Blogging with OPSEC

The Internet is a great place for communicating with friends and Family. The Internet has become virtually an indispensible tool for Soldiers, civilians, and Family members. It is also a place where deployment stories are shared through social networking sites, forums, and blogs.

- The Army respects everyone's lawful right to free expression under the First Amendment, provided OPSEC is enforced as outlined in Army Regulation (AR) 530-1.
- According to AR 530-1, Department of Army employees must consult with their immediate supervisor and their OPSEC officer for an OPSEC review before publishing or posting information on a public forum.
- Everyone is encouraged to review the Army CIO/G-6 policy memorandum on Use of Social Media Tools and Army Guidelines for Social Media Use at *https://itt.eur.army.mil*, under *News*.
- Personally identifiable information postings are common OPSEC violations on social networking sites.
- In addition to the regulatory requirements, all users must use common sense before posting information that may have an adverse effect on the Army's mission.

Got Questions? Need More Info?

Visit these websites:

United States Army Europe
Information Technology Training
Program
https://itt.eur.army.mil

Information Assurance Program
Management
https://iassure.usareur.army.mil

United States Army Europe
http://www.hqusareur.army.mil

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

AE MISC PUB 25-2 ● 10 Dec 09

Information Assurance Program Management

SECURE USE OF SOCIAL NETWORKING SITES

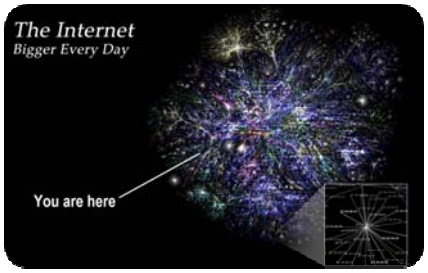
Headquarters
United States Army Europe
United States Army Installation
Management Command, Europe Region
Heidelberg, Germany

What is a Social Networking Site?

- A social networking site (SNS) is the 21st century "virtual community."
- SNSs provide a means for people to communicate with each other 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 each other by voice, chat, instant messaging, videoconference, and blogging.
- As the military continues serving around the globe, SNSs have become an effective medium to facilitate communication between Family members, friends, and Soldiers.

Fact

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



SNSs Blocked by Joint Task Force – Global Network Operations

- BlackPlanet
- FileCabi
- Hi5
- IFilm
- live365
- Metacafe
- MTV
- MySpace
- Pandora
- Photobucket
- StupidVideos
- YouTube

SNS Awareness

- Scams, worms, and Trojans 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 web-server 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, with 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 are severe. Using this means of communication requires vigilance.