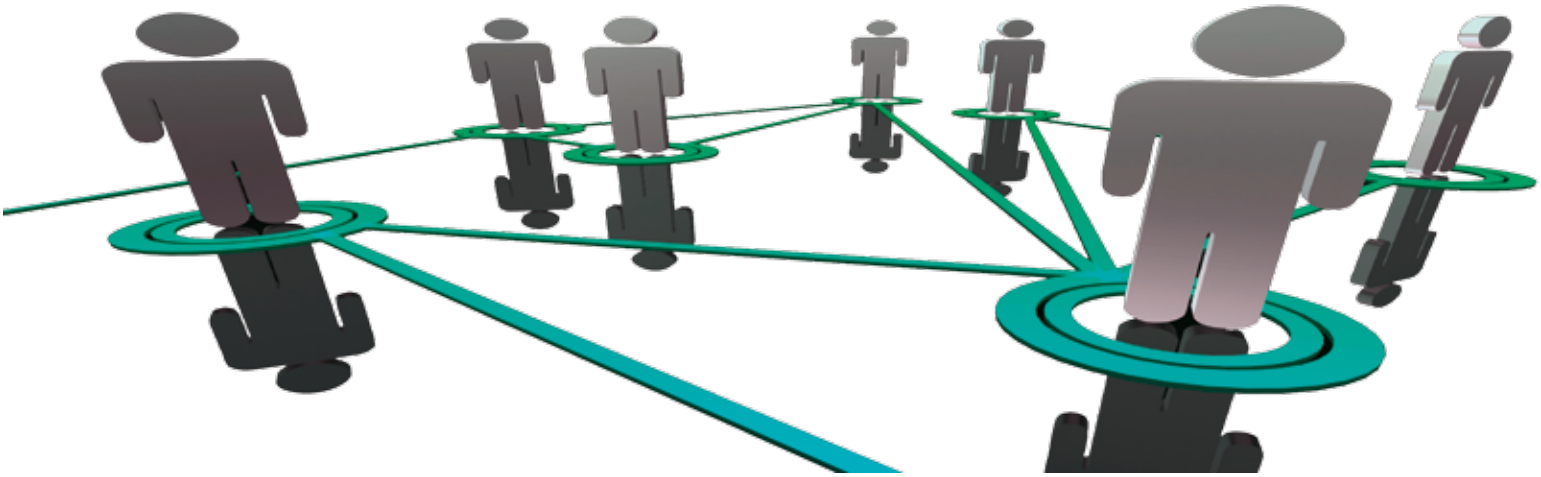
SAFE SOCIAL NETWORKING

Think. Protect. OPSEC.
www.ioss.gov

SOCIAL NETWORKING SITES

Social networking sites (SNSs), like Facebook® and Twitter®, are great ways to connect with people, share information, and market products and services. However, these sites can also provide adversaries, such as terrorists, spies and criminals, with the critical information they need to disrupt your mission and harm you, your co-workers, or even your family members.

The more information adversaries can obtain, the more opportunities they have to cause damage at your expense. Practicing good operations security (OPSEC) will minimize the risks that come from participating in SNSs, and help you to recognize and protect your critical information..



CRITICAL INFORMATION

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

- Names and photos of you, your family and co-workers;
- Usernames, passwords, computer and networking information;
- Job title, location, salary, grade, clearances;
- Operational, security, and logistical data;
- Mission capabilities or limitations;
- Schedules and travel itineraries;
- Social Security numbers, credit card, and banking information;
- Work or personal addresses and phone numbers; and,
- Interests, hobbies, likes, and dislikes.

COUNTERMEASURES

Follow computer security guidelines: Adversaries prefer to go after easy targets. Keep your computer security up-to-date and make yourself a hard target.

Never login from risky locations: Public SNSs generally do NOT have secure login available (HTTPS with the lock icon). If you login from a hotel, cyber-café, or airport hotspot, particularly ones in foreign countries, your name and password can be captured at any time.

Keep your password secure: Use different, strong passwords for each online account. Never give your password away.

Modify your search profile: Do a search for yourself and if too much data comes up, go to your settings and restrict your search profile.

Don't depend on the SNS for confidentiality: Even SNSs that aren't open and public by design can become so due to hacking, security errors, poor data management practices, and data brokering. In some cases, the site terms of service explicitly claim ownership of all your posted content.

Treat links and files carefully: Social engineers and hackers post links in comments and try to trick you into downloading an "update," "security patch," or "game."

Don't trust add-ons: Plugins, games, and applications are often written by other users, not the SNSs themselves. The authors can easily gain access to your data once you install them.

Don't post critical information: If you don't want it public, don't post it. Search engines and functions make it easy for adversaries to find what they're interested in. Once information is on the Internet, it is there forever.

Review your friends' profiles: The photos or information they post about you may be a problem.

Control "friend" access: Verify a "friend" request by phone or other means before allowing access. Group "friends" (e.g., real life, co-workers, strangers, etc.) and control access permissions based on the groups.

Did you know?

- A U.S. Government official on sensitive travel to Iraq created a security risk for himself and others by tweeting® his location and activities every few hours.
- A family on vacation kept friends up-to-date via online profiles; their home was burglarized while they were away.
- New computer viruses and trojans that successfully target information on SNSs are on the rise.
- Some foreign investors, including government and commercial entities known to be involved with organized criminal activity, own large stakes in certain SNSs.
- Information in SNS profiles has led to people losing job offers, getting fired, and even being arrested.
- SNSs have become a haven for identity thieves and con artists trying to use your information against you.
- Several kidnapping, rape and murder cases were linked to SNSs where the victims first connected with their attackers.
- Over 90,000 registered sex offenders were removed from one popular SNS… and those were the ones who used their real names.
- According to the Al Qaeda Handbook, terrorists search online for data about "Government personnel, officers, important personalities, and all matters related to them (residence, work place, times of leaving and returning, and children, places visited)."

Be Smart...
Be Safe...
Practice Good OPSEC!

Think. Protect. OPSEC.
www.ioss.gov

6411 Ivy Lane, Suite 400 Greenbelt, MD 20770
(443) 479-IOSS (4677)
ioss@radium.ncsc.mil