UNITED STATES CYBER COMMAND

SOCIAL NETWORKING BEST PRACTICES & AWARENESS

QUICK REFERENCE GUIDE

[2015/03]

Social Networking

Social Networking has become a way of life for many employees and organizations. Networking and collaboration tools are an important part of expression, idea and opinion sharing, and help each of us stay connected. **Social Networks** provide users innovative methods for interacting with organizations and friends through third-party applications via a variety of devices with access to the Internet, and allow users to check and update their accounts from virtually any location with a Wi-Fi or cellular signal. Organizations often use social networking tools to enable employee collaboration, information sharing and recruitment.

Connecting People

Social Networking is a means for Service Members and civilian employees to connect across geographical and organizational boundaries in order to maintain contact with friends, colleagues and family members.

Organizational Use

Government social networking sites provide a means to share information, announcements and situational awareness. These sites should be managed by an individual/custodian designated by organizational leadership. The custodian should monitor the site for manipulation, spoofing, distortions, etc. intended to mislead site followers and the public.

Threats and Pitfalls

As a culture, we depend on social media, but social media use comes with risks. Know the restrictions on information that can be posted as it pertains to a member's job. Be aware that adversaries can use social media to collect information and use to steal individual's identity. Know that you are at risk even if you don't use social media; there are proactive measure we should all take to safeguard our personal information.

Adversaries can access information posted to social networking sites and may use this information to initiate social engineering attacks.

Visit the Resource sites listed in the footer for more information and guidance on these topics.

Resources:

US CYBER COMMAND, Cybersecurity (IA) Branch (J65): https://www.cybercom.mil/Pages/Cybersecurity.aspz

Additional Government Resources:

DoD Social Media Site & Guide:www.defense.gov/socialmedia; and www.defense.gov/documents/WEB_Guide_to_Keeping_Your_Social_Media_Accounts_Secure_2015.pdf

Defense Privacy and Civil Liberties Division Site: dpcld.defense.gov

DOJ Identity Theft Threat and Mitigations Site: www.justice.gov/criminal/fraud/websites/idtheft.html

FBI Summary of Social Media and Networking Threats:www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks/

UNITED STATES CYBER COMMAND

SOCIAL NETWORKING BEST PRACTICES & AWARENESS

QUICK REFERENCE GUIDE

[2015/03]

OPSEC

OPSEC should be maintained at all times. Information concerning orders, capabilities, internal initiatives, budgeting, etc. should never be posted on social networking sites.

OPSEC for Organizations

Protecting OPSEC goes beyond personal use of social media. 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.

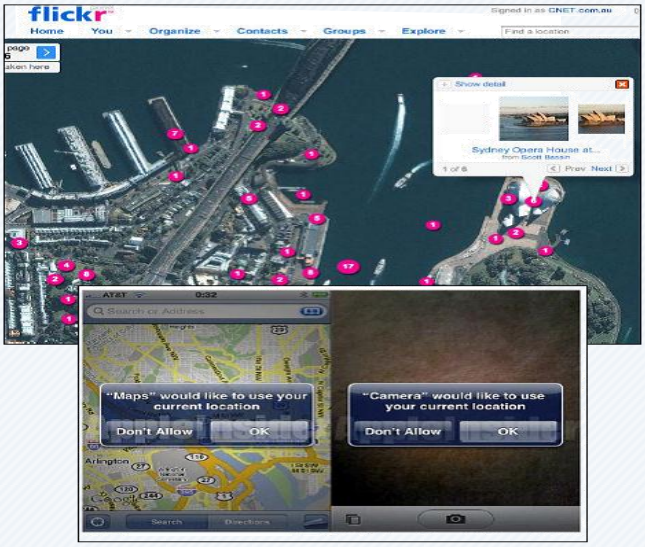
CHECKLIST FOR OPERATIONS SECURITY FOR OFFICIAL PAGES

- ☐ 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.

OPSEC Concerns for Families and Family Readiness Groups (FRGs)

Social media helps FRGs and family members stay connected, and OPSEC should always be the primary concern. Posting sensitive information can be detrimental. **Following are some OPSEC Tips:**

- Ensure that information posted online has no significant value to the enemy.
- Always assume the enemy is reading every post made to a social media platform--seemingly innocent posts about a family member's deployment, to include the date, can put that member and others at risk.
- Do not reveal sensitive information about yourself such as schedule and event location.
- Closely review photos before posting the file. Make sure they do not give away sensitive info (visual and data – time/location stamp).
- Geotagging is a feature that reveals your location at time of post. Consider disabling all positioning features on your mobile device.



Visit the Resource sites listed in the footer for more information and guidance on OPSEC and social media.

Resources:

US CYBER COMMAND, Cybersecurity (IA) Branch (J65): https://www.cybercom.mil/Pages/Cybersecurity.aspz

Additional Government Resources:

DoD Social Media Site & Guide:www.defense.gov/socialmedia; and www.defense.gov/documents/WEB_Guide_to_Keeping_Your_Social_Media_Accounts_Secure_2015.pdf

Defense Privacy and Civil Liberties Division Site: dpcld.defense.gov

DOJ Identity Theft Threat and Mitigations Site: www.justice.gov/criminal/fraud/websites/idtheft.html

FBI Summary of Social Media and Networking Threats:www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks/

UNITED STATES CYBER COMMAND

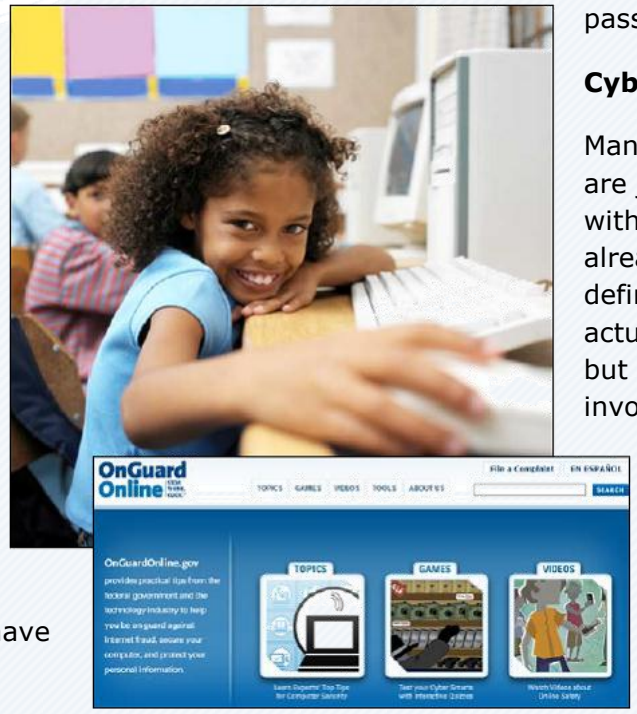
SOCIAL NETWORKING BEST PRACTICES & AWARENESS

QUICK REFERENCE GUIDE

[2015/03]

Social Networking Concerns for Children

Generally kids feel pretty safe social networking with someone online. They may think that telling people information is no big deal. Some kids trust the people they have met online, and may feel fine telling them something personal because it seems so different from interactions in person with strangers where right from wrong is understood.



Sexual Predators

Parents need to explain that there are people online, called online sexual predators, who are very dangerous. They may seem friendly, and will befriend to gain personal information. Parents need to explain to children that it is not okay to give out personal information about themselves to people they have met online. Giving full names, addresses, school names, phone numbers, birthdays, and other types of personal information is very dangerous. Sexual predators can use any combination of personal information to find the child and harm them.

Identity Theft

If kids are social networking they may give out personal information such as their Social Security number or their bank account information.

Parents need to explain to children that they should never give out personal information, especially not their Social Security number, bank account number, credit card numbers, or passwords.

Cyber Bullying

Many times kids and teens are just keeping in touch with friends that they already know. This is definitely safer since they actually know the person, but there are other dangers involved with kids networking with friends online.

Cyber bullying can go on via social networking. This can be very harmful to a child and can be hard for adults and parents to monitor. Parents need to talk to their children about what they do online and discuss with them cyber bullying.

Make sure you check out www.Onguardonline.com to find more resources that will help protect your family and yourself online.

Resources:

US CYBER COMMAND, Cybersecurity (IA) Branch (J65): https://www.cybercom.mil/Pages/Cybersecurity.aspz

Additional Government Resources:

DoD Social Media Site & Guide:www.defense.gov/socialmedia; and www.defense.gov/documents/WEB_Guide_to_Keeping_Your_Social_Media_Accounts_Secure_2015.pdf

Defense Privacy and Civil Liberties Division Site: dpcld.defense.gov

DOJ Identity Theft Threat and Mitigations Site: www.justice.gov/criminal/fraud/websites/idtheft.html

FBI Summary of Social Media and Networking Threats:www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks/