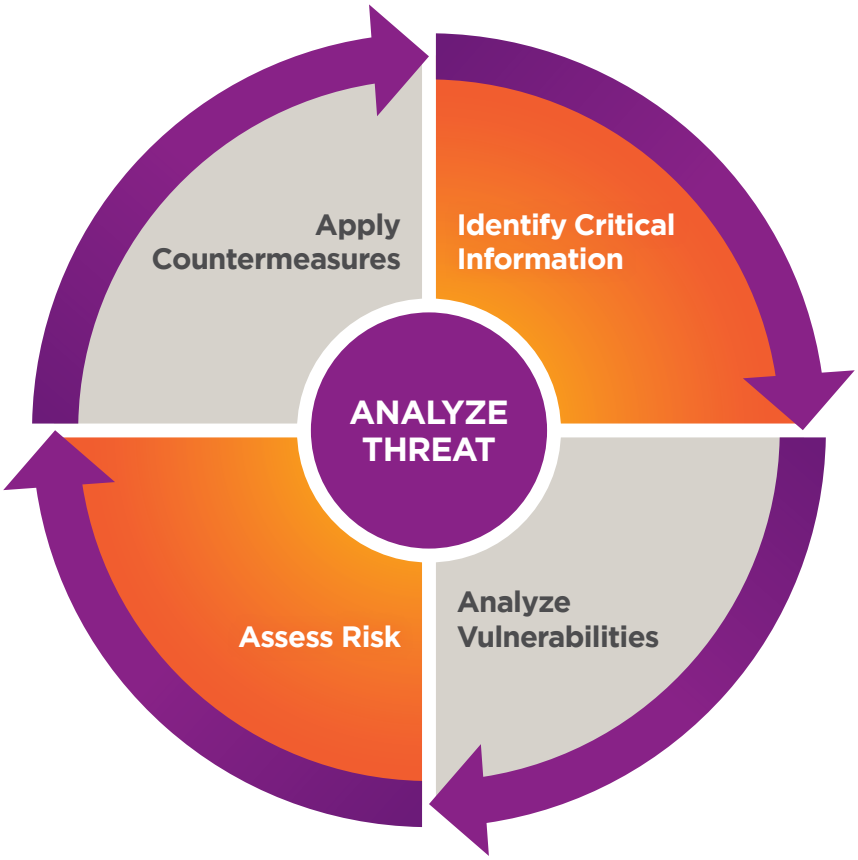
KEEPING SAFE on Social Media

SOCIAL MEDIA SITES

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 your mission and harm you, your co-workers, or even your family members.

Practicing good operations security (OPSEC) will minimize the risks that come from using social media and help you protect your critical information.

THE OPSEC PROCESS



CRITICAL INFORMATION

Your critical information is any information that you or your mission considers sensitive. Here are some examples:

- Names and photos of you, your 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 clearances
- Schedules and travel itineraries
- Social Security numbers, credit card, and banking information
- Work or personal addresses and phone numbers
- Interests, hobbies, likes, and dislikes

KEEPING SAFE on Social Media

Being aware of your critical information and using simple countermeasures will help keep you safe while on social media.

COUNTERMEASURES

- **Follow Good Security Guidelines:** Adversaries prefer easy targets. Install updates on your devices when available and monitor your security settings to help keep your information private.
- **Be Aware of Your Physical and Virtual Surroundings:** Accessing your social media applications by open internet hotspots provided at hotels, cafés, and airports may leave your device susceptible for adversaries to spy on your activities both physically and virtually. Adversaries can also access your device and your information if you leave Bluetooth and Wi-Fi enabled.
- **Keep Your Password Secure:** Use unique and strong passwords for each online account and update your passwords every three to six months. Never share your passwords.
- **Monitor Your Cyber Footprint:** Search for yourself online to determine what information about you is already available to an adversary. Know what they know about you before you post.
- **Don't Depend on Social Media for Privacy:** Social media sites/applications that aren't open and public can become so due to hacking, poor data management practices, and data brokering. In some cases, the site terms of service explicitly claim ownership of all your 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're 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 your profiles and store them for all the world to see. Nothing deleted on the internet is ever truly removed.
- **Review Your Friends' and Family's Profiles:** Photos and information they post about you may reveal your critical information. This includes posting pictures while you're still on vacation. 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 may know. Adversaries create profiles of those you may know to get close to you.

Think. Protect. OPSEC.

www.ioss.gov
(443) 479-IOSS (4677)
ioss@radium.ncsc.mil

MP217887KP