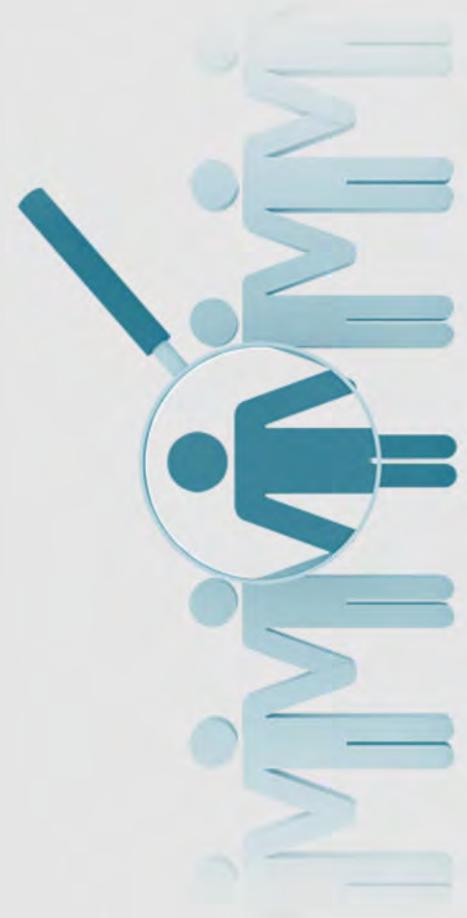


TABLE OF CONTENTS

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
27	Facebook
39	Amazon
48	Pinterest
53	Snapchat
59	YouTube
64	LinkedIn
71	Hidden Apps
73	Mobile Payment Apps
75	Dating Apps
77	Fitness Tracking Apps
83	iOS Settings
87	Android Settings
91	Traveling Safely with Smartphones
92	Identity Theft
94	Keeping Your Kids Safe Online
96	Photo Sharing Services
100	Smartphone EXIF Removal
102	Lock Down Your Computer
104	Securing Your Wireless Network
107	Delete Browser Artifacts (Cookies, Cache & History)
114	Additional Resources



IDENTITY THREATS SMART CARD

Top Data Breaches of FY 19 That You Should Be Aware Of

- ◆ Choice Hotels - Aug 2019
- ◆ State Farm - Aug 2019
- ◆ Asurion - Aug 2019
- ◆ Facebook - Dec 2018, April 2019 & Sept 2019
- ◆ Disney Plus - Nov 2019
- ◆ T-Mobile - Nov 2019
- ◆ Wyze - Dec 2019
- ◆ Wawa - Dec 2019
- ◆ Microsoft - Jan 2020
- ◆ ClearView - Feb 2020
- ◆ MGM - Feb 2020
- ◆ Google Photos & Takeout - Feb 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
- ◆ 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
- ◆ Watch what you post online, to include your product and service reviews
- ◆ 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>

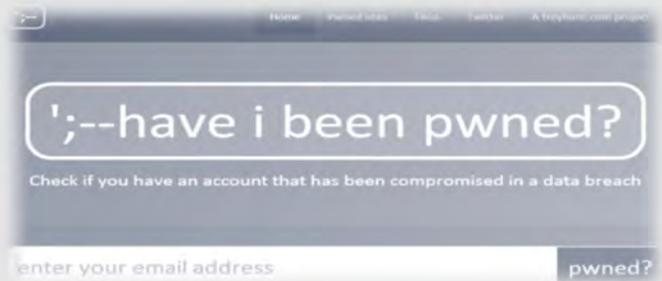
<https://www.consumer.gov/articles/1015-avoiding-identity-theft>

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

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



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...

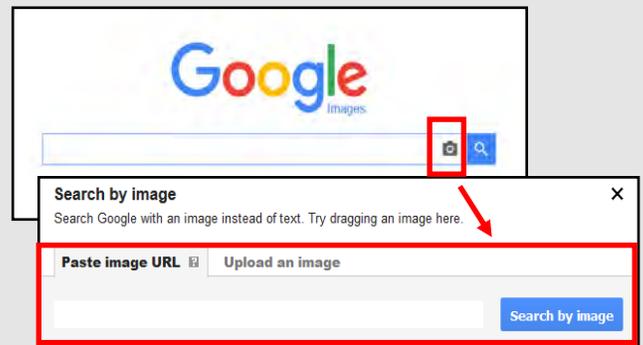
Please note that search terms **within quotations marks** " " will yield results that have the same terms in the **same order** as the ones inside the quotes. So "John Edward Smith" will not necessarily return the same results as "Edward, John Smith."

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 viewable to anyone and everyone.

HOW TO CONDUCT A SELF-ASSESSMENT



Search Engine's 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.

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.⁽¹⁾

- 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.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.

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.⁽²⁾

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.

References:

1. <https://www.socialtalent.com/blog/recruitment/the-beginners-guide-to-boolean-search-operators>
2. <https://searx.me/about>

Examples of Common Social Media Sites

- www.facebook.com
- www.linkedin.com
- www.myspace.com
- www.twitter.com
- www.tumblr.com
- www.classmates.com
- www.instagram.com
- www.vk.com
- www.pinterest.com
- www.flickr.com
- www.meetup.com
- www.youtube.com
- www.snapchat.com
- www.reddit.com
- www.tiktok.com

Additional Examples of People Finder Open Source/Fee Required Sites

- ◆ www.privateeye.com
- ◆ www.peoplefinders.com
- ◆ www.usa-people-search.com
- ◆ www.spokeo.com
- ◆ www.lookupanyone.com
- ◆ www.locateplus.com
- ◆ www.peakyou.com
- ◆ www.thatsthem.com
- ◆ www.familytree.com
- ◆ www.instantcheckmate.com
- ◆ www.zabasearch.com
- ◆ www.peoplelookup.com
- ◆ www.publicrecords.com
- ◆ www.phonesbook.com
- ◆ www.whitepages.com
- ◆ www.reversegenie.com
- ◆ www.yasni.com
- ◆ www.social-searcher.com
- ◆ www.infospace.com
- ◆ www.lullar.com
- ◆ www.publicrecordsnow.com
- ◆ www.findoutthetruth.com
- ◆ www.truepeoplesearch.com
- ◆ www.checkpeople.com
- ◆ www.peoplelooker.com
- ◆ www.persopo.com
- ◆ www.peoplefinder.com

If you post something on your social media account, it may show up on a Search Engines 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. Find the source of content, and who controls it to remove it.

Google

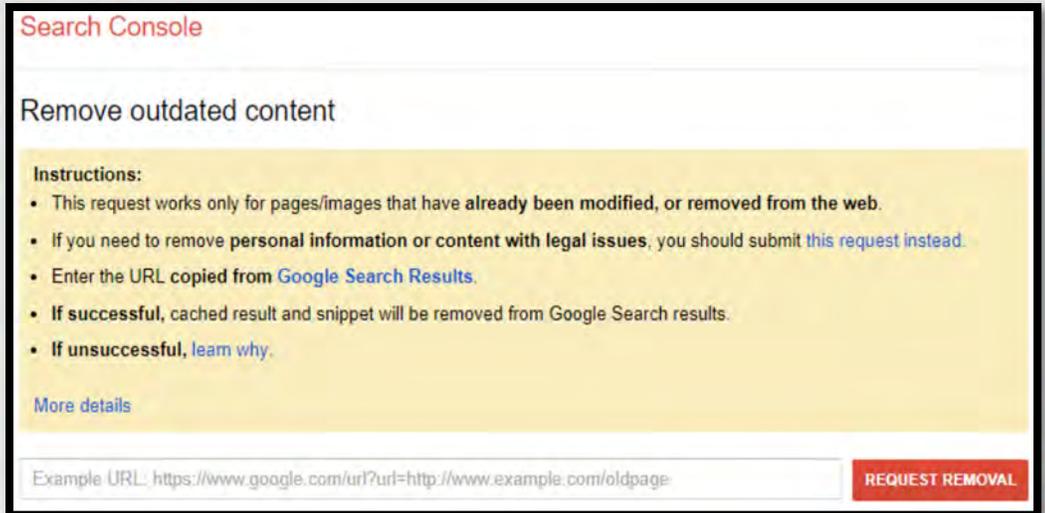
<https://www.google.com/webmasters/tools/removals>

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.

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! You can 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 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

This process will not delete your data but instead suppress it. In addition, these sites update periodically with new information, it is important to repeat this process every six to nine months.

Opting Out of Public Records and Data Aggregators



- ◆ 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

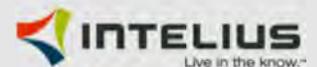
To opt out of Radaris follow the instructions at: <http://radaris.com/page/how-to-remove>



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 <http://www.ussearch.com/privacylock>. Here you will be redirected back to Intelius.com. 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>



Changing or suppressing information could be detrimental to your ability to obtain credit. It is important to know what is worth suppressing and what is worth keeping. #themoreyouknow

Opting Out of Public Records and Data Aggregators



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/. 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 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. 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.

<http://www.mylife.com>



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.peekyou.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.peekyou.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



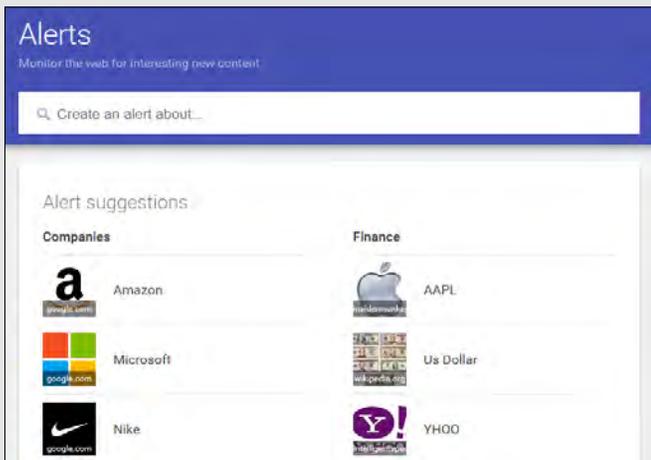
Help keep your identity safe by staying up to date on new Data Breaches – create an Alert for “Recent Data Breach” and monitor results for your information. #databreach

Background

Google Alerts is a service that generates search engine results, based on criteria provided by you, and delivers the results to your e-mail account. This service is useful for many reasons, such as monitoring the web for specific information about your employment, your kids, your online content's popularity or your competition. Google does not require a Gmail account in order to use the service; any email will work.

Step 1: Open the Website

Once you have a web browser open, type “Google Alerts” into your search engine, or you can go directly to the website “http://www.google.com/alerts”. It might be useful to bookmark this page for easier access in the future.



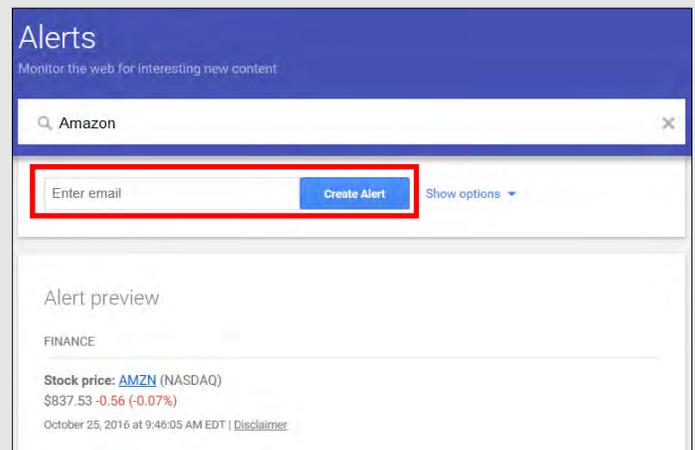
Step 2: Enter Your Search

Under “Alerts” (highlighted below), enter the topic you would like to receive alerts on. As soon as you begin typing, a sample of your first alert will appear. If you are not getting the results you expected, you can change your input right away. It might be a good idea 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”.



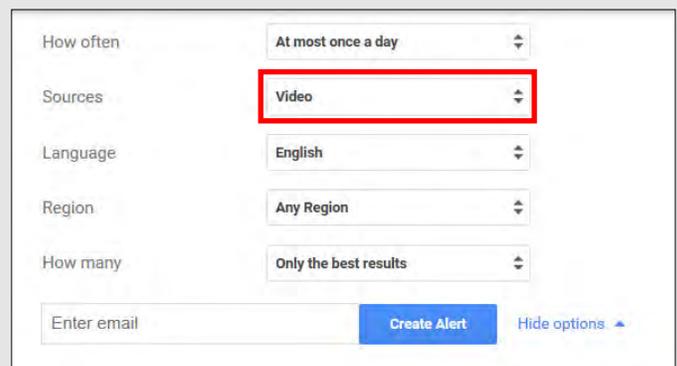
Step 3: Create the Alert

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. 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. It is recommended that you select “Show Options” and see Step 4 after completing this process.



Step 4: Choose Source Type

There are some additional options available to tailor your search to your particular needs. Click the “Show options” drop down menu (highlighted in red), to customize your alert. For instance, you may choose the type of source you wish to search or how often you wish to receive each alert. The default is “Automatic”, which is a good choice if you are not entirely certain what you are looking for. Otherwise it might be a good idea to select a more specific “Source” to narrow your search results. The example below (*Amazon*) is the same topic previously selected, but the source was changed to video. By changing the source, the type of results you receive will vary.



HOW TO SET UP GOOGLE ALERTS



Step 5: Choose the Frequency

You can now indicate how often you would like the results to be delivered to your inbox. You have the options of “once a week”, “once a day”, or “as-it-happens”. The default for this option is once a day. The “as-it-happens” setting may deliver the results to your inbox multiple times a day, depending on how often the query appears in the news stream. If that happens you can modify your “Alert” to decrease how often it is sent to your email (see “Modify Alerts” to the right). Once a day and once a week will stockpile the results and only deliver them according to the chosen schedule.

How often: **At most once a day**

Sources: Video

Language: English

Region: Any Region

How many: Only the best results

Enter email [] Create Alert Hide options

Step 6: Select Search Volume

The last choice you have is to set the “How many” of the results you want delivered. This allows you to switch the volume between only the best results, in which Google filters your results for relevance to the topic, and all results. If you are not yet certain what you are looking for, or perhaps do not have a specific time period in mind, you may want to select "All Results." Once you are able to narrow down what you are looking for, you can always go back and modify your settings to “Only the best results.”

How often: At most once a day

Sources: Video

Language: English

Region: Any Region

How many: **Only the best results**

Enter email [] Create Alert Hide options

Modify Alerts

If you would like to modify your current Alerts, it's fairly simple to do by just following a few steps. Next to each alert is an "Edit" button (see the Pencil icon as highlighted below). This allows you to modify your keywords as well as the volume and frequency of how alerts are delivered. You also have the choice of having the alert delivered to your inbox or directly into an RSS feed. Click the “Update alert” button to save your changes.

Alerts

Monitor the web for interesting new content

Create an alert about...

My alerts (2)

Amazon [Pencil icon] [Trash icon]

Nike [Pencil icon] [Trash icon]

Alerts

Monitor the web for interesting new content

Amazon

How often: As-it-happens

Sources: Automatic

Language: English

Region: Any Region

How many: Only the best results

Deliver to: RSS feed

Update alert Hide options

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 (highlighted below).

Amazon [Pencil icon] **[Trash icon]**

ONLINE REGISTRATION SMART CARD



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 perhaps consider having a profile picture that is something other than your photo.

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.

Location: Address, Zip Code, Country

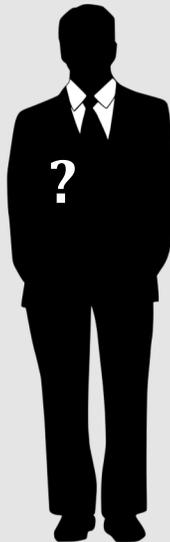
Location information is required to various levels of granularity depending on the service. It may include address, zip code, and/or country.

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.

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 birth-day, 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.

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.

Sexual Orientation / Relationship Status

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

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.

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

ONLINE REGISTRATION SMART CARD



Identity Information Required During Online Services Registration

							
First and Last Name	X	X	X	X	X	X	X
Username	*Uses name by default	x	X	X	Optional	*Uses name by default	*Uses name by default
Password	X	X	X	X	X	X	X
Birthday	X	X		X	X	Optional	
Gender	X	X		X	X		X
Email Address	X	**Optional	X	X	X	X	X
Phone Number		**Optional	Optional	Optional	Optional	Optional	
Country	X	X	X	X	X	X	X
Company/Employment Info	X						
Job Title	X						
Zip Code	X					X	
Facebook Account	Optional	X	Optional	Optional	Optional	Optional	Optional

*Social media sites default to the “name” provided when settings up the account as your Username, instead of asking Users to create a “handle.”
 ** Facebook requires a mobile number or email address when registering an account. Consider using a Google Voice number for two factor authentication for additional security.

It is a lot easier to simply sign up or register on a social media site when you link other accounts to them. Usually, it is a simple click of the button; however, it is recommended that you DO NOT do this. If someone gains access to your Facebook account and you have signed up for other SM accounts using Facebook, then that likely gives them access to those other accounts as well. Treat SM account creation just like your password; create a new and unique one for each site you wish to sign up for.

Additionally, it is always best to use a current email for any social media use. This way, if something were to happen to your account, you’re immediately notified and can quickly correct the problem. If you have an email account that you do not check routinely, or that has suffered a major data breach, you might not know if someone hacked into your social media account(s) until it is too late to fix.

Rewards

- Join Social Communities
- Connect Instantly
- Self-Expression
- Collaborate With Others
- Real-Time Information

Risks

- Cyberbullying
- Identity Theft
- Overuse
- Posts are Permanent

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

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”

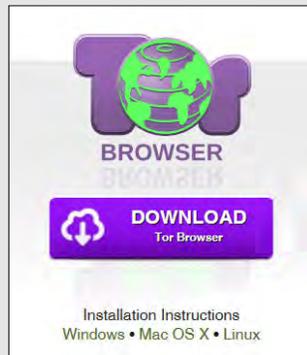
Tor Browser is a free, open source web browser that uses a volunteer network of virtual tunnels and a layered encryption process to anonymize your IP address. Note that Tor anonymizes the origin of your traffic and encrypts everything inside the Tor network; however, it *cannot* encrypt the data after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

No matter how many tools you use to mask your IP, your payment or sign-up information could identify you

Visit torproject.org.

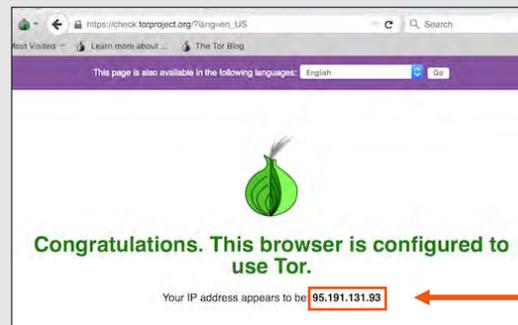
Download and Install the **Tor Browser Bundle** to your hard drive or a flash drive.

1

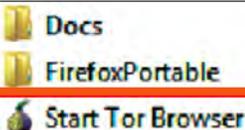


Ensure your Tor Browser is providing you with an anonymous IP address.

3



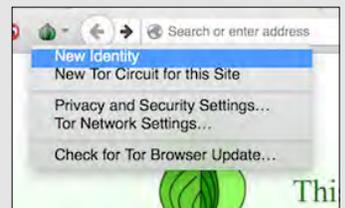
IP address



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
Hide My Ass!	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.
CloakMy	One time message and chat service	CloakMy is accessible through Tor, it is one time messaging and chat. You have to send the recipient a unique URL to go retrieve the message.	None, no personal information required	None, there is no data retained	Free
ProtonMail	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
HushMail	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.	No person information retained, although there is a payment required so you can be identified that way.	Hushmail 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
Signal	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	Free
Wickr	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
Mailinator	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

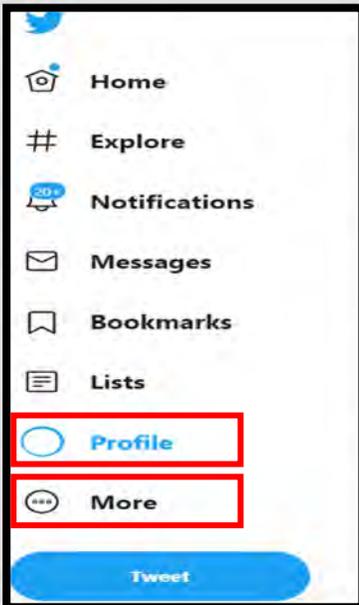
TWITTER SMART CARD



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 follower's access to your profile that you do not know. 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

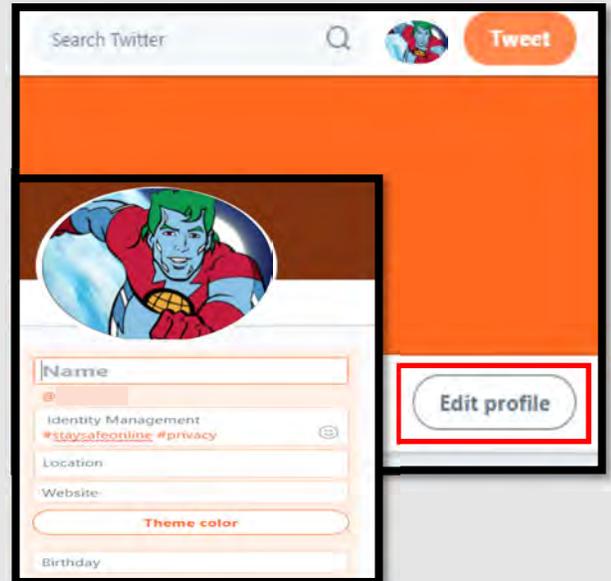


Let's start to lock down your account by first checking out what your "Profile" says about us.

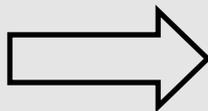
Click the "Profile" icon at the lower left of the screen (this is likely your profile picture). Then click "Profile".

Click "Edit Profile" as shown to the right.

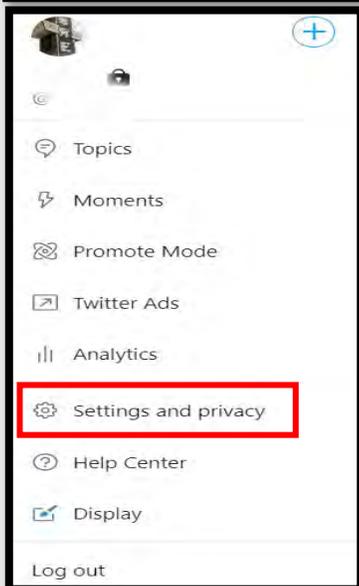
It is highly recommended that you do **not** use photos of yourself for your profile or header photo. These are viewable to the public and therefore presents an unnecessary vulnerability.



It is also recommended that no PII or information that may identify you specifically be included in your profile. The "Bio", "Location", "Website", and "Birthday" areas of the profile do **not** have to be filled in. Even if you use old location data, it is still possible for someone to tie that back to you utilizing data aggregator sites. PII information is often used as a means to gain access to certain accounts (banks, credit cards, school etc.), 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. It is important to remember that these setting should be updated on every device you use to access Twitter, to include your home computer. As with any social media account and mobile device, it is also important to ensure your "Location" is set to "Off."



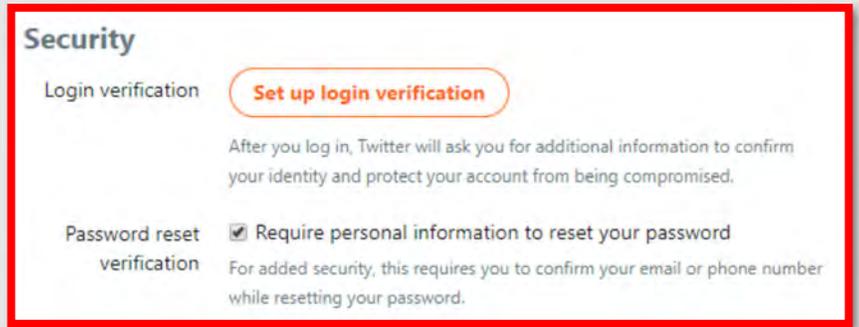
TWITTER SMART CARD



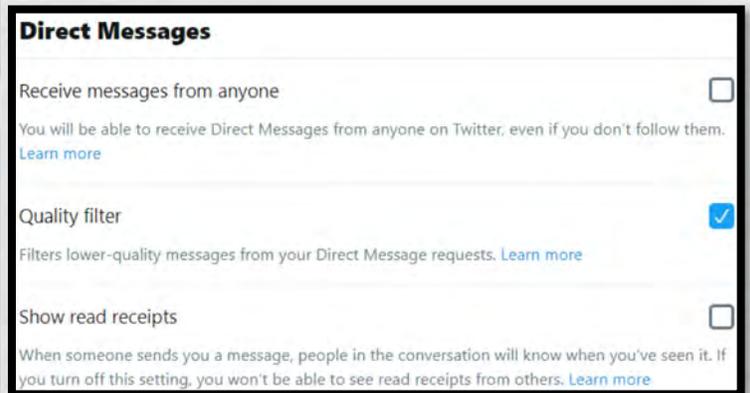
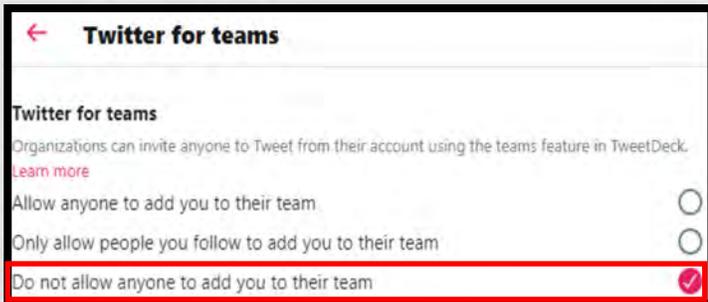
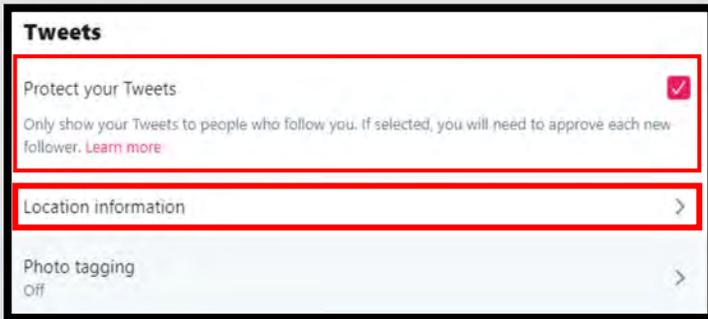
Here you can review your account information, including “Security” settings and how data, such as your “Username” is displayed. Remember to stop and think about what your “Username” says about you, what is it giving away? Select “Account” then “Security,” it is highly recommended that you “Set up login verification” as well as the “Password reset verification”. This way if someone does try to access your account there are layers of security that will help to prevent them from gaining access as well as notify you should any of that occur.



Next, go back to the left column and select “Privacy and Safety”. Here it gets a bit tricky, but it’s important to review what should and what should not be selected. All the sections in RED below are recommended settings that should be selected. Remember it’s always better to control your information than it is to allow someone else to decide for you.



Let’s scroll to the bottom of the page and select “Twitter for teams.” It is recommended here that you stay in control of who has access to your profile, therefore select “Do not allow anyone to add you to their team”. Directly below that it is recommended that you not check any of the “Direct Messages” section, which will help to limit incoming messages from people you do not know.



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



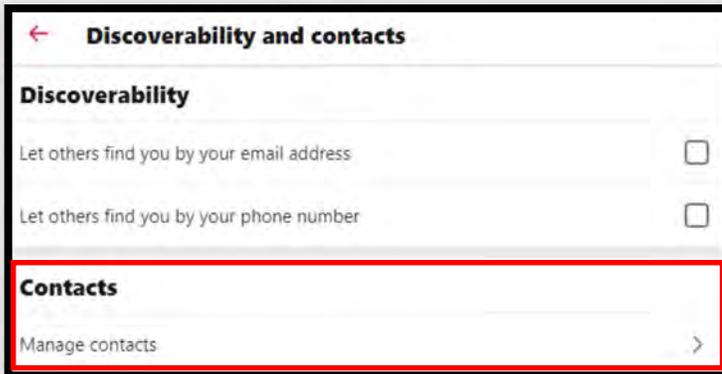
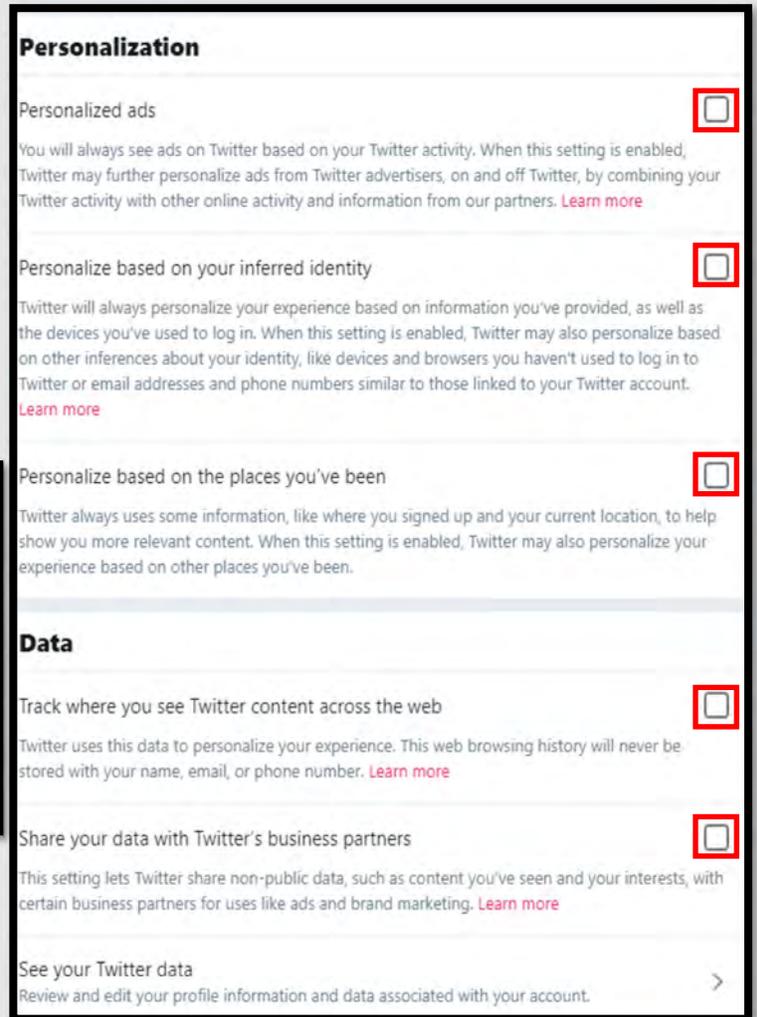
If your account is locked down, you're doing GREAT! If you reach out and post on a public account your comment will be visible. #privacymatters



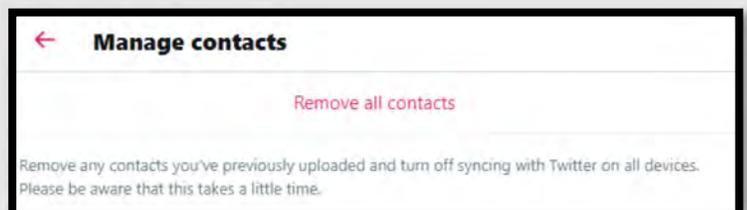
Please see the section under “Privacy and Safety,” entitled “safety,” (framed in green to the left). This section is really at your discretion, but if your children have a Twitter account, you may want to review these settings to help keep them from seeing unwanted or objectionable content.

Quickly, lets go back and select the arrow right next to the “Personalization and Data” section closer to the bottom of the page. As always it is highly recommended that you limit what Twitter ads have access to and this is the section to help. Once you “Disable All” items make sure to save your changes and you have completed this section.

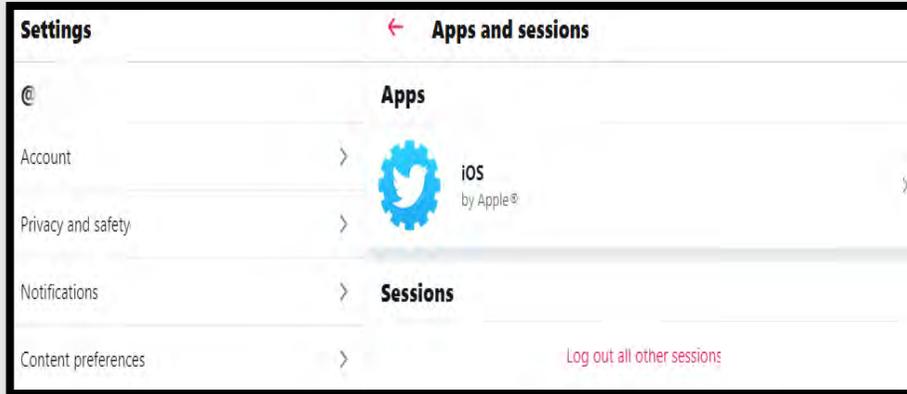
Now, let’s go back to the “Privacy and Safety” menu and select “Discoverability and contacts. Here you will be able to manage any uploaded contacts from any of your devices and remove them if present by the following procedures detailed below. Here you will also be able to see if more than one email is linked to your twitter account and limit how other individuals can discover you on Twitter..



From here, click on the “Contacts” link, shown above in red. Here you can review and remove any contacts Twitter has collected. It is highly recommended that you not synchronize any of your accounts together, to include any email accounts with contact information on them. Synchronizing your email accounts allows Twitter to do more than just upload your contacts; they also use the information to find out more about you and your contacts.



TWITTER SMART CARD



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. It is highly recommended that you significantly limit which apps have access to your account and your personal information.

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 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.

Now, if you are adamant that Twitter not show you any Interest-based ads, there is only one place you can go to in order to turn them off. In the address bar type in **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.

#DataSecurity

#TheMoreYouKnow

#dataprivacy

#identitytheft

#cyberresilience

#ThinkHappyThoughts

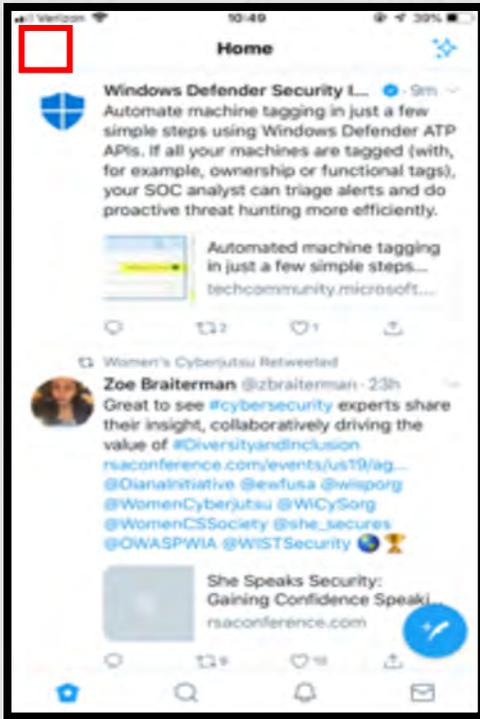
Hashtags # are used to index key words and topics on Twitter, think of them as the topic of your “tweet” or “post”. **Please note that if your account is public and you use a hashtag on a tweet, anyone who does a search on that hashtag may find your tweet. Many people use a “Hashtag” as a way to improve crowdsourcing requests. When you add a hashtag to a tweet, Twitter adds the message to the hashtag group so that more Twitter 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.

Even if your Tweets are private, your followers are still able to screenshot them and post as they see fit. #thinkbeforeyoupost

TWITTER SMART CARD

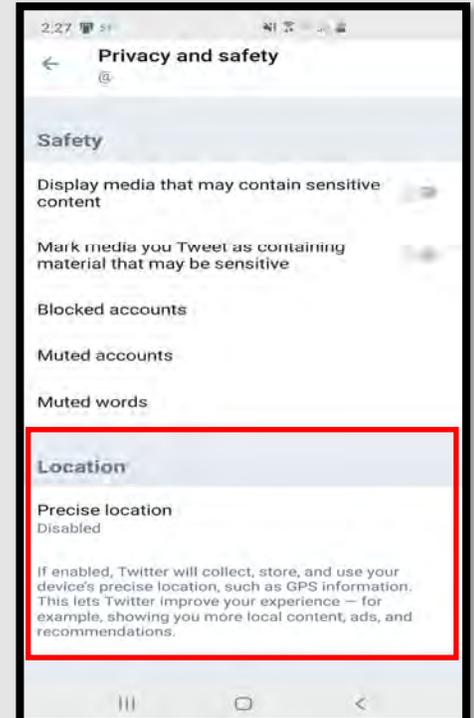
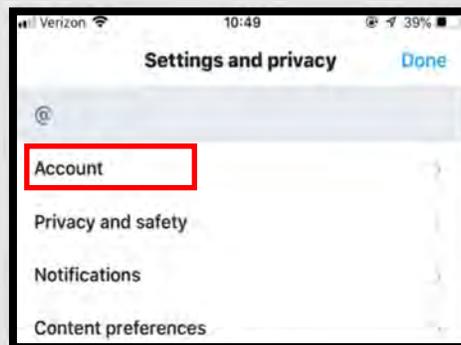
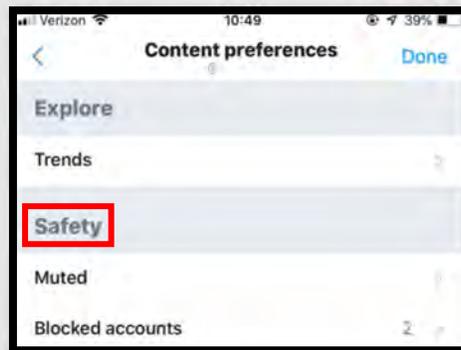
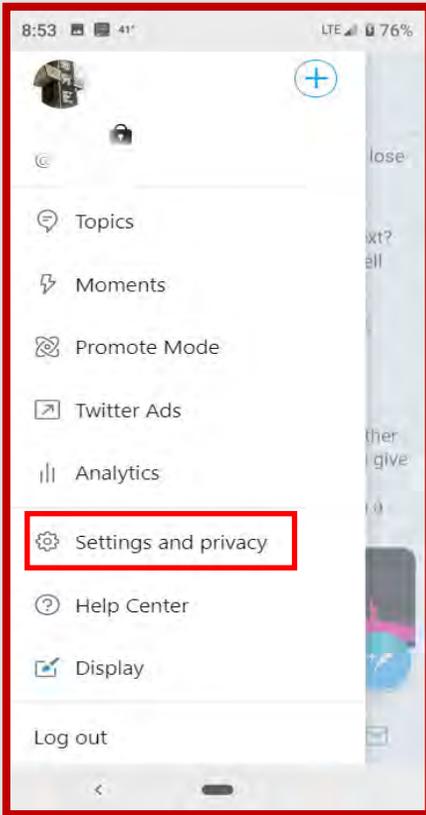


Always check to make sure your location settings are locked down on Twitter. This means on your smart device in the "Settings" section and via the App.



If you are planning to lock down your Twitter account from a smart phone the process is fairly similar. 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. The most important lock down feature you will need to make sure you turn off and that can only be turned off on your smart device is the "Precise Location" feature which is separate from the location in any other place on Twitter. First, head to the top left of your screen and select the icon to make the pop-up menu appear (shown highlighted in red all the way to the top left).

Now for iPhone users ONLY; Finding the "Settings" section can be done as described above or by the following: Select "View Content Preferences" and once there select the "back arrow" at the top left of your screen, this will take you to your "Settings and Privacy" page. For 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."



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
- * 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 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 in fact 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 always contact Twitter using their Support handle @TwitterSupport.

A six character password can be cracked in one second

PASSWORD LENGTH	POSSIBLE COMBINATIONS	TIME TO CRACK		
		S = SECONDS	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 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.

INSTAGRAM SMART CARD

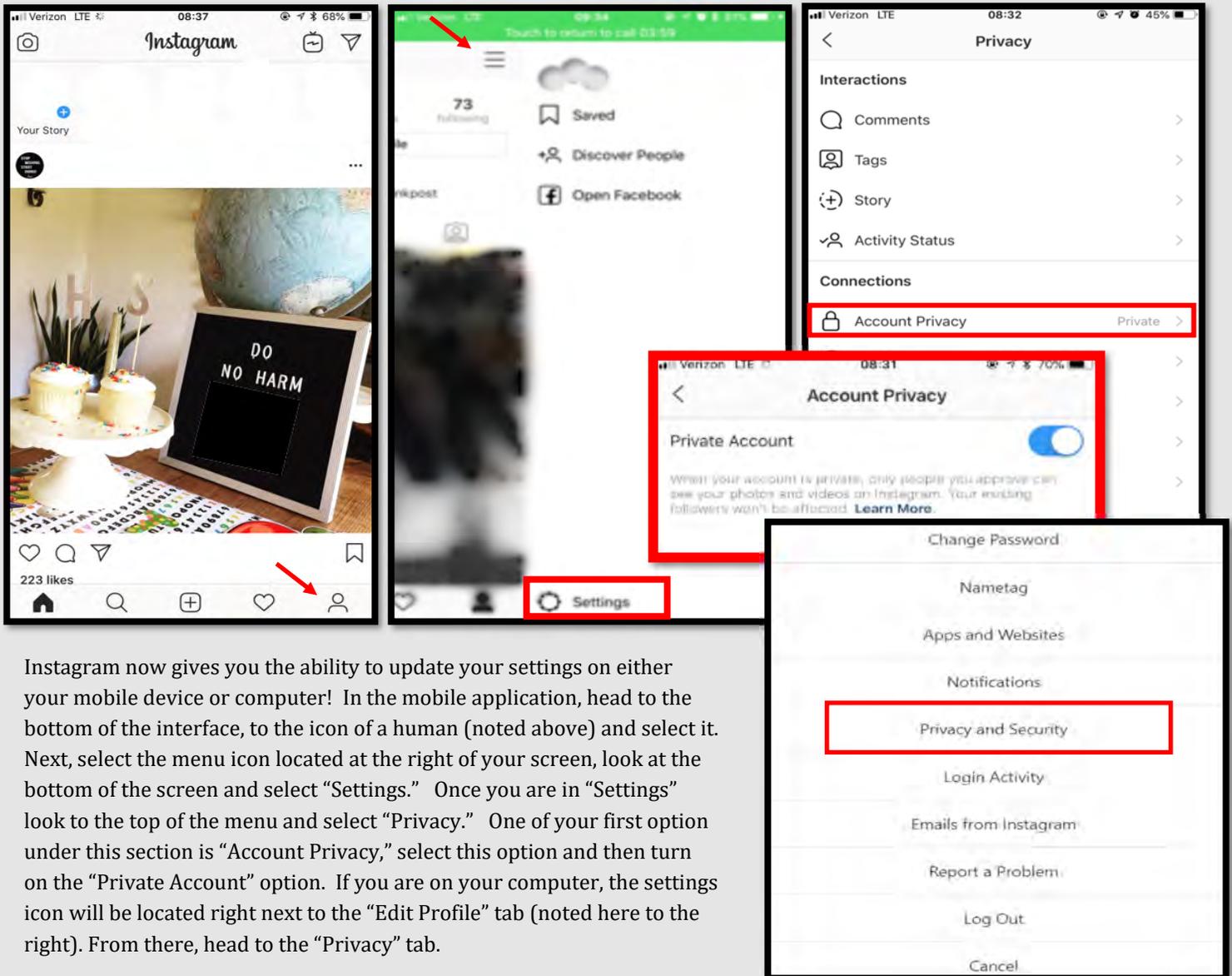


(Mobile Application)

Do's and Don'ts

- Don't use geo-location tags to prevent others from seeing your location. Instagram deletes metadata from a photo the moment of uploading; however, geo-tags that spell out your location pose a personal security risk.
- Don't establish connections with people you do not know. Understand that not everyone is who he or she says 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.

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



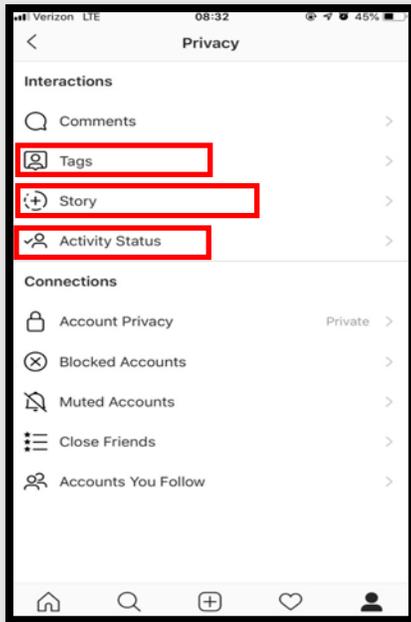
Instagram now gives you the ability to update your settings on either your mobile device or computer! In the mobile application, head to the bottom of the interface, to the icon of a human (noted above) and select it. Next, select the menu icon located at the right of your screen, look at the bottom of the screen and select "Settings." Once you are in "Settings" look to the top of the menu and select "Privacy." One of your first option under this section is "Account Privacy," select this option and then turn on the "Private Account" option. If you are on your computer, the settings icon will be located right next to the "Edit Profile" tab (noted here to the right). From there, head to the "Privacy" tab.

INSTAGRAM SMART CARD



(Mobile Application)

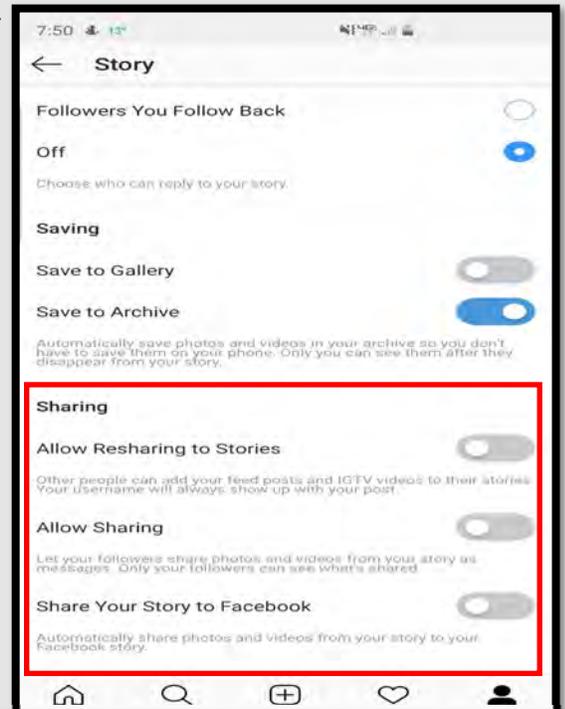
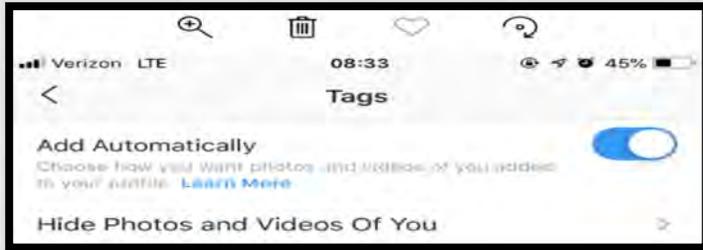
80% of Instagram users are from outside of the US, therefore it is extremely important to vet your followers before you trust them with your profile. #trustbutverify



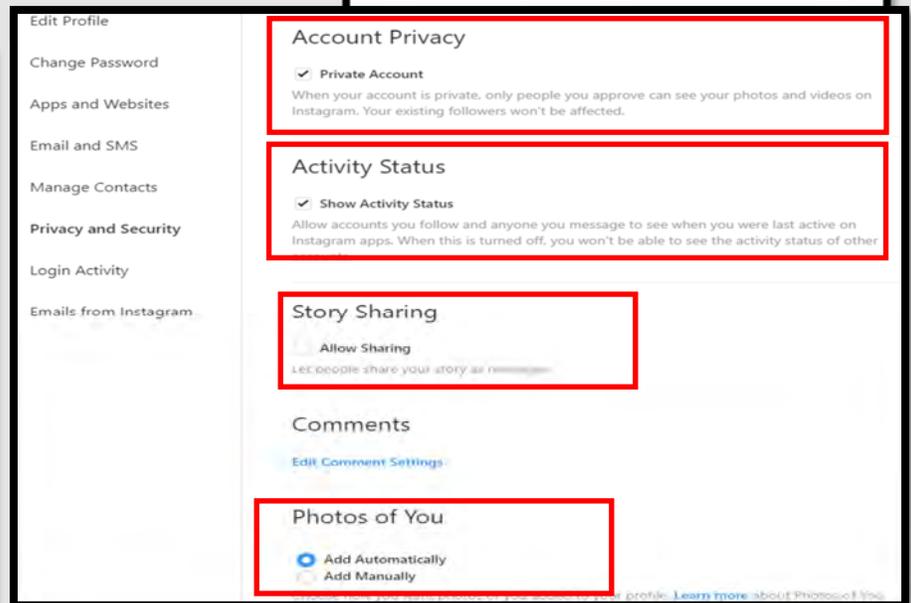
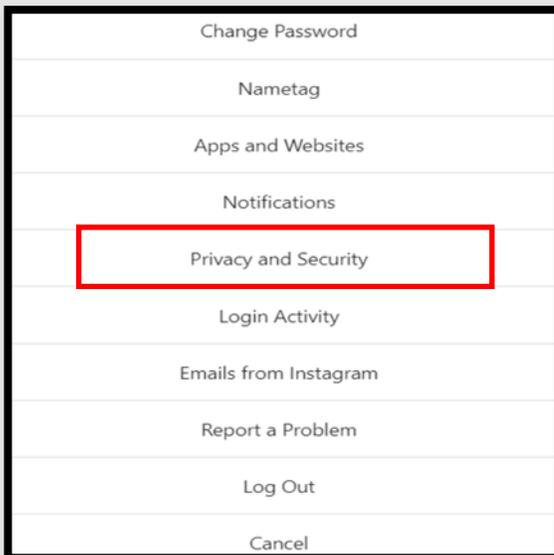
In order to control what photos and videos do and do not go onto your profile, it is important to ensure you lock down your settings. Let's go back to the side menu (shown to the left of this text in the first **red** box) and select "Tags." Next, there will be an option to turn off having photos and/or videos added automatically. It is recommended that you opt to turn off the "Add Automatically" function.

Next, head to "Story" listed under "Privacy" and shown here in **red**. Here you will be able to turn off the "Allow Sharing" function, which allows others to share stories that you have posted. It is also recommended that you take a second to ensure you have not allowed Instagram to "Share Your Story to Facebook." You can turn this function off at the bottom of the "Story Controls" sections.

To the left you will also see "Activity Status" this 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."



Once you have gone over the "Tags" and the "Story Controls" from your mobile device, it is a good idea to check these settings from your computer (as shown below) to ensure any changes you made have been updated.



INSTAGRAM SMART CARD

(Mobile Application)

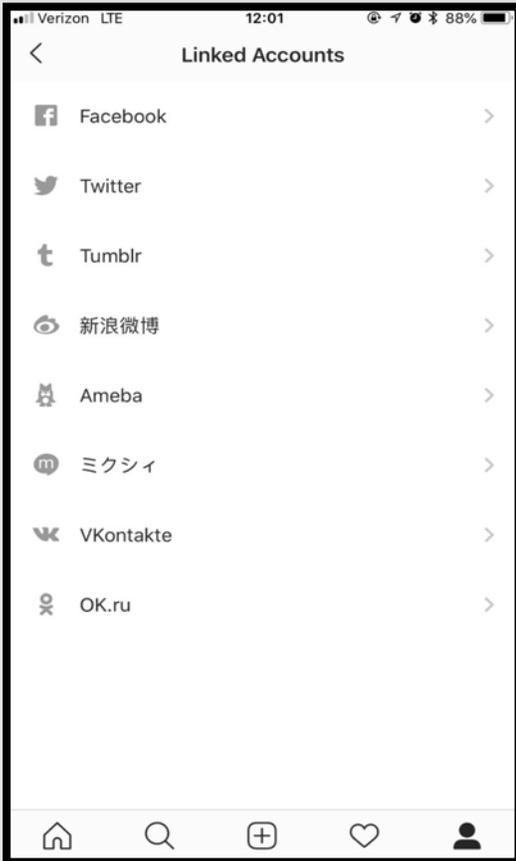
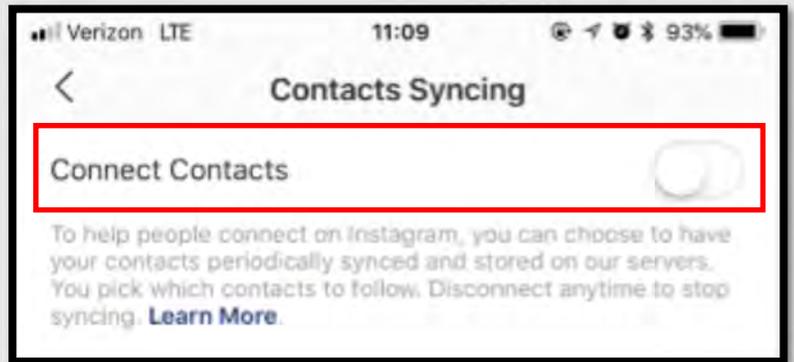


Teenagers use Instagram more so than any other social networking site. It is important to know who they know and what they are talking about. #keepthemsafe

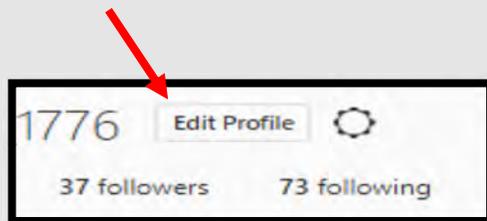
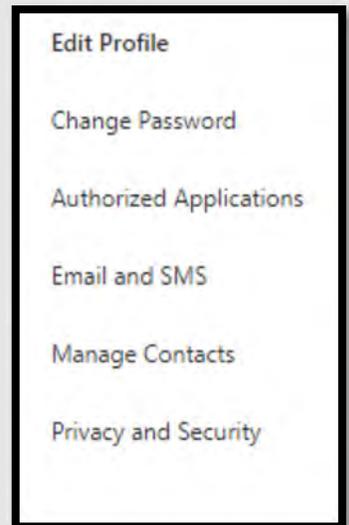


Now, let's head to the "Security" menu and select "Two-Factor Authentication." It is very highly recommended that you turn on the Two-Factor Authentication function in order to better protect your account.

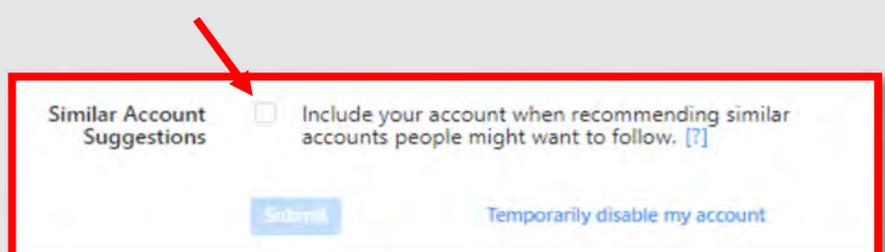
Next, head back to the "Settings" menu and select "Account" then "Contacts Syncing" It is recommended that you do not allow Instagram to upload your contacts by turning off the "Connect Contacts" option.



Let's go back to the "Account" menu and scroll down to the "Linked Accounts" tab. Here you want to make sure that you have not linked any of your social media accounts to Instagram. If you have, simply select the arrow next to the social media app and delink that account.



Next, let's go back to your profile (icon of the human), and select "Edit Profile." Once there, scroll to the bottom of the page and find the "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.

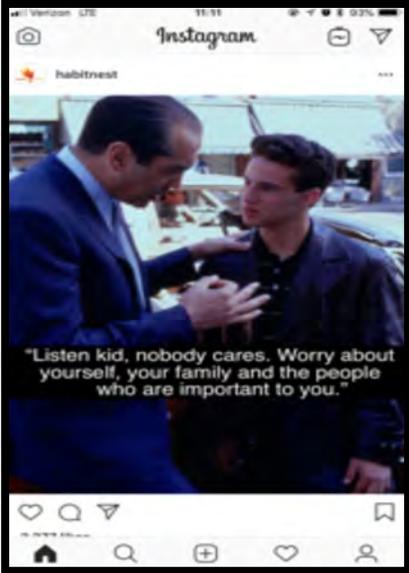


INSTAGRAM SMART CARD

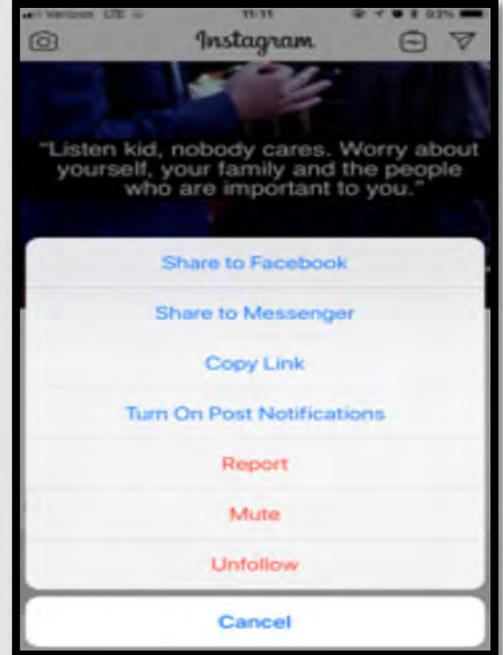
(Mobile Application)



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

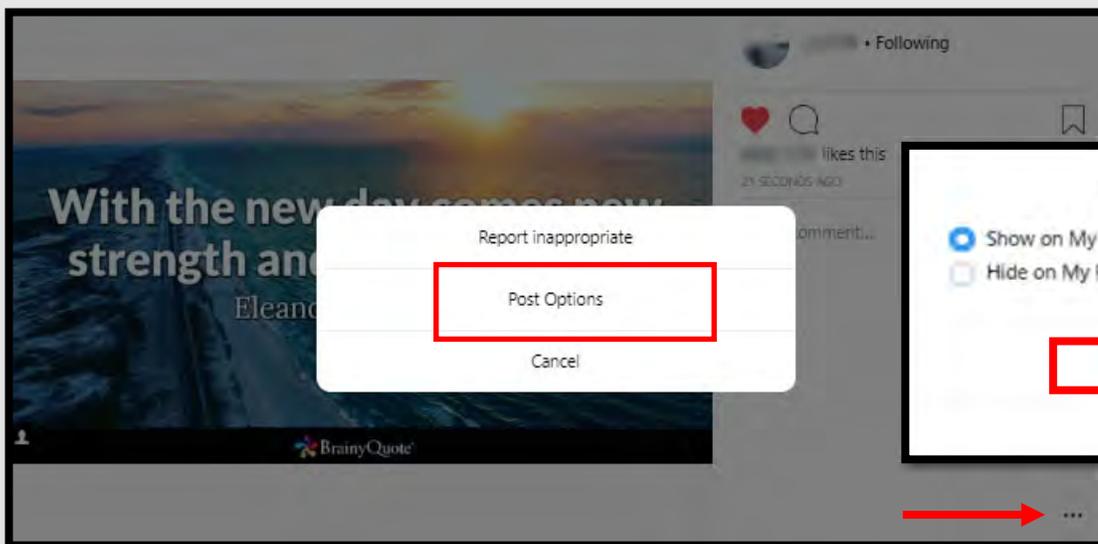
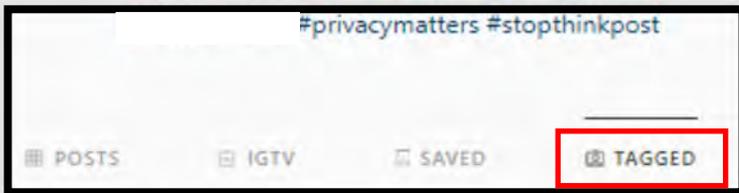


Instagram allows you to report, or remove from your feed, any offensive post you come across. Simply select the menu button at the top left of the post and select which option best applies to that particular post from the drop-down menu.



Removing unwanted tagged photos/posts is important. If you have a profile that is "Private," you are on the right track to staying safe online. It is important for you to know that even if your profile is locked, a comment or tag on a post whose user profile is public will make your "tag" or comment visible to everyone.

In order to remove a tag of yourself from someone else's post you can follow these simple steps. First, go back to your profile (human icon) and select the "Tagged" icon (shown on the left). Next, select the post you are tagged in that you wish to un-tag yourself from, this can be from your phone or computer. 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." Now you can decide whether you would like to allow the post to show on your profile. Next, if you would like, you can "Remove Tag" simply by selecting the link highlighted here in **red**.



INSTAGRAM SMART CARD



(Mobile Application)

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 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

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

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	37 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	52n years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	16bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

Key:
 k – Thousand (1,000 or 10³)
 m – Million (1,000,000 or 10⁶)
 bn – Billion (1,000,000,000 or 10⁹)
 tn – Trillion (1,000,000,000,000 or 10¹²)
 qn – Quadrillion (1,000,000,000,000,000 or 10¹⁵)
 qn – Quintillion (1,000,000,000,000,000,000 or 10¹⁸)

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

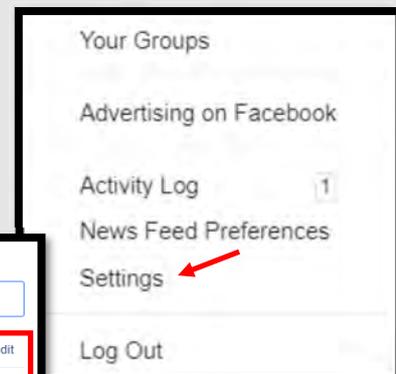
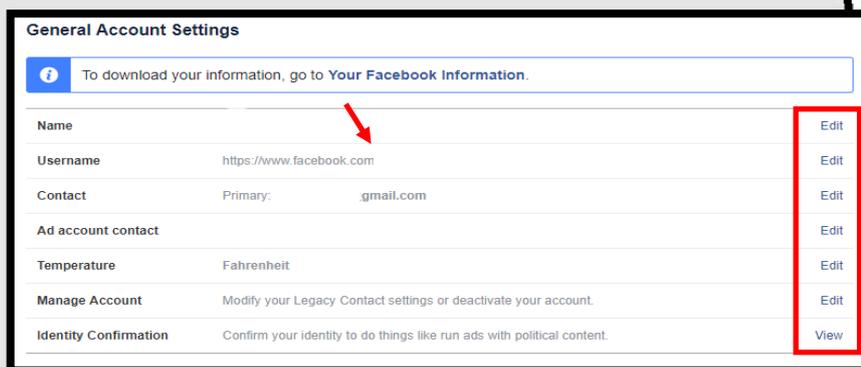
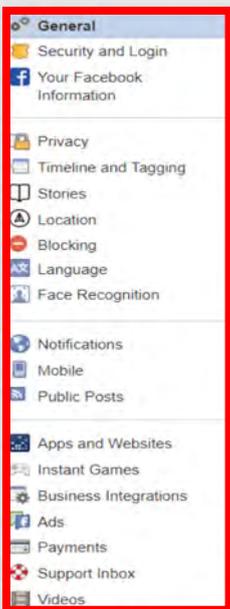


Do's and Don'ts

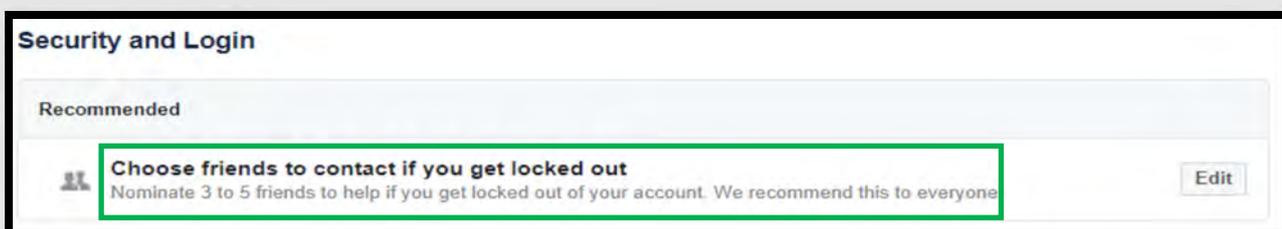
- ◆ Do use pictures of something other than yourself for your cover and profile photos. Cover and profile photos are viewable to the public. Remember if you change your profile picture you must change the privacy setting on it from "Public" to perhaps "Friends", Facebook will not do it for you.
- ◆ Do 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 any gaming apps. #protectyourusername
- ◆ 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, try to stay broad or wave top in your discussions. Also, when posting pictures try to stay more generic. For instance, if you are posting a picture of your car you will want to make sure the license plate is not showing.

Facebook has recently worked to enhance its privacy efforts and better protect user's data. As a result, many settings have changed and more have been added. Now, lets get started. Click the down arrow at the top right of the Facebook screen. From the drop down, select "Settings". From here it is good idea to review each different section listed on the left-hand side of your screen.

Starting, in the "General" section, go through and review your information. Remember your Username (which is located in the URL) will be public just as your "Name" is on Facebook. In this section you also have the option to deactivate your account should you want to.



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 highly recommended that you choose friends that can help you to log in to Facebook should you ever become locked out.

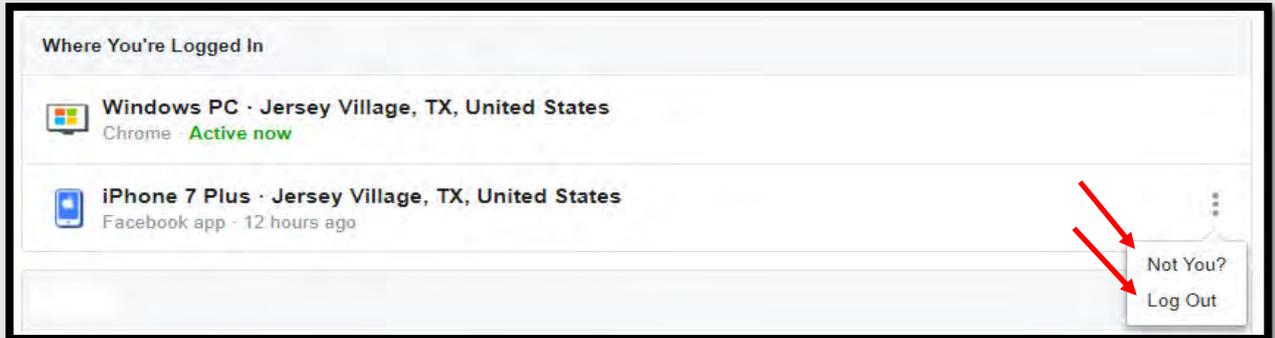


Facebook quizzes could be taking more from you than you realize, it's time to think twice about finding out which Star Wars character you are. #keepyouridentitysafe

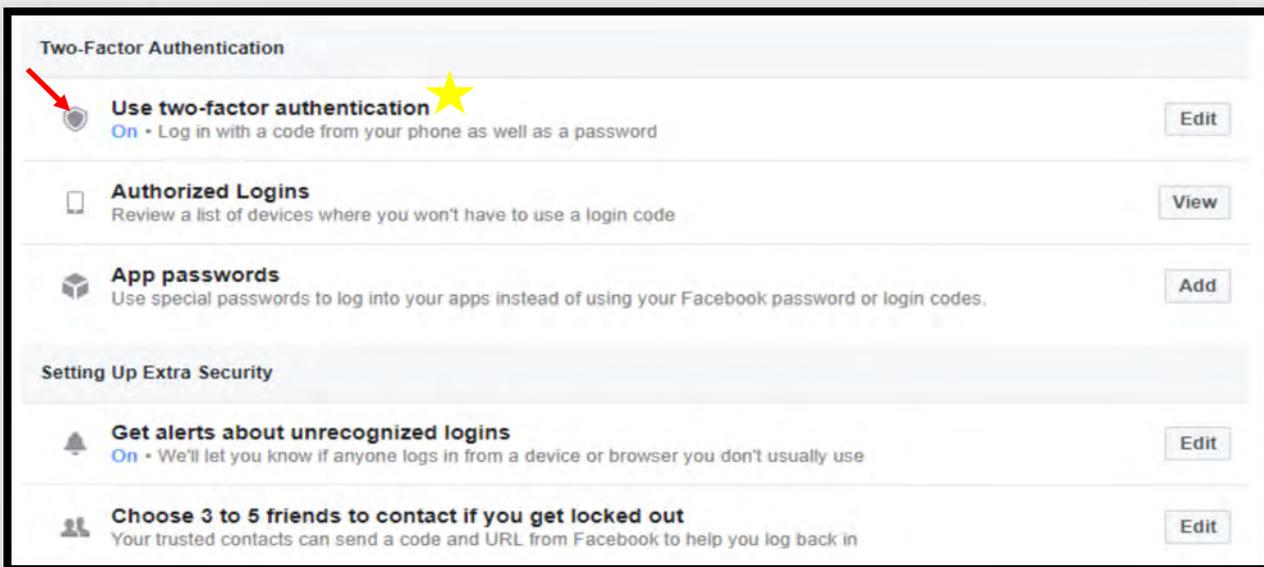
FACEBOOK SMART CARD



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.

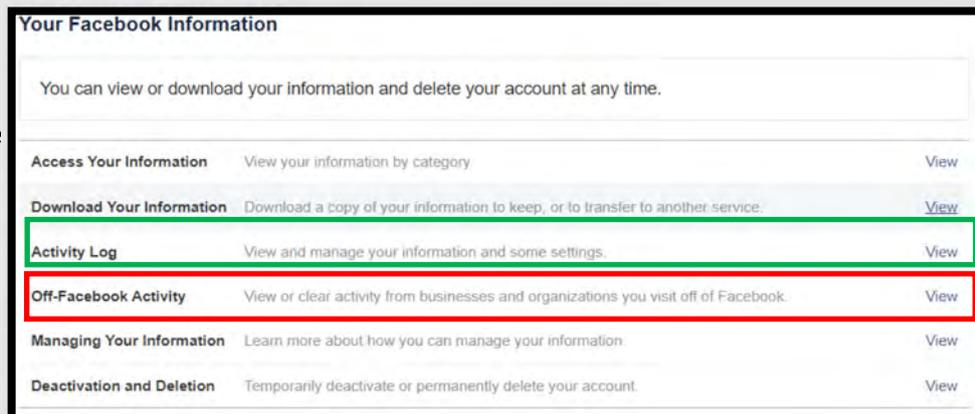


If you do not recognize a location you can select the “Not You Tab” and log out of that session, (perhaps consider changing your password).



Lastly in this section it is very highly recommended that you turn on “**Two Factor Authentication**” as an additional security measure. It is also a good idea to allow Facebook to notify you if a login is unrecognized.

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 allow you to manage your information. **Next select “Off-Facebook Activity” to clear your history. It is highly recommended that you not allow Facebook to track your offline activity.**

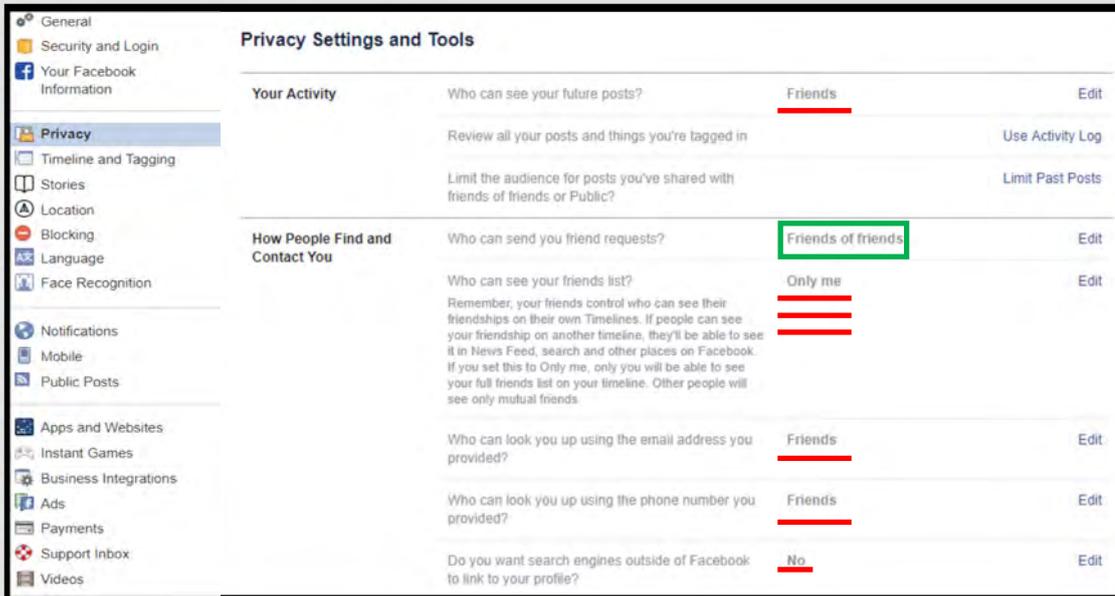


It is not possible to lock down someone else's account so it is important to note the privacy setting on a post before you comment or "react" to each post. #privacymatters

FACEBOOK SMART CARD

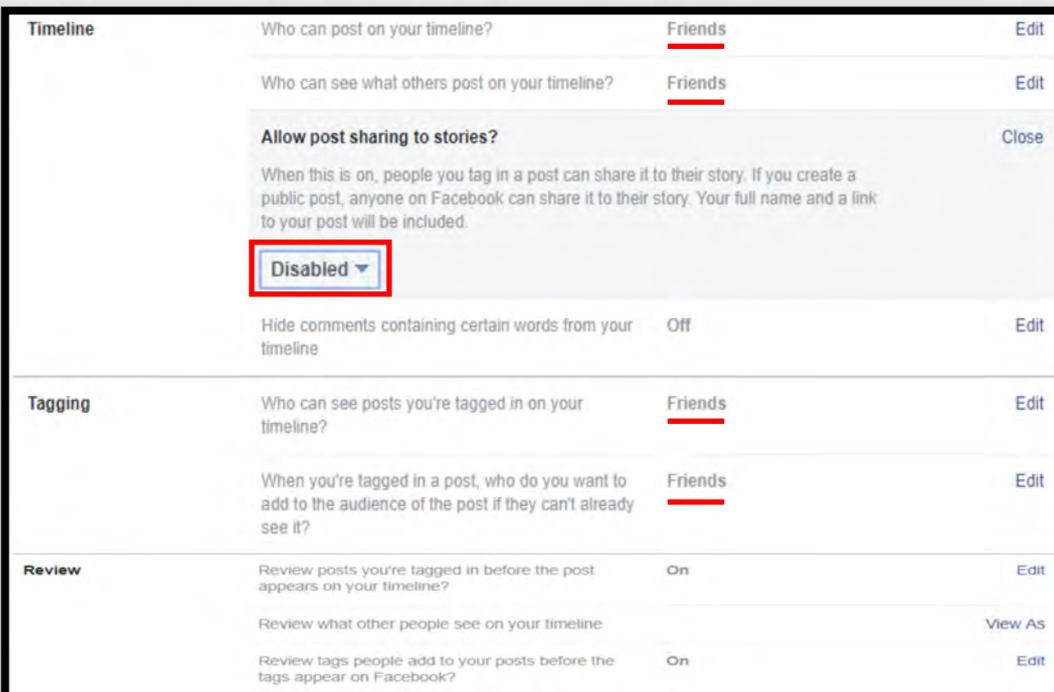


Never become complacent with your Privacy settings. Checking your settings once a quarter could help to keep your information safe online. #updateyourprivacysettings



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 the drivers seat to make decisions about where your data goes and who can see it. Take some time here to ensure each section is set to your specification.

It is recommended that no category be open to the public, the safest choice is, of course to select "Only Me". This does take away from the social aspect of the Facebook and therefore selecting "Friends" is the next best option. It is highly recommended that your Friend's List be locked down however to "Only me". Finally, it is recommended that you not allow Facebook to link other search engines to your profile.



Next up, "Timeline and Tagging". This section is yet another section that puts the control of your data in your hands. Take a few moments again here to make sure you agree with all the settings. Some recommendations for this section are the following: Ensure nothing is allowed for Public dissemination, 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, simply select "View As". While reviewing your profile from the public's perspective take note of anything you see that



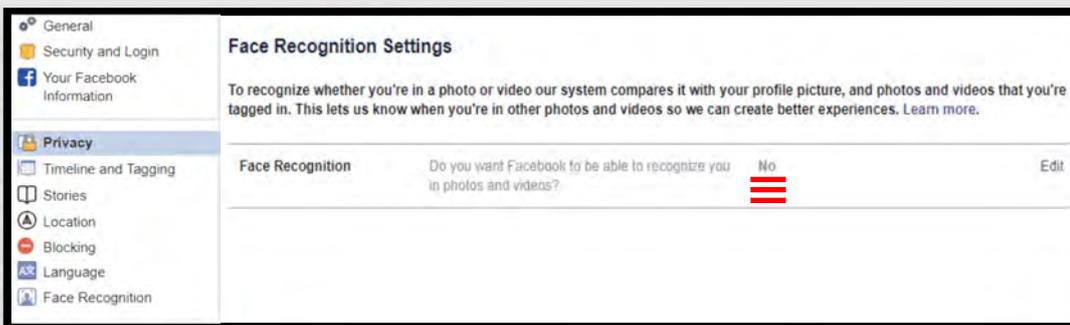
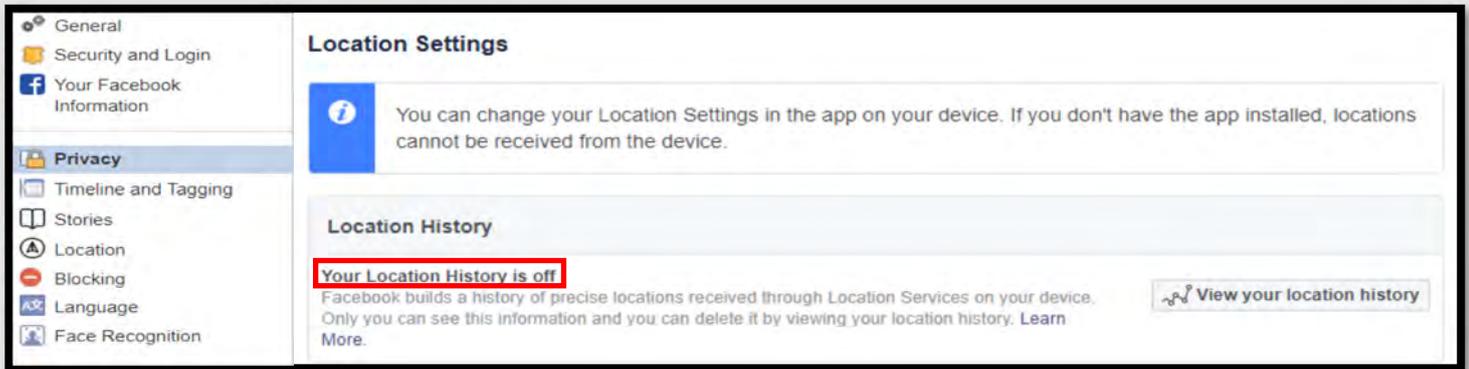
Now, along with noting in the "Timeline and Tagging" section, you will also need to lock down your stories in the "Stories" section shown directly above.

you might want to lock down later such as old profile pictures. Since the "Stories" function has become more and more popular amongst all users it is important to remember it too needs to be locked down. Facebook has created a lock down feature in order to prohibit other individuals from sharing your "Stories" as shown above. It is recommended that you turn this function to "Disabled."

FACEBOOK SMART CARD

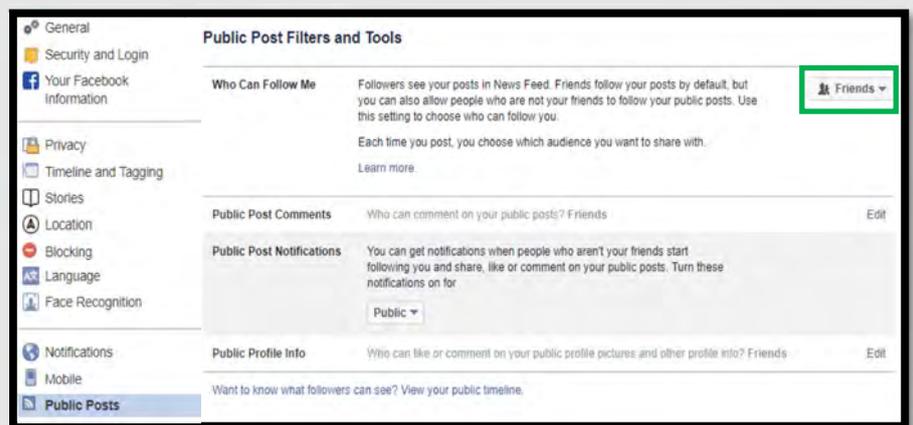


In the "Location" section make sure Facebook shows your location is "Off". You must also turn your location settings to "Off" on each of your mobile devices to ensure the pictures/data you post do not contain geolocation information.



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

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



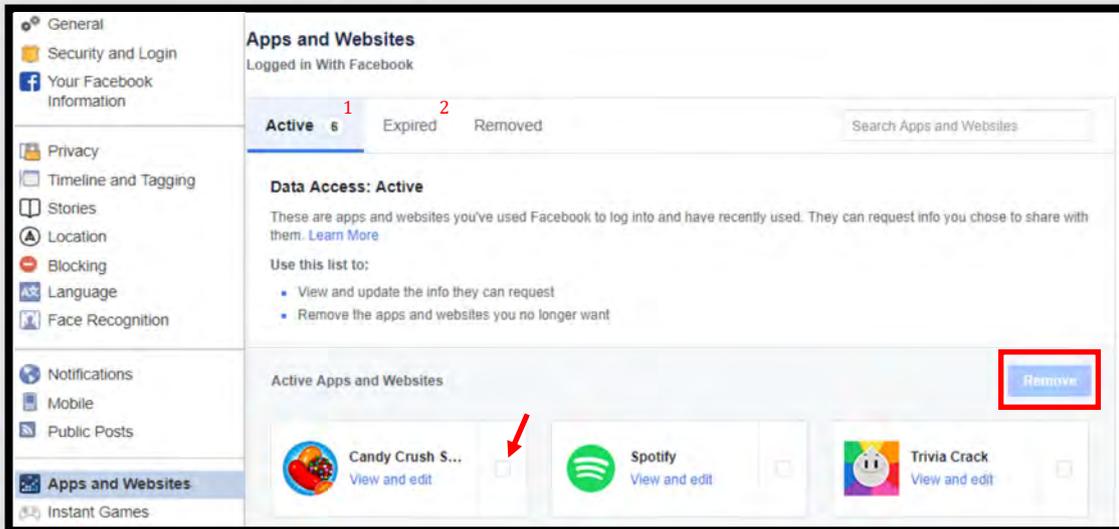
Next, in the "Public Post Filters and Tools" section lets review public filtering. It is recommended that you do not let the public follow you. Remember, allowing the "Public" to follow you means anyone with a Facebook profile, and possibly even without one, can see what you are posting.

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

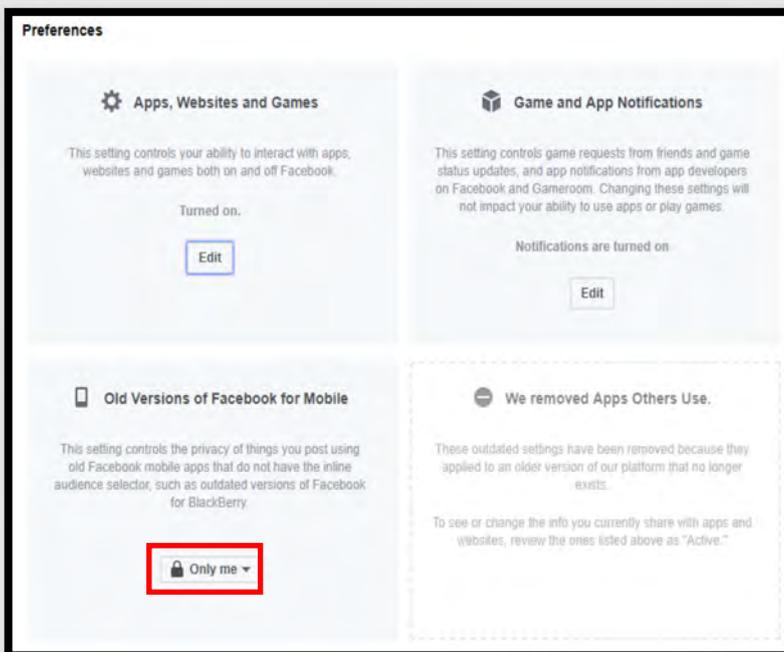
FACEBOOK SMART CARD



Next, lets clean up all the “Apps and Websites” that have been allowed to use your information. Here you can review all the applications you may have allowed access to your Facebook account.



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.



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.

It is recommended 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.

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.

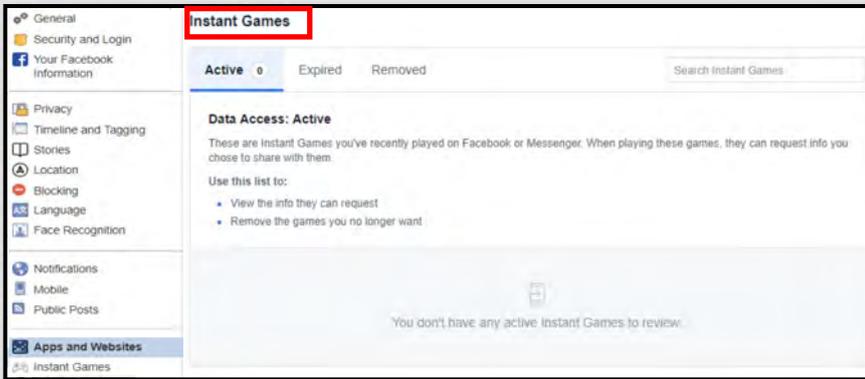
References:

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

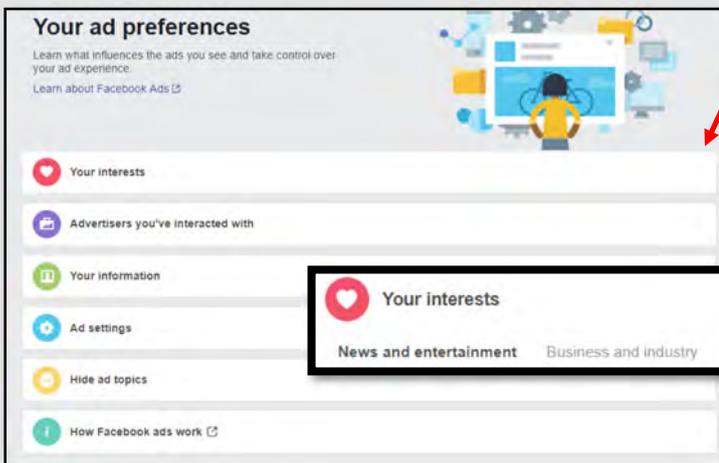
FACEBOOK SMART CARD



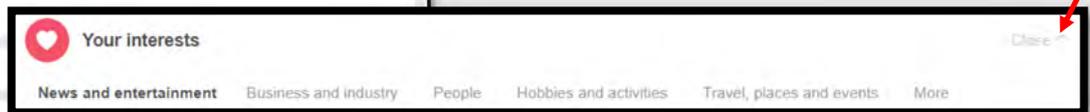
Never give up too much information, drawing out your family members on Facebook could help an Identity Thief answer security questions about you. #themoreyouknow



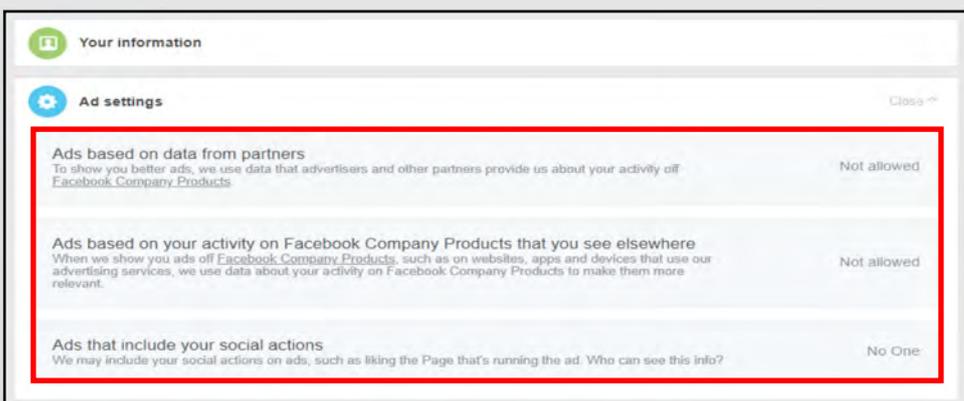
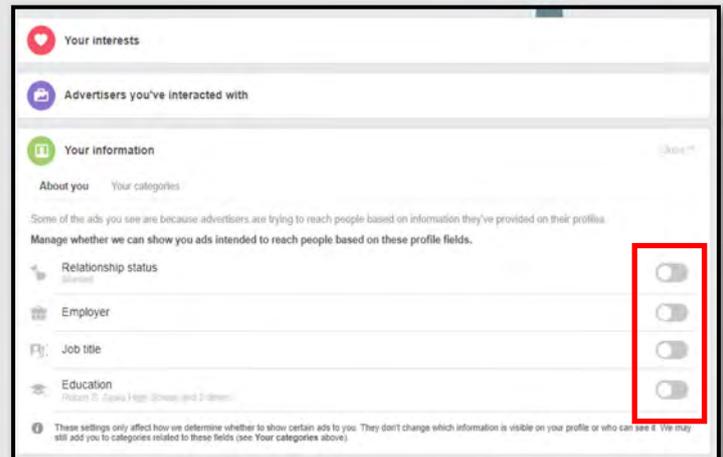
Now click on the “Instant Games” tab on the left hand side. Review any games you may have allowed access to your account, the type of data they are collecting, and whether or not you want them to remain on your Facebook account. If you choose to, you can delete any of the games much like you just did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



Now lets look at “Your ad 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 categories simply by clicking the “x” at the right of each block.

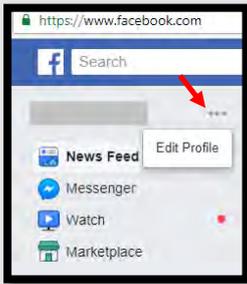


Under the “Your Information” tab, ensure all the sliders are off (greyed out) so that none of your information is provided by Facebook to advertisers.” It is important to limit the information advertisers have access to about you. This will help to ensure your information doesn’t show up on advertisements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

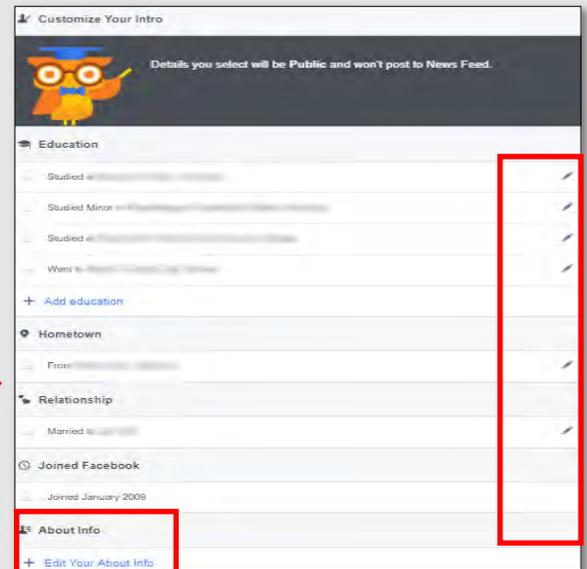


Under the “Ad Settings” it is recommended that you select “Not Allowed” or “No One” for each category.

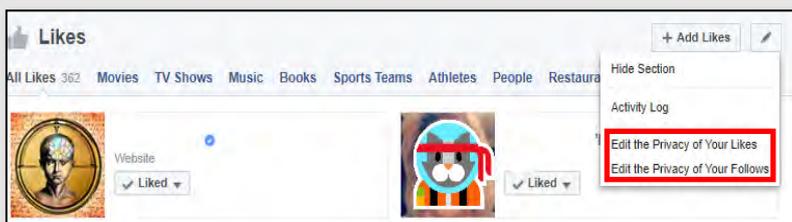
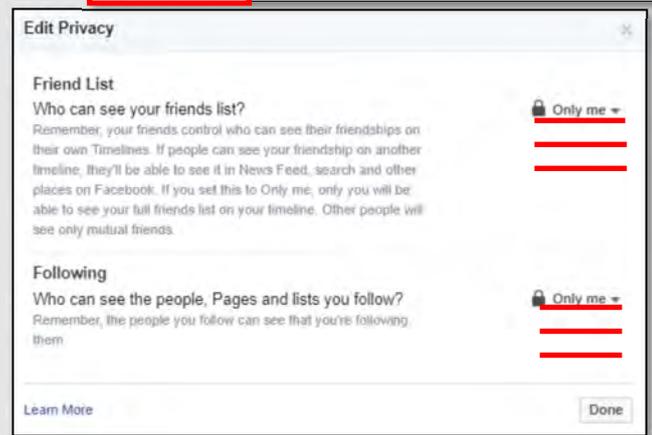
FACEBOOK SMART CARD



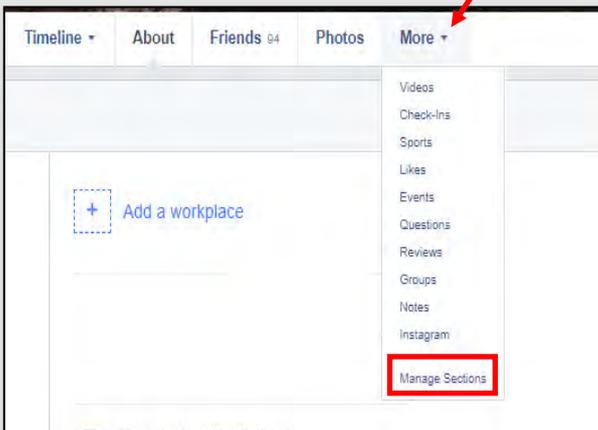
Now that you have completed the Settings sections lets move on. From the Home screen, select the three dots on the left hand side of the screen near your profile picture. A drop down menu will appear that allows you to edit your profile and change the privacy settings on your personal information. Once you review the privacy settings in this section scroll to the bottom of the page and select "Edit Your About Info".



Now you can scroll through each tab in the "About You" section to ensure the privacy settings there are not set to "Public" view. Next up is your Friends List. Click on the pencil icon to display the Edit Privacy box. From here you can change the settings to "Only Me" or "Friends" so that only you and your friends can see the information. It is highly recommended you set your "Friends List" to "Only Me".



Now, there are two different spots on your **profile** where you need to lock down your "likes". The first is simply by scrolling down in the section you are already in and selecting the pencil icon to edit the privacy setting. The second, shown below, can be found in the "More" tab at the top of the page.

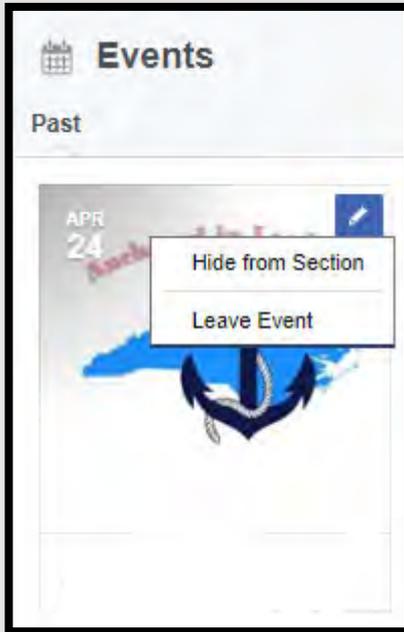


Locking down your "likes" will help to limit what criminals can figure out about you and your family. In this day and age you never want to give away even the slightest clue as to who you are, which includes, any of your hobbies/interests or perhaps the fact that you "like" your child's school or youth sports team. Recommended setting here "Only Me".



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

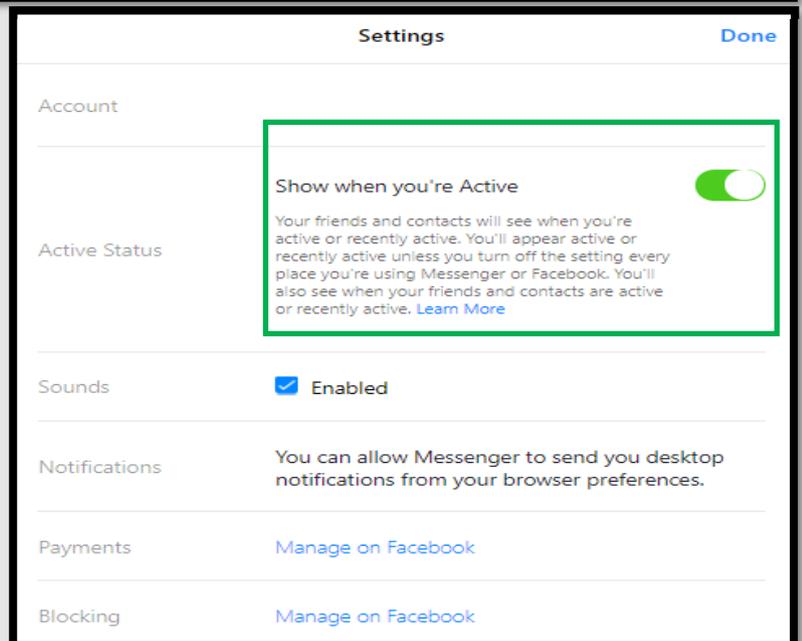
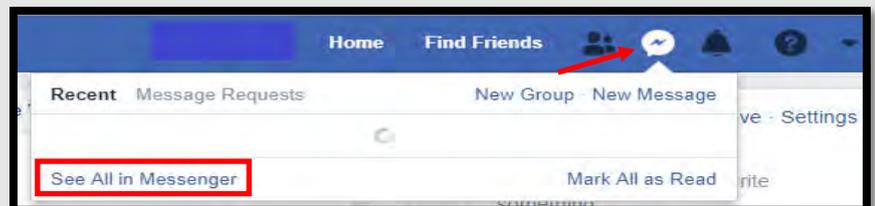
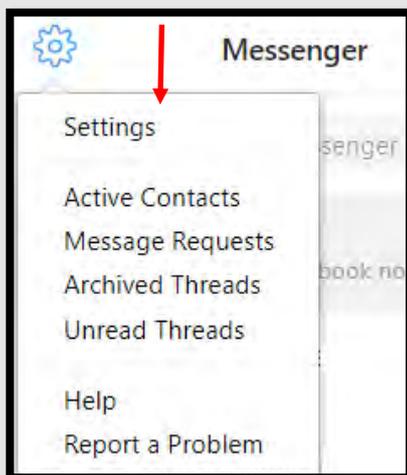
FACEBOOK SMART CARD



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 and to make sure all your events are “Private” (which can only be done through the Event Creator). If you have an upcoming “Event” or an “Event” that you are “interested in” that is not set to “Private”, be aware that anyone will be able to see that you will be attending that event. You also have the option of hiding the ‘Events’ section by unselecting it from the “Manage Selection” discussed on page 31.

*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 no limit to the dangers. They could convince you to meet in person, lend them money, steal your identity or worse get close to your children. The best option is to limit who can see such critical information about you to your “friends” people that you trust and already know.

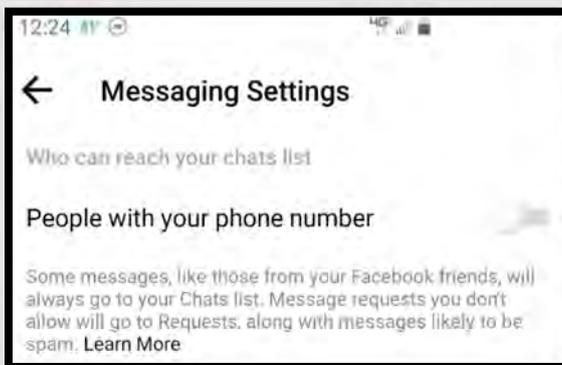
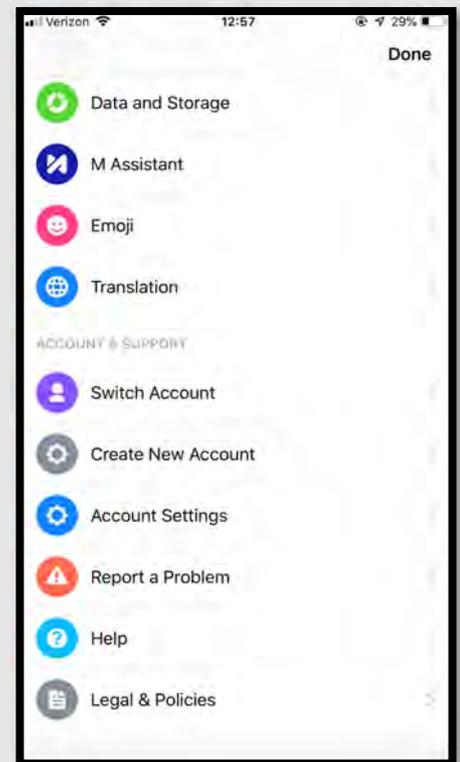
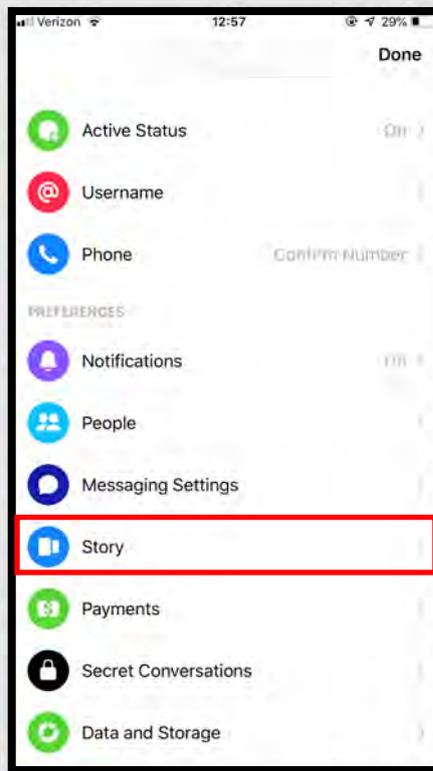
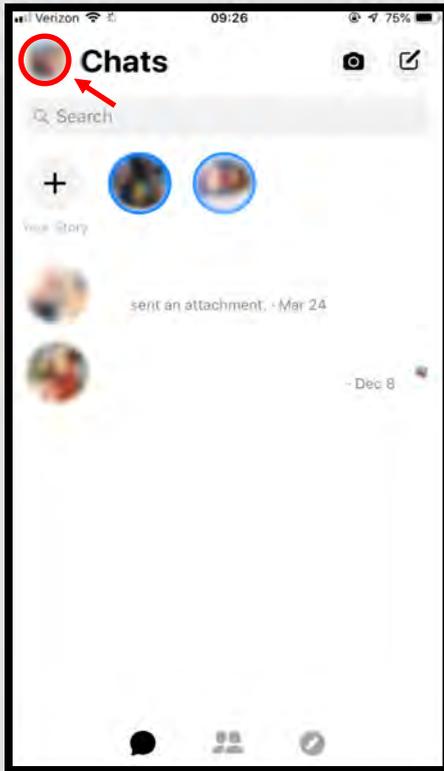
You may want to go back to the top of the page to the conversation Icon. This Icon will take you to your Messenger page. Here you will be able to turn on and off your “status” on messenger.



Here you can manage some of the settings associated with your Messenger account, most notably the “Active” status button. If you do not want to allow people to know whether or not you are on Facebook Messenger you can turn off the “Active” status. #keepthemguessing

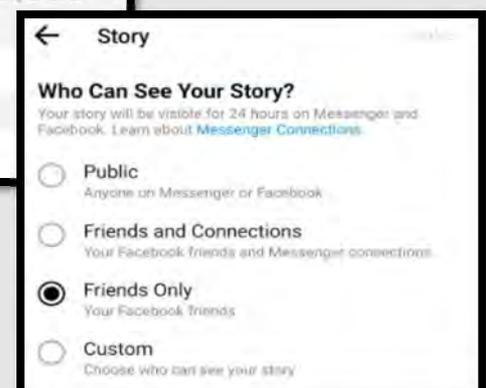
How many “friends” do you have on Facebook? Would you recognize them if they were standing right in front of you? #FBpurge #whoareyourfriends

FACEBOOK SMART CARD



In order to accurately lock down your Facebook, you will need to also review your Messenger App. Once logged in, head to the top left of the screen select the picture icon (highlighted here 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.” Next scroll down to the “Messaging Settings” where you can select who can and cannot reach you via Facebook Messenger. It is recommended that you not allow “others you’re not connected to” contact you via Messenger.

Facebook Messenger has a new feature called “Secret Conversations” where you conversations are encrypted end-to-end. To turn this feature on Go back to your settings and 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.



Also, located in the “Settings” section of your Facebook Messenger select “Story” (shown above highlighted in red). This is another location where you can set the settings for your Stories on Facebook. It is recommended that you only allow your friends to see your “Story”.

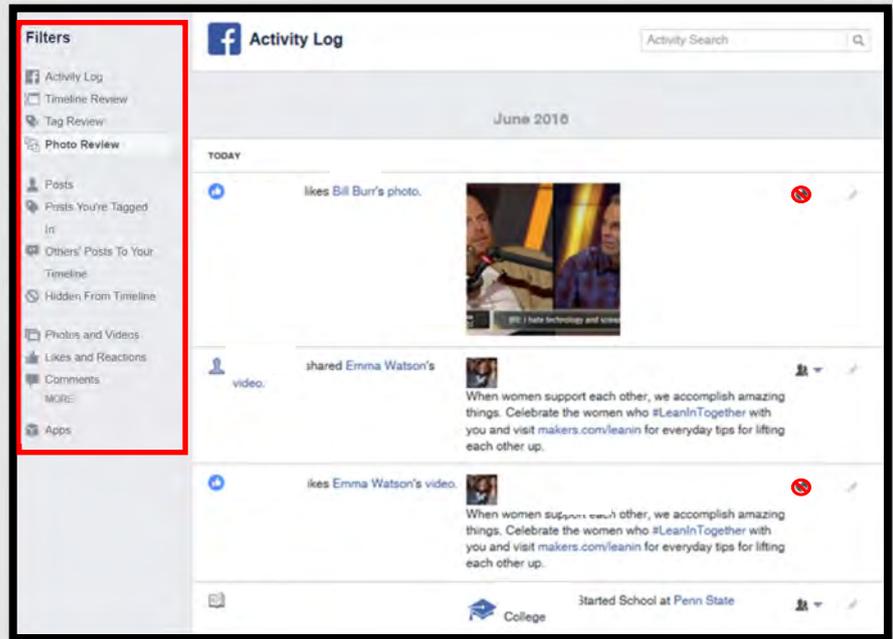
Remember, it is important to lock down your Facebook Messenger the same way you lock down the rest of your Facebook.

FACEBOOK SMART CARD



Finally, lets go back to Facebook's **Activity Log**, accessed from the upper panel of your **Timeline**. The **Activity Log** allows users' to review any click of the button (photos, comments, Likes, posts, etc.) or tag that has ever occurred and been associated with that users profile. It's essentially your one stop shop for cleaning up your entire Facebook profile.

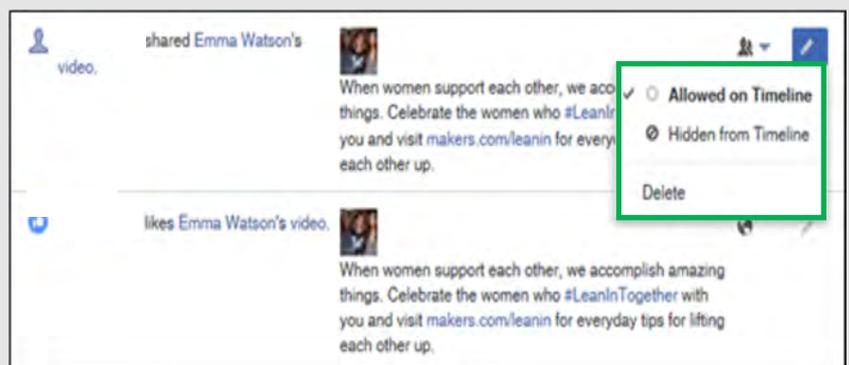
More specifically, from the **Activity Log**, users are able review information by date, all the way from the creation of the profile to the present. Users can also see if a post is viewable to the public or just to friends, as well as review any and all posts they have been tagged in. Finally, the **Activity Log** also allows users to remove any actions they have taken on Facebook and decide whether or not to remove a tag of themselves that someone else may have posted.



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 (yours or anyone else's), so be aware of how others treat their privacy as well.



You can also choose to **Delete** or **Hide** each post from your Timeline. For other users' posts you have Liked, you can also choose to Unlike them. This will remove the post from your Activity Log and profile.



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



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

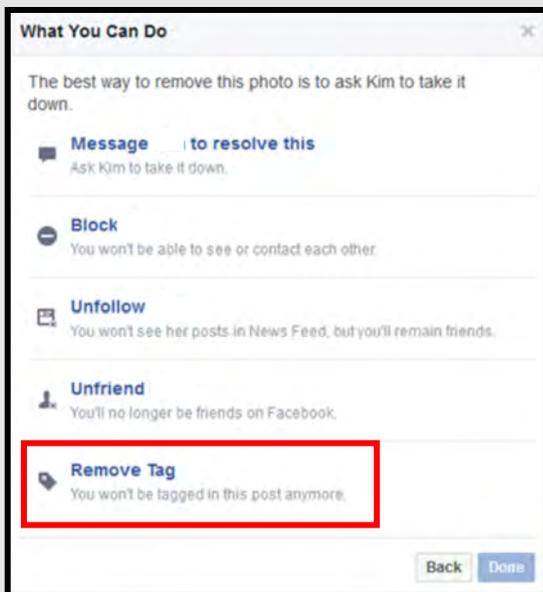
To “Untag” a photo, click the **Pencil** icon at the top right of the post and select **Report/Remove Tag**.



Facebook will then ask why you want to Report/Remove the picture or tag.

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.

You will then be given several options on what you would like to do with the picture/post, including **Remove Tag**. Once you have selected the **Remove Tag** option and are **untagged** from the post/photo, it will no longer appear on your profile.



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

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

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

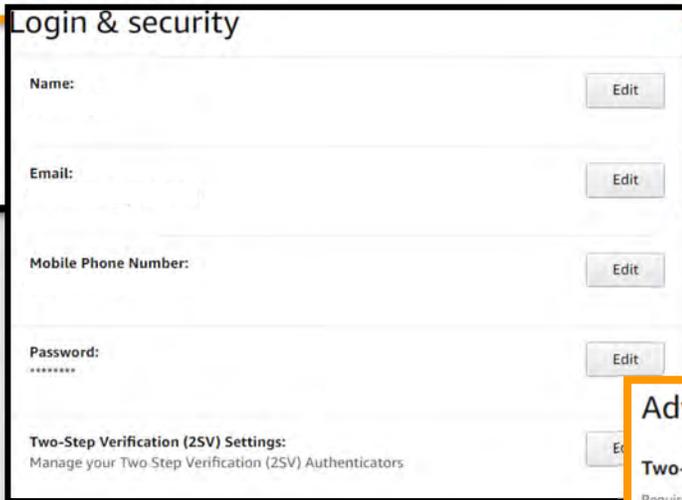
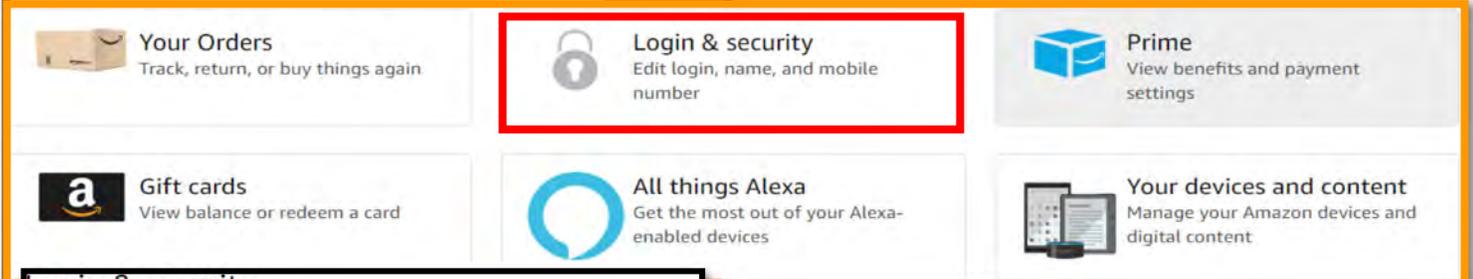
LOCKING DOWN amazon

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 vitally 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 to 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 wherever possible to protect yourself from Identity theft and scams.



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" icon, 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. It is highly recommended that you enable this 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. This process is an important feature to help secure your account given the credit card, addresses, and other personal information maintained by Amazon.

Advanced Security Settings

Two-Step Verification

[Get Started](#)

Require a secondary passcode to sign in to your account

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 code.
3. You'll enter the code, 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

Ordering and shopping preferences

- Your addresses
- Payment options
- Your Amazon profile
- Archived orders
- Manage your lists
- Download order reports
- 1-Click settings
- AmazonFresh settings
- Language preferences
- Coupons

Digital 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

photos Amazon Photos All Files

Your storage

Photos
0 B used | Unlimited
0 Photos

Videos and files
0 B used | 10 GB total storage
Available: 10 GB

- Settings
- Family Vault
- Amazon Drive
- Send feedback
- Help
- Prints order history
- Shared items
- Blocked contacts
- Hidden items
- Switch accounts
- Sign out

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, re-move accounts you no longer use.

Manage Third-Party Apps

Login with Amazon allows you to log in to registered third-party websites or apps using your Amazon user name and password. It also allows you to opt-in to letting third-party websites or apps read or modify content in your Amazon Photos account. [Learn more](#)

Manage Login with Amazon

Next, go back to the “Amazon Drive” link and from the left hand corner select “Amazon Photos.” Once there head to the right side of the window and select the drop down menu.

You consented on September 4, 2017

This connection allows access to:

- Updates you make to the following profile info
- Name
- Business list
- Email address: [redacted]@gmail.com

Remove

- Settings**
- Family Vault
- Amazon Drive
- Get the apps
- Send feedback
- Help
- Prints order history
- Shared items
- Hidden items

From the drop down menu select “Settings” and scroll to the middle of the page where you will find the “Find People, Places, and Things” section. This function, when left on allows Amazon image recognition to identify images in your pictures so you can search for them later. It is recommended that you turn this function off to prevent Amazon from collecting additional data on you.

Find People, Places, and Things OFF

Automatically tag your photos by keyword, group together photos of the same people and places, and more

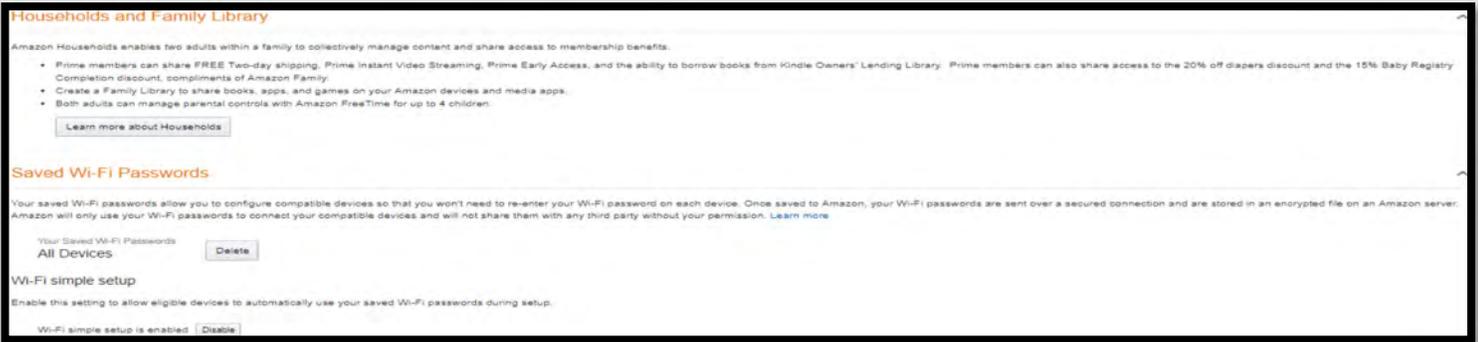
Turn on image recognition to use Search or People. Image recognition organizes and lets you search for photos based on things in your pictures. This setting applies to all members of your Family Vault.

[Learn more](#) [Illinois residents, by turning on image recognition features, you agree to this important legal information](#)

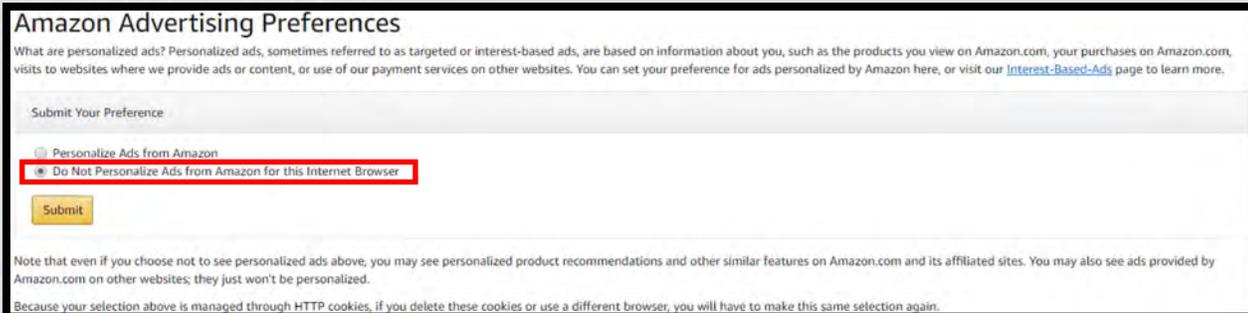
You can call the customer service department and ask about suspicious emails to see if it's authentic. Whatever you do, don't try to get to Amazon through the suspicious email. #trustbutverify

LOCKING DOWN amazon

Now, let's go back to "Your Account" and select "Your devices and content", then select "Change your digital and device settings" section you may want to review the settings below to make sure the content comports with your needs. It is recommended that you review the "Saved Wi-Fi Passwords" to make sure there are no passwords saved that you do not wish Amazon to retain.

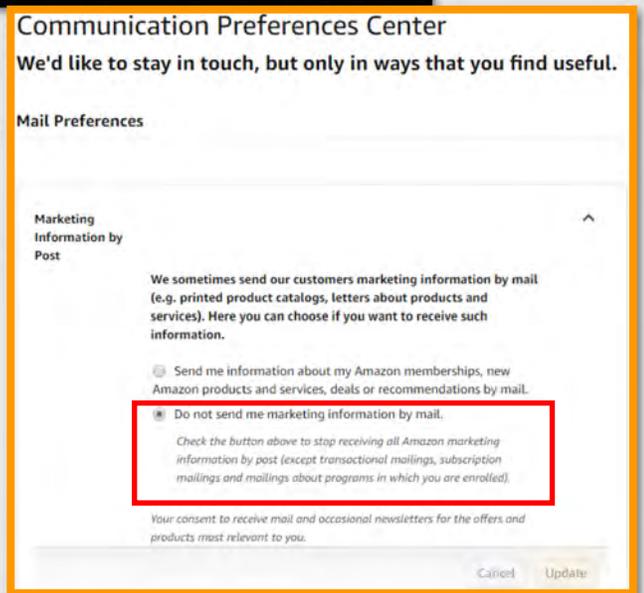


Now let's head back to "Your Account" and in the "Communication and Content" section, select "Advertising Preferences" so we can review what Amazon provides to you and to advertisers. Personalized ads, sometimes referred to as targeted or interest-based ads are based on information about you, such as the products you view or purchases you make on Amazon, or websites you visit where Amazon might provide ads or content.



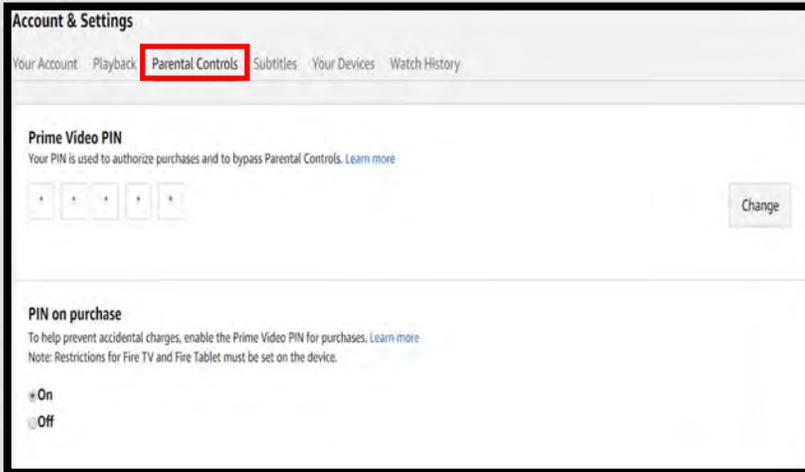
It is recommended you select "Do Not Personalize Ads from Amazon for this Internet Browser." What this does is exactly what it says in the title, but for the current browser only. Amazon has been known to reset your privacy and other settings if it is opened from a browser different from the one used 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 and / or clear your browser history.

Now, let's go back to "Your Account" and select "Communication Preferences." From there it is recommended you select "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



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 simply select "Video Settings." Now at the top of the page find and select "Parental Controls" and let's begin. For parents, it is always important to monitor and protect our children from non-age appropriate material on the internet and television screen. Amazon allows parents to set Prime Video PINs and viewing restriction. Settings 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 of your PIN to bypass any purchase or viewing 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](#).

It is highly recommended that you take time to re-view each device you may 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 utilizing the credit card on file.

LOCKING DOWN



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 like is. #themoreyouknow

Ordering and shopping preferences Your addresses Payment options Your Amazon profile Archived orders Manage your lists Download order reports 1-Click settings AmazonFresh settings Language preferences Coupons	Digital 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
---	--	--

Moving on, go back to "Your Account" and review the following sections: "Ordering and shopping preferences;" "Other accounts;" and "Shopping programs and rentals."

One of the most public sections of Amazon are the "Wish Lists." If not made private, anyone can view your list(s) and gain or infer information about who you are or who the people in your family are (How many, gender, age, etc.). Many times, you may find yourself making Christmas lists, birthday lists, or even grocery lists. The titles of these lists are usually specific (i.e. a child's name for a birthday or Christmas list). These small tid bits of information could be extremely useful to a Social Engineer or identity thief when combined with other bits of data on you. It is important to note that Amazon has changed their privacy for "Wish Lists," a User now needs 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 or not, Alexa with access to your "Lists," it is not recommended that you provide such access but instead continue to lock down and privatize each list.

Select "Manage your list" from "Ordering and Shopping Preferences" in order to begin the process of locking down any of these lists you may have. 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



Much like a “Wish List”, your registries can also be displayed publically unless you say otherwise. While still in your “Wish List”, go to the top menu and select “Baby Registry.” To create your Registry select “Get Started” from the center of your page. Scroll down to the “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 also be included 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 any Registries you use when they are no longer needed.

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

Who can see your registry? (you can change this at any time)

- Public:** Anyone can see this registry
 - Include my registry on TheBump.com [Learn More](#)
- Shared:** People with a link can see this registry
- Private:** Only you can see this registry

Email options

- Gift alerts when items are purchased
- Exclusive Baby Registry discounts
- Baby Registry Email Newsletter – filled with exclusive deals, tips, and more



In order to lock down your Wedding Registry, go back to the “Wish List” menu and select “Wedding Registry.” From there, scroll to the middle and select the appropriate privacy settings for your Registry. It is recommended that you not make your Registry “Public” and remember that once you no longer need the registry, be sure to delete it.

Like the “Baby Registry,” the “Wedding Registry” may also be listed on a third party vendor, TheKnott.com. It is recommended that you not make your registry searchable on The-Knott.com

Would you like to share your registry?

- Anyone can see this Wedding Registry. Your name(s) will be publicly available, and elsewhere on Amazon.
- Only people with a link can see this Wedding Registry. Your name(s) will be visible on your Wedding Registry and elsewhere on Amazon.
- Only you can see this Wedding Registry
- Make my registry searchable on TheKnot.com. [Details](#) ▾
- I want to receive emails about my registry.
- I want to receive wedding product offers and special discounts.

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



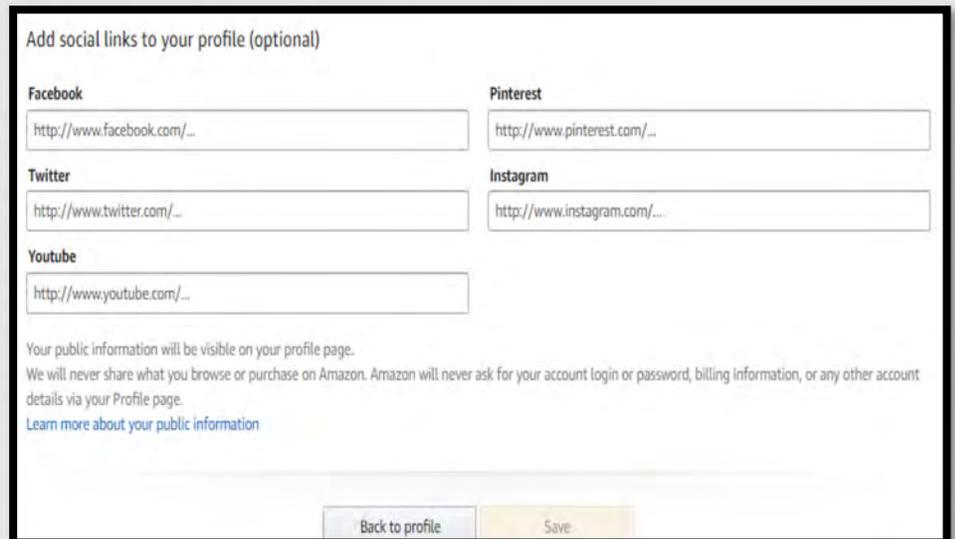
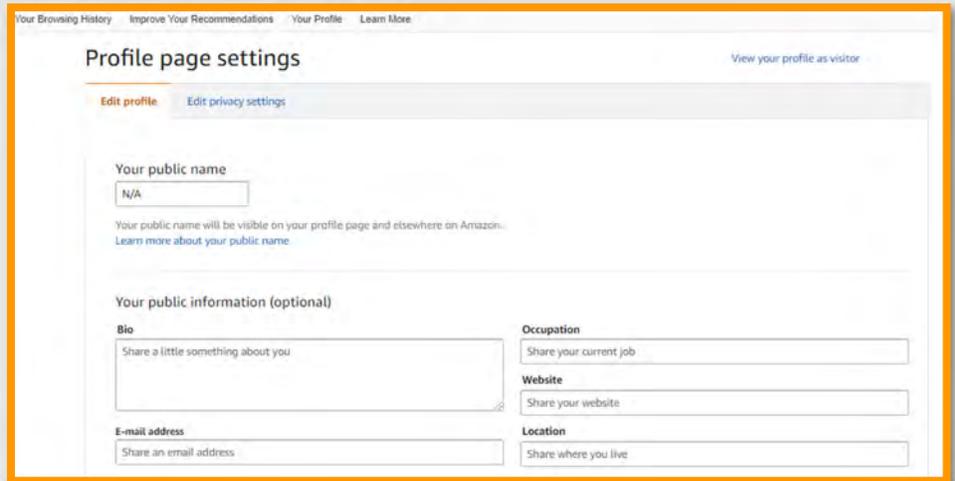
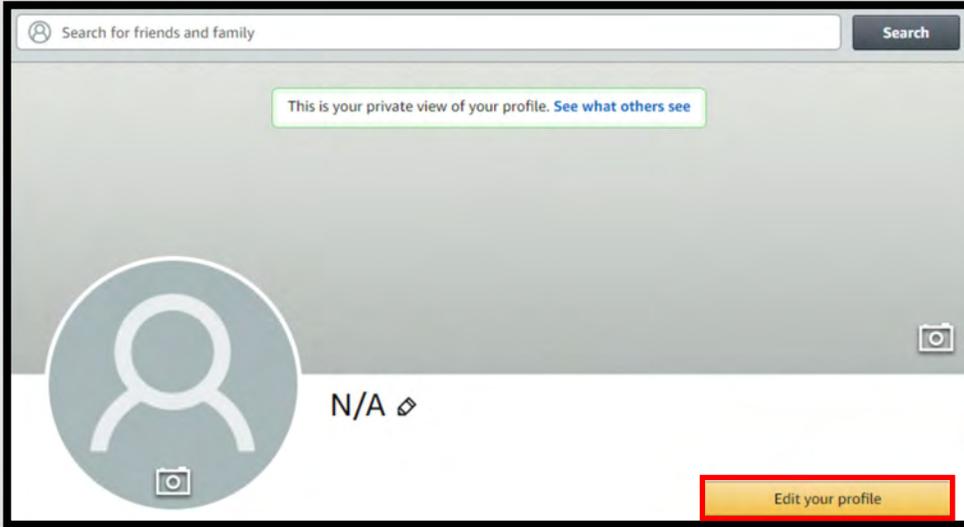
Ships from and sold by [seller]: Third-party seller that ships an item from them directly to you. Amazon doesn't touch the item. This is where scammers thrive. #themoreyouknow

What most people do not realize about Amazon is that it comes 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" and select "Your Amazon Profile." From there, follow the steps below and on the remaining pages to best secure your profile.

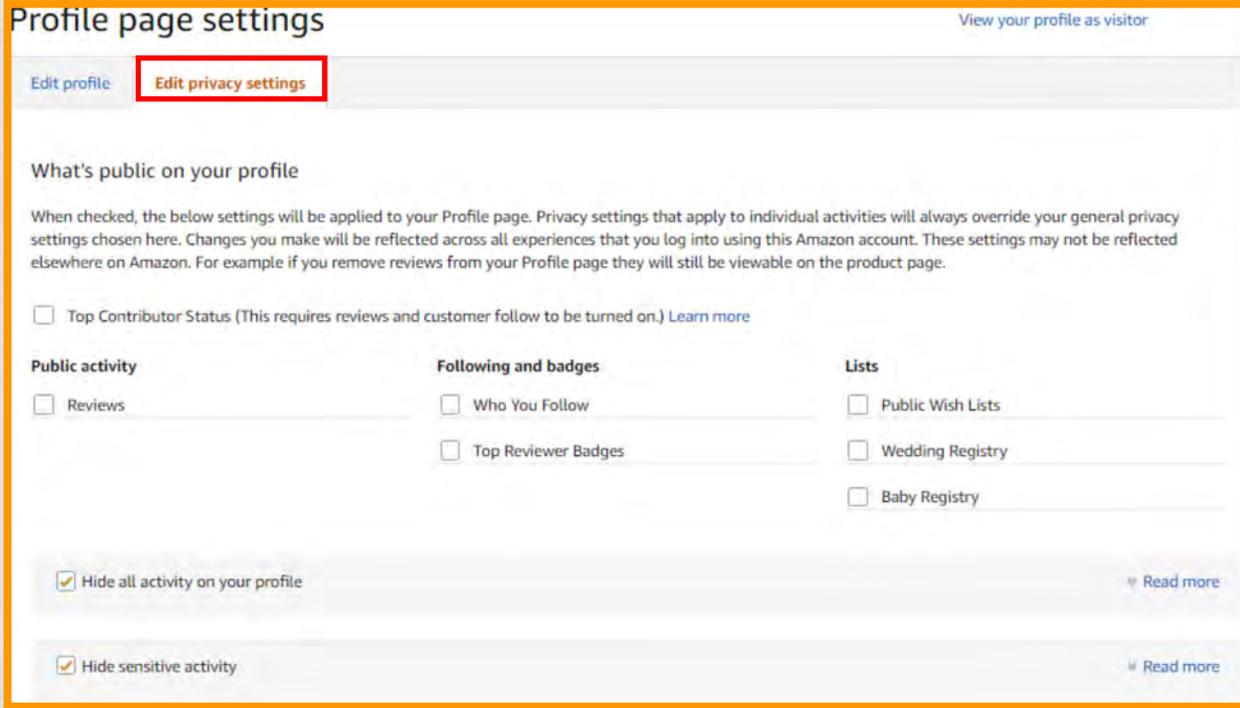
Now let's begin the process of making sure your "Profile" is locked down. Select "Edit your profile" as shown above in **red**. In the "Profile page settings" review, all of your information to make sure, only information you want on public profile is filled in. It is recommended that you not display 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 may post on Amazon. It is recommended that if you do review products that you try not to put any personal in-formation inside your review.



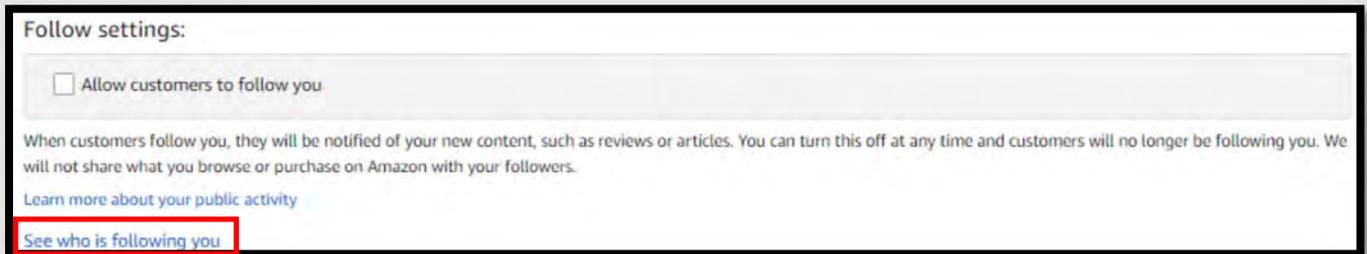
Sold by [seller] and Fulfilled by Amazon: A third-party seller sends the product to Amazon's warehouse, then Amazon ships it to. These items can be "Prime" eligible, but are still third-party.

LOCKING DOWN amazon



Let's now 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. It is recommended that you select the box "Hide all activity on your profile" as well as "Hide sensitive activity."

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.



If you have any followers, you can delete / remove them from this link and then update your privacy settings as shown above to preclude any other followers. It is not recommended that you allow people to follow you on Amazon, but especially if you do not know them.



LOCKING DOWN



Now let's take a look at your Browsing history. Simply 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 many 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, but the parents maintain control over any 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.

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.



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

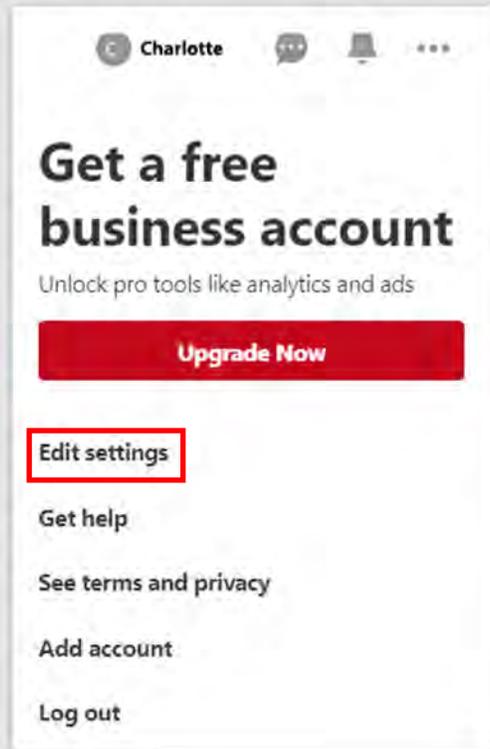
LOCKING DOWN



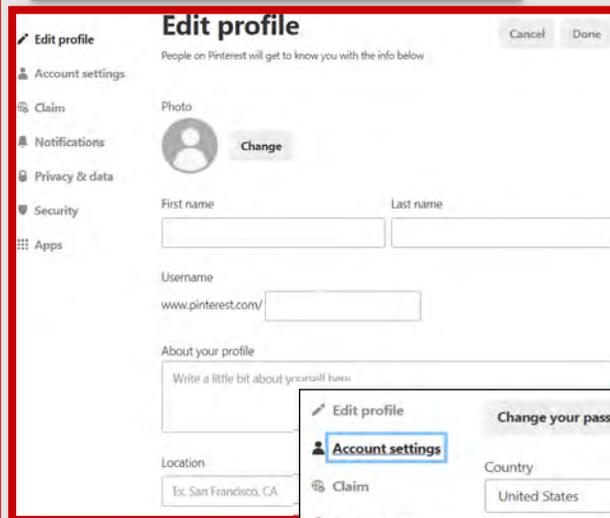
Check your credit report at least once a year. You may also want to check your credit report if you feel any of your social media accounts have been compromised. #beatidentitytheft

Do's and Don'ts

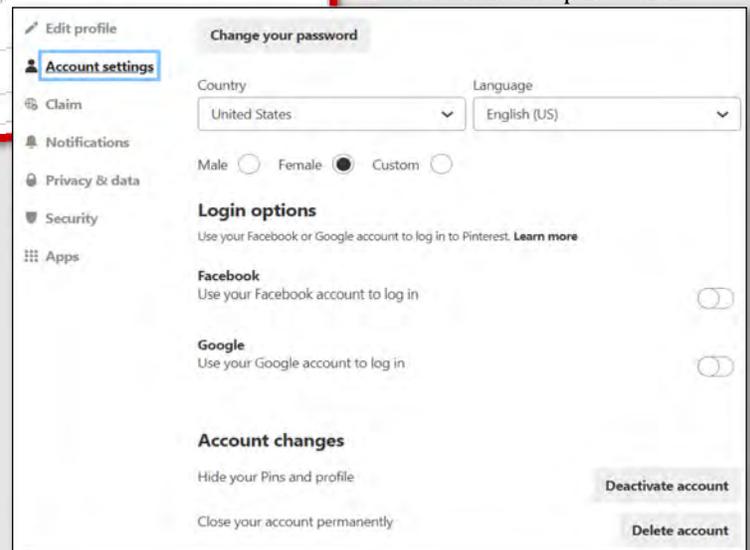
- ◆ Do use Two-Factor Authentication to protect all your information. Like all other social media accounts, it is important to make sure your Pinterest is as secured as possible. Two-Factor Authentication is one of the best ways to control your information.
- ◆ Do make sure your email is up to date! 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 not 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.).
- ◆ Do not forget it is highly recommended that you 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 not forget to make your boards private once you create them so that they are not searchable by any and all Pinners.



While there aren't many privacy settings to manage on Pinterest, it is no less important to ensure those settings are locked down. In order to change your Pinterest settings look to the top right of your screen and select the horizontal ellipsis to expand the menu. It is recommended you make your account private by selecting "Search privacy" (highlighted below). Once you are in the "Edit Settings" page you will be able to go through each of the settings provided by Pinterest. The first settings to review are the "Edit settings," which provides your basic information on Pinterest. It is recommended that you do not include your "location" when building your Pinterest Profile.



Under "Account settings" you will find the options to delete or deactivate your account in case you decide you no longer want to use your Pinterest. Here you can also chose (or not) the option to login from other social networking accounts. This step is highly discouraged, it is instead recommended that you login to your Pinterest with only your Pinterest username and password.



LOCKING DOWN



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.

Edit profile	Claim other accounts Connect your other content with Pinterest. We'll attribute Pins from your claimed accounts to you. You'll get stats about each Pin. We will also use claimed account information to help distribute your content and offer you additional Pinterest features and content. Learn more
Account settings	
Claim	
Notifications	
Privacy & data	
Security	
Apps	

Instagram Add your name and profile picture to Pins from your Instagram account.	Claim
Etsy Add your name and profile picture to Pins from your Etsy shop.	Claim
YouTube Add your name and profile picture to Pins from your YouTube channel.	Claim

The next few settings have to do with linking (or not) your other social media accounts to Pinterest. **As always, it is highly recommended that you do not link any other social media accounts to each other.** If by some possibility someone was able to access, one of your social media accounts, not linking your accounts together prevents an intruder from accessing all your other accounts.

Search Privacy

Hide your profile from search engines (Ex. Google). [Learn more](#)

Next, continue down the screen to find "Privacy & data" and review the settings. These settings will help to limit what Pinterest Ads gather about you. It is recommended here that you do not enable these settings and allow Pinterest to push ads based on other internet habits of yours. It is also highly recommended that you not allow Pinterest to display your profile in Google's searches.

Personalization

Use sites you visit to improve which recommendations and ads you see. [Learn more](#)

Use information from our partners to improve which recommendations and ads you see. [Learn more](#)

Use your activity to improve the ads you see about Pinterest on other sites or apps you may visit. [Learn more](#) in Help Center.

Share activity for ads performance reporting. [Learn more](#)

Security

Enable Two-factor Authentication.

Require code at login

This makes your account extra secure. Along with your password, you'll need to enter the secret code that we text your phone each time you log in.

This is a list of devices that have logged into your account. Revoke any sessions that you do not recognize.

Show sessions

Cancel **Save settings**

Now, let's ensure that you enable Two-Factor Authentication. As recommended for all your accounts, it is highly recommended that you enable Two-Factor Authentication. This will help to ensure you have taken all steps to secure your account and keep it safe.

Below, highlighted in **red**, you will see a smaller section labeled "Show Sessions" which will be discussed on the next page.

LOCKING DOWN



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

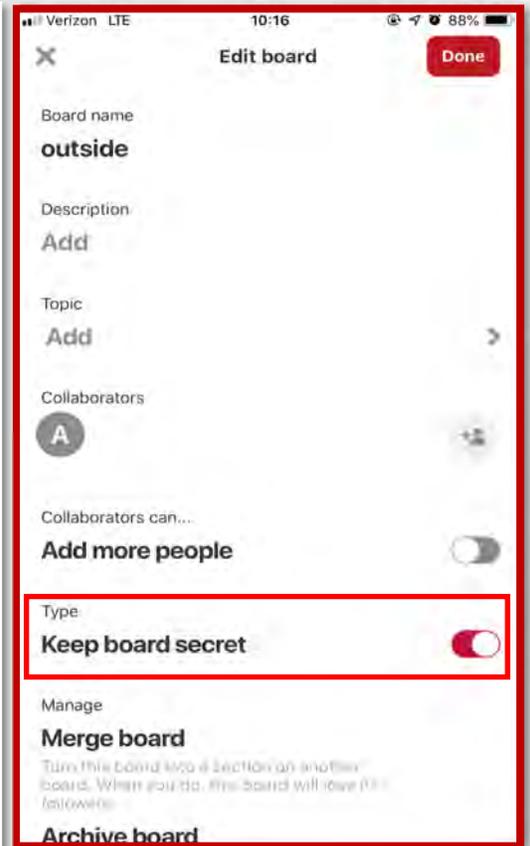
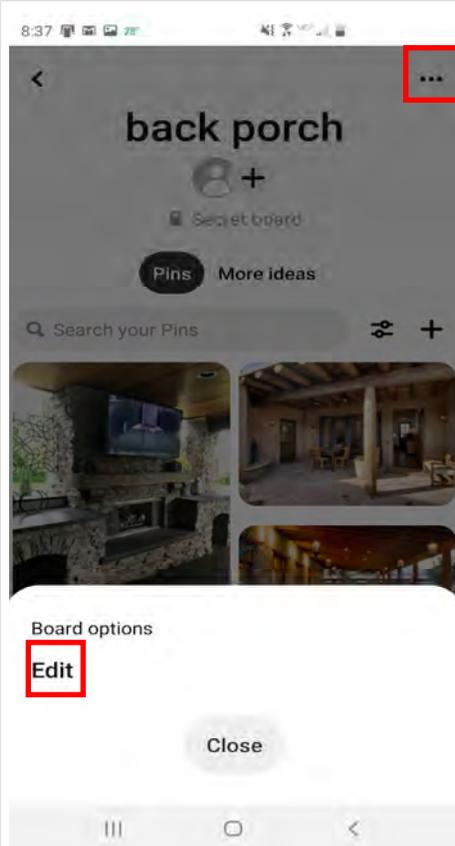
This is a list of devices that have logged into your account. Revoke any sessions that you do not recognize.

Hide sessions

Last accessed:	October 25, 2018, 8:14 AM	Current Session
Location:	Texas, United States (Approximate, based on IP = 162.210.1.1)	
Device type:	Chrome on Windows 10	
Last accessed:	October 24, 2018, 11:46 PM	End Activity

After selecting "Show Sessions" directly under the "Two-Factor Authentication" section, you will be provided the opportunity to "End Activity" for all sessions that may seem suspicious or that you do not see a need to be active any longer. If you suspect that your Pinterest account may have been compromised, the "Show Sessions" section may help you to identify the account and "End Activity" so that you can then secure your account and change your password. It is a good idea periodically, to go through the "Show Sessions" section to make sure nothing looks suspicious and end older activity.

Lastly, let's look at your boards and make sure that there isn't too much, if any, information available for others to see. In order to review or to lock down your boards via your smart device, head to the bottom of your screen, select your profile picture and then select a board to review and edit. To edit, select the three dots at the top of your board screen, then select "Edit" as shown below in red. If you are not going to make your board private, then the title of your board becomes important. Try to make sure the title of your board doesn't provide too much information about you or your family; for instance naming the board after a child or stating their birthday. Finally, it is recommended that you enable "Keep board secret" so that your boards are not viewable to the public. Boards often times provide likes and dislikes of a person as well as other hobbies and interests that may make it easier for an Identity Thief to steal your identity.

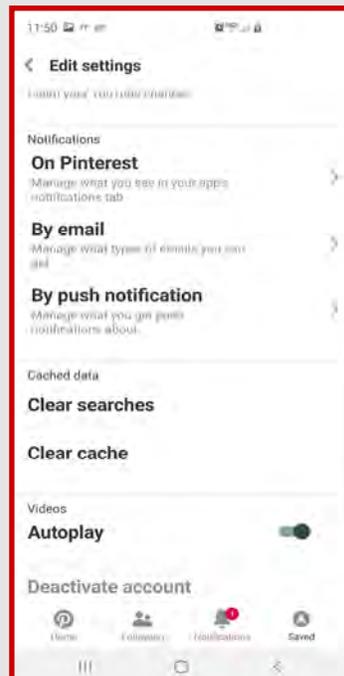
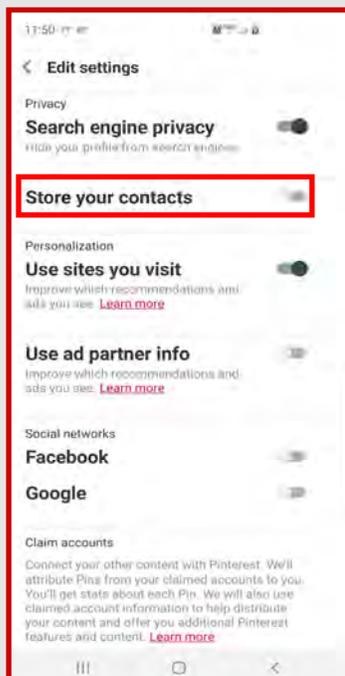
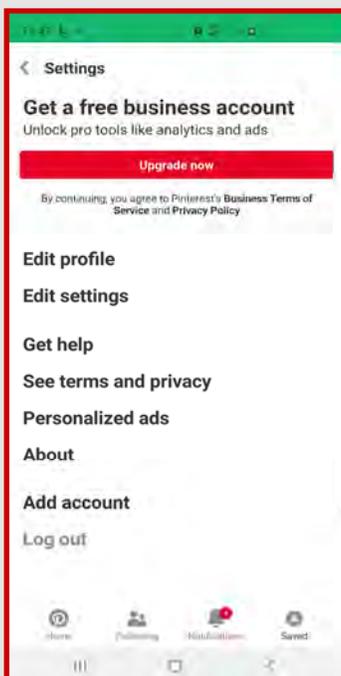
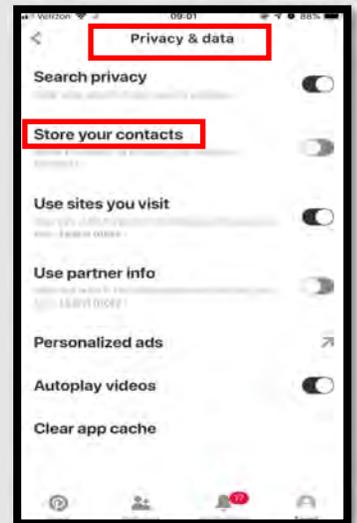
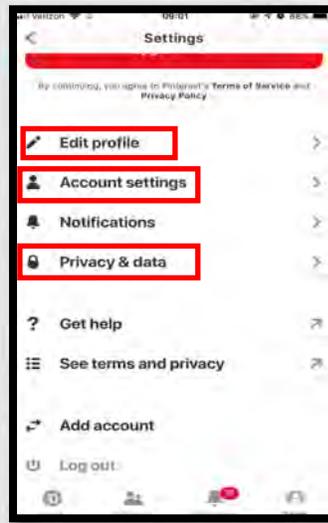
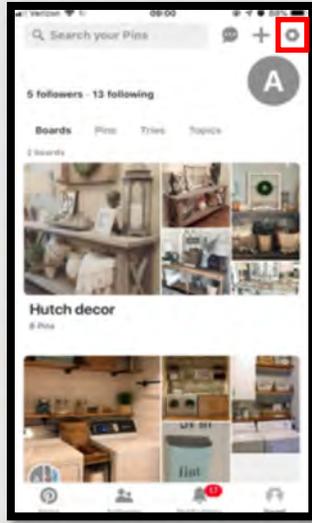


LOCKING DOWN



Using your smart device to lock down your Pinterest account might just make the entire process even easier. As shown below, in just a few simple clicks you can be in your “Edit Profile” section, “Account Settings” and most importantly your “Privacy & data” setting. You will still want to lock down each section as previously discussed in the beginning of this Smartcard most of which is now in the same format as it is on your computer, however the “Privacy & data” section is a bit different and therefore renders some extra looking into. One important section to note in the “Privacy & data” section is the “Store your contacts” section, it is recommended that you do not link your phone contacts to your Pinterest account. It is a good idea to check your Pinterest App settings on your smart device even if you have changed or updated the settings on your computer to make sure they also transferred to the app. As a reminder, the recommended settings that you should set are highlighted by the red box.

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.



If you have an Android Smartphone, the “Edit Settings” functions may be a bit different (as shown to the left). All the necessary settings for the Android phone will be located all under the “Edit Settings” section. Simply scroll down the list of options in order to decide what best suits your security needs. As noted earlier it is recommended that you do not allow Pinterest to store your contacts (highlighted to the left in red).

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
- * 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 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.

Also, 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 still need help or have questions, you can always contact Pinterest by: 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 also 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

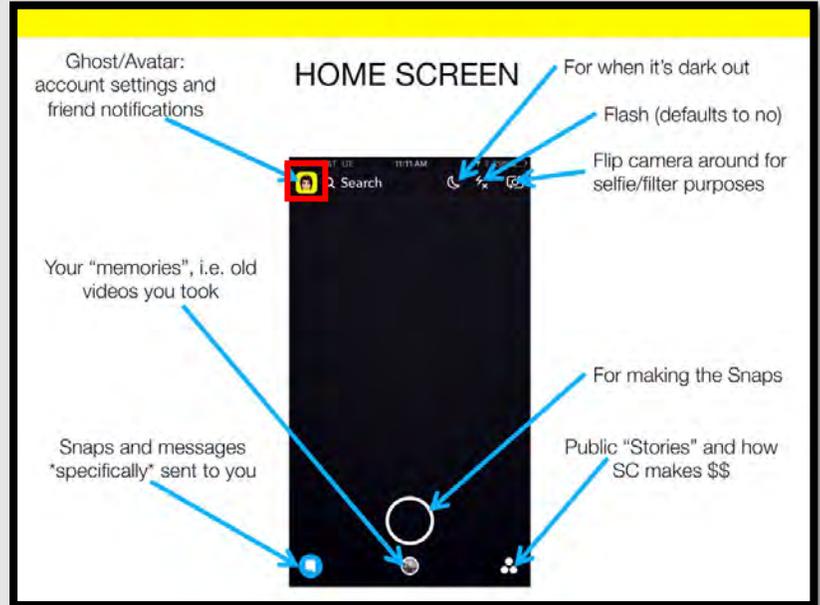


There are an estimated 82 million users, the majority of which are 13 to 25 years old. Make sure you know who your children are talking too. #keepourkidssafe

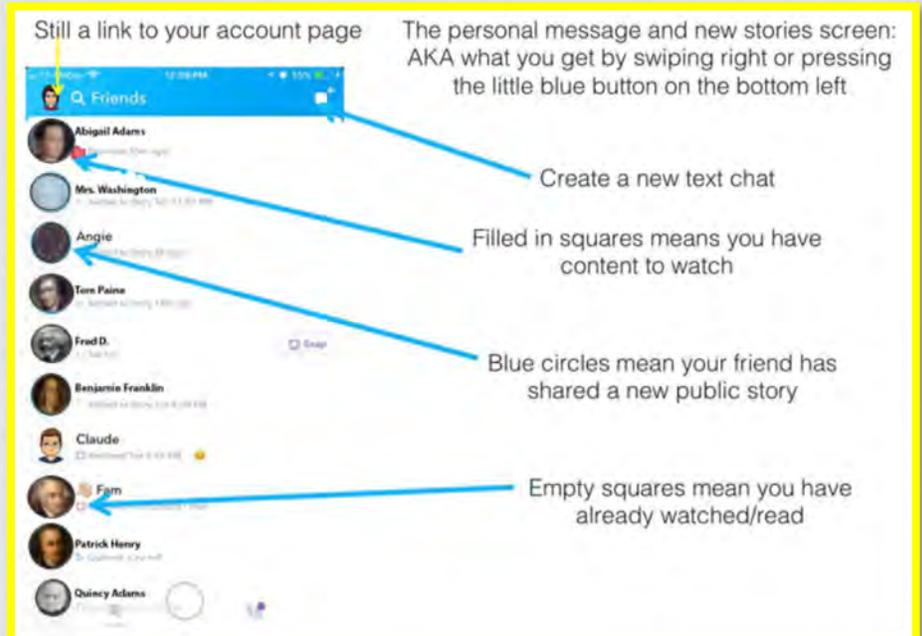
Do's and Don'ts

- ◆ Do set up privacy and security settings on your Snapchat and help your Teenager to do the same.
- ◆ Assume ALL information and images you share are publicly viewable, regardless of your settings.
- ◆ Do talk to your Teenager(s) about the dangers Snapchat might pose. Make sure they know to come and tell you if someone should talk to them that they do not know or provides them pictures that are inappropriate.
- ◆ 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 think that all pictures and videos are automatically deleted, assume if you send it that someone can keep it or that it could be shared.

Shown to the right is an overview of the chat features of Snapchat. Here you can see if someone has sent you a message, posted a story, or review posts you've already read. You can also start a chat or again select the icon at the top left and head to your Snapchat statics and "Settings" section.

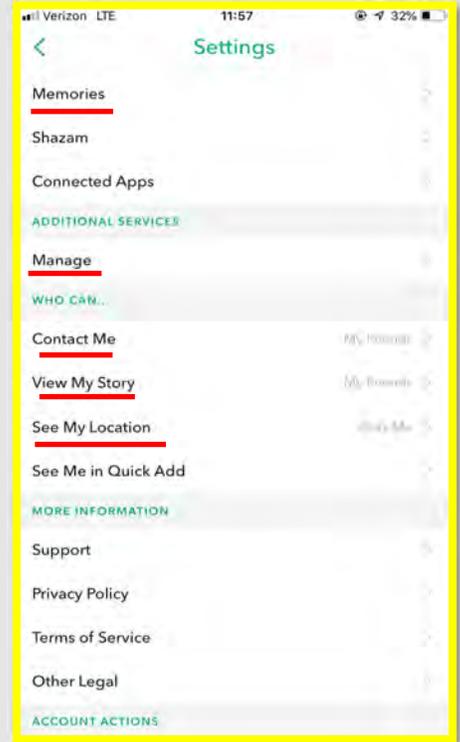
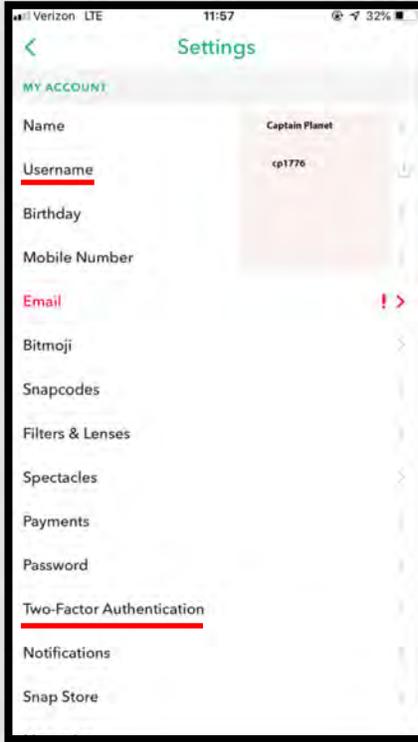
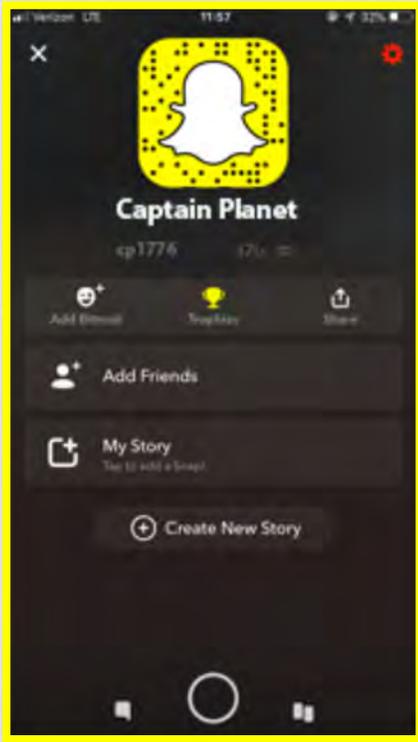


The best way to begin understanding and locking down Snapchat's capabilities is to familiarize yourself with Snapchat basics. In the box above you can look over the main icons and functions located in Snapchat. The most important icon to note is the Ghost or Avatar picture at the left of the box (highlighted in red), this icon will take you to your Snapchat statistics and lead you to the "Settings" icon. The icons may differentiate slightly depending on the device that you are using but the location of each function should remain the same.



The Pew Internet and American Life Project found that 15 percent of teenagers between the ages of 12 and 17 acknowledge they received a “sext” from someone they know.

LOCKING DOWN YOUR SNAPCHAT



After reviewing the different sections on page one of the Snapchat Card let us begin locking down our actual account.

Let’s begin by selecting your Profile picture “Account Settings” for the top of the screen on your “home page” as shown on page one.

Now, 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

Please note that the Android Snapchat App may have slightly different wording for each section, but the process is the same.

While you are reviewing and familiarizing yourself with all of Snapchats settings, one item to make sure you review is your “Username”. It is recommended that you create a username that does not give too much away about you or any personal information i.e. birthday, full name etc.

If not properly locked down any individual will be able to look you up as well as certain pieces of information, therefore, it is important to review each section here periodically to make sure everything remains locked down to your comfort level.

We will be reviewing settings from each of the **Red** underlined.

Snapchat Lingo:

Geo-filters: These are location-specific elements that can only be unlocked by visiting a specific place. Businesses use geo-filters as a way for customers to check in and advertise them. A teenager could create a special geo-filter for their sweet-16 party for attendees to add to their photos.

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

Memories: If you don’t want your snaps to disappear, you can store them to send later.

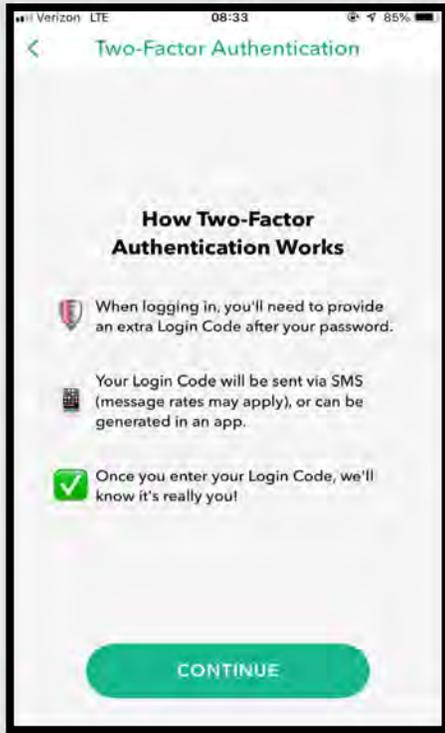
Snapstore: This is exactly what it sounds like: a place to buy Snapchat-related items.

Shazam: A feature that helps you identify a song.

LOCKING DOWN YOUR SNAPCHAT

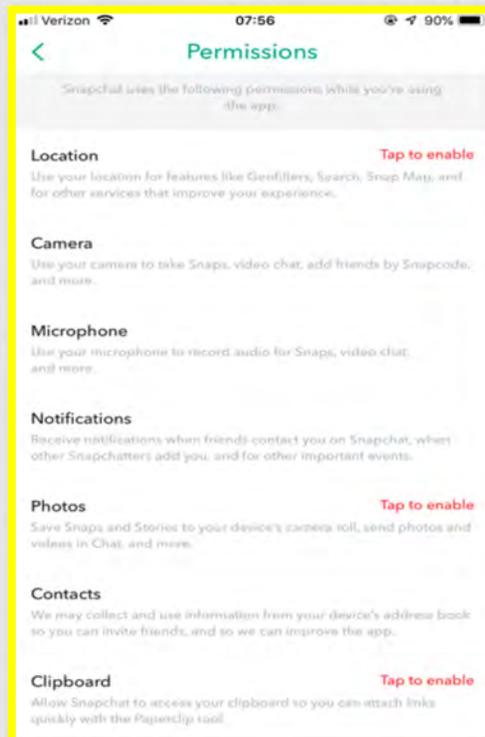
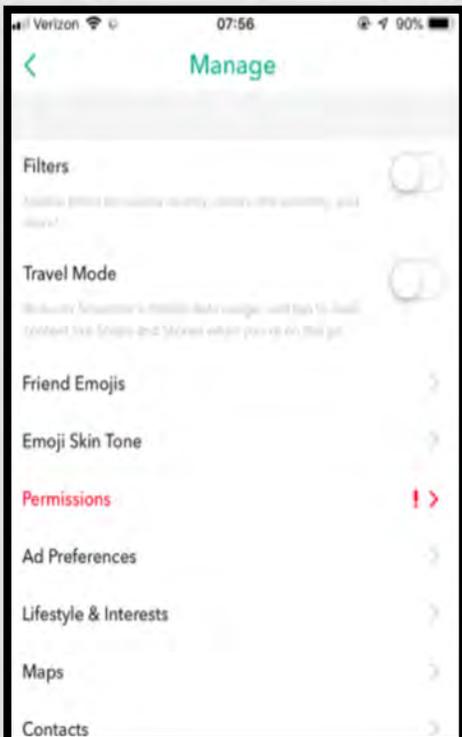
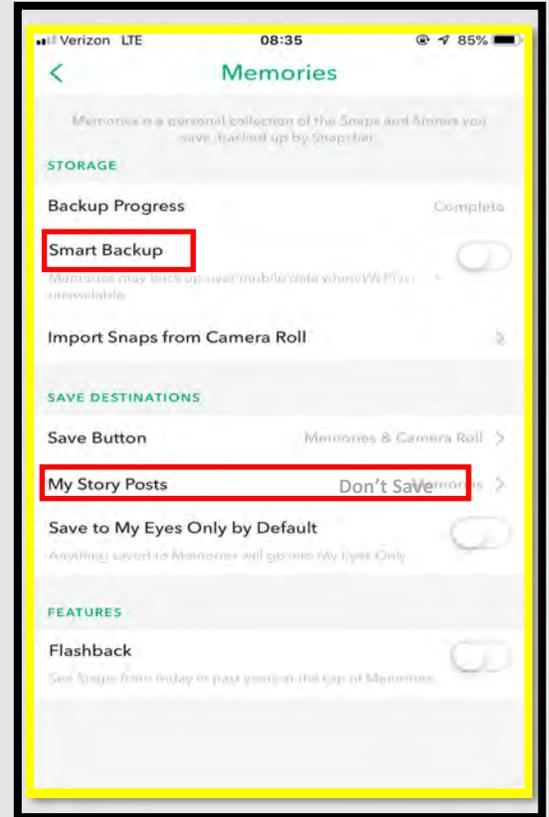


Hackers have been known to publish thousands of snaps mainly of 13 to 17 year old's. Talk to your teenagers periodically about who they are connecting with.



As always, it is important to and highly recommended that you enable Two-Factor Authentication for your Snapchat, to help minimize other individuals from accessing it. Simply select the "Two-Factor Authentication" from the settings menu (shown on page 2 of this card) and follow the few steps to complete the process.

Next, go back to the "setting" section and select "Memories." From here, it is recommended that you not enable to "Smart Backup" or "My Story Posts" to prevent Snapchat from storing your photos and videos.

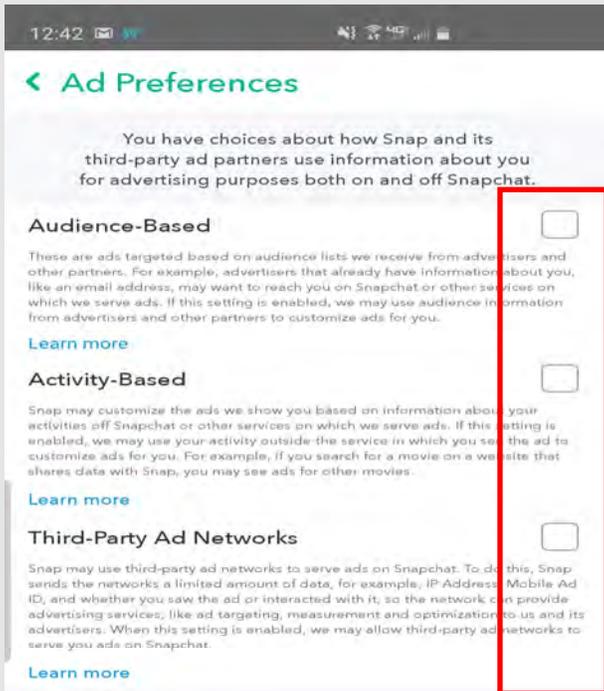


Let's head back to the "Settings" section and scroll down to select "Manage" once there scroll to select "Permissions." Note: If you have an Android this settings is listed under the "Settings" section. From here, there are a few important section to "disable" or to ensure you do not "enable," such as "Location." It is highly recommended that you not enable the "Location," "Photos" or the "Clipboard" from this section. Each of these functions allows Snapchat to have access to your phone that you limits your privacy and allows Snapchat to access and store photos/information from your device onto their cloud.

LOCKING DOWN YOUR SNAPCHAT



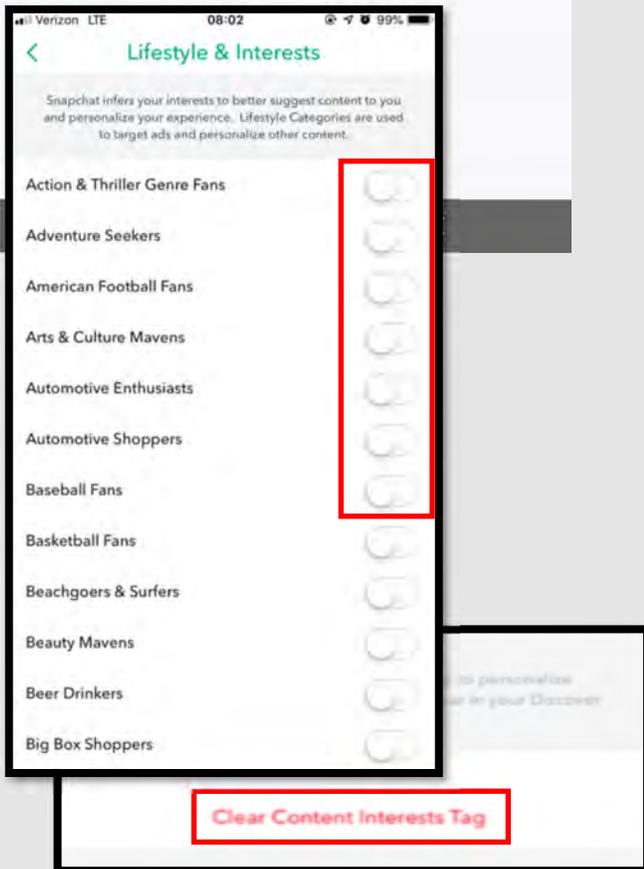
According to TeenSafe.com 47 percent of users admit to using screenshots and 52 percent note that others have used screenshots of their messages. #Staysafeonline



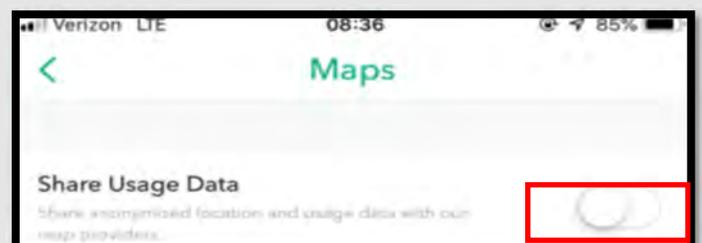
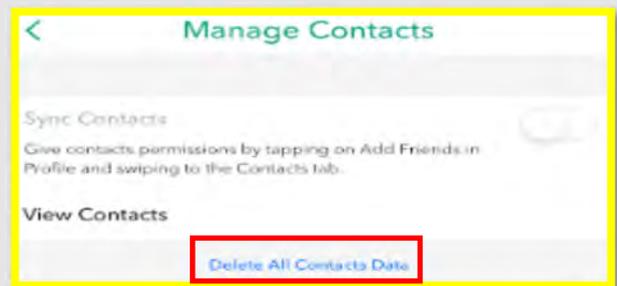
After you have finished locking down the “Permissions” section, go back to the “Manage” section (as shown on page four) and select “Ad Preferences.” Here it is recommended that neither selections (“Audience-Based” or “Activity Based”) be enabled to decrease what Snapchat learns about you.

Note: If you have an Android Based Smart phone “Ad Preferences” will be located on the “Settings” page. You will also find “Lifestyle & Interests” under “Ad Settings.”

Next, go back to the “Manage” section and select “Lifestyle & Interests,” its recommended that you unselect any section that is enabled. You can also clear any tags that may have specified your interests by selecting “Clear Content Interests Tag” (shown at the bottom left in red) periodically from this section. Next, go back to “Manage” and select “Contacts” (If you have an Android this function is in the “Settings” section) there it is recommended that you make sure you have not enabled Snapchat to view your device contacts. If you had enabled “Sync Contacts” but have now disabled it, it is important to also “Delete All Contacts Data” as shown below in Red.



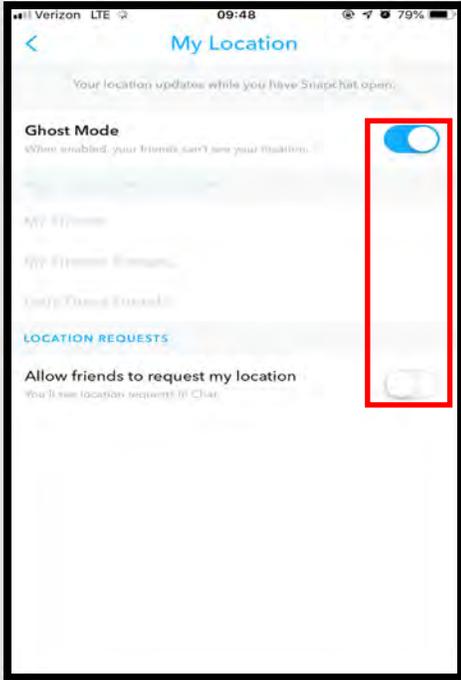
Now, let’s go back to “Manage”, select “Maps”, and make sure that “Share Usage Data” is not enabled. It is always recommended that you hide your location or ensure it is not enabled wherever possible.



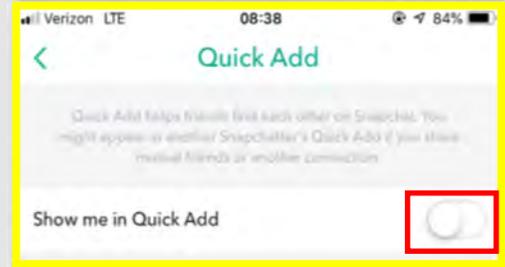
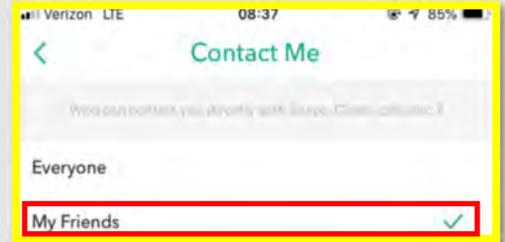
LOCKING DOWN YOUR SNAPCHAT



The FBI warns parents that pedophiles are using Snapchat to solicit images from young teens. These images are used for personal use or are sold to others in the underground.

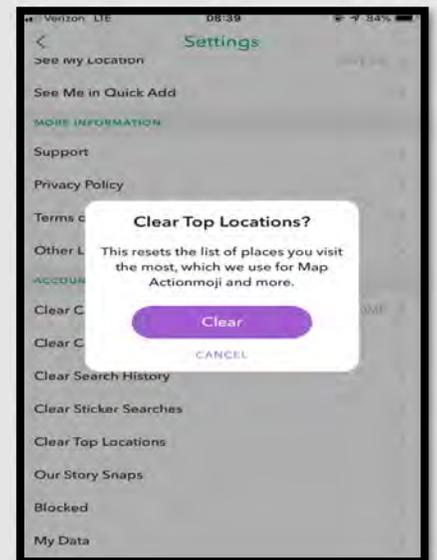
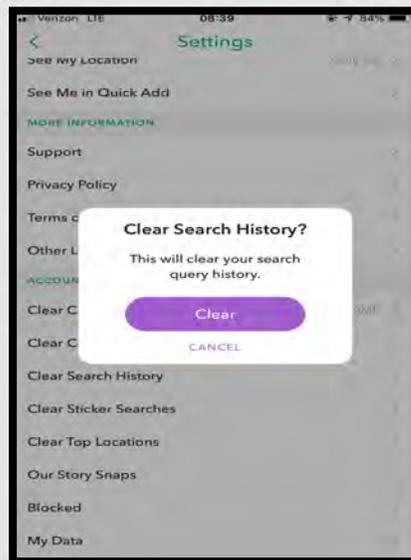
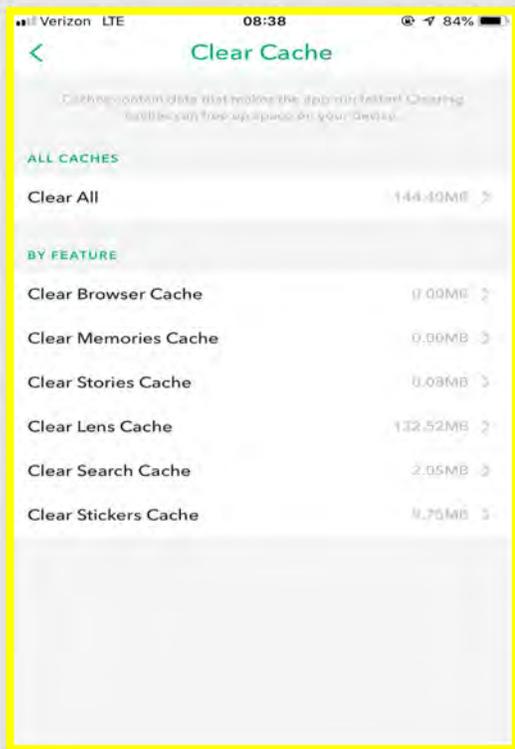


Let's go back to "Settings" and select "Contact Me" under the "Who Can..." section. It is recommended here that only "My Friends" are able to contact you, in order to help keep you and your children safer while using this App. Under the same "Who Can..." section select "View My Story" where it is also recommended that "My Friends" be enabled to ensure that your videos and pictures are not available to the public. Now, 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 profiles as a suggested contact.



Heading back to the "Settings" section, let's review the "See My Location." Snapchat allows users to be in "Ghost Mode" to prevent even their friends from viewing their location. It is highly recommended that you enable "Ghost Mode" while using Snapchat in order to prevent individuals from viewing your precise location on the Snapchat Map. It is also recommended that you not enable "Allow friends to request my location."

Snapchat also provides you the opportunity to Clear your Cache, conversations, search history, and top locations (as shown below). It is recommended that you periodically go through and clear these much like you would your Internet Browser.

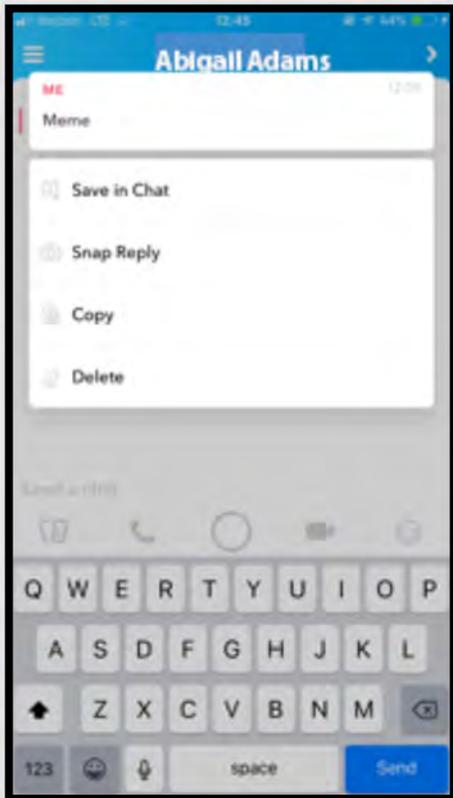


LOCKING DOWN YOUR SNAPCHAT

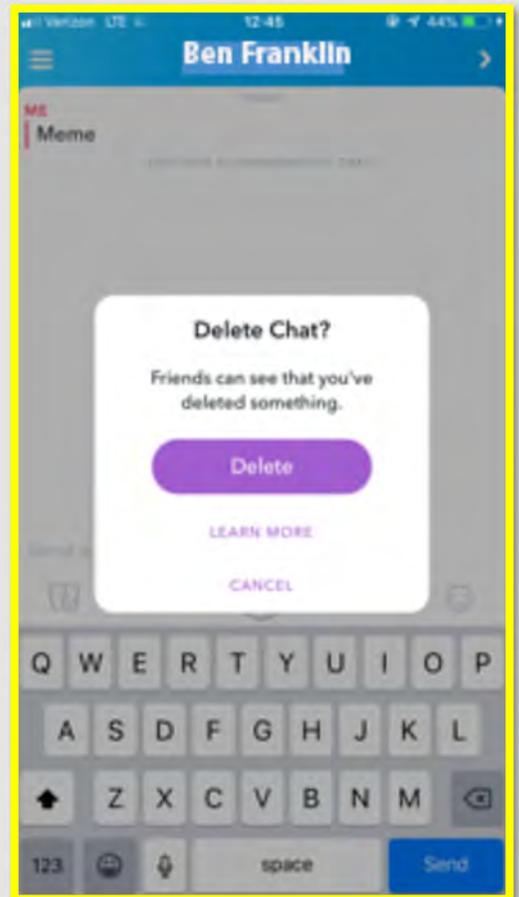


Depending on the State, parents can be held liable for a child's cyberbullying or sexting if they fail to take appropriate action. #theforeyouknow

Snapchat created a new feature to Snapchat that lets you unsend a sent message regardless of whether recipient(s) saw it. This feature is different from the already available “Clear Conversation” option, which only deletes the 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. Important to note that the person(s) in the conversation will be alerted that a message was deleted; the function's purpose is to clean up a typo or prevent unintentional messaging.



In order to delete a chat that you may have already sent simply hold down the chat (shown here to the left as “Meme”) and then 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 even though the message will be deleted, your friends will still be able to see that something was deleted, just not the deleted content itself.



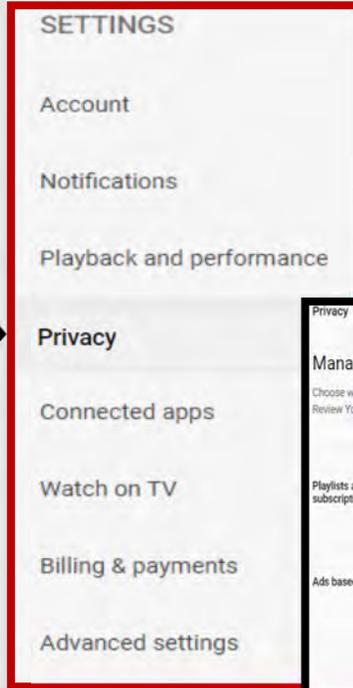
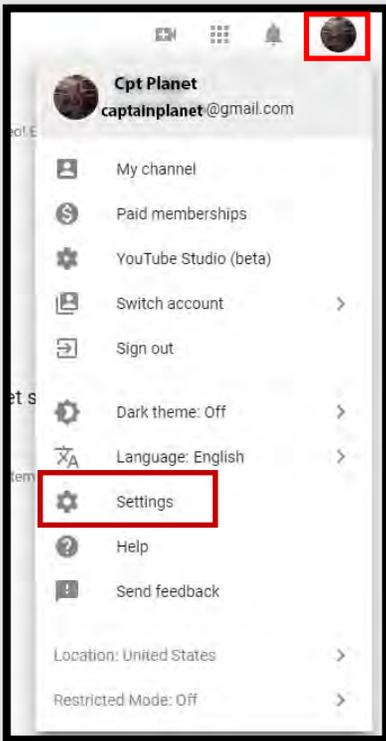
LOCKING DOWN



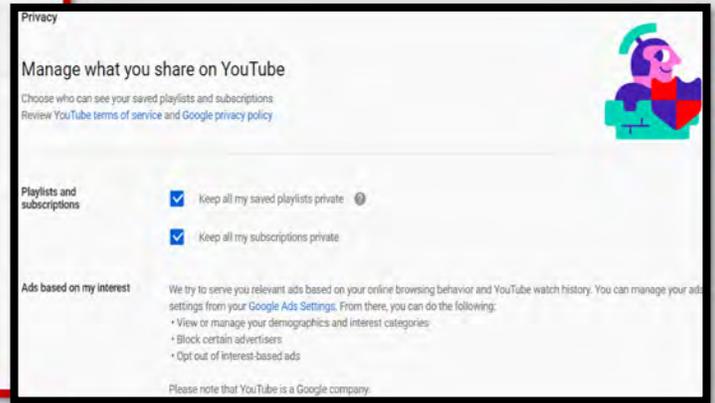
Do's and Don'ts

- ◆ Do monitor the videos that your children are watching, even if they are on “Restricted Mode.”
- ◆ Do use Two-Factor Authentication to protect all your information. If you have a YouTube account that likely means you also own a “Google” account which is where you can turn on Two-Factor Authentication.
- ◆ Do lock down your videos so that they are not public for everyone to view.
- ◆ Do not allow your children to post public videos to their YouTube account. Posting public videos will allow “subscribers” to follow your children on YouTube.
- ◆ Do not ignore the comments and feedback from your published videos. They may contain personal information about you or your video that you would otherwise not want put out.

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



In order to ensure the privacy on your YouTube account lets being with our Settings. Head to the top right of your screen and select your Google Profile picture (shown to the left in red). Once the drop down menu appears, look towards the bottom and select “Settings.” To the right of your screen are a list of functions in YouTube, select “Privacy” to manage your YouTube privacy.



Now that you are in the “Privacy” section scroll through each of the settings to make sure they are locked down to your satisfaction. It is recommended that your keep all sections in “Manage what you share on YouTube” private. Finally, in order to turn off the “Ads based on my interest” select the link “Google Ads Settings,” then select “turn off.” It is recommended that this feature be turned off for all social media sites.

Ads based on my interest

We try to serve you relevant ads based on your online browsing behavior and YouTube watch history. You can manage your ads settings from your [Google Ads Settings](#). From there, you can do the following:

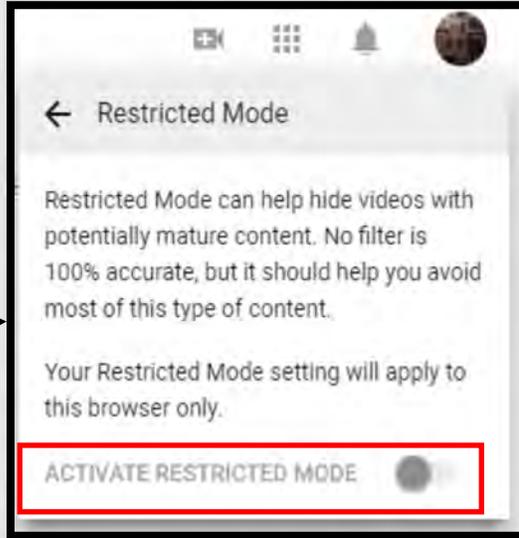
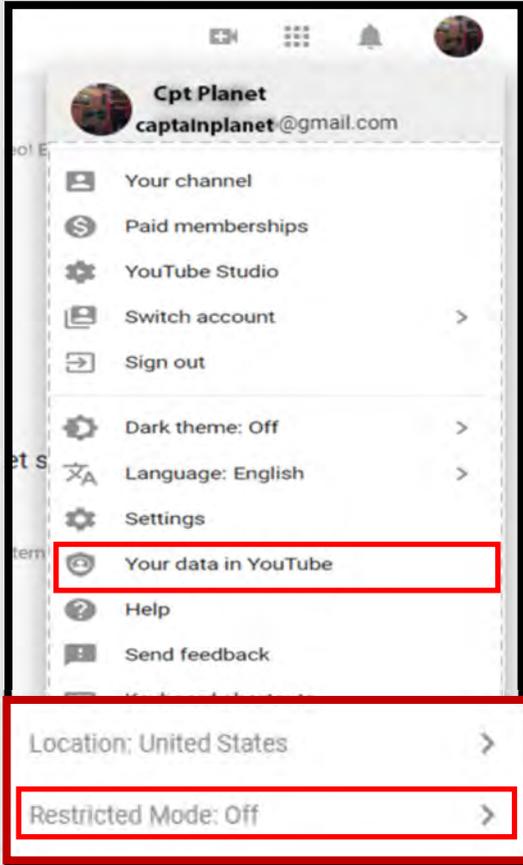
- view or manage your demographics and interest categories
- block certain advertisers
- opt out of interest-based ads

Please note that YouTube is a Google company.

LOCKING DOWN



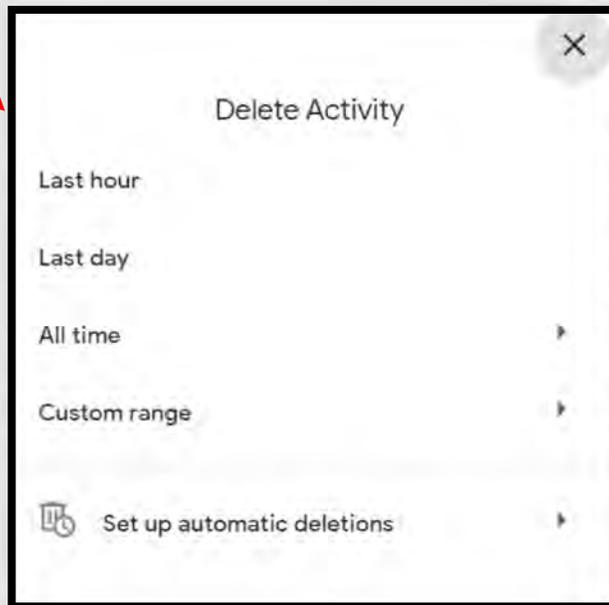
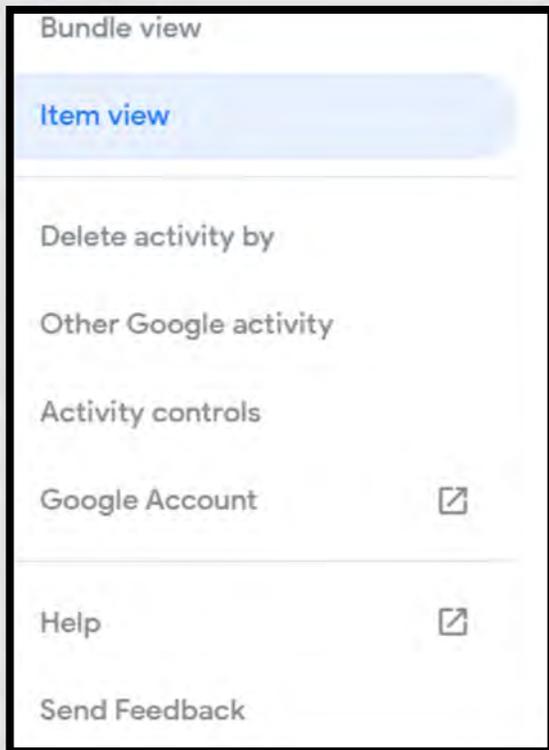
Unlike any other social networks, YouTube doesn't require you to create an account before you or your child can search for content or view videos.



Parents do you worry about what your child is watching on YouTube? Now you are able to put them in what YouTube is calling the "Restricted Mode" to help protect what your children are watching. There are a few ways to turn on this function, first by going back to your profile settings picture at the top of the screen and selecting the drop down menu.

Once the drop down menu appears, look towards the bottom of the menu and select "Restricted Mode" (as shown to the left in red). Selecting the "Restricted Mode" function will bring up an additional pop-up box to confirm that you in fact, want to "Activate Restricted Mode" (as shown above in red).

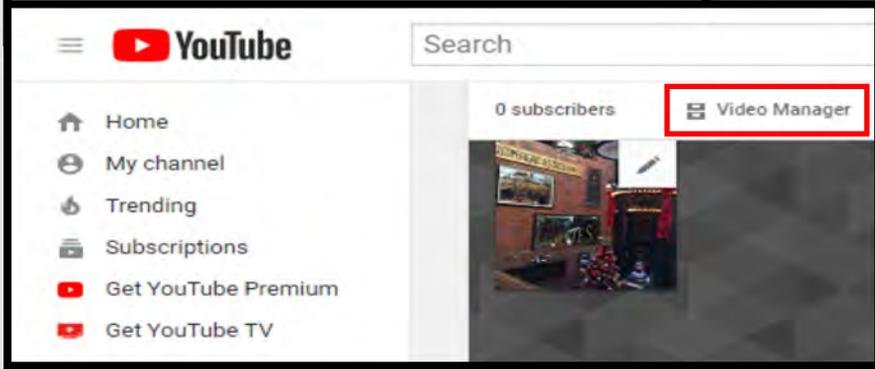
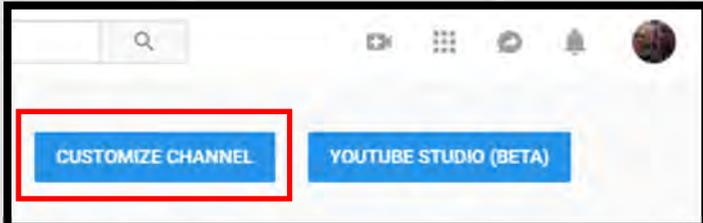
There is one other important feature located at the bottom of your YouTube Main Menu (shown here in the upper left) and that is the "Your data in YouTube" tab. Just as it is important to clear your browser history on your Search Engines, it is important to manage and clear your history on your YouTube account. Scroll down and select the "Manage your YouTube Search History." From here, look to the left of your screen to see a menu of available options to manage and delete your history. It is recommended that you



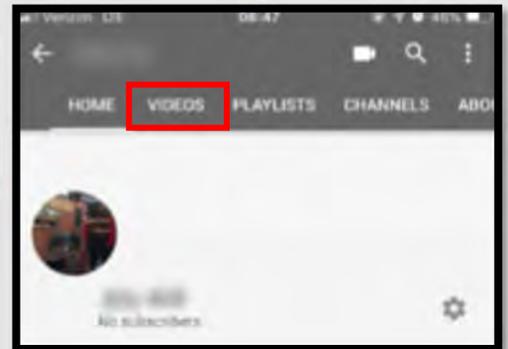
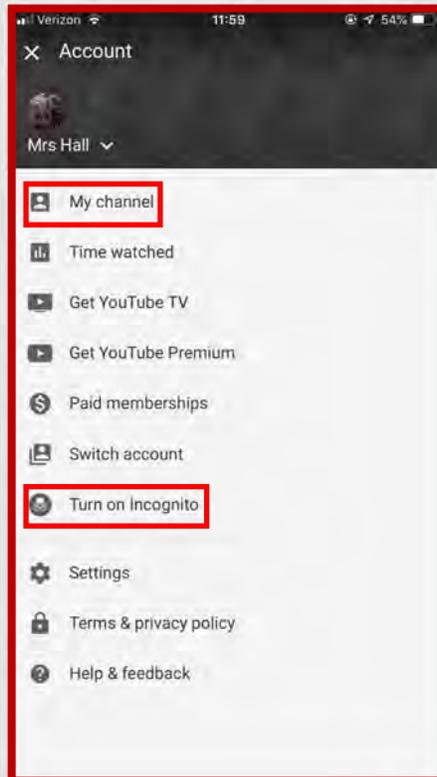
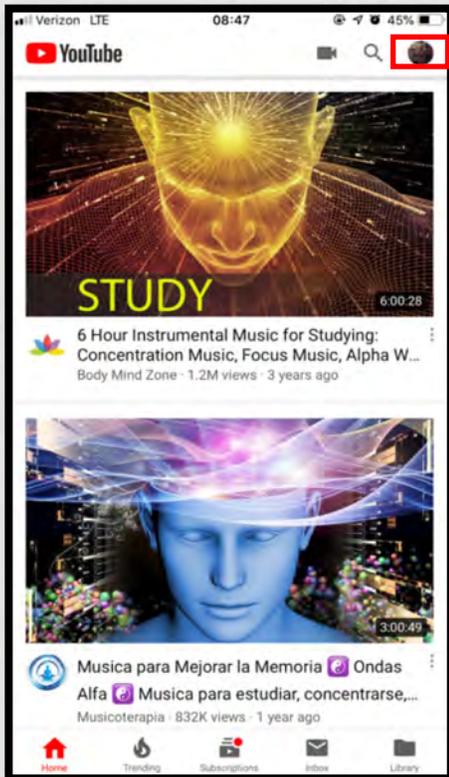
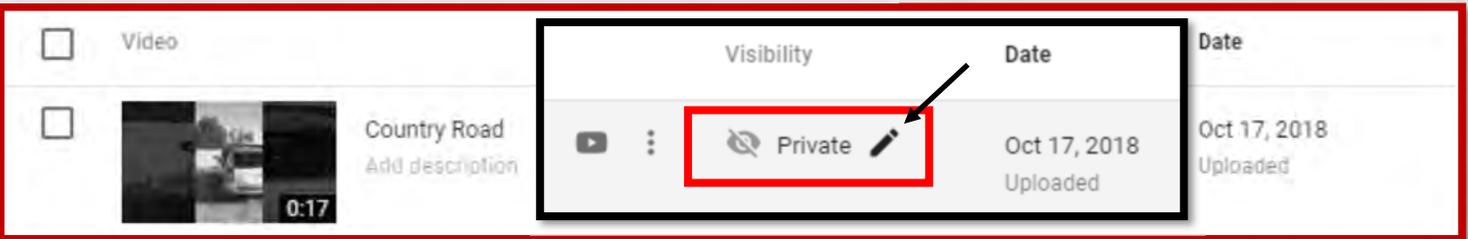
“Clear All Watch History” periodically from your YouTube account. After having selected “Clear All Watch History” a pop up box will appear on your screen to confirm that you would in fact like to clear your history. Simply select “Clear Watch History.”

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

LOCKING DOWN



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 "Profile" drop down menu and select "My Channel." Then select "Customize Channel" in the blue box (highlighted here in red). Next, select "Video Manager" from the middle of the page. Here you will be able to upload videos and edit any videos you have already uploaded. In order to edit the "Visibility" of a video simply hover over the current visibility of the video and select the "pencil" icon. From the drop down menu that will appear simply select the desired privacy setting. It is recommended that your videos remain "Private."

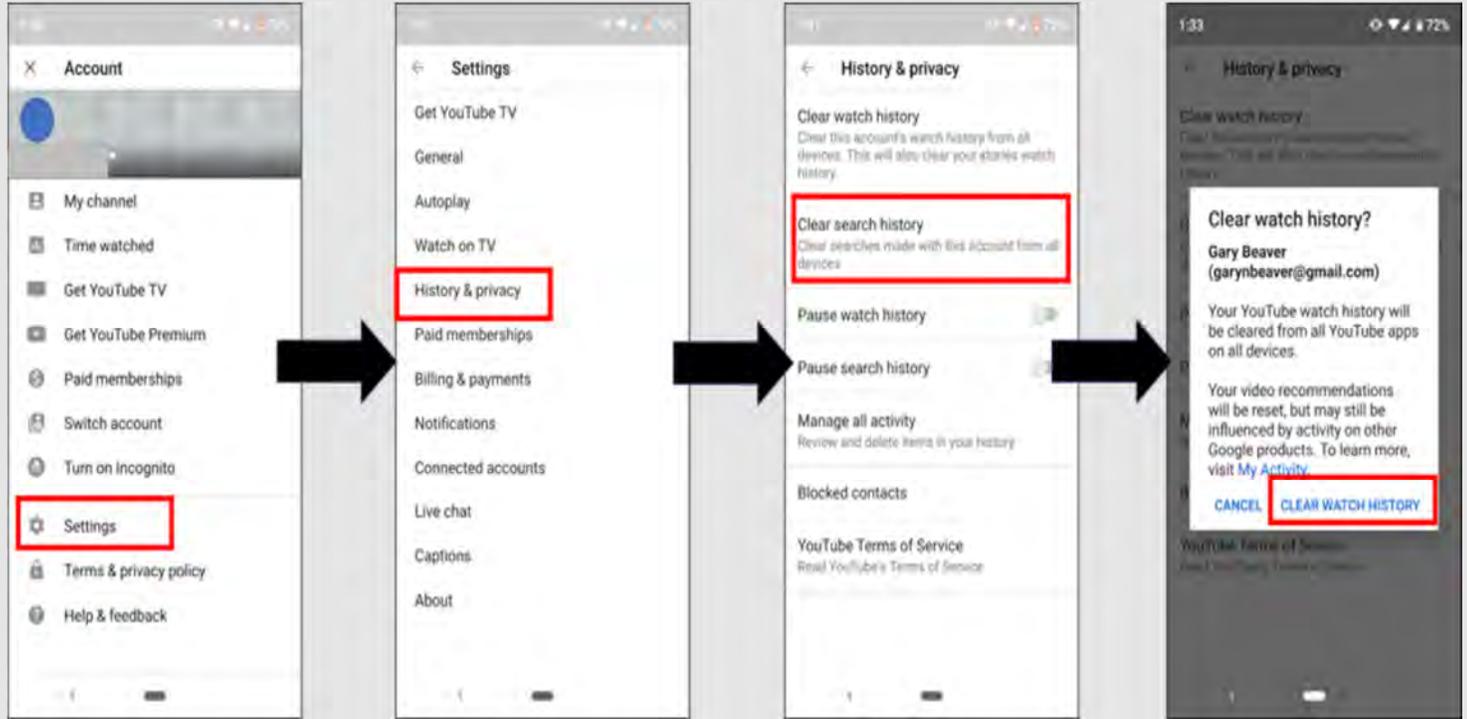


In order to access uploaded videos and change their privacy settings via your smart devices the process is a bit different. From the App and like the Browser version, select your profile settings, then select "My Channel." Next head to the top menu and select "Videos" to take you to the video upload and settings section. YouTube now allows its users to be in Incognito mode. Simply select the "Turn on Incognito."

LOCKING DOWN



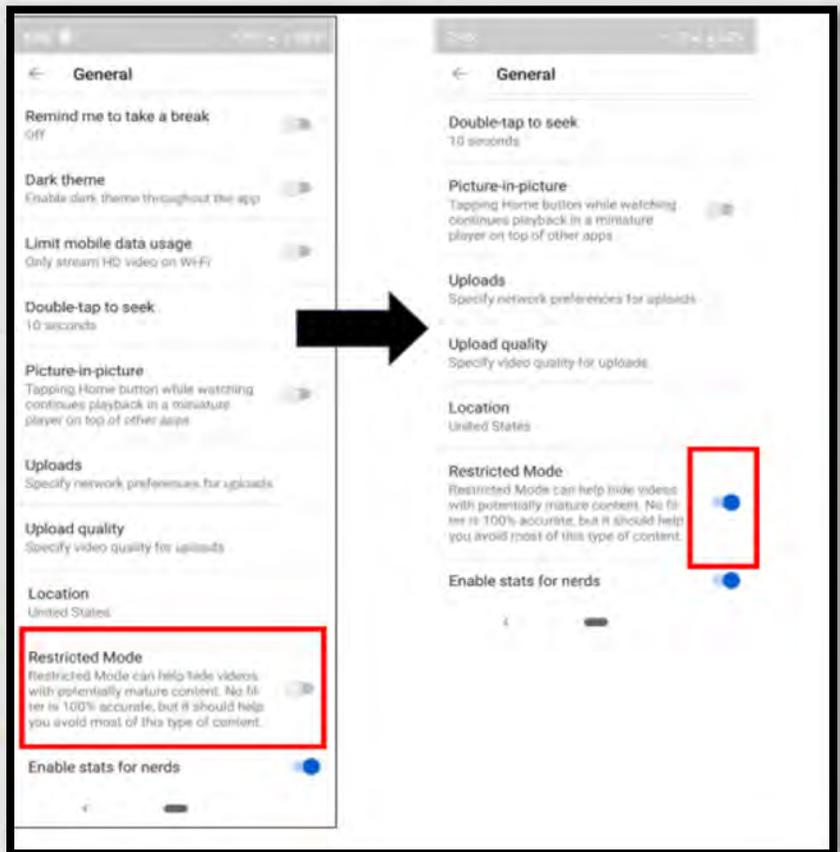
Your phone is your ultimate endpoint. You likely carry it everywhere and it typically holds your most sensitive information. Make sure to check for updates quarterly. #Staysafeonline



If you are an iPhone user, most of these settings will be found directly under the "Settings" section, instead of having to go into multiple different tabs. Above are the steps necessary to get to the "History & Privacy" section as well as to clear your History on YouTube.

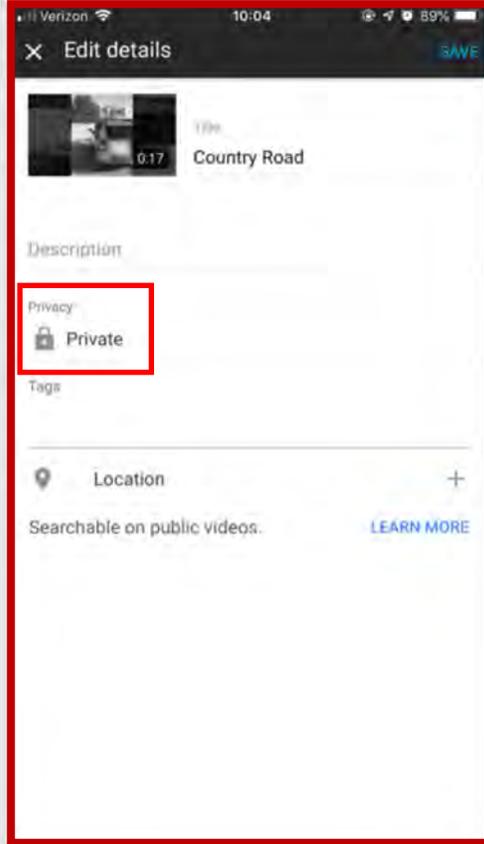
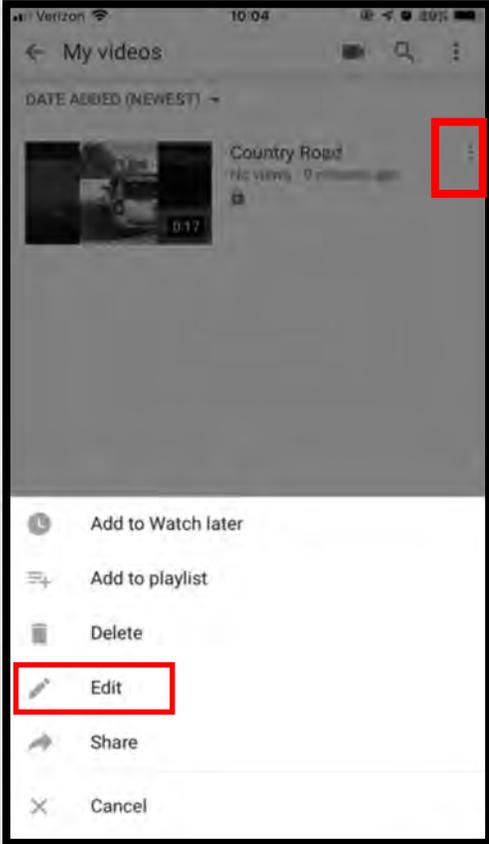
If you are sharing your device or just wanting to protect your privacy, it is a good idea to make sure you clear your history at any time by accessing the YouTube app's settings and following these steps.

In order to turn on "Restricted Mode" from your Android simply follow the steps to the right. Remember this is a good idea if you have children that use your YouTube account.



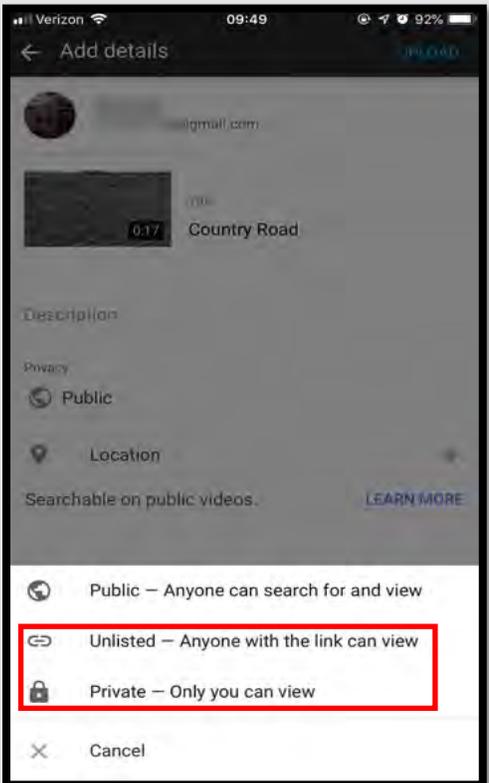
Social media sites can cover people in anonymity, allowing them to attempt to exploit children without the fear of being caught. Monitor your child's Internet usage to help keep them safe.

LOCKING DOWN



In order to edit the privacy settings of your video from your smart device, now locate the vertical ellipsis (three vertical dots to the right) and select it to show a pop up menu appearing from the bottom of the screen.

Next, select "Edit" from the pop up menu where you will then be able to select "Privacy", set or turn off the "Location" of a particular video, or provide a description of the video for viewers, if you allow any.



Now you will be able to select how private you would like to keep you videos. The purpose of YouTube is to upload and watch videos; therefore, with that in mind, it is recommended that you select "Unlisted" as your privacy setting for all videos. An "Unlisted" privacy setting on YouTube means that your video is only public to individuals that have a link directly to the video. If you make your video "Public" or your child makes his or her video "Public" then anyone will be able to view 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 very quickly at which time you lose any ability to pull it back from the public eye.



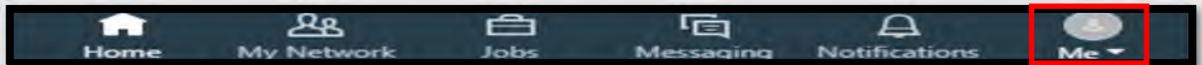
LINKEDIN SMART CARD



Do's and Don'ts

- Do not use an email account that is associated with 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. Understand that 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 personal information. Similarly, apps/websites can access and share your personal data.
- Review your connections often. It is important, periodically to check to ensure that your connections are current and that you are not providing your information to individuals who no longer need it.
- Posting a profile picture is optional. It is recommended that if you do decide to post a picture, select one in professional business attire.
- Ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose your personal data.

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

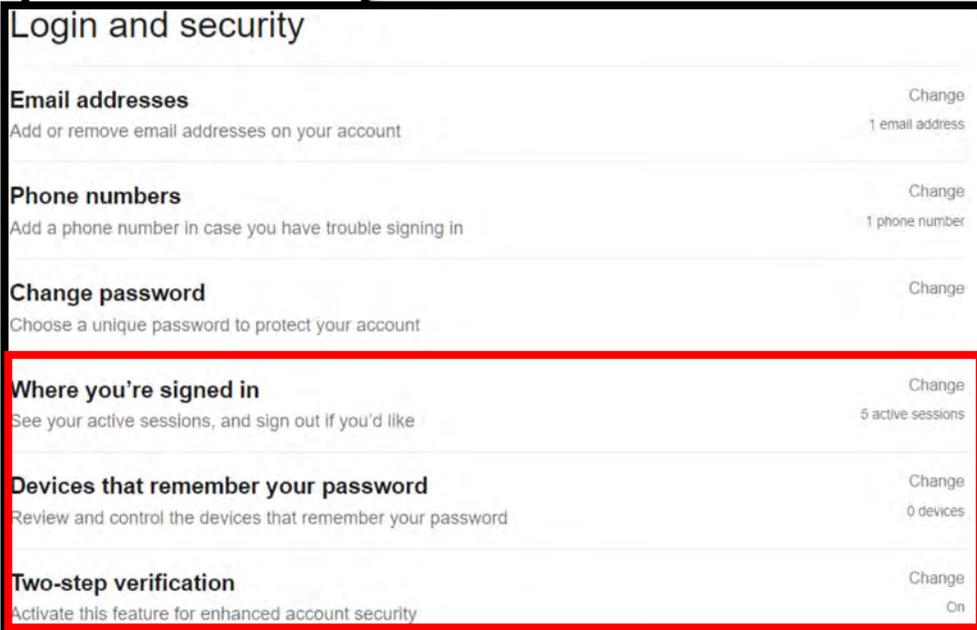


The privacy settings for LinkedIn can be found in the “Me” section on the top right corner of the website (shown above). From the drop down menu, select “Settings & Privacy” (highlighted in red to the left). A new screen will appear with a header like the one shown below. The first section we are going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



One item in the “Login and Security”

menu that is important to highlight is the “Where you’re signed in” section (shown on the right). In this section you can review any “Active” session you have on your account and where those sessions are located. If you see an active session or location that does not look familiar, it is recommended to close all unfamiliar sessions and change your password. Next, at the bottom of the “Login and Security” section, the “Two-step verification” setting allows a user to add a phone number so that a code will be sent as a text acting as a second password. It is recommended you enable this process to add an additional layer of security to your LinkedIn account. This will prevent access to your account in the case your password has been exposed in a security breach.



LINKEDIN SMART CARD



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



How others see your profile and network information

- Edit your public profile** Change
- Who can see your email address** Change Only you
- Who can see your connections** Change Connections
- Viewers of this profile also viewed** Change No
- Who can see your last name** Change Full
- Representing your organization and interests** Change No
- Profile visibility off LinkedIn** Change No
- Microsoft Word** Change No

Next, go to the menu at the top of the “Settings & Privacy” section and select “Privacy” (shown here 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. 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

How others see your LinkedIn activity

- Profile viewing options** Change Private mode
- Manage active status** Change
- Share job changes, education changes, and work anniversaries from profile** Change No
- Notifying connections when you're in the news** Change No
- Mentions by others** Change No

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 re-viewed 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.

Manage your data and activity

- Download your data** Change
- Manage who can discover your profile from your email address** Change Nobody
- Manage who can discover your profile from your phone number** Change Nobody
- Sync contacts** Change
- Sync calendar** Change
- Salary data on LinkedIn** Change
- Search history** Change
- Personal demographic information** Change
- Social, economic and workplace research** 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. It is recommended that 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”.

Blocking and hiding

Followers Change Connections

Choose who can follow you and see your public updates

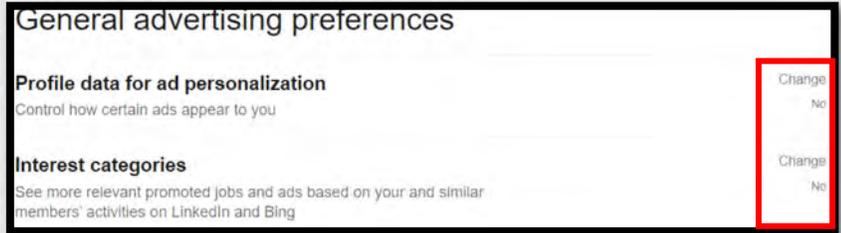
Finally, at the bottom of the “Privacy” section under “Blocking and hiding,” you can turn off the ability of others to “follow” you, especially those not in your “Connections.” From the drop down menu, change “Everyone on LinkedIn” to “Your Connections”.

LINKEDIN SMART CARD

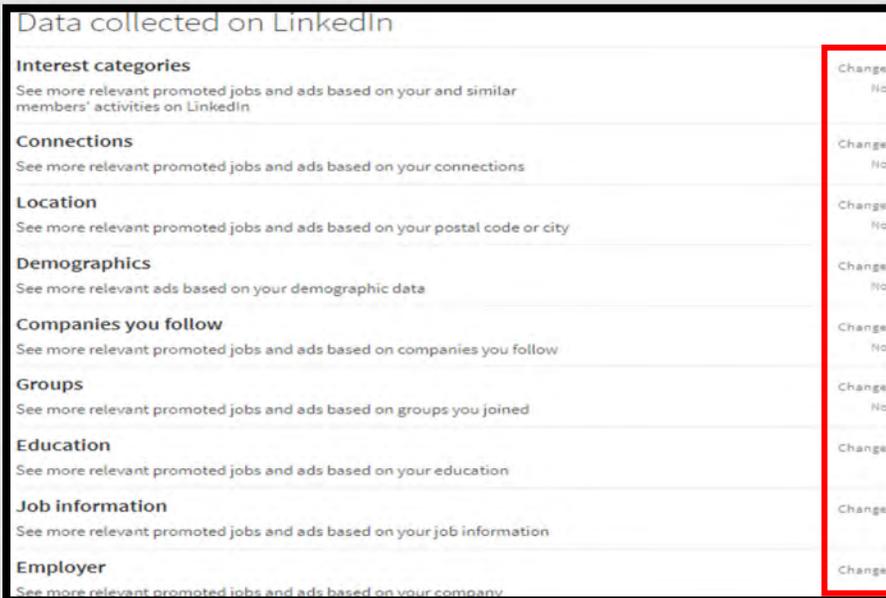


Now let's tackle Advertisements by selecting "Ads" from the top of the "Settings and Privacy" menu. It is recommended you limit the amount of information that LinkedIn is allowed to share with other third party apps / ads as much as possible.

Recommended setting are highlighted in red (to the right).



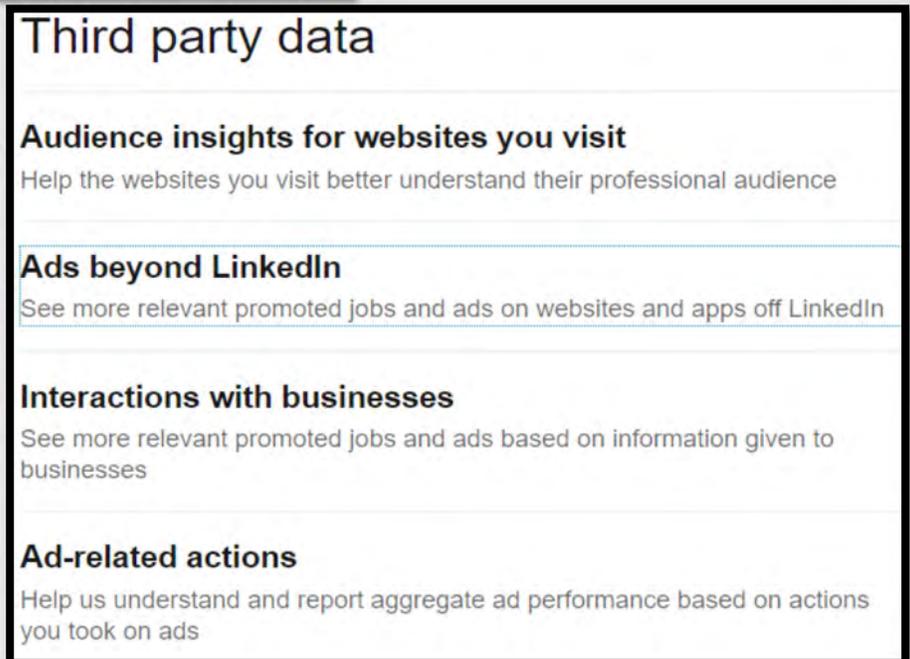
Even LinkedIn recommends not putting your email address, home address, or phone number in your profile's Summary. #staysafeonline



Under the "Data collected on LinkedIn" settings, you will find the breakdown pictured to the left. Sharing this information with LinkedIn will leave it, and you vulnerable even if your account is otherwise locked down. It is important to know into exactly how your information is shared should you enable any of these categories. It is recommended that, regardless of your intent in using LinkedIn that you choose NOT to share your data with LinkedIn to avoid it being shared with and used by third party apps.

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

Remember, 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 in order to generate usage analytics for our services, which analytics (they) may share in aggregate form with (their) advertising customers.¹ #manageyourdata

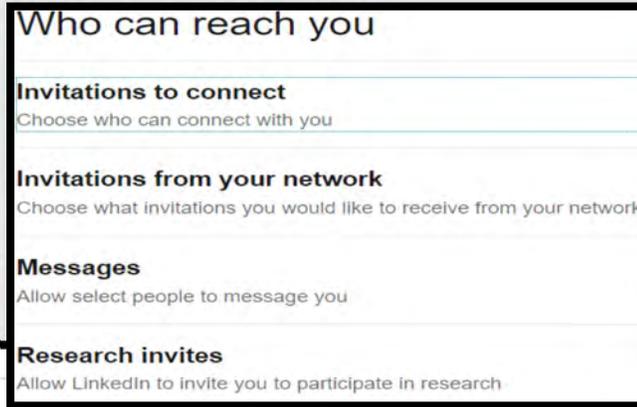


Reference: 1. <https://www.linkedin.com/legal/cookie-policy>

LINKEDIN SMART CARD



Under “Communications” it is important to review each of the “Who can reach you” because this is the way either anyone can reach out to you or certain people to which you decide can reach out to you.



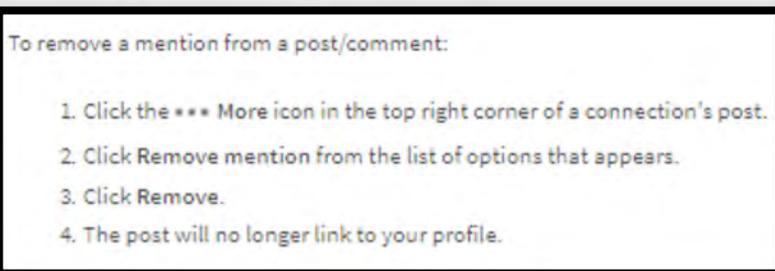
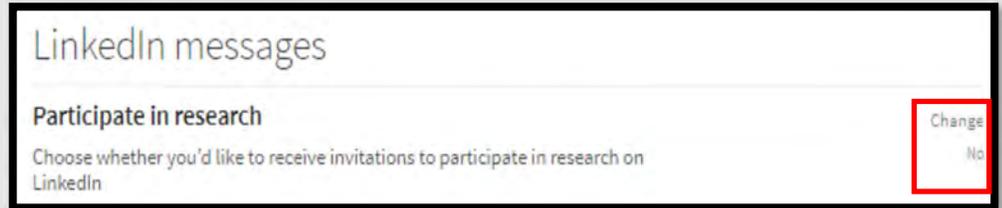
When reviewing your “Communications” on LinkedIn, it is important to consider why you are using LinkedIn...what benefit(s) you hope to gain. Do you desire a job? Are you simply trying to connect with specific people? Depending on your intent, following the recommendations herein will restrict available information on you, therefore limiting LinkedIn’s benefits. What is important is to go back and lock these settings down once you have attained your desired goals.



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 – it is highly recommended that you choose to not “Participate in research” that LinkedIn conducts. Participating in research events could mean giving up information about yourself that you wouldn’t otherwise give up to third parties.

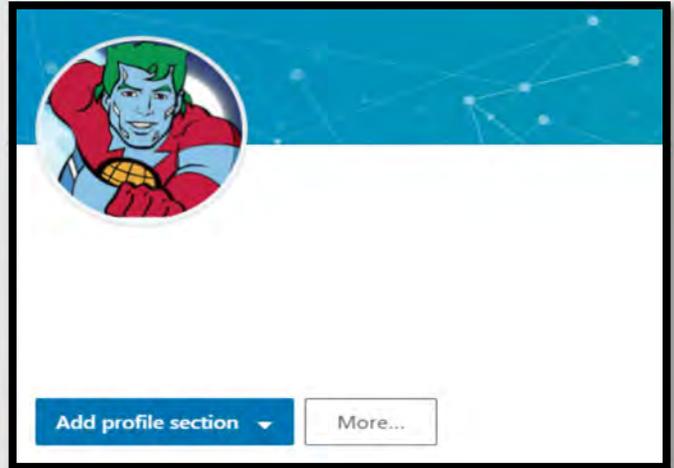
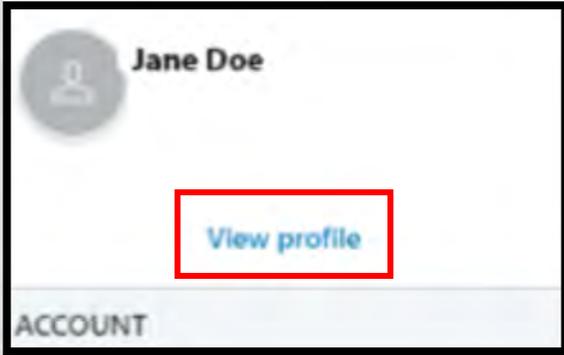


If you happen to be “mentioned” in a post on LinkedIn, you can easily remove yourself from the tag following a few steps as noted above. It is important to manage what these “mentions” link you to or imply about you.



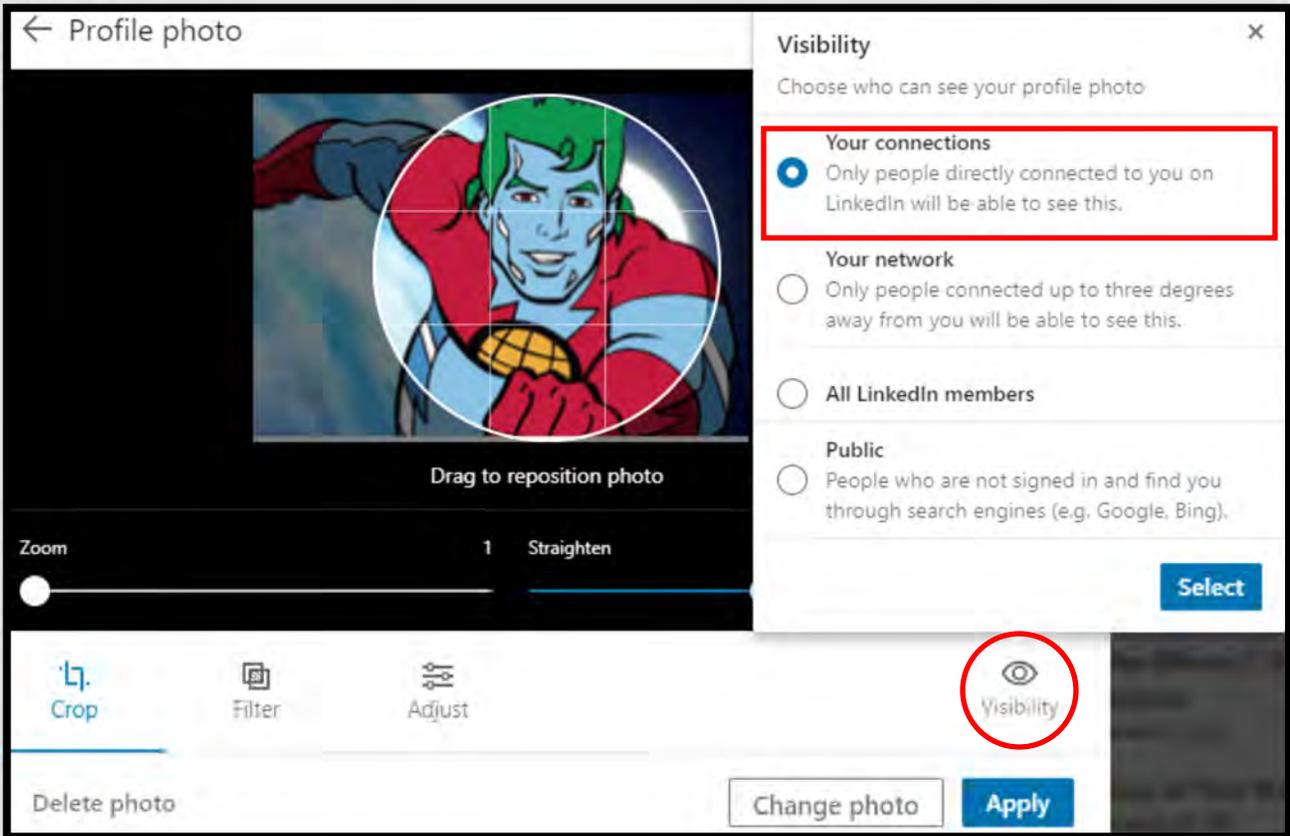
#PHISHINGALERT: Messages containing bad spelling, grammar, and that aren't addressed to you personally, or asking you to act immediately are major red flags.

LINKEDIN SMART CARD



It is highly recommended that you do **not** use photos of yourself for your profile or header photo. These are viewable to the public and therefore presents 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 any other site or even in person.

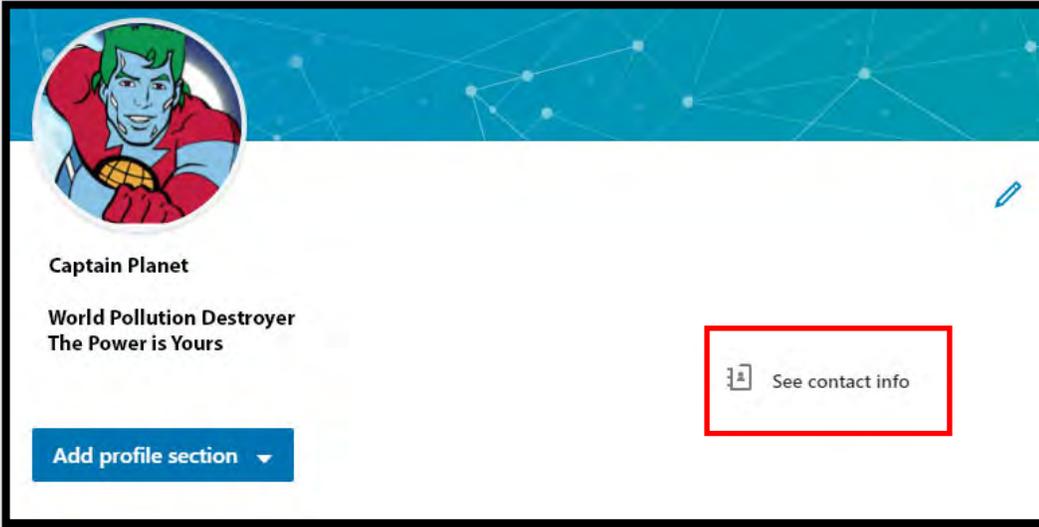
To add a picture to your profile, simply select the “View Profile” link in the Menu drop down on the top of your screen. Once there, select the “Picture” icon and navigate to and upload your preferred picture. When complete, look down at the bottom of the window (shown below in the red circle) and select “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, would you open it? Does your action depend on whether or not you think you know, and therefore trust the sender? Even if someone you know sends you an attachment, it is always a good idea to verify with that person (over the phone or face to face) they are the sender before opening it. Remember, people don’t always know immediately when they’ve been hacked. 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

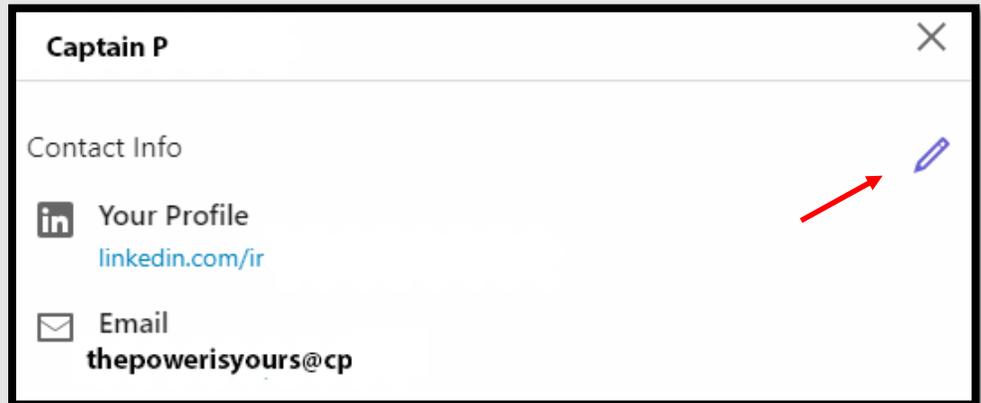
LINKEDIN SMART CARD



To further protect your information you will need to check whether your Date of Birth (DoB) 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-viewing page.

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

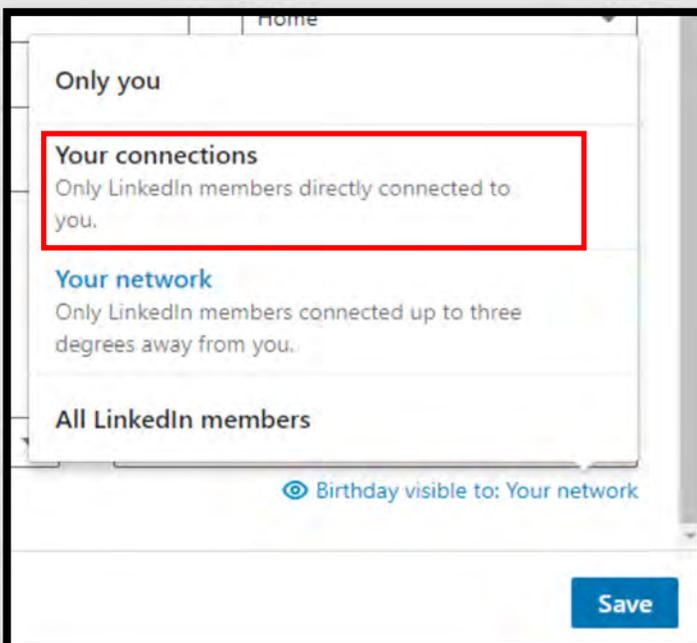
On the “view profile” page, locate the “See contact Info” icon as shown above. Find and click on the “Pencil” icon, located to the upper right of the window (see the red arrow to the right). From there review the information shown and edit as necessary. Keep in mind; this is what others can view on your profile.



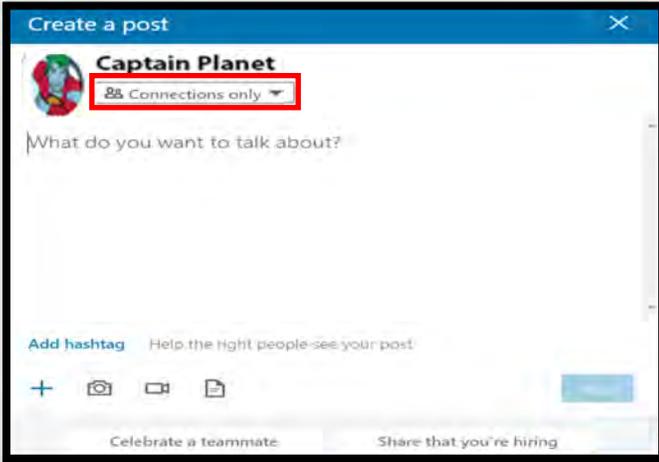
Ensure the information listed in the “view profile” section is not displaying identifiable information to the public. It is recommended to not add a phone number, birthdate, or address to this section, as they are not required.

If it is important to display the birthdate, ensure that it is only visible to Your Connections. This is done 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” are selected to not expose your private information the public.

Select “Save” before you exit out of this screen to keep selected settings.



LINKEDIN SMART CARD

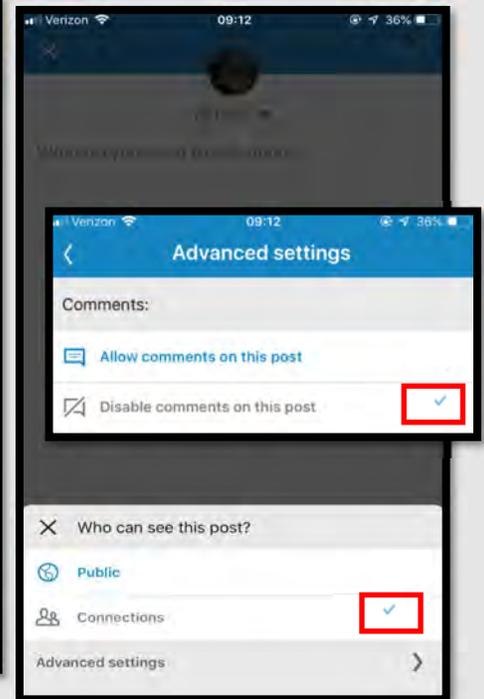


When and if you decide to post on LinkedIn, be sure to set the privacy settings of the posts containing personal information so those posts not appear to the public. As shown in the box to the left, posts made public on LinkedIn can be viewed by anyone.

In order to change your privacy settings for your post simply locate the “Post Settings” drop down menu located on the post itself (shown here to the left highlighted in red). From there select the appropriate audience for your post likely “Connections.”

Shown to the right and below are the steps necessary to lock down your posts via your mobile device.

In order to change privacy settings for individual posts: simply locate the “Who Can See This Post” (If using an Android smartphone it will be the “visibility settings”) drop down menu from the top of the post under your picture (shown here to the right, highlighted in red). From the drop-down, select the appropriate audience for your post. It is recommended to choose “Connections”. You can also select “Advanced Settings” to disable comments on the post.



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 icon in the upper right corner.
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:

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.

Try Substituting numbers for letters that look similar (for example, substitute "0" for "o" or "3" for "E") for your password to help its strength #updateyourpassword

Hidden Phone Apps



Hidden Apps Defined

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 your 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	
	Gallery Vault—Hide Pictures & Videos
	Hide Photos, Videos- Hide it pro
	Hide Pictures and Videos
	Keepsafe Photo Vault
	Vault -Hide

iPhone Hidden Apps	
	Fake Calculator App
	Private Photo Vault
	Secret Calculator Fake Vault
	Secret Photo Vault
	Secret Vault Lock Photos

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 you children and teens about the dangers of taking and sending nude photos or videos on their smart devices and what repercussions doing so could bring.
- ◆ 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 review 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 your child to make up his or her own password that they keep to themselves. Always ensure that you can access your child/teens phone at any time.

Hidden Phone Apps



Making sure children put up their smart device before bed, in the kitchen or living room, helps to limit the amount of unsupervised time your child has on their device.

Finding 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 devices- In the Google Play Store select the menu then select “My apps & games.” Now, select “Installed” in the middle of your screen. Here you can review all Apps that have been downloaded to this particular device. Additionally, from your “Account” you can review the “Order History” which will also provide you an overview of all purchased apps.
 - ◆ iPhone devices- In the App Store find and select the “Account” icon at the top right of your screen. Then select “Purchased” and the account (if you have an Apple Family Sharing Plan more than one account will appear) you wish to review purchases from.
- ◆ Another way to review purchased history on smart devices is to find their respective App store and search for “hidden Apps.” Once a list of available apps appears on the screen, you can scroll through the list and if any are downloaded on the device it will be noted to the left side of the screen. This method runs the risk of missing certain apps depending on their category.

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 usually means one is a Hidden App.
- II. If your child seems to try and hide his or her screen any time you enter the room, that may indicate that they are trying to hide their phone activity from you.

How to Prevent Your Child from Downloading Hidden Apps

- ◆ iOS has a “Apple Family Sharing Plan” that allows parents to turn on a feature called “Ask to Buy” and when turned on any time your child/teen tries to download something on their iPhone; they must first get it approved by their parents.
- ◆ 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.” 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 the password.
- ◆ Android Users can setup parental controls in Google Play Store by creating a pin and choosing the maturity levels you want to allow. It is important to note that where many of the Hidden Apps are concerned, Google Play Store rates them “E” for everyone.
- ◆ Android Users can also create a password for authentication to authorize Google Play Store purchases.

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 Play stores.

Even if you rely solely on Mobile Pay Apps, it is important to have some other form of payment handy in case you are unable to access your phone.

DEFINED

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 both 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.

What if your phone battery dies?!?



The Privacy Policy for each Pay App states what a User consents to when signing up for the Application. Be aware that 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 as well as other possible information. Also be ware that the company may be able to keep the information, for as long as they deem necessary, 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, and any other password protection available to ensure the safety of your data.

App	Apple Pay	Venmo	Facebook Messenger	Cash	Zelle	Xoom	Google Pay
Security	High	Low-Medium	Medium-High	Medium-High	High	Medium	High
International Pay Feature	No	No	Yes, limited	No	No	Yes	US/UK Only
Linked to Bank Account	Transfer to Bank account	Yes	No	Transfer to	Yes	Yes	Yes
Linked to Debit Card	Yes	Yes	Yes	Yes	No	Yes	Yes
Linked to Credit Card	Yes + Fee	Yes + Fee	No	Yes + Fee	No	Yes	Yes
Paying on the Web	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
In Store Payments	Yes	Limited acceptance at retailers.	No	No	No	No	Yes

	Apple Pay	Venmo	Facebook Messenger	Cash	Zelle	Xoom	Google Pay
Pros	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. You can cancel payments after you send them.	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.
Cons	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.	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 put in place.
- ◆ Do not use dating app sites on any public Wi-Fi. It is important to always make sure your connected through a secured 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 such as your place of work, in your profile or initial communications. Likewise it is a good idea not to include your contact information such as your email address, home address, or phone number on your profile

Create a Different Username/email

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 save that for the date, this will help to prevent you from giving away to much information.

It is a good idea to stay sober the first few or several encounters.

When possible you should do a search of the individual on the internet (see the Self Assessment Smart Card) before meeting up with the individual.

Online dating scams could run as long as six months before you notice anything suspicious so always be on the look out for unusual conversations such as needing money, or suddenly needing a ride somewhere.

Things to watch out for:

- ◆ An early request for photographs or videos
- ◆ Anytime anyone asks you 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 very well could be.



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

When you decide to give someone your phone number, use your cell, rather than your home or work phone. If things don't work out, cell phone numbers are easier to change

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 necessarily including or requiring emotional bonding or long-term commitments. These types of sites pose a serious danger to Users because it often calls for meeting up someone you do not know and trusting that they are on the up and up.

With these types of apps it is extremely important to make sure that someone you trust knows where you are going and who you are going with before you meet up with someone you may have just met. It is important to note that these apps are not just used for hooking up and can be used to develop relationships however it is not its primary function.

CASUAL DATING SITES: Match, Zoosk, POF, 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 type of dating sites usually mean a person is looking for something a bit more long term than a "hookup" and many times lead to a relationship, in fact many of these sites let you pick your level of interest in the dating world.

These sites target specific demographics based on features like shared interests, location, religion, or relationship type. Most of these sites 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 (much like eHarmony) that helps to match with people who don't just fit or share interests, but instead are compatible with each other in terms of emotional and relationship values. These sites go a bit deeper than any of the other It also helps you pace your communication with your matches, so that each of you remains comfortable and things don't move too quickly.

These sites or this level of online dating usually requires a form of payment and a membership to the site for access to its full content. Mainly these are sites people use when they are serious about dating and looking for a partner that they can marry.

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

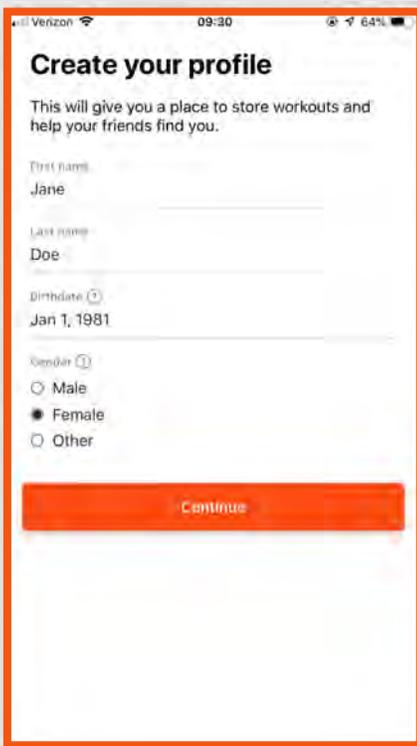
Fitness Apps



Do's and Don'ts

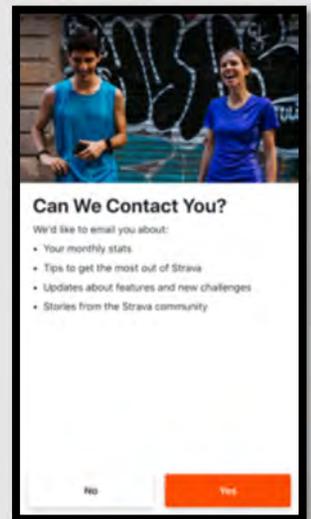
- Do make sure that your profile is not Public. It is also recommended that you limit what information you put on your profile even if it is private.
- Do make sure you keep your fitness app activity private by default so that your routes cannot be tracked online.
- Do ensure that family members take 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 could publish your routes and times you exercise on those 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.

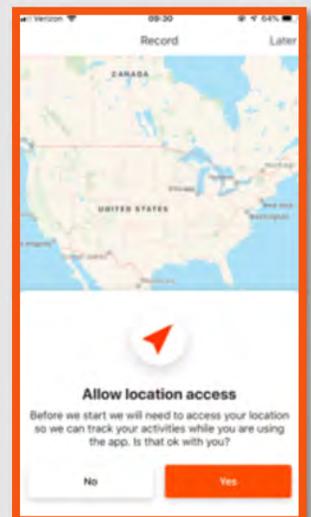


Strava sells itself as an activity tracker with the ability to also social network: Users can view the most popular bike or running paths among other Strava users, follow their friends' running routes, even log group exercises. It's almost vital to the app that you share your location data in order to get the most out of it, and that comes with a big privacy trade-off. Late last year Strava's heat map came under fire for posting its users whereabouts publicly online. Allowing others to view your route location leaves users extremely vulnerable to potential attacks by stalkers or by criminals looking to know when you may or may not be home. The following describes the best way to create an account on Strava while maintaining the utmost privacy to ensure one's safety.

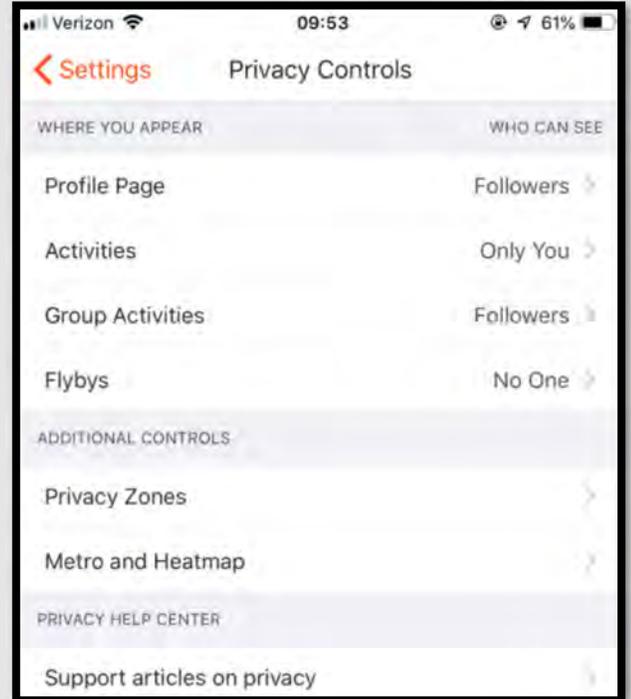
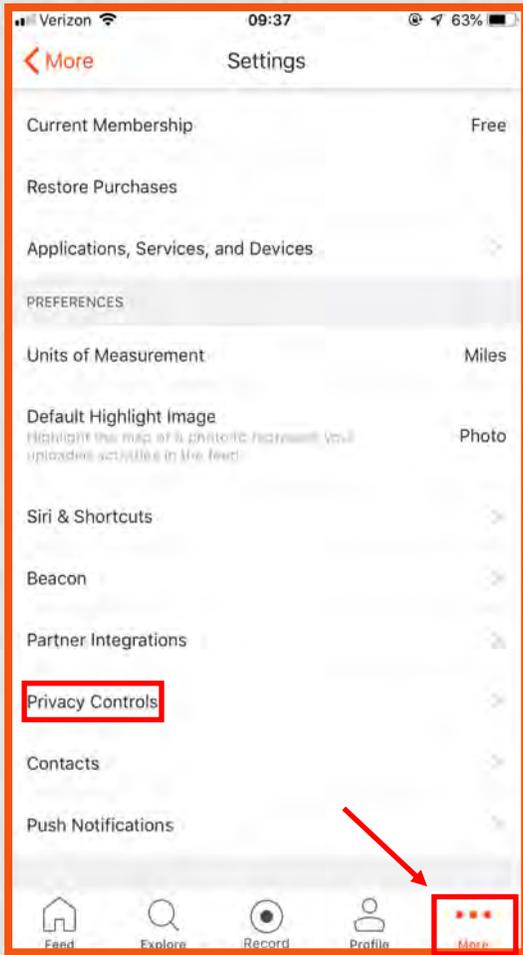
First, start by creating your account, only putting in the minimum personal information required to create your log on (shown here to the left). Later you will have the option to build upon your "Profile" by adding additional information about yourself, but this is not recommended.



Next (shown on the top right), Strava will ask you if they can contact you to push you monthly reports etc. Though this seems benign, it is not recommended that you allow this function as there could be more information Strava shares with you or about you to others. The next screen will ask you if you want to allow Strava to utilize your location. Although this is a big part of the app, it is strongly recommended that you not allow your location to be accessed.



Fitness Apps

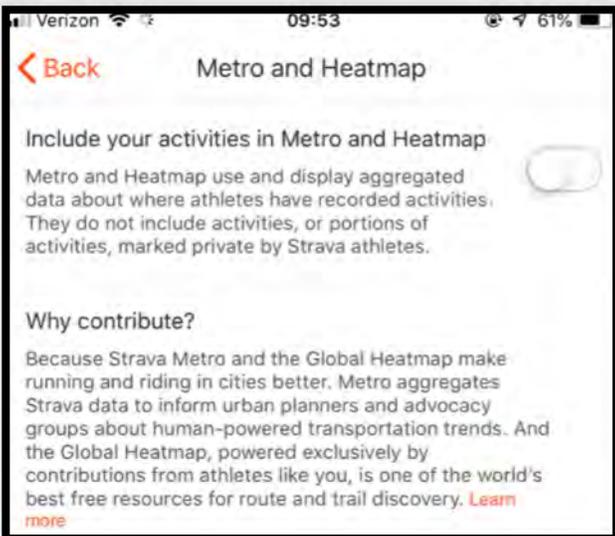


Even with phone apps, it is important to make sure you keep a strong password to prevent anyone from accessing your account.

Once you have completed the set-up process, there are still several settings that must be set in order to best protect your privacy. From the Home screen, look to the bottom of the page (top left if you are using an Android) and select the "More" tab (shown to the left highlighted in red). From there select the "Settings" tab and scroll to the bottom and select "Privacy Controls" (shown to the left).

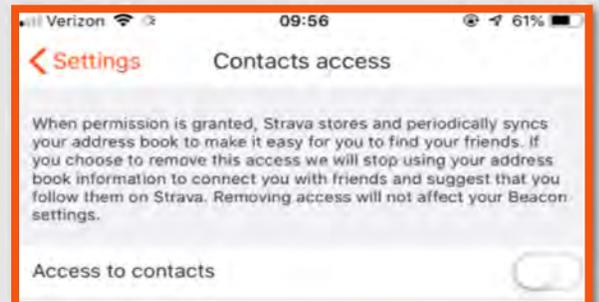
Under "Privacy Controls" it is recommended that you change any of the tabs under "Where You Appear" from Public to either Followers or Only You to maximize your privacy.

The "Privacy Zones" function allows its Users to draw a privacy circle around a certain area such as their house or work. When the User runs in that circle it is automatically hidden from all other Users. The down side is that if the User steps outside of that designated circle, that data will become public automati-



Strava now has a function that allows you to turn on or off whether or not a users activities show up on their "Metro and Heatmap." It is recommended that

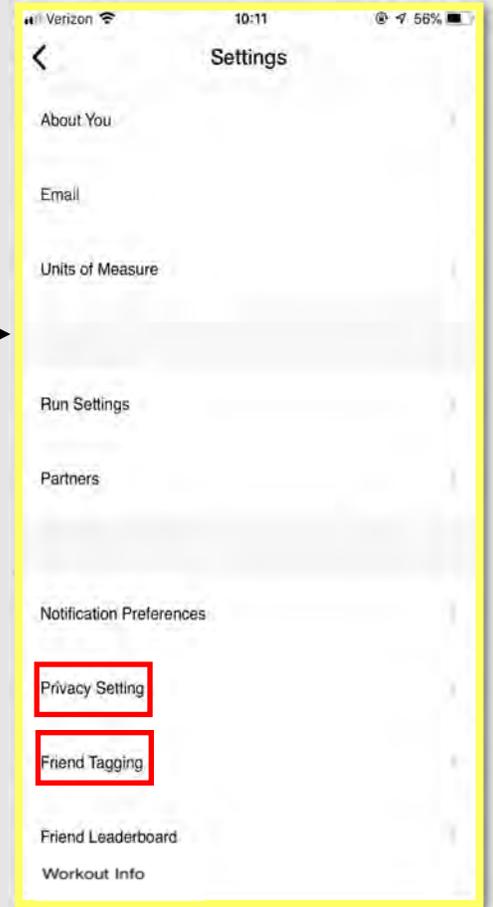
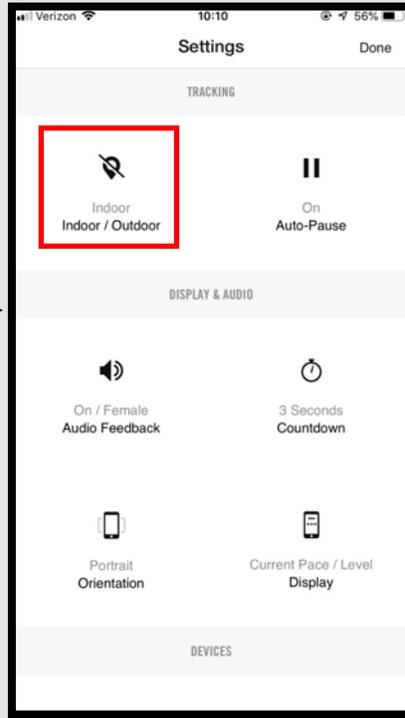
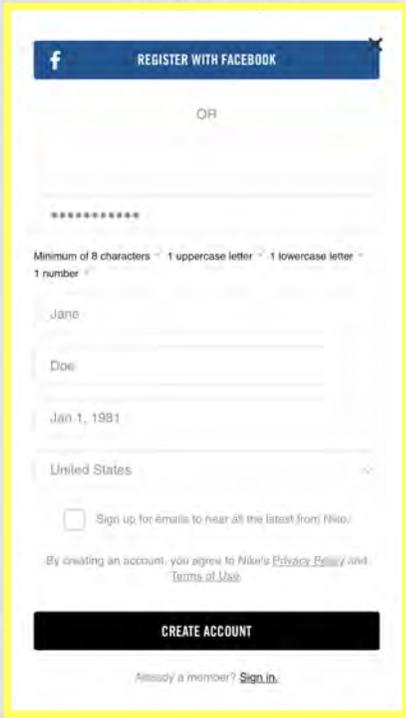
users leave this function "off". Next, go back to the "Settings" section and scroll to the "Contacts" tab. Here it is recommended that users do not allow Strava to access your Contacts.



Fitness Apps

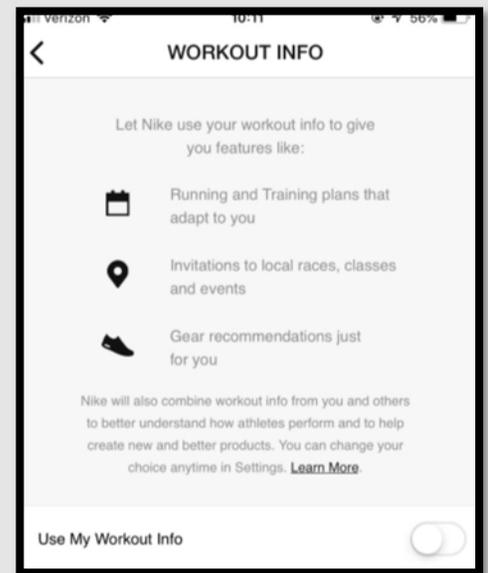
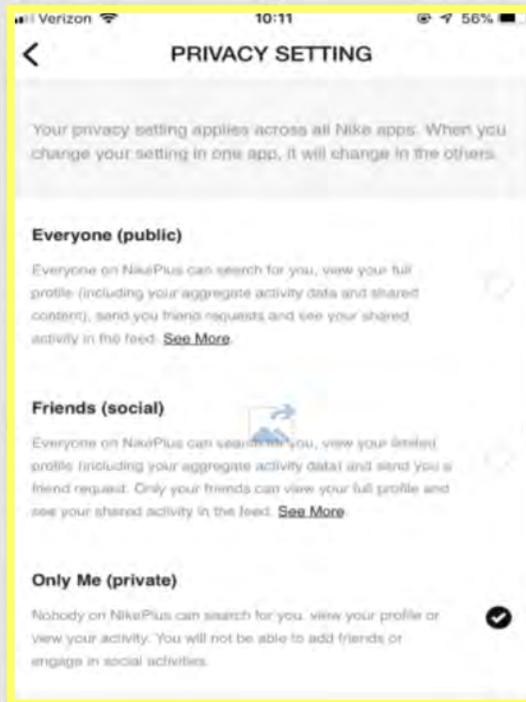


If you allow other third party apps to connect to your fitness app be sure to check both apps for up to date privacy settings.

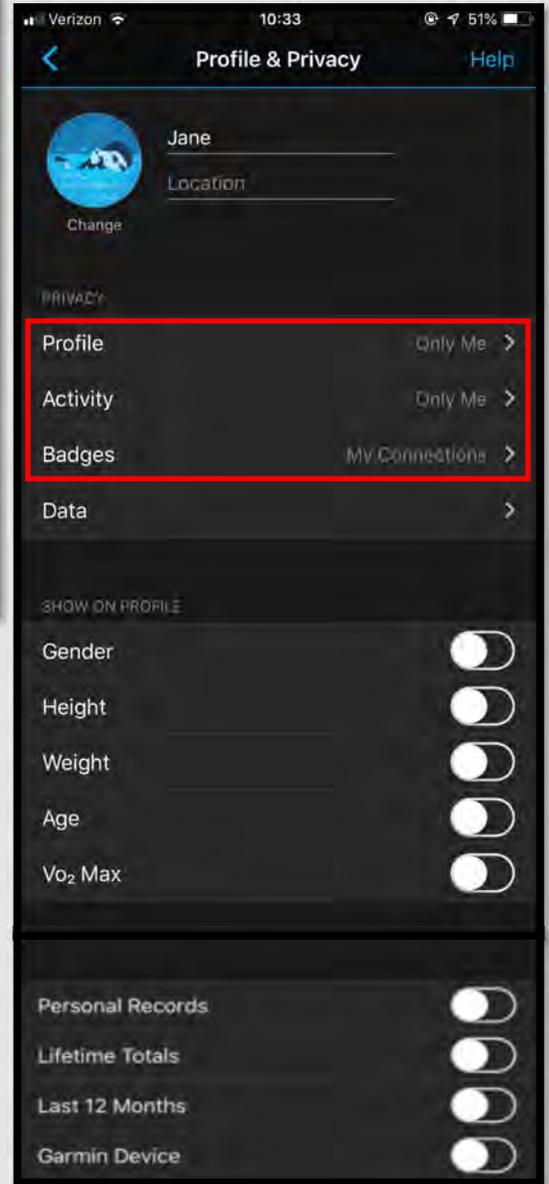
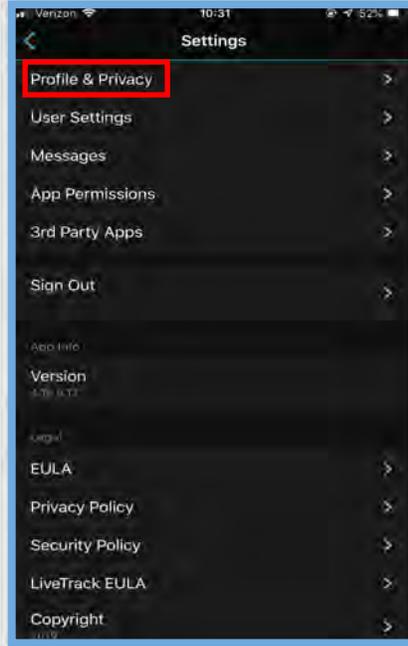
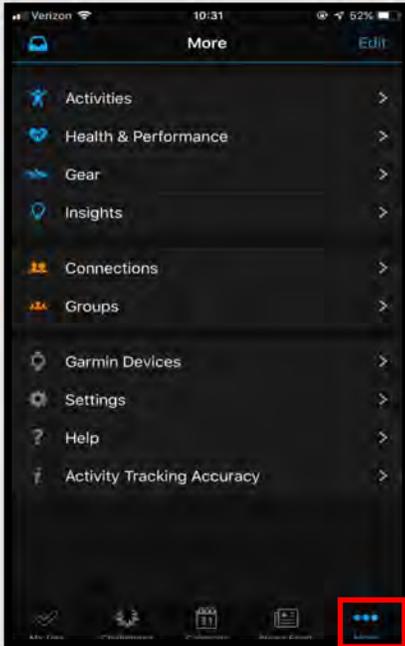


Nike's Run Club fitness app is widely popular and is known for being able to publish your run or other activities directly to your social media upon completion. Unfortunately, this also includes a user's run routes. When creating a User Account for this app it is important to limit the amount of information about one's self to only the minimum required. After putting in your basic information and creating your account, Nike will ask you a series of "Settings" questions, one of which (shown in the middle top screen in red) is whether or not the user wants to allow the App to track them (or use their location). It is recommended that

In order to get to the main "Settings" the User will need to select the "Picture" icon at the top left of their screen and then select the "Settings" icon in the middle of the page. Scroll to the "Privacy Setting" tab. It is recommended that Users set their privacy to "Only Me" or "Friends." Next, head back to the "Settings" menu and select "Friend Tagging" to turn off this function. Finally scroll to the Workout Info tab where it is recommended that Users turn this function off so as not to share unwanted information.

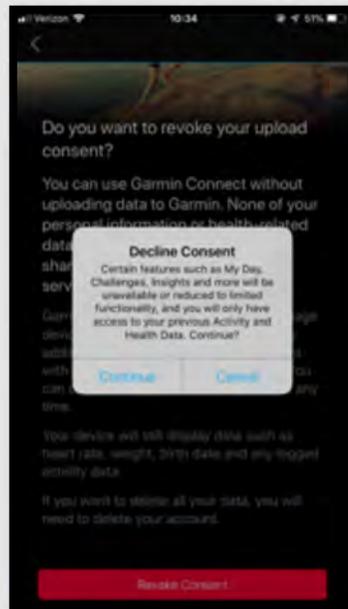
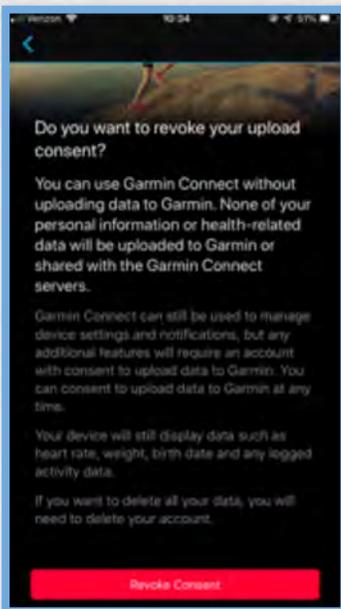


Fitness Apps



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

Many of the Garmin exercise apps offer a lot for the user to share with friends or the public. If these settings are not set correctly, they will automatically share your information with the Public. From the Home screen look to the bottom of the page (top left for Android users) for the "More" tab (shown above to the left in red), select this, then select the "Settings" tab to begin locking down your profile. Now select "Profile & Privacy" to look over the "privacy" section. It is recommended that the tabs in this section (highlighted to the right in red) be set to "only me" or "My Connections." Here you can also limit what details about yourself are shown on your profile.



Now, select the "Data" tab under the "Privacy" section, here you will find three different tabs; "Data Upload," "Insights," and "Popularity Routing." It is recommended that you select and turn off the "Popularity Routing" function. Next, Users may want to review the "Data Upload" section to review what information they have allowed Garmin access too and decide whether or not they want to continue to provide consent (shown here to the left). Users can do the same for the "Insights" tab after reviewing the consent policy.

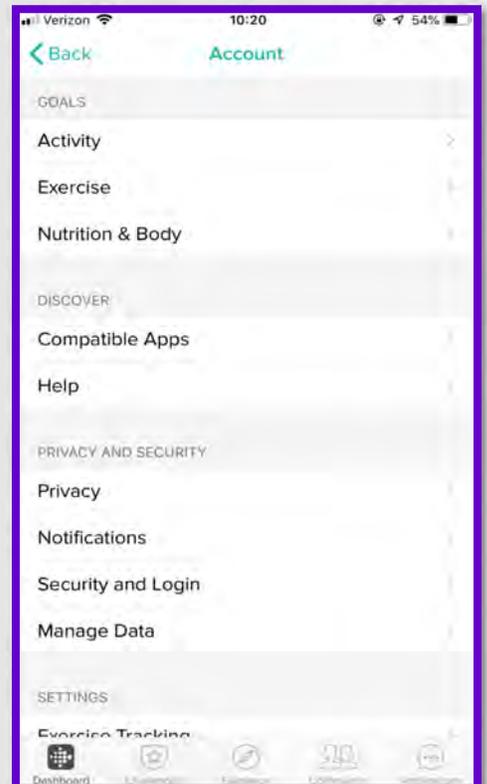
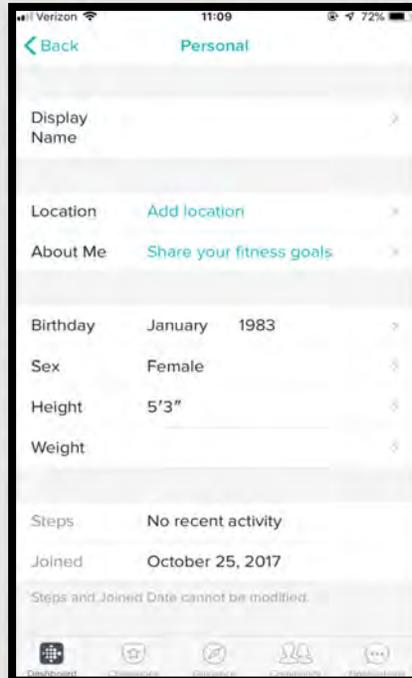
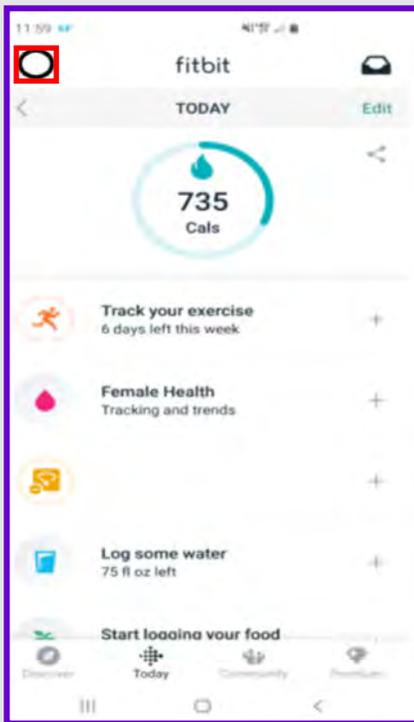
Fitness Apps



Finally, head back to the “Settings” section and select the “App Permissions” tab to review what permissions you have allowed Garmin access to. Here it is recommended that you not allow Garmin access to your “Contacts” or “Calendar” and carefully consider whether or not you want to allow the app to have access to your “Camera” and “Location.”



Fitbit



FitBit is a physical activity tracker designed to help users become more active. By default, older versions of FitBit pushed user’s workout information to the public. The company has since changed this setting in order to protect its Users. Now, user information is private until it is configured otherwise. Though it is presumed that your privacy settings are set in this app, it is a great idea to review those settings to make sure they are set to your personal standards.

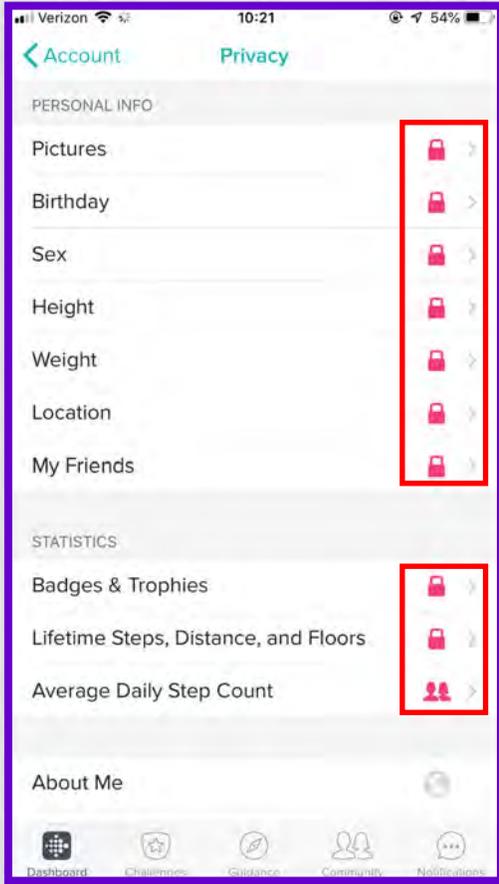
In order to review your Fitbit account head to your Home Screen and select the “Picture Icon card” in the top Left corner (shown above in red). From here you can select your user account at the top of the page. Now, select “Personal” where you will then want to review whether or not you have allowed for your “location” to be turned on along with which personal data you have provided to Fitbit. Next, you will want to head back to the “Account” section. 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.

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

Fitness Apps

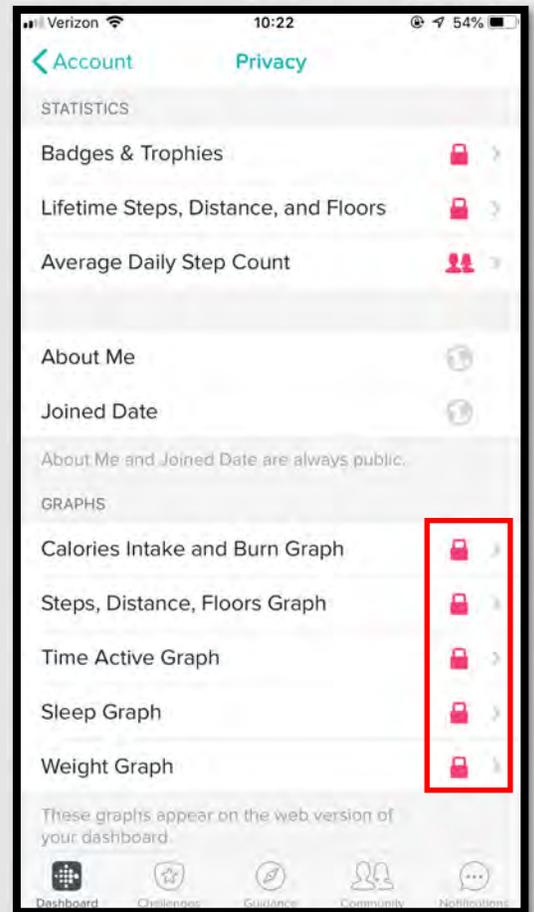


Don't just set the settings within the Fitness App, make sure you go into your phones settings and update what you do and do not allow for that app from your phone.



Once you are in the “Privacy” section there are a lot of different tabs (highlighted in red to the left) that will need to be checked for privacy. It is recommended that you not share any information that might be considered PII or that you would not otherwise want available to the public. Remember the “About me” section is always going to be available to the public so it is important to note what information is available there.

Now that you have reviewed and updated all privacy settings you may want to 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.



Polar is a company that produces fitness tracking watches and hardware, all of which connect to its popular app, Polar Flow. According to an investigation that began last June, 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:

- Go to Settings and then Privacy to set the default for future runs to Private.
- Change the privacy of each of your past runs individually.
- Make sure to set your profile to Private as well.

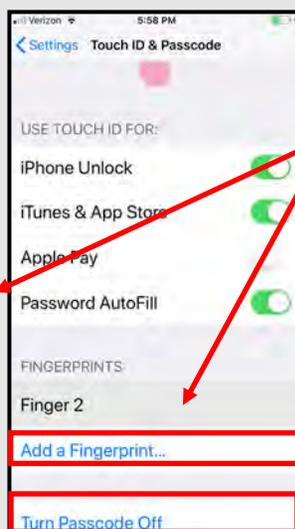
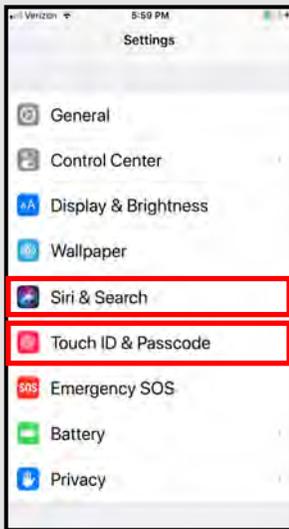
iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD



“Best Practices”

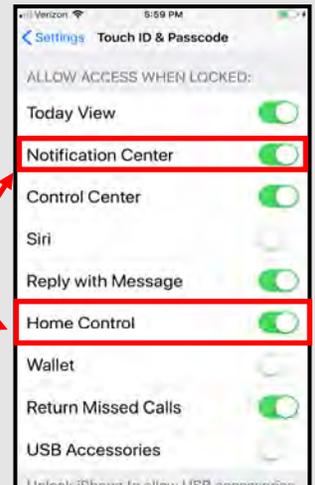
- Smartphones and tablets are not impenetrable. Secure your smartphone with a password, and use apps such as Find My iPhone to locate lost or stolen devices.
- All smartphones and tablets have cameras and microphones that can be remotely activated. Caution should be used when device is near anything 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 now 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 or the vendor. Whether turned on or off, location services are always available to 911 and first responders.

“Physical Security”



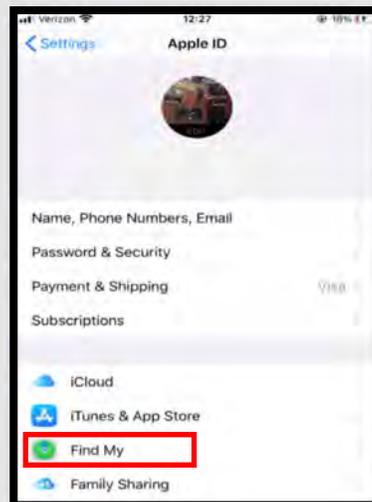
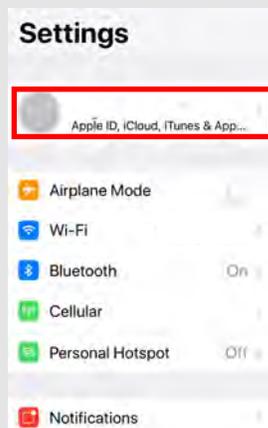
Under “Settings” and “Touch ID & Passcode,” select “Add a Fingerprint” and “Turn Passcode On”. Be sure to use at least a 6 digit passcode. Alpha-numeric passcodes are even better options. Additionally, it is recommended that you turn off *Siri* due to the programs’ listening capabilities and bugs associated with accessing your phone through *Siri* without a password.

Turn off the settings highlighted to the right in **red**. These settings allow others access to areas of your phone without a passcode.



“Find My iPhone”

To start, 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.



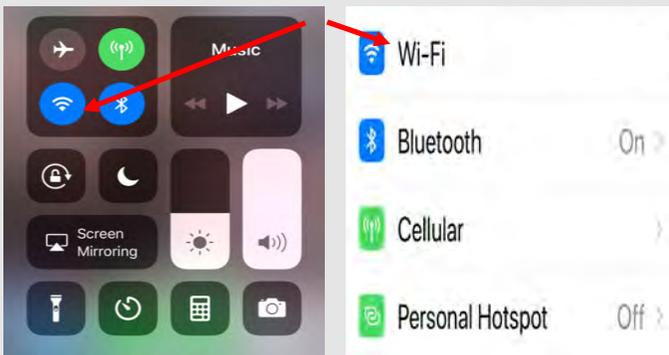
Smartphones contain extremely sensitive personal data and therefore should be treated with extra security precautions #protectyourdata



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”

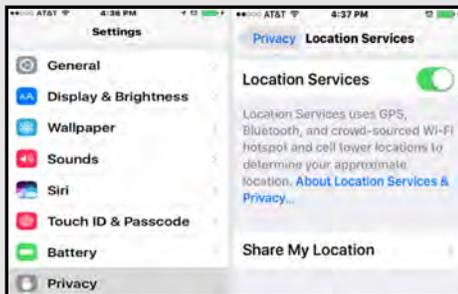
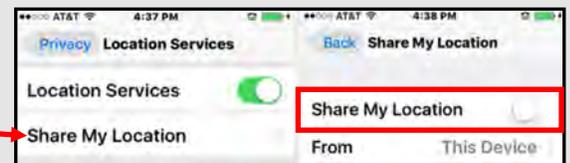


Bluetooth is a wireless technology standard for exchanging data over short distances from fixed and mobile devices. When Bluetooth is enabled on your iPhone or tablet, hackers can gain access to your device and obtain contacts, messages, calendars, photos, and notes without your knowledge. It is therefore 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”

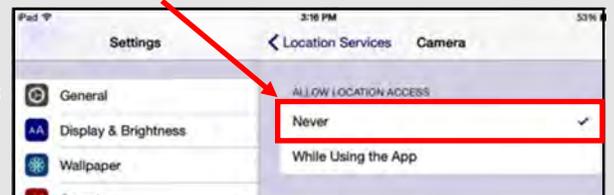
Whenever you take a photo, your phone records the location and saves that information inside the photo’s EXIF data. When you send that photo to someone else, they may be able to see where you took it, in some cases, down to a specific street. If you post a picture taken from your home, anyone who can 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 located 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 locating your phone 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.”



iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD



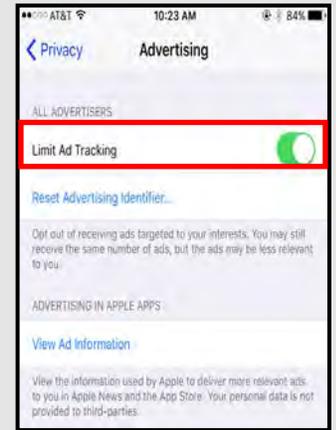
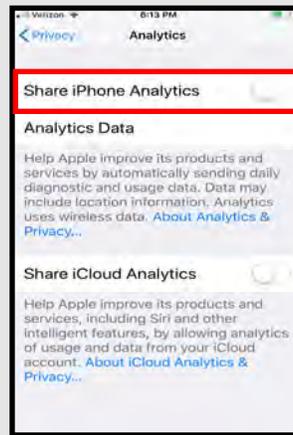
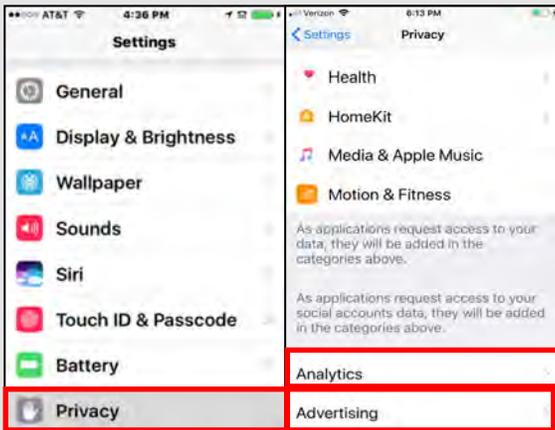
“Analytics Data and Ad Tracking”

“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”

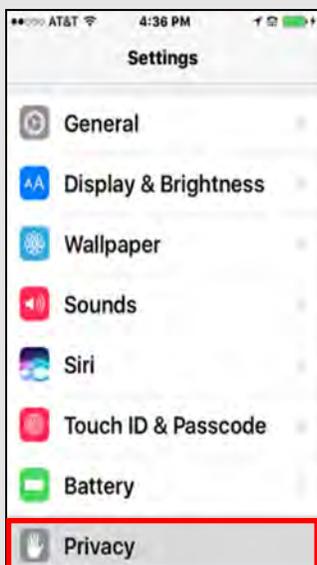
3) Then go back and select “Advertising” Turn ON “Limit Ad Tracking.”



“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.

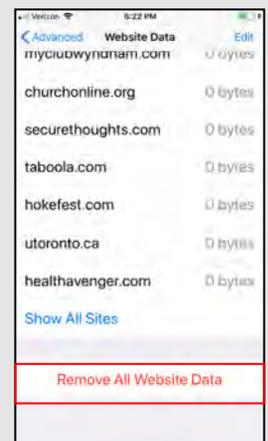
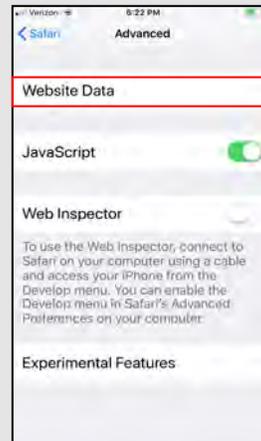
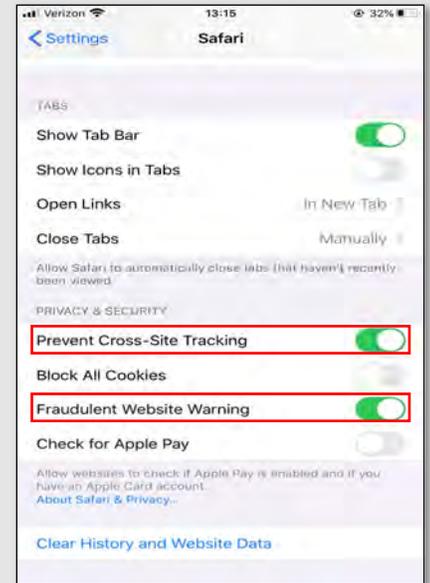
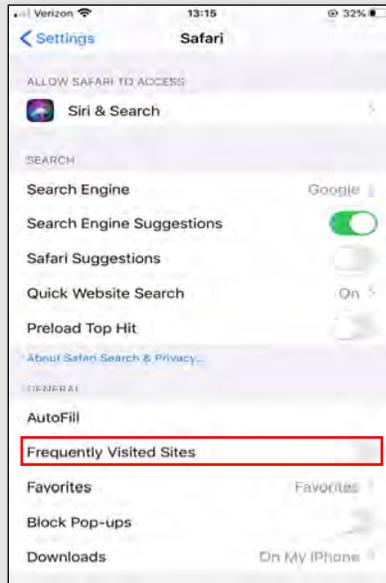
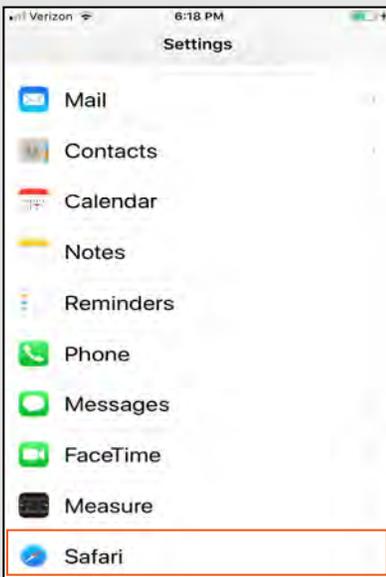


iOS PRIVACY SETTINGS (iOS 13.0) SMART CARD



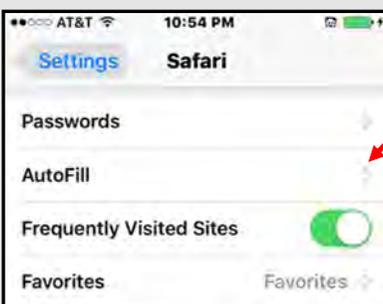
Safari's "Do Not Track"

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 12.0 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, however, under "General" turn off "Frequently Visited Sites." This prevents Safari from tracking sites you regularly visit. Next, under "Privacy & Security" turn on prevent "Cross-Site Tracking", "Block All cookies", "Ask Websites Not to Track", and "Fraudulent Website Warning."



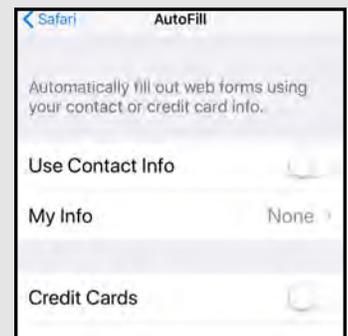
It is also best practice to clear the browser history periodically. To do so, continue to scroll down in the Safari settings, at the very bottom select "Advanced" > "Website Data", then select "Remove All Website Data"

"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"



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

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. Caution should be used when your 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.
- ◆ Prior to downloading apps on your device, read the developers permissions. Many apps request permission to access your camera, microphone, text messages, and phone contacts.
- ◆ Keep your locations services turned off until they are actually needed. Otherwise, your daily movements are likely being tracked by various apps and/or the vendor. Location services are always available to 911 and first responders.
- ◆ If you have a google account, you can use your google credentials to login at maps.google.com/location-history to see your device's 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.*

In order to make sure your Android is up to date with the latest Android Version follow these quick and simple steps. 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 .

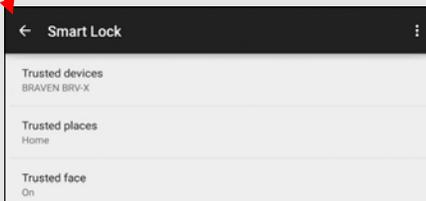
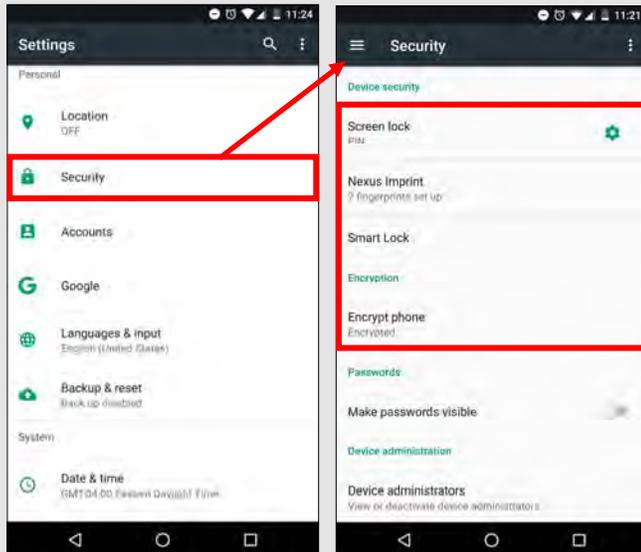
Physical Security

The first line of defense in preventing unauthorized access to your device is to protect it with a passcode. Android 9.0 adds a slew of enhanced security features to accommodate this, including fingerprints, facial recognition, encryption, and setting of app-level permissions.

Tap the "Settings" icon and then tap "Biometrics & Security" or "Lock Screen".

Here you can configure your screen lock method. The options are Swipe, Pattern, PIN, Face, Iris, Fingerprints, and Password. The most secure way to protect your phone is to use the **biometric** options. A password is the strongest backup solution.

However, this can be cumbersome when unlocking your phone. Smart Lock (which may be under "Lock Screen" instead of "Security" for some Android users) allows you to set trusted places (home, car, etc.) so that when you are within a certain range, your phone will not lock. You can also set up trusted devices or trusted faces which will allow you to simply look at the device to unlock it. Set any Smart Lock option with caution.



Biometrics: You can also add your fingerprint, face, or iris and set conditions for its use. This requires PIN entry and access.

Iris is the most secure of these Biometric options, but may not be a suitable option for those who wear glasses or contacts on a regular basis.

Selecting "Encrypt phone" 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.

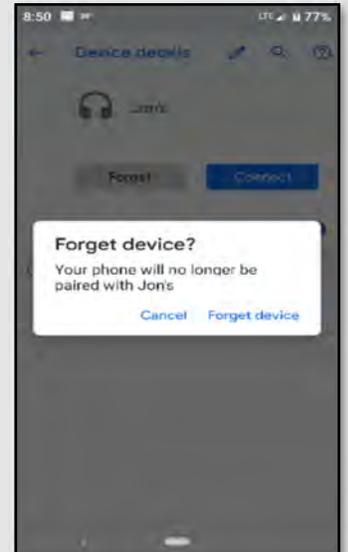
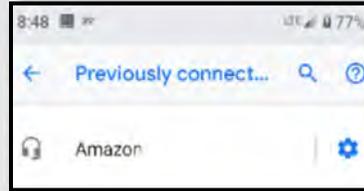
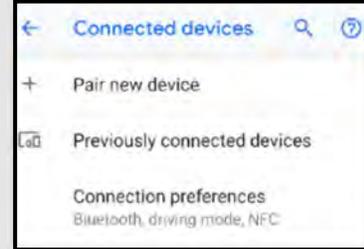
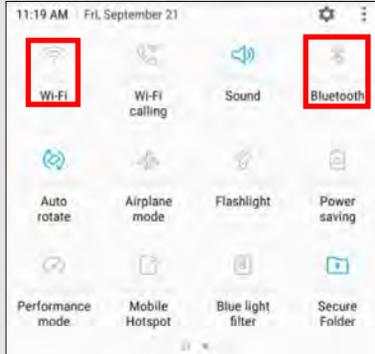
ANDROID PRIVACY SETTINGS (ANDROID 10.0)



Mobile Hotspot and Bluetooth

Rather than connecting to public Wi-Fi, most mobile carriers have an option to use the mobile device as a mobile hotspot. You can turn this option on and off under “Settings” > “Wireless & Networks” or “Connections” > “Mobile Hotspot and Tethering”. Bluetooth is a wireless technology standard 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”.

Wireless Networks



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

If public networks must be used, avoid logging into accounts that require passwords and always use a VPN client to encrypt online transactions.

If you would like to delete old Bluetooth devices with a few additional steps. While in the Bluetooth section select “Previously Connected Devices” then select the settings icon and hit “Forget.”

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.

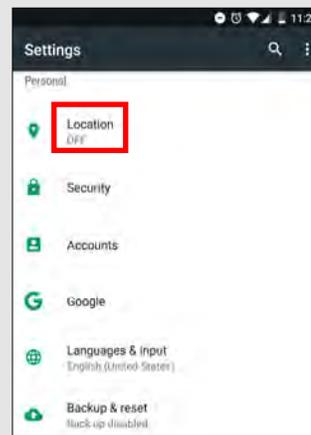
Turn off NFC when not in use by tapping “Settings” > “Wireless & Networks” or “Connections”.

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”.

ANDROID PRIVACY SETTINGS (ANDROID 10.0)



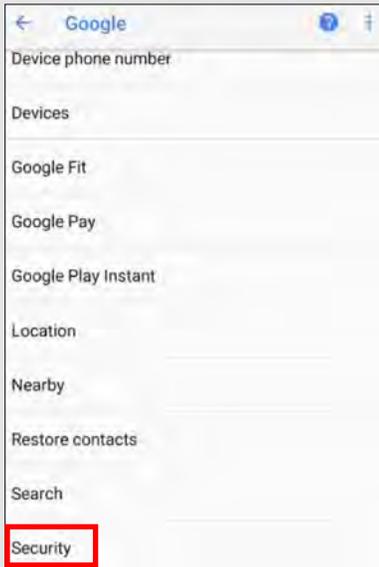
Lost/Stolen Phone

In the U.S. it has been reported that over 100 cell phones are stolen or lost every minute. This fact alone proves it is necessary to keep your device secure and locked with biometrics or a passcode. Since all Android phones work by syncing your phone to a google account, "android.com/find" is the native "Find my Device" tool for Android phones. Though this feature is automatically enabled, you may download the "Find my Device" app from the Google Play store to verify it's function, or to find a different device.



- ◆ 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.



If your device is lost or stolen, you can go to Google's device management page and access your device's current or last reported location. You can make the device ring at full volume to help you find it or remotely lock or erase the device.

To enable:

Tap "Settings" > "Google" > "Security" > "Find My Device".

Ensure Location services are turned ON (follow instructions on previous page).

Go here: android.com/find and check that your device can be located.



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

Ad Tracking

Ads can track everything you do. Not all Android devices and OS versions have settings to turn Ad tracking off. For those that don't have this setting, you can download and use any number of ad blocking / privacy-oriented browsers or browser add-ons. These are just a few examples.



For those devices with the option:

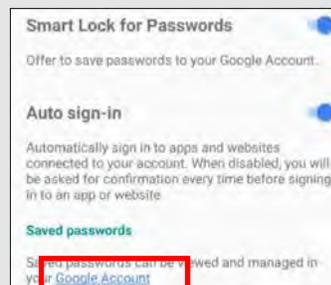
Go to "Settings" > "Google" > "Ads".

Tap the toggle switch to the "on" position for "Opt out of Ads Personalization".

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.



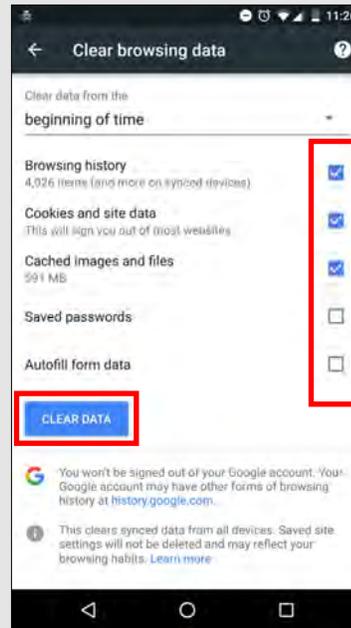
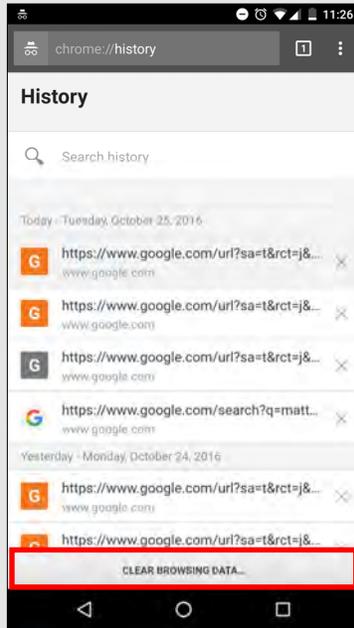
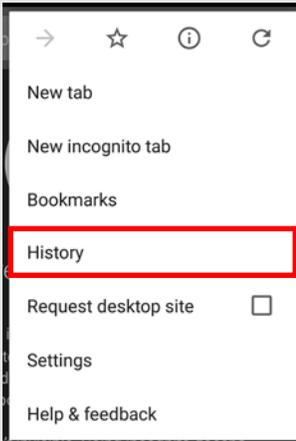
All saved passwords are encrypted and stored in the Google cloud storage that comes with your account. Although it is recommended that you turn off the above options, only you can balance your security with the convenience of saved passwords.

ANDROID PRIVACY SETTINGS (ANDROID 10.0)



Internet Privacy Settings

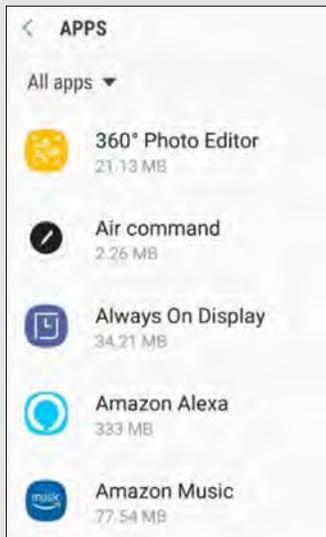
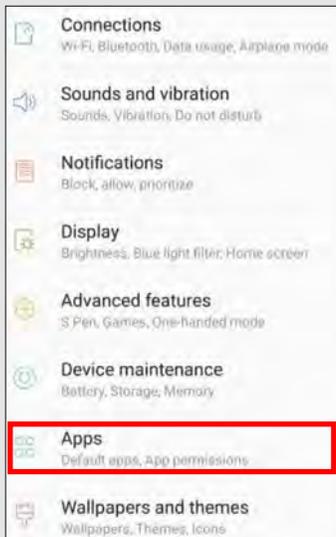
Browser history and cookies are tracked when browsing the web from your mobile devices. To ensure privacy, open your browser (Chrome) and tap the three dots in the upper right-hand corner. Tap “History” then “Clear Browsing Data” at the bottom of the screen. On the next screen, select the applicable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



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

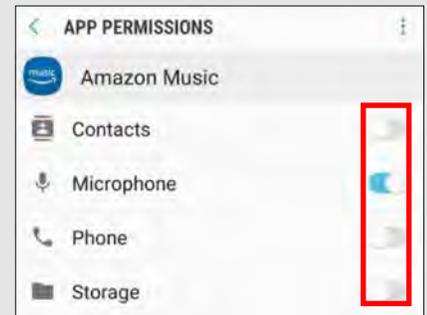
The applications you load access different capabilities on your device regardless of whether they are active or working in the background. You can see, and to some degree control what access each application has in the Application Manager.



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

Then tap “Permissions”.

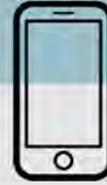
This will show you what permissions are granted when you accept the user agreement to download the app. In most instances these permissions can be controlled individually.



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.

Pay attention to user agreements when downloading new apps. This will tell you what the app is requesting access to on your device.

TRAVELING SAFELY WITH SMARTPHONES



Do's and Don'ts

- ◆ Enable password and fingerprint locks on your device. Also, protect “Settings” changes on your phone by requiring a password.
- ◆ Assume that all information on your device can be accessed remotely. Don't store passwords and sensitive information on your phone
- ◆ Always use complex passwords, the stronger and longer the password the more difficult it will be for someone to hack into.
- ◆ 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. Only use networks that the business provides the name, don't assume if its named appropriately it is safe. and WiFi off when you are not using them.

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 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

“Just pay with Amazon gift cards or I will send the police to your house tonight!”

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.

“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 consumer’s 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:

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 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 (You can also call: 1-800-876-7060)

to protect them. Their smartphone is yours for the monitoring, after all who gets the bill? #keepourkidssafeonline

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

- ◆ Only connect with gamers and online profiles of people you know and trust. Review connections often.
- ◆ Assume ALL information and images you share are publicly viewable, regardless of your settings.
- ◆ Use a picture of something other than yourself for your profile photo. Profile photos are viewable to the public.
- ◆ Tell kids to let parents or responsible adults know if 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** allow children to go to sleep with their smartphone or other device in their room. Pick a certain time that your tweens/teens have to bring you their device, roughly a hour before they go to bed.



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/>

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.

Be a role model:

IF you have privacy concerns on your social media, your child will too.

KEEPING YOUR CHILDREN SAFE ONLINE

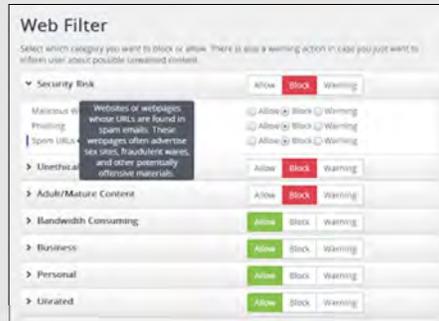


Security Applications

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, where you can also track kids' spending and add money to their Microsoft accounts.

Google has it's own Safety Center to help ensure your kids remain safe Online, stay up to date at www.google.com/safetycenter/families/start/ #themoreyouknow



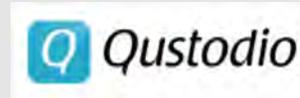
Net Nanny Social lets you keep track of all your children on social media including Facebook, Twitter, Google+, Instagram, Pinterest, and LinkedIn. Features include:

- 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"> • Do share photos only with known and trustworthy people. • 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 ensure that family members take similar precautions with their accounts. Their privacy and share settings can expose personal data. | <ul style="list-style-type: none"> • Don't tag geolocations. The information in these tags can disclose location of where the photo was taken. • Don't give apps permissions to access the cellphone location services. • Don't post photos of others, especially children, without getting permission beforehand. |
|---|---|

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	Public ; 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.	Public ; 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	Public ; 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	Private ; 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	Public ; Only You, Your Friends, Your Family	Yes for original uploaded file (not for resized file) ; 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	Public ; Private (optional password protection)	Yes for original uploaded file (not for resized file)	Location data is available unless you disable it	Yes; 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

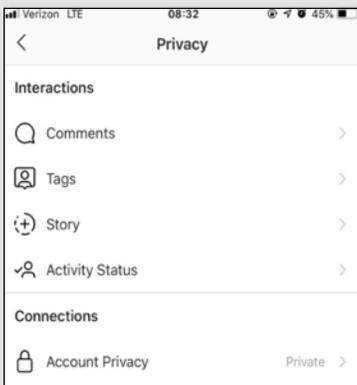


EXIF Removal Tools

- ◆ **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/>

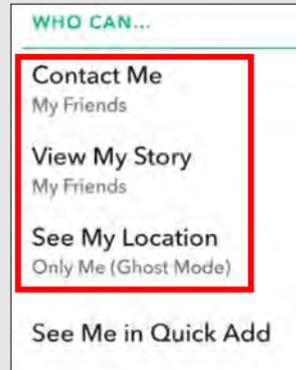
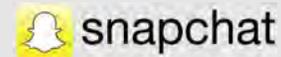
For more information, please see the EXIF Data Smartcard

Privacy Settings

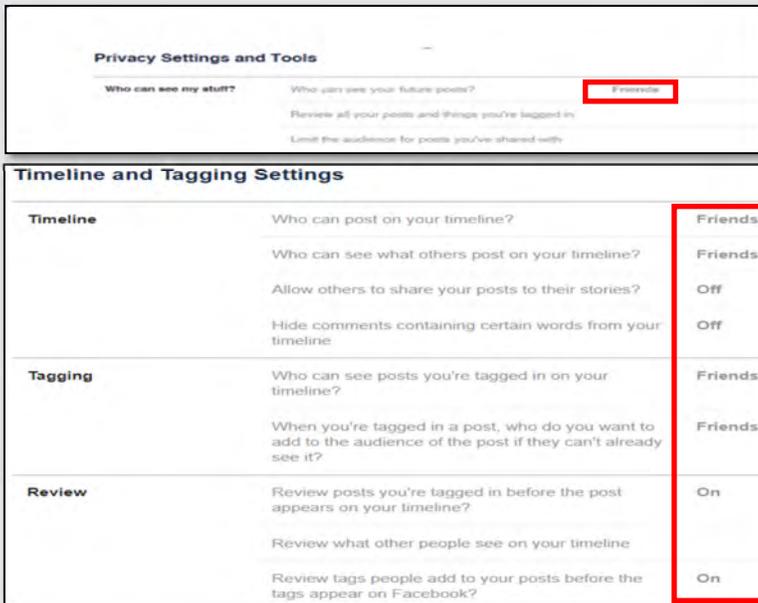


Tap on the bottom right. Then tap the menu icon at the top right. Tap at the bottom of the screen. Scroll to find "Privacy" and then "Account Privacy," make sure the toggle is on for "Private Account".

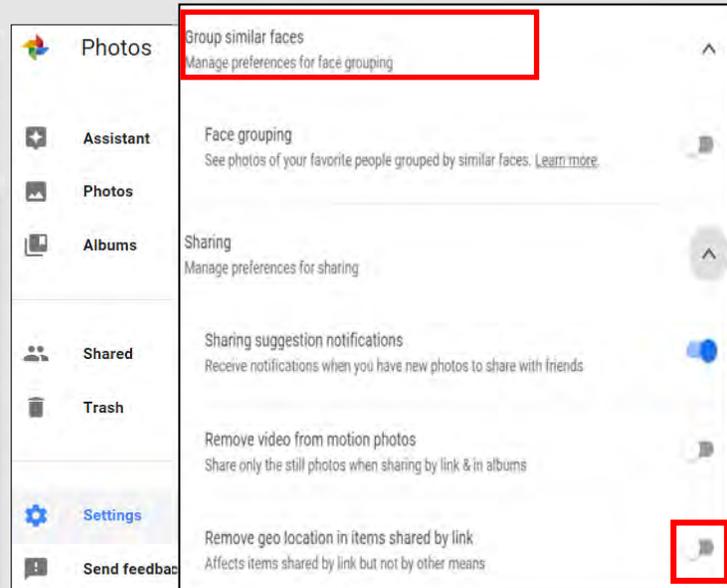
When your account is private, only people you approve can see your photos and videos.



Tap at the top. Tap to access Settings. Scroll down to the "Who Can" 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.



Tap on the top left corner. Tap "Settings". Ensure that the toggle is *on* for "Remove geolocation" from the Share section. Ensure that the toggle switch is

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"> Email address: Only you Real name: Your friends and family Current city: Your friends and family Edit your IM names, real name, or current city
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"> View: Only you Comment on: Only you Add notes, tags, and people: Only you
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"> Safety level: Safe Content type: Photos

Content filters

Search settings	<ul style="list-style-type: none"> SafeSearch: On Content type: Photos / Videos
-----------------	---

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

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.

Album Privacy

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

Twitter

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 utilize the information internally. EXIF metadata are listed as tags that stores 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
Geo-location	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.
Timestamps	ModifyDate, DateTimeOriginal, CreateDate	Creates a log of behavioral patterns and personal timelines.
Camera	Make, Model, Serial Number	A unique serial number identifies the particular device for an image or sets of images.
Authorship	Artist, Owner Name, Copyright	Links images with a name or organization.
Image Summary	ImageDescription, UniqueImageID, UserComment	Potentially reveals identifying information about the content of the images, such as captured persons or locations.

Do:

- ◆ Prevent your device(s) from capturing geo-location data when taking pictures. Remove EXIF metadata from images taken by smartphones or digital cameras.
- ◆ Use privacy settings from the app to limit the audience to only yourself or close friends and family, before uploading pictures.
- ◆ Even with no EXIF data, the content of images may contain identifying information, including persons and locations. Assume that anyone can see, copy, or forward photos that are posted online.

Don't:

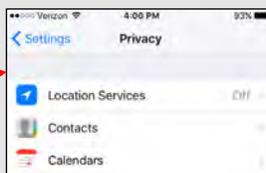
- ◆ Allow apps to automatically upload and share captured images (e.g. Instagram, Flickr).
- ◆ Assume that device settings remain the same after updates or over time. Verify the settings routinely.
- ◆ Upload pictures with landmarks, easily identifiable structures, or signs indicating location.
- ◆ Give 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.

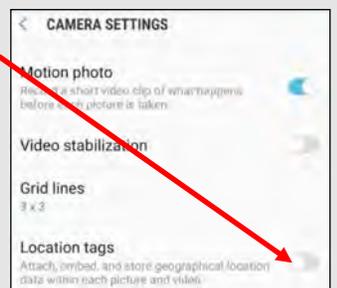
- 1 Select the "Settings" app. Click "Privacy" > "Location Services".
- 2 Turn off location services altogether or for the iPhone's camera applications.
- 3 Return to the "Settings" app. Click "Privacy" > "Photos".
- 4 Disable permissions for other apps to have access to the photos stored in the device's 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 for your smartphone's camera application, as shown on the previous page.
- ◆ Remember that uploading or sharing a lower quality image will still 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 the 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.

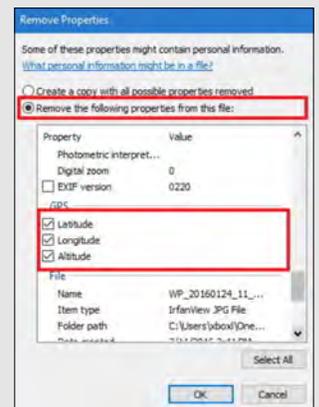


Reviewing & Removing EXIF Data in Windows

Use the Windows OS to verify EXIF data has been removed.

Navigate to an image in File Explorer. Right click the image and select "Properties".

- 1 Select the "Details" tab. You can examine EXIF metadata that is available.
- 2 Click "Remove Properties and Personal Information".
- 3 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 the EXIF metadata removed, images containing, vegetation, addresses, business names, road markings, and landmarks, could allow someone to identify the location of where a photograph was taken. Geo-localization, the determination of a location of an image through visual information, is currently being researched and 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 the computer can apply the location metadata of one picture

Remove EXIF data before sharing or posting images, especially images captured in private homes or businesses. #PhotoSafety

LOCK DOWN YOUR LAPTOP SMART CARD

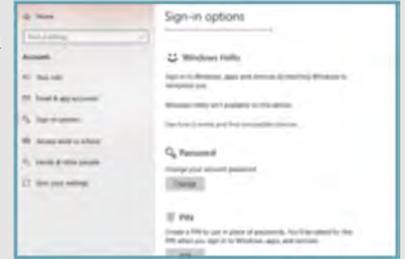


Creating a Windows Log-in Password

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 > 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 > 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 though likely 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 > 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 **Start Button > Settings > System and Security** and select the BitLocker slider to secure your hard drive data.

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.

Laptop Security Tip: If possible, set-up two factor authentication on your laptop by pairing it with a Bluetooth device you carry on your person.



LOCK DOWN YOUR LAPTOP SMART CARD

Virtual Private Network (VPN)

A Virtual Private Network (VPN) connection could save your life. No, really, it could. Well, maybe that's a bit dramatic, but it *can* safeguard your data and protect your personal 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 rarely 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. In fact, there are few reasons not to use VPN, whether you're connecting at home or on the go.

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. It really is that simple.

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 ISP 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

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
- <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

Wireless Router	Physical hardware that allows users to connect their devices to a shared internet network.
Service Set Identifier (SSID)	Public name of a wireless network.
Pre-Shared Key (PSK)	Authentication mechanism that mandates a password. Adds additional security to wireless networks.
Hypertext Transfer Protocol Secure (HTTPS)	Uses various encryption protocols to add additional security to HTTP.
Media Access Control (MAC) Address	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.

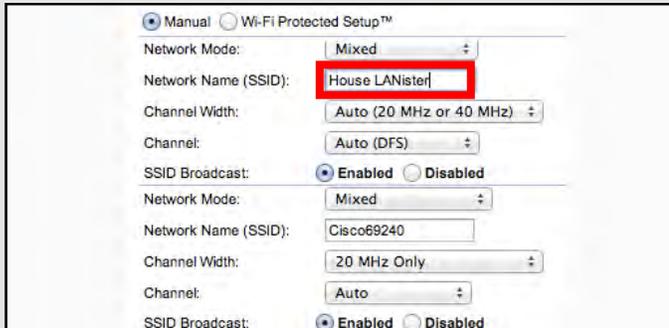
When changing your username and password for the WIFI, it is important to consider the following: choose a username that does not include you or your family members’ names; creating a password that is long and complex. Lastly, it is important to change any Guest account password to something other than 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

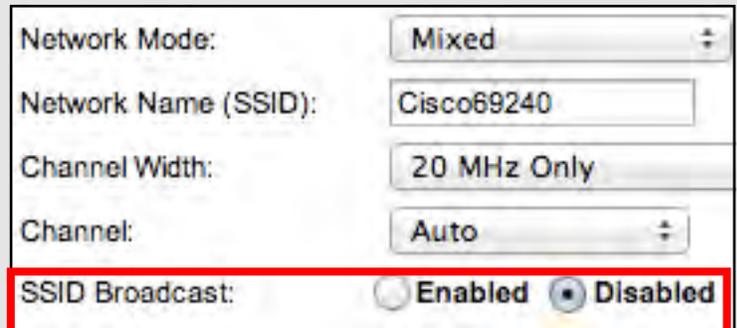
SECURING YOUR HOME WIRELESS NETWORK



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 chose 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. Remember, that while it is nice to be able to disable the broadcasting of your SSID, it is important to note that it can be easily unhidden should an individual request to find “hidden Wi-Fi’s”.

If you have smaller children in your home who have devices like the Leapfrog or Vtech games, and you disable your SSID broadcasting your child’s device will not be able to find your network and connect to the internet. In order for those devices to connect, you will need to go back into your router settings and re-Enable the broadcasting of your SSID.

Router Firewall

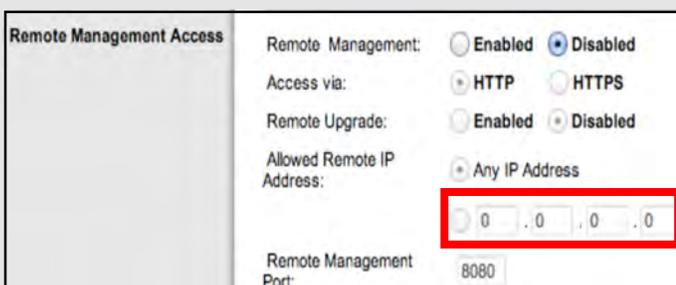


The next two settings are usually found in “Router Settings” but you may have to look around a bit to find them.

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



Enabling HTTPS

Router Password:

Re-Enter to Confirm:

Access via: HTTP HTTPS

Access via Wireless: Enabled Disabled

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 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

Local Management

Management Rules

All the PCs on the LAN are allowed to access the Router's Web-Based Utility

Only the PCs listed can browse the built-in web pages to perform Administrator tasks

MAC 1:

MAC 2:

MAC 3:

MAC 4:

Your PC's MAC Address:

Add or Modify Wireless MAC Address Filtering entry

MAC Address:

Description:

Status:

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.

Enabled Disabled

Prevent PCs listed below from accessing the wireless network.

Permit PCs listed below to access the wireless network.

Wireless Client List

MAC 01:	<input type="text" value="00:00:00:00:00:00"/>	MAC 17:	<input type="text" value="00:00:00:00:00:00"/>
MAC 02:	<input type="text" value="00:00:00:00:00:00"/>	MAC 18:	<input type="text" value="00:00:00:00:00:00"/>

Encryption

WPA-PSK/WPA2-PSK

Version:

Encryption:

PSK Password:

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 examples, but different from the administrative router access password.

Useful Links

Practically Networked

www.practicallynetworked.com/support/wireless_secure.htm

Wi-Fi.org

www.wi-fi.org/discover-wi-fi/security

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

ADDITIONAL RESOURCES



Free Annual Credit Report

www.annualcreditreport.com

USA.Gov

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

Stay Safe Online

www.staysafeonline.org

On Guard Online

www.onguardonline.gov

Equifax—ID Protection Kit

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

IRS—ID Protection, Prevention, Detection and Victim Assistance

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

Would you pick up a used chewing gum off the floor and stick it in your mouth? So why would you put a random USB stick in your computer. Don't put things in things without knowing things.

MO CYPHER



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

Kids Games
<https://sos.fbi.gov/>

Safety Reviews for Games, Websites, & Apps
www.commonssensemedia.org

Opt Out of Interest-Based Advertising
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>

