Keeping Safe on Social Media

Social media sites and apps are great ways to connect and share information. User profiles, timelines, social media status, friend lists, and message services grant your contacts insights into your day-to-day activities. However, these sites can also provide adversaries with the critical information they need to disrupt your life and harm or harass you, your co-workers, or even your family members.[1] The following guidance can better prepare you to protect against online threats.

Practicing good operations security (OPSEC) and using simple countermeasures will minimize the risks that come from using social media and help you protect your critical information. The first step in this process is to identify this critical information.

Identify Critical Information

Critical information is any information considered sensitive or that could do harm if compromised. Here are some examples:

- Names, photos, and relationships
- Usernames, passwords, computer and networking information
- Operational, security, and logistical data
- Mission capabilities or limitations
- Job title, location, salary, grade, and clearance
- Schedules, travel itineraries, and locations
- Social Security numbers, credit cards, and banking information
- Work or personal addresses and phone numbers
- Interests, hobbies, likes, and dislikes

Vulnerabilties and Risks – What's the Problem?

Unauthorized access to data is a growing problem, especially for critical information. People unwittingly expose private information, privileged work data, medical details, and travel plans. Exposure of this information can lead to monetary loss, identity theft, and loss of property. Social media exploits, such as phishing and malware-embedded games, can lead to account take over, misuse of materials, and escalated access into users' private life. Exposed personal information is also used to craft targeted spearphishing emails, which can lead a person to unwittingly download malware or give away login credentials. Compromised personal accounts can be used to message friends, family, and work colleagues, further spreading the damage. Understanding the risks associated with your social media presence is key to limiting your overall exposure.

To find where you are vulnerable, consider the following countermeasures and what you might not be doing to protect your information. Based on these vulnerabilities and the potential consequences described above, you may realize that you were unaware of the risks that come with exposure of your critical information.

Apply Countermeasures

After identifying critical information, analyzing vulnerabilities, and assessing risk, it's time to apply countermeasures. These countermeasures include practicing good security hygiene; locking down location information, privacy settings, and passwords; and familiarizing yourself with social engineering and misinformation tactics, among other things.

Update immediately and frequently review privacy settings

Adversaries prefer easy targets. Ensure computing devices, software, and applications are updated as soon as patches are available. Review your privacy settings after each update to ensure they have not reset.

Protect your location data

What you post on social media, even when that information is set for private audiences, could someday become public…

Using a mobile device can potentially expose location data. Mobile devices inherently trust cellular networks and providers, which receive real-time location data for a mobile device every time it connects to the network. Apps, even when installed using the approved app store, may collect, aggregate, and transmit information that potentially

exposes a user's location. Many apps request location permission and other resources that are not needed to function. Users with OPSEC concerns should be extremely careful about sharing location information on social media. If errors occur in the privacy settings on social media sites, critical information may be exposed to a wider audience than intended. Pictures posted on social media may be recognizable or have additional data stored in metadata, which may expose a person's location. Tracking features can potentially allow outside parties to monitor activities for malicious gain. Applications may share location details that may be vulnerable to unauthorized collection.

To mitigate this, disable location services settings on the device/application and don't voluntarily give your location away by using social media platforms to geo-tag or "check-in" at various public locations. Additionally, apps should be given as few permissions as possible, especially social media apps.

Know your "friends"

Adversaries may create duplicate or copycat profiles of current friends, family, or coworkers to get critical information. Fake or impersonated accounts can expose you to fraud. Targeted spear-phishing, where adversaries query you for privileged information, can reveal personal information. Verify every friend request you receive to make sure it is actually the person you know. Call or meet the person face-to-face to confirm they sent the invite. Don't accept invites from people you don't know.

Lock down your privacy settings

What you post on social media, even when that information is set for private audiences, could someday become public due to data breaches, poor data management practices, or data brokering. In some cases, a site's terms of service explicitly claim ownership of all posted content.

Enable strict privacy settings that block data sharing between apps. Opt out of saving login passwords within application settings. Disable all error/debug reports. Review privacy settings quarterly. Failure to set security measures can provide adversaries access to your data.

Don't post critical information

If you don't want it public, don't post it. Details normally protected from public view can be exposed if you aren't cautious. Internet archives take snapshots of profiles and store them, which may make them publicly available forever: nothing deleted from the Internet

is ever truly removed. Additionally, refrain from filling out surveys asking personal questions for social media posts. These surveys often ask for personal information such as, “Where was your first date with your spouse?” This information may be used by adversaries to compromise accounts and reset passwords if the information posted matches potential security questions.

Don’t post sensitive, privileged, or proprietary data in your status messages or timelines. When selecting who can access your posts, pages, or profiles, limit access to friends-only and avoid allowing full public access to any of your content. Malicious parties can also use pictures and private messages to blackmail you.[2] For social media, gaming, and entertainment, use separate machines from the ones you use for banking, credit card services, and medical activities.

Minimize pivoting to home and work networks

Leisure activities on social media may seem safe, but may hide malicious compromises (such as by viruses or ransomware) that allow cyber actors access to or control over home and work networks, including the data stored on those networks. Adversaries can leverage information on your social media accounts or use social media to conduct phishing operations to compromise your personal devices. Then, they can use that access as a foothold to get further into your network. Avoid connecting personal accounts to work networks and work devices.

Be aware of your physical and virtual surroundings

Accessing social media applications from open Internet hotspots provided at hotels, cafés, and airports may leave devices susceptible for adversaries to physically and virtually spy on activities. Adversaries can also access devices and information if Bluetooth® and Wi-Fi® are enabled. If you need to connect to a public wireless hotspot, use a virtual private network (VPN) to encrypt your web traffic. Don’t connect to networks if you’re not familiar with them or can’t verify their authenticity.

Secure and strengthen your passwords

Use unique and strong passwords for each online account. Reusing passwords across multiple accounts can expose data from all of the accounts if the password is discovered. Make sure that your password is of adequate length and complexity, using a combination of letters, numbers, and special characters. Where possible, implement multi-factor authentication using an authentication token or app so that someone can’t

access your account even if your password is compromised. Never share passwords and avoid using information that could be guessed based on your social media profiles or public information.

Monitor your cyber footprint

Nothing deleted from the Internet is ever truly removed.

Search for yourself online to determine what information about you is already easily available to an adversary. It is critical to know what information can be found by a free, open-source search, as it is likely the adversary's first step in reconnaissance. Disallow tagging, as friends may not be as diligent with their location settings. Be wary of information posted about you on your own profile and the profiles of close friends and family. Photos and information they post about you may reveal your critical information. This includes posting pictures while still on vacation or traveling. Don't let those you trust tell the adversaries what they want to know.

Report suspicious activities

Adversaries employ phishing techniques to get you to click on a link or download an attachment that may contain malicious software (malware). A social media site that looks legitimate can hide malicious embedded web links that can secretly redirect users to other sites. If you are unsure of something, navigate directly to the site or use a search engine instead of clicking the link. Be careful of web links embedded on a user page. Enable anti-spam and anti-phishing security features. Domain checkers can be useful to gauge the origin of the unknown link.

If you see that your account has been compromised, reach out to the site support staff immediately. They should be able to help you get access to your account again. If you see that a friend or family member may be compromised, reach out to them through other means and ask them to verify any posts you think might be fraudulent. That way, if they've been compromised, they can take the necessary steps to regain control of their accounts. A compromised account can be used to compromise other accounts, so be aware of "friends" posting in suspicious ways.

Recognize social engineering tactics

The weakest link in any cyber defense is always going to be the user, and the easiest way to get confidential information from someone is to ask for it. This is especially prevalent on social media. Be aware of surveys, shared posts, or quizzes that ask for

personal information that could lead to an answer for a security question. For example, a seemingly innocuous post may state: “Everyone remembers their first concert! Share yours in the comments below!” Since this is a common security question, an adversary can use posts like these to collect answers for future malicious attempts.

Adversaries can also use professional networking sites to try to lure users to click a malicious link, either with an article about a certain industry or a fake job posting. If anyone is asking for personal information, be cautious and think who might use that information and for what purposes.

Social engineers can use inflammatory language with clickbait to get users to go to malicious sites. Be wary of unknown blog sites that ask you for login credentials or have you download something.

Close the window into your private life

By identifying critical information, learning how it can be used against you, and applying countermeasures to deny access to that information, you make it harder for malicious actors to harm or exploit you. You also keep yourself, your friends, coworkers, and family—and everyone’s personal data—a little bit safer.▪

Works cited

[1] A. Holmes. “533 million Facebook users’ phone numbers and personal data have been leaked online.” Business Insider, 3 April 2021. [Online article.] Available: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4

[2] “Two Federal Cases Illustrate the Consequences of Sextortion.” Federal Bureau of Investigation, 30 October 2018. [Online article.] Available: https://www.fbi.gov/new/stories/sentences-in-separate-cyberstalking-cases-103018

Defense-in-Depth - Complementary Cybersecurity Guidance from nsa.gov

- Mobile Device Best Practices
- Telework Best Practices
- Identity Theft Threat and Mitigations
- Limiting Location Data Exposure
- Compromised Personal Network Indicators and Mitigations
- Transition to Multi-factor Authentication
- Best Practices for Keeping Your Home Network Secure
- NSA’s Top Ten Cybersecurity Mitigation Strategies

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed to share operations security guidance and in furtherance of NSA’s cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media Inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov