United States Army
Criminal Investigation Command

Media contact:
571-305-4041

FOR IMMEDIATE RELEASE

CID Lookout
On Point for the Army

Protecting your social media accounts

QUANTICO, Va., March 2, 2015 – In January 2015, the Twitter and YouTube accounts of U.S. Central Command (CENTCOM) were hacked and defaced. In February 2015 a Twitter account dedicated to military spouses was hacked and defaced, and Newsweek's Twitter account was also commandeered. In each case, alleged violent extremist groups spewed threats and anti-U.S. rhetoric.

Spreading propaganda is hardly a new tactic. However, hijacking personal, corporate and government social media is a more recent phenomenon and demonstrates a level of technological adaptability and competence. There are steps the greater Army community can take to protect themselves and their online presence.

"Social networking sites empower people to connect and organize with others based on common interests, background and associations," said Daniel Andrews, director of the Computer Crime Investigative Unit. "Indeed, these technologies have impacted modern society and are interwoven in daily activities. Unsurprisingly, criminal elements and adversaries also harness the power of social networking sites to conduct surveillance and otherwise further their causes. Our goal is to help users understand online risks and make informed decisions to mitigate those risks, ultimately leading to safer online activities."

As a result of recent world events and a continual effort to protect the force, special agents with the U.S. Army Criminal Investigation Command's Computer Crime Investigative Unit (CCIU) strongly recommend that anyone affiliated with the U.S. military, review their social media accounts to make sure they are using the best security settings to protect their online profiles.

With that in mind, CID provides the following information to help the greater Army community protect themselves online and significantly reduce the chance of becoming a victim of cybercrime.

-more-

Recommendations:

- Do not accept friend/follower requests from anyone you do not know; independently verify identities.
- Securely configure your social networking accounts to minimize who can see your information.
- 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 same password for all of your accounts.
- Use strong, unique passwords. Consider passphrases for an additional level of safety.

Tips to Avoid being Socially Engineered via Phishing Emails:

- Be suspicious of unsolicited email messages from individuals and companies. If an individual claims to be from a legitimate organization, try to verify their identity with that organization.
- Do not use contact information provided in the email or on a website connected to the request.
- Do not respond to email solicitations.
- Do not follow links sent in email solicitations.
- Do not provide personal, financial, or account (username and password) information to email solicitations.
- Pay attention to the URL of a website in email solicitations. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain.
- Employ the use of a spam filter.
- Treat all e-mail attachments with caution. Turn off the option to automatically download attachments.

Links to CCIU Criminal Alert Notices and Cyber Crime Prevention Flyers:

- Social Networking Safety Tips
- Configuring Facebook for a More Secure Social Networking Experience
- Configuring Twitter for a More Secure Social Networking Experