OPSEC and Safe Social Networking

Agenda

- Introduction
- Did you know?
- Social media access
- What not to post
- Privacy settings
- Geotagging
- Social Media OPSEC for units
- Social media concerns for Families and Family Readiness Groups
- Social media concerns for Army children
- Countermeasures
- Resources

Safe social networking

- Social media has become a big part of our lives. Social media can help people and Army organizations share information. It also helps Soldiers, family members and Army civilians to stay connected to loved ones.
- As a culture, we depend on social media, but social media use can be extremely dangerous if you're not careful.
- Do you know what information you can post about your job? Did you know people can use social media to collect information and steal your identity? Did you know you can be at risk even if you don't use social media.
- Operations security (OPSEC) and personal privacy concerns should be paramount when using social media.

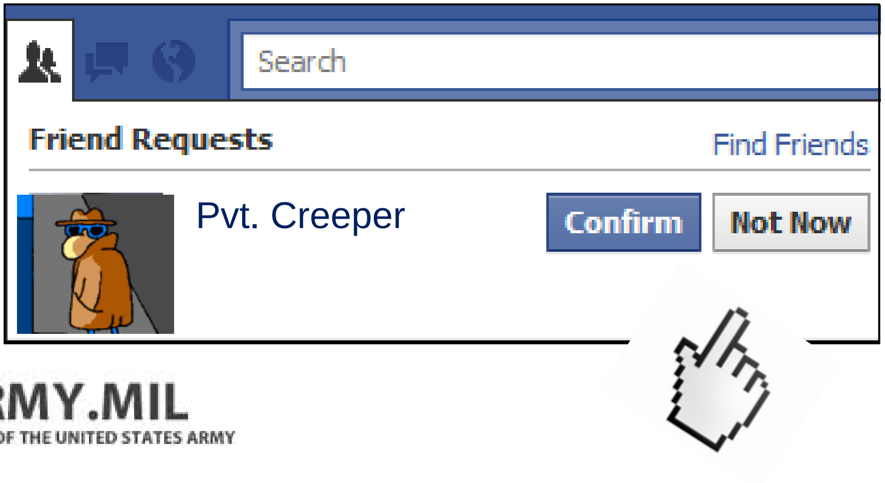
Did you know?

- 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 social networking sites are on the rise.
- Information on social networking sites has led to people losing job offers, getting fired and even being arrested.
- Social networking sites 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 social networking sites where the victims first connected with their attackers.
- According to the Al Qaeda Handbook, terrorists search online for data about “Government personnel and all matters related to them (residence, work place, times of leaving and returning, children and places visited.)”

