# OPSEC AND SOCIAL NETWORKING SITES

SOCIAL NETWORKING SITES (SNS), like Facebook® and Twitter®, are software applications that connect people and information in spontaneous, interactive ways. While SNS can be useful and fun, they can provide adversaries, such as terrorists, spies, and criminals, with critical information needed to harm you or disrupt your mission. Practicing operations security (OPSEC) will help you to recognize your critical information and protect it from an adversary. Here are a few safety tips to get you started.

## SAFETY CHECKLIST

### Personal Information

Do you:

- Keep sensitive, work-related information OFF your profile?
- Keep your plans, schedules and location data to yourself?
- Protect the names and information of coworkers, friends, and family members?
- Tell friends to be careful when posting photos and information about you and your family?

### Posted Data

Before posting did you:

- Check all photos for indicators in the background or reflective surfaces?
- Check filenames and file tags for sensitive data (your name, organization or other details)?

### Passwords

Are they:

- Unique from your other online passwords?
- Sufficiently hard to guess?
- Adequately protected (not shared or given away)?

### Settings and Privacy

Did you:

- Carefully look for and set all your privacy and security options?
- Determine both your profile AND search visibility?
- Sort “friends” into groups and networks, and set access permissions accordingly?
- Verify thorough other channels that a “friend” request was actually from your friend?
- Add untrusted people to the group with the lowest permissions and access?

### Security

Remember to:

- Keep your anti-virus software updated.
- Beware of links, downloads, and attachments just as you would in e-mails.
- Beware of “apps” or plugins, which are often written by unknown third parties who might use them to access your data and friends.
- Look for HTTPS and the lock icon that indicate active transmission security before logging in or entering sensitive data (especially when using wi-fi hotspots).

THINK BEFORE YOU POST! Remember, your information could become public at any time due to hacking, configuration errors, social engineering, or the business practice of selling or sharing user data. For more information, visit the Interagency OPSEC Support Staff’s website.

**Think. Protect. OPSEC.**

**www.ioss.gov**