Cyber Crime Prevention Flyer

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]
E-mail:
usarmy.cciuintel@mail.mil

CCIU Web Page:
www.cid.army.mil/cciu.html

CPF 0037-14-CID361-9H 5 December 2014

Social Networking Safety Tips

Overview:

Social networking sites allow people to interact with others and find people with similar interests or backgrounds. Social networking sites enjoy worldwide popularity, underscoring the need to understand poten tial risks associated with the use of these sites. A person's online activities may inadvertently expose excessive information about their identity, location, relationships, and affiliations, creating an increased risk of identity theft, stalking, or targeted violence.
A safer social networking experience is available by accepting some basic assumptions and following a few recommendations.

Assumptions:

- Once something is posted on a social networking site, it can quickly spread. No amount of effort will erase it – the Internet does not forget.
- You are not anonymous on the Internet.
- There are people on the Internet who are not who they purport to be and will take advantage of you if afforded the opportunity.
- Participating in more social networking sites increases your attack surface and overall risk.
- Everyone on the Internet can see what you post, from where you post it, who your friends and associates are, the comments your friends make and your "witty" replies.
- An embarrassing comment or image will come back to haunt you… one day…when you least expect it…at the least opportune time.
- There is a complete record of your online activity...somewhere.

Recommendations:

- Do not post anything you would be embarrassed to see on the evening news.
- Do not accept friend/follower requests from anyone you do not know; independently verify identities.
- Avoid using third-party applications; if needed, do not allow them to access your social networking accounts, friends list or address books.
- Do not post personally identifiable information.
- Be cautious about the images you post. What is in them may be more revealing than who is in them. Images posted over time may form a complete mosaic of you and your family.
- Do not allow others to tag you in images they post. Doing so makes you easier to locate and accurately construct your network of friends, relatives and associates.
- **Securely configure your social networking accounts to minimize who can see your information**.

CONFIGURATION GUIDES

- Facebook
- Twitter

CLICK FOR DETAILED RECOMMENDATIONS
ADDITIONAL GUIDES FORTHCOMING

Cyber Crime Prevention Flyer

Recommendations (continued):

- Do not use “check-ins. If check-ins are enabled, disable them. Do not post your specific location.
- Be cautious when accessing online accounts from public Wi-Fi connections. Someone might have installed software capable of capturing your login credentials and other sensitive information.
- Do not use the **save password**, **remember me** or **keep me logged in** options from public or shared computers.
- Limit social networking to personal use.
- Do not use the same password for all of your accounts. Make sure the passwords for your financial sites are not permutations of your other passwords.
- Do not use your social networking site to login to other sites. Create another user account on the new site instead
- Use strong, unique passwords. Consider passphrases for an additional level of safety.
- Keep anti-virus software current.
- Do not arrange meetings with people you meet online.

For more information about computer security and other computer related scams, we encourage readers to visit the CCIU website to review previous cyber crime alert notices and cyber crime prevention flyers.

Additional Resources

- Safer Computing and Social Networking, USA.gov
- 11 Tips for Social Networking Safety, Microsoft
- Social Networking Safety, National Crime Prevention Council
- Staying Safe on Social Network Sites, United States Computer Emergency Readiness Team
- Kids and Socializing Online, OnGuardOnline.gov
- Facebook Help Center
- Twitter Help Center

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide us with feedback.