Source: Interagency OPSEC Support Staff

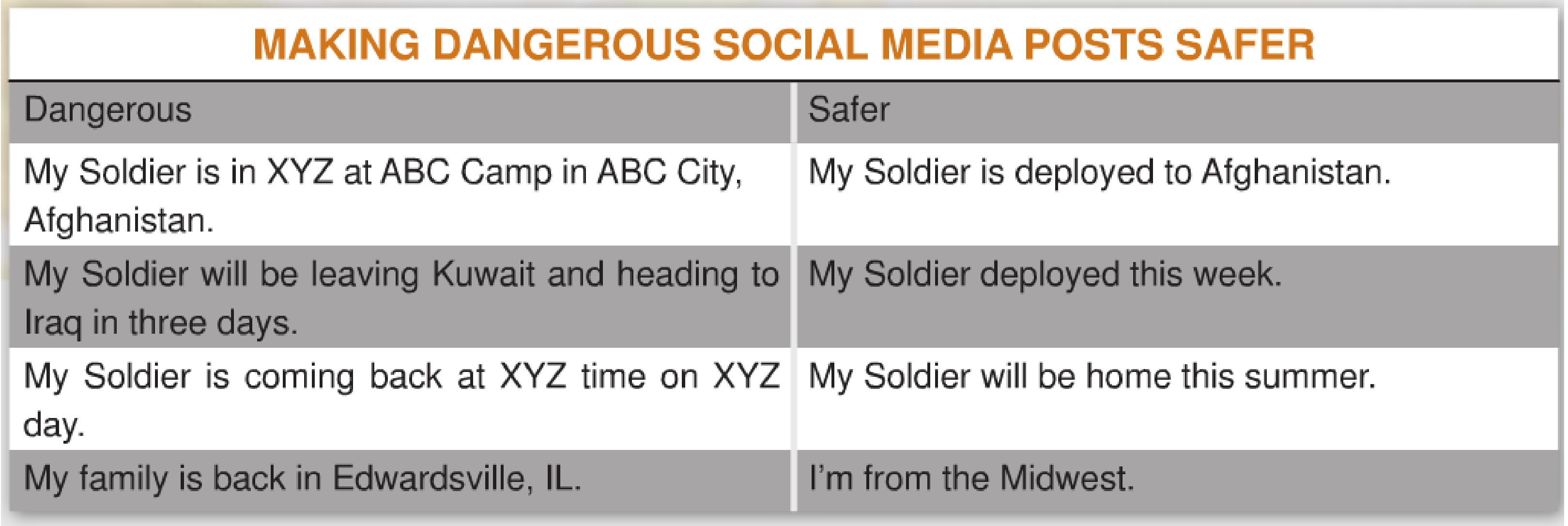
Daily social media interactions

- Be cautious when accepting friend requests and interacting with people online. You should never accept a friend request from someone you do not know, even if they know a friend of yours. For more on this, check out this article about the Robin Sage Experiment: “Fictitious femme fatale fooled cybersecurity” http://goo.gl/Ocf7e
- Don’t share information that you don’t want to become public. Be careful about what you post about yourself on social media platforms. Once you put something out there, you can’t control where it goes. Someone might target you based simply because you work in the DoD. Be cautious when listing your job, military organization, education and contact information.
- Providing too much information in your profile can leave you exposed to people who want to steal your identity or steal sensitive operational information.



What not to post

- When using Facebook and other social media platforms, do not post personally identifiable information and any information that can damage Army operations.
- Think about what you're posting before hitting share. Many times, you can avoid releasing sensitive information by simply rephrasing your social media post.
- If you aren't comfortable placing the same information on a sign in your front yard, don't put it online.



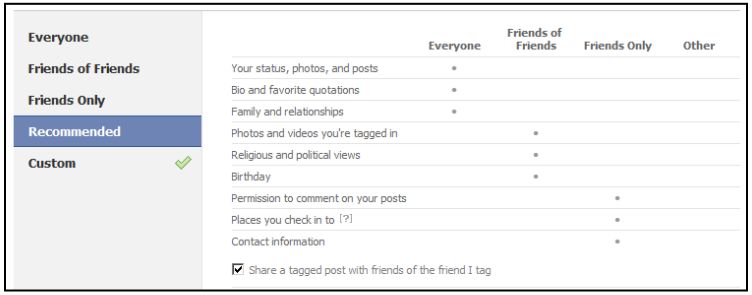
MAKING DANGEROUS SOCIAL MEDIA POSTS SAFER

Dangerous	Safer
My Soldier is in XYZ at ABC Camp in ABC City, Afghanistan.	My Soldier is deployed to Afghanistan.
My Soldier will be leaving Kuwait and heading to Iraq in three days.	My Soldier deployed this week.
My Soldier is coming back at XYZ time on XYZ day.	My Soldier will be home this summer.
My family is back in Edwardsville, IL.	I'm from the Midwest.

Privacy settings

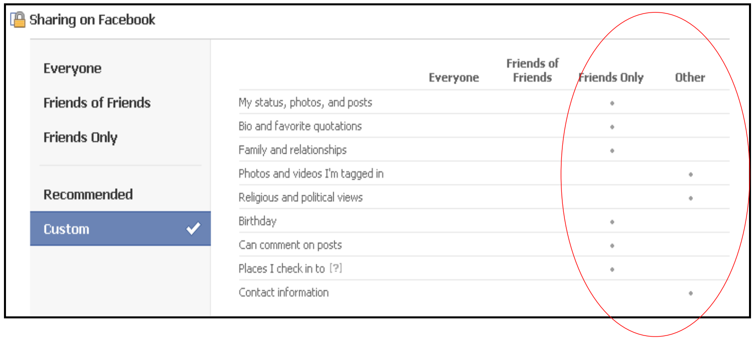
- Understanding what you can and cannot post on social media platforms goes a long way in protecting yourself online, but more can be done by adjusting your privacy settings on social media sites.
- Facebook's default privacy settings are often public, but Facebook provides various setting options that help Facebook users adjust privacy settings.
- Twitter allows users to keep their Tweets private and Flickr gives users the option of keeping photos private. The settings are easily accessible, the trick is setting them to meet your privacy needs. Similar privacy settings can be found on other social media sites like Myspace and LinkedIn.

Facebook



	Everyone	Friends of Friends	Friends Only	Other
Your status, photos, and posts	•			
Bio and favorite quotations	•			
Family and relationships	•			
Photos and videos you're tagged in		•		
Religious and political views		•		
Birthday		•		
Permission to comment on your posts			•	
Places you check in to [?]			•	
Contact information			•	

☑ Share a tagged post with friends of the friend I tag

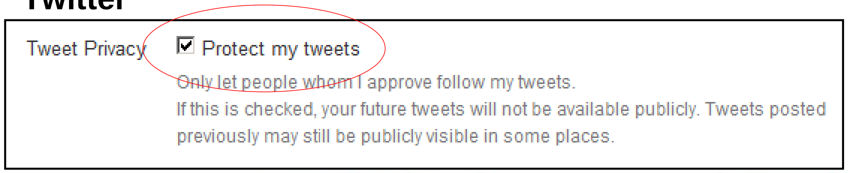


Sharing on Facebook

	Everyone	Friends of Friends	Friends Only	Other
My status, photos, and posts			•	
Bio and favorite quotations			•	
Family and relationships			•	
Photos and videos I'm tagged in				•
Religious and political views				•
Birthday			•	
Can comment on posts			•	
Places I check in to [?]			•	
Contact information				•

On the top are Facebook's sharing recommendations, on the bottom are the Army's sharing recommendations. For more information about protecting yourself on Facebook, check out this Social Media Roundup: http://goo.gl/2WAlu

Twitter

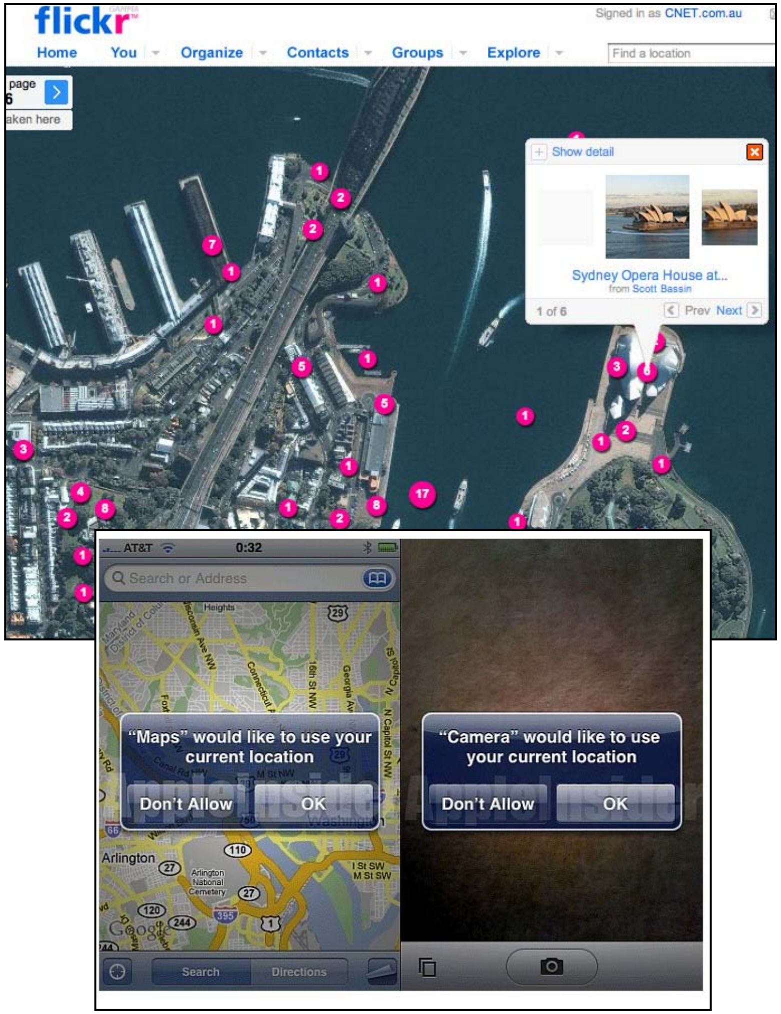


Tweet Privacy ☑ Protect my tweets

Only let people whom I approve follow my tweets.
If this is checked, your future tweets will not be available publicly. Tweets posted previously may still be publicly visible in some places.

Geotagging safety

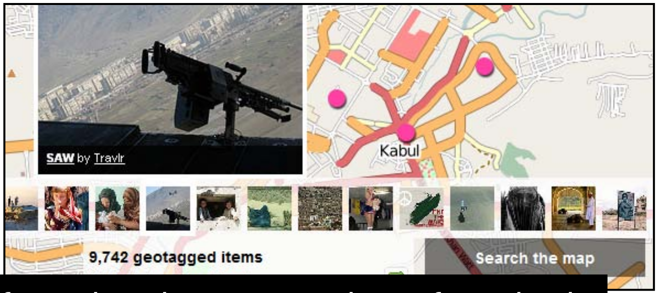
- Geotagging is the process of adding geographical identification to photographs, video, websites and SMS messages. It is the equivalent of adding a 10-digit grid coordinate to everything you post on the internet.
- Geotags are automatically embedded in some pictures taken with smartphones. Many people are unaware of the fact that the photos they take with their smartphones and load to the Internet have been geotagged.
- Photos posted to photo sharing sites like Flickr and Picasa can also be tagged with location, but it is not an automatic function.
- For more information about geotagging, check out this website: http://goo.gl/DmJoq


“Maps” would like to use your current location

“Camera” would like to use your current location

Geotagging safety

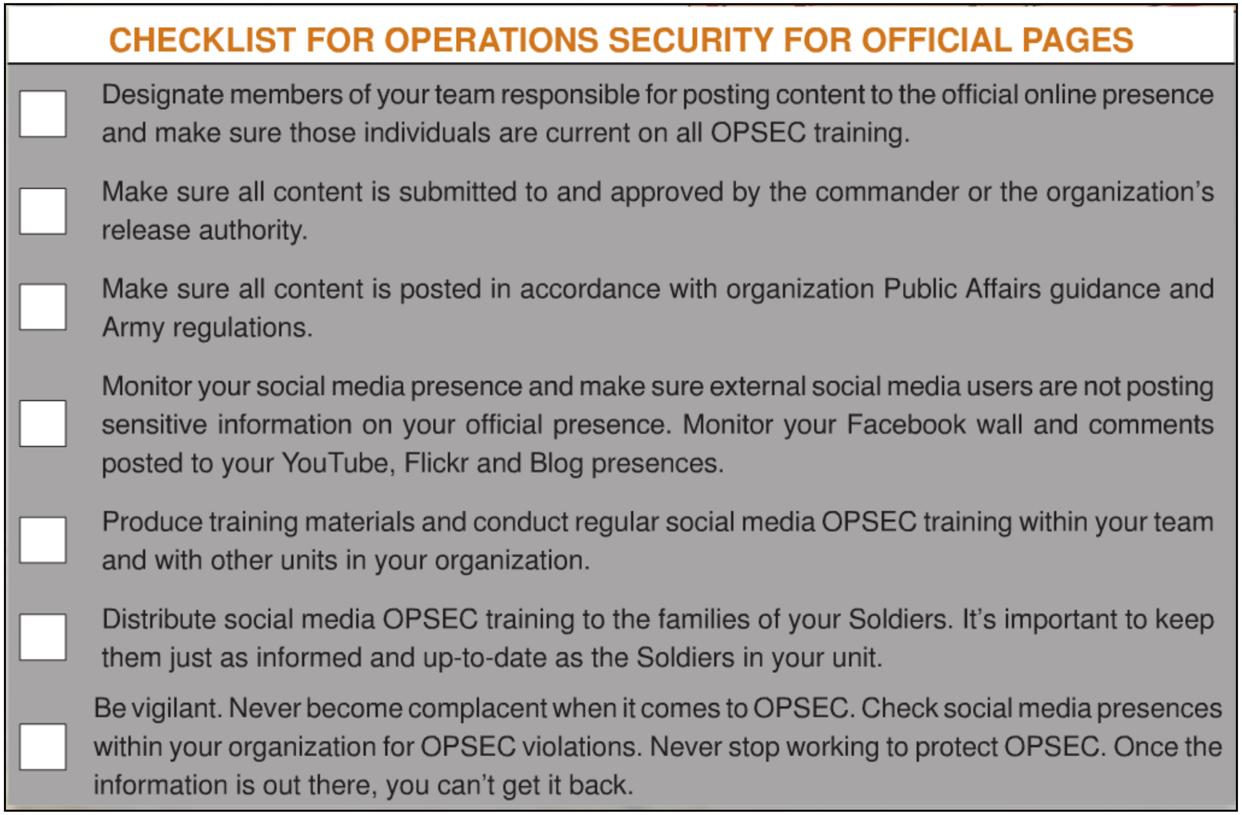
- Location-based social networking is quickly growing in popularity. A variety of applications are capitalizing on users' desire to broadcast their geographic location.
- The increased popularity of these applications is changing the way we as a digital culture view security and privacy on an individual level. These changes in perception are also creating OPSEC concerns on an Army level.
- Deployed Soldiers, or Soldiers conducting operations in classified areas should not use location-based social networking services. These services will bring the enemy right to the Army's doorstep.
- Want to avoid giving away location? Disable the GPS function on your smartphone. For instructions on how to do that, check out this website: http://goo.gl/IAmsY



For more information about geotagging safety, check out this Social Media Roundup: http://goo.gl/dyIjB

Social media OPSEC for units

- Protecting OPSEC goes beyond personal use of social media. Hundreds of Army organizations use social media to put out information, so it's important social media managers keep the checklist below in mind during organizational social media use.



CHECKLIST FOR OPERATIONS SECURITY FOR OFFICIAL PAGES

□ Designate members of your team responsible for posting content to the official online presence and make sure those individuals are current on all OPSEC training.

□ Make sure all content is submitted to and approved by the commander or the organization's release authority.

□ Make sure all content is posted in accordance with organization Public Affairs guidance and Army regulations.

□ Monitor your social media presence and make sure external social media users are not posting sensitive information on your official presence. Monitor your Facebook wall and comments posted to your YouTube, Flickr and Blog presences.

□ Produce training materials and conduct regular social media OPSEC training within your team and with other units in your organization.

□ Distribute social media OPSEC training to the families of your Soldiers. It's important to keep them just as informed and up-to-date as the Soldiers in your unit.

□ Be vigilant. Never become complacent when it comes to OPSEC. Check social media presences within your organization for OPSEC violations. Never stop working to protect OPSEC. Once the information is out there, you can't get it back.

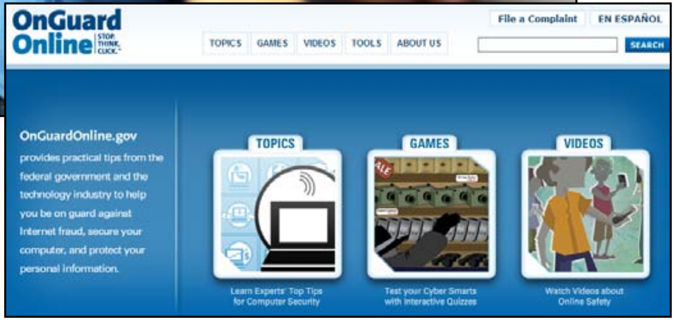
Social media OPSEC concerns for families and Family Readiness Groups

- Social media helps Family Readiness Groups and Army family members stay connected, but OPSEC should always be the primary concern.
- Family Readiness Groups, Army spouses and Army Family members need to know that posting sensitive information can be detrimental to Soldier safety.
- Ensure that information posted online has no significant value to the enemy. Always assume that the enemy is reading every post made to a social media platform.
- Even seemingly innocent posts about a family member's deployment or redeployment date can put them at risk.

Security items to consider

- Take a close look at all privacy settings. Set security options to allow visibility to "friends only."
- Do not reveal sensitive information about yourself such as schedules and event locations.
- Ask, "What could the wrong person do with this information?" and "Could it compromise the safety of myself, my family or my unit?"
- Geotagging is a feature that reveals your location to other people within your network. Consider turning off the GPS function of your smartphone.
- Closely review photos before they go online. Make sure they do not give away sensitive information which could be dangerous if released.
- Make sure to talk to family about operations security and what can and cannot be posted.
- Videos can go viral quickly, make sure they don't give away sensitive information.

Social media concerns for Army children



OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

Learn Experts' Top Tips for Computer Security

Test your Cyber Smarts with Interactive Quizzes

Watch Videos about Online Safety

- What is the best way to protect your kids online? Talk to them. Research suggests that when children want important information, most rely on their parents.
- The important thing is to start the education early. Talk to your children about online risks and make sure you create an honest and open environment.
- Some social media sites like Facebook, provide family safety resources and tools for reporting issues: http://goo.gl/sLBym
- Make sure you check out www.Onguardonline.com to find more resources that will help protect your family and yourself online.

Countermeasures

- These tips will help you protect critical information while using social media

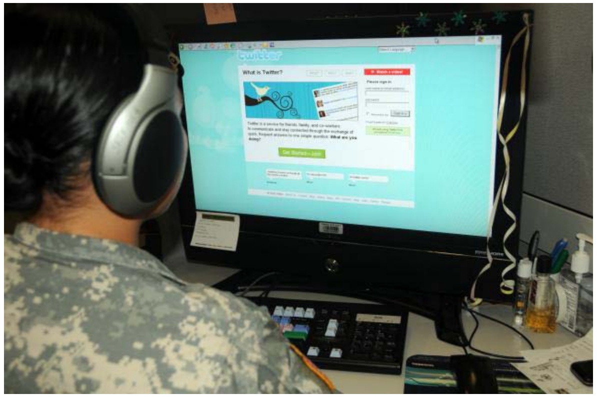
- **Follow computer security guidelines:** Adversaries prefer to go after easy targets. Keep your computer security up-to-date and make yourself a hard target.
- **Never login from risky locations:** Public social networking sites generally do not have secure login available. If you login from a hotel, cyber-café or an airport hotspot, particularly ones in foreign countries, your name and password can be captured at any time.
- **Modify your search profile:** Do a search for yourself and if too much data comes up, you should consider adjusting your settings.
- **Keep your password secure:** Use different, strong passwords for each online account. Never give your password away.
- **Don’t depend on the social media site for confidentiality:** Even social media sites that aren’t open and public by design can become so due to hacking, security errors and poor data management practices. In some cases, the site terms of service explicity 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.”

Countermeasures (cont.)

- These tips will help you protect critical information while using social media

- **Don’t trust add-ons:** Plugins, games and applications are often written by other users, not the social media sites 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 make it easy for adversaries to find what they’re interested in. Once information is online, it’s 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.



OPSEC resources

- OPSEC resources
  - Interagency OPSEC Support Staff: www.ioss.gov
  - Anti-Phishing Phil: http://goo.gl/ZFkY3
  - OnGuard Online: www.onguardonline.com
- Social media training: http://goo.gl/AqmE1
- Social Media Roundups
  - 9 Critical Steps to Protecting Yourself on Facebook: http://goo.gl/igGzN
  - Geotags and Location-based Social Networking: http://goo.gl/wqKwZ
  - Social Media For Family Readiness Groups: http://goo.gl/rS88l
- Army Slideshare site: http://goo.gl/cJM9T

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

Learn Experts' Top Tips for Computer Security

Test your Cyber Smarts with Interactive Quizzes

Watch Videos about Online Safety