**Opt Out of Interest-Based Advertising**

[www.networkadvertising.org/choices](http://www.networkadvertising.org/choices)

**Google Privacy**

<https://policies.google.com/privacy>

**DMA Choice**

<https://dmachoice.thedma.org>

**Social Media Help (for updated Privacy information)**

<https://www.facebook.com/help>

<http://search.twitter.com>