Keeping Safe on Social Media

Executive summary

Social media sites and applications are great ways to connect and share information. However, these sites can provide adversaries with the critical information they need to disrupt mission and harm you, co-workers, or even family members.

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 OPSEC process: identify critical information

Critical information is any information considered sensitive to mission or personnel. Here are some examples:

- Names and photos of you, family, and co-workers
- 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 card, and banking information
- Work or personal addresses and phone numbers
- Interests, hobbies, likes, and dislikes

Apply countermeasures

Follow good security guidelines

Adversaries prefer easy targets. Keep devices up to date when available and monitor security settings to help keep information private.

Be aware of your physical and virtual surroundings

Accessing social media applications by open internet hotspots provided at hotels, cafés, and airports may leave devices susceptible for adversaries to spy on activities both physically and virtually. Adversaries can also access devices and information if Bluetooth and Wi-Fi are enabled.

Keep your password secure

Use unique and strong passwords for each online account and update passwords every three to six months. Never share passwords.

Monitor your cyber footprint

Search for yourself online to determine what information about you is already available to an adversary. It is critical to know what information can be found by free open source search, as it is likely the adversary's first step in reconnaissance.

Don't depend on social media for privacy

Social media sites/applications that aren't public can become so due to data breach, poor data management practices, and data brokering. In some cases, the site terms of service explicitly claim ownership of all posted content.

Be alert to suspicious activities

Adversaries employ phishing techniques to get you to click on a link or download an attachment which may contain malicious software (malware). If you are unsure of something, navigate directly to the site or use a search engine instead of clicking the link.

Don't post critical information

If you don't want it public, don't post it. Internet archives take snapshots of profiles and store them, which may be publicly available. Nothing deleted on the internet is ever truly removed. In addition, refrain from filling out surveys asking personal questions for social media posts. These surveys often ask for 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.

Review your friends' and family's profiles

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 need to know.

Know your "friends"

Verify every "friend" request you receive to make sure it is actually the person you know. Adversaries may create duplicate or copycat profiles of current friends, family, or coworkers to get critical information.

Protect your location data[1]

Using a mobile device can potentially expose location data. Mobile devices inherently trust cellular networks and providers, who 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 for the function of the app. Users with location concerns should be extremely careful about sharing 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 have additional data stored in metadata, which may expose a person's location.

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.

Purpose

This document was developed by the Interagency OPSEC Support Staff (IOSS) and NSA Cybersecurity in furtherance of NSA's OPSEC and cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

[1] For more information, view the "Limiting Location Data Exposure" Cybersecurity Information Sheet (U/OO/155603-20) on NSA.gov.

Contact

OPSEC Inquires: 443-479-IOSS (4677), ioss@radium.ncsc.mil, www.ioss.gov
Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov