

## Blogging with OPSEC



The Internet is a great place for communicating with friends and Family. It has virtually become an indispensable tool for Soldiers, Civilians, and Family members. It is also a place where deployment stories are shared through SNSs, forums, and blogs.

- The Army respects everyone's lawful right to free expression under the First Amendment to the U.S. Constitution, provided OPSEC is enforced as outlined in AR 530-1.

- According to AR 530-1, Department of the Army employees must consult with their immediate supervisor and their OPSEC officer for an OPSEC review before publishing or posting information in a public forum.

- Everyone is encouraged to review DOD Directive-Type Memorandum 09-026 on the responsible and effective use of Internet-based capabilities at <http://www.defense.gov/Portals/1/Documents/DTM%2009-026.pdf>.

- Postings of personally identifiable information are common OPSEC violations committed on SNSs.

- In addition to adhering to regulatory requirements, all users must use common sense before posting information that may have an adverse effect on the Army's mission.

## Questions? Need More Info?

Visit these websites:



United States Army Europe  
Information Technology Training  
Program

<https://aeitt.ext.eur.army.mil>



Cybersecurity Program Management  
<https://intranet.eur.army.mil/hq/iaasure/SitePages/Home.aspx>



United States Army Europe  
<http://www.eur.army.mil>

This publication is available at  
<https://aepubs.army.mil>

AE MISC PUB 25-2 • 18 JUL 16

## Cybersecurity Program Management

## SECURE USE OF SOCIAL-NETWORKING SITES



Headquarters  
United States Army Europe  
Wiesbaden, Germany

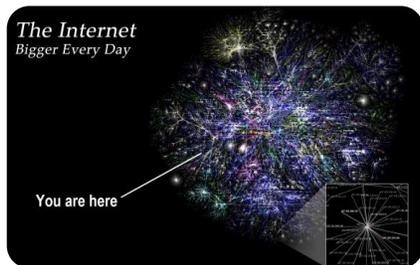
Headquarters  
United States Army Installation  
Management Command, Europe Region  
Sembach, Germany

## What is a Social-Networking Site?

- A social-networking site (SNS) is a link to the 21st century “virtual community.”
- SNSs provide a means for people to communicate with one another using the Internet.
- People interested in “hanging out” use virtual communities by creating their own online profiles with biographical data, pictures, and other information they may choose to post.
- SNS users can communicate with one another by voice, chat, instant messaging, videoconferencing, and blogging.
- As the military continues serving around the globe, SNSs have become an effective medium for Soldiers to communicate with their Families and friends.

### Fact

Because they increase the odds of personally identifiable information being disclosed to adversaries, SNSs raise some serious security concerns. SNSs provide an easy conduit for “information leakage” and place communications security, operations security (OPSEC), and personal security at an elevated risk.



**Based on operational requirements, SNSs may be blocked by Joint Task Force–Global Network Operations to ensure mission capabilities. Sites that may be blocked include, for example, Facebook, YouTube, Pandora, Twitter, and Instagram.**

### SNS Awareness

- Scams, worms, and Trojan horses often spread unchallenged throughout social-media sites, passed along from one online friend to the next.
- SNS sessions can be “hijacked” and used to impersonate you.
- Cybercriminals hide embedded links to malicious sites, masking their true destination. These links will redirect an unsuspecting user to a site he or she has no interest in visiting.
- Some sites track your online activity through cookies. Cookies are small pieces of information stored as a text file on your computer that a webserver uses when you browse certain websites, leaving traces of sites that were visited.

## Information Prohibited on SNSs

The following are examples of information that should never be published on a public site:

- Classified information
- Casualty information before the next-of-kin has been formally notified by the military Service concerned
- Information protected by the Privacy Act
- Information regarding incidents undergoing investigation
- Information considered essential elements of friendly information
- For Official Use Only information
- Information identified on current critical information lists
- Personally identifiable information
- Sensitive acquisition or contractual information

### SNS Usage Tips

- **Passwords:** Ensure passwords are at least 15 characters long and include 2 or more lowercased letters, uppercased letters, numbers, and special characters.
- **E-mail:** Delete spam messages without opening them. Never open an attachment unless you know who it is from and what it contains. Opening a spam message may allow a virus to attack or compromise your computer.

**NOTE:** Threats resulting from SNS use can be severe. Using this means of communication requires vigilance.