Think Before You "Click"...

Social Networking Sites (SNS) provide Airmen the opportunity to tell their story to a very diverse audience.

Consider what your posts, photos and videos say about you, your values and beliefs and the image you portray of the AF.

SNS, such as Facebook and Twitter, will face more sophisticated threats as the number of users grow.

The explosion of applications on SNS are an ideal vector for cybercriminals taking advantage of friends trusting friends.

SNS have also become a haven for crime and identity theft.

Terrorists are using SNS to identify military members, inspire home grown violent extremists into action, as propoganda to gain sympathizers for recruitment and to promote hate crimes.

Terrorist organizations have used SNS to dredge for information on, and suggest, potential military targets.

"See Something - Say Something"

USAFAVA33-101, 23 January 2019 (Per AFI 33-100)
Certified Current 27 September 2022
OPR: HQ USAFA/IP
Releasability: There are no releasability or restrictions on this publication.
Supersedes: USAFAVA33-101, 05 June 2011

Questions about SNS?

Contact:

Your Unit Security Mgr, AMT or AOC
333- _ _ _ _

OPSEC
333-3933

Privacy Act
333-6231

Public Affairs
333-7627

Information Protection
333-5601

Security Forces
333-2000

For more info visit:
http://www.usafa.af.mil/shared/media/document/AFD-090406-036.pdf

USAFA INFORMATION PROTECTION DIRECTORATE
CONVERGENCE

United States Air Force Academy

Security Measures for Social Networking Sites (SNS)

Don't Be A Leaky Faucet!

Social Networking Sites (SNS) offer significant opportunities for networking and building relationships. When used responsibly, social networking can positively influence our personal and professional lives. However, SNSs are also a breeding ground for criminals and our adversaries.

This brochure is intended to build your awareness and help keep you, your family, friends, and wingmen safe while communicating via SNS. Remember, information you post can be used to harm you, your family, and/or disrupt the AF mission.

Tips to Stay Safe Online

• Protect your computer by installing and updating antivirus software programs, firewalls.

• Configure security and privacy settings to limit the amount of personal information you make available or release - review them regularly.

• Determine both your profile and search visibility.

• Verify “friends” contact through means other than the SNS.

• Sort “friends” into groups and networks, set access permissions accordingly. Place “untrusted” people in the group with the lowest permissions and access.

• Use unique, hard-to-guess passwords that include upper and lower case letters, numbers and symbols. Protect them from compromise. Avoid sharing passwords.

• Don’t assume because something comes from a “friend” that it’s safe.

SNS Checklist ☑

Personal Information:

☐ Do not post personally identifiable information which can be used to steal your identity (e.g., Date of Birth, Place of Birth, Mother’s Maiden Name, Social Security Number, home address).

☐ Protect personally identifiable information of coworkers, friends, and family members.

☐ Inform friends and family to be careful when posting personal information and photos about you.

Posted Data:

☐ Do not post your unit’s critical information (e.g., deployment, travel, security plans, weapons, recall rosters). If in doubt, contact your Unit Security Manager or Supervisor.

☐ Check all documents and the reflective surfaces and background of both photos and videos for critical information. This will help prevent exposure of critical information that could lead to a potential compromise of OPSEC.

☐ Disable GPS features, especially at sensitive or deployed locations, that automatically track, broadcast, or tag texts, photos, and videos with their location.

☐ Do not discuss, talk-around or post classified information. Do not post For Official Use Only and/or Privacy Act materials.

☐ Stay in your lane. Be credible and factual. Only discuss issues of which you have personal knowledge or expertise. Don’t be argumentative, confrontational, or make accusations. False statements are punishable under the UCMJ.

☐ Identify yourself. Do not impersonate or attempt to disguise your identity. Be aware of the image you present. Remember, your opinion, although sometimes unintentional, may be viewed by others as those of the Air Force and the nation.

☐ Replace error with fact. Admit mistakes. Be first to acknowledge and correct misinformation.

☐ Avoid offensive, abusive and foul language. Be conscious of racial and ethnically charged issues. Inappropriate language or statements are unbecoming of AF personnel.

☐ Do not use the AF name to endorse, or promote, products, opinions, or causes.

☐ Be conscious of copyright and trademark materials. Don’t post copyright or trademark material without the expressed written consent of the owner.

Safety and Security:

☐ Be general. Do not make activities, vacations and related dates readily available to the public. Consider posting upon your return home.

☐ Be cautious of links, downloads, attachments just as you would emails; they may be harmful or contain malicious content.

☐ Beware of ‘apps’ or plug-ins, which are often written by unknown third parties who might use them to access your data and friends.

☐ Look for the “HTTPS” and the “lock” icon that indicate active transmission security before logging in or entering sensitive data (especially when using Wi-Fi hotspots).

Remember, the enemy is engaged in this battlespace. Are you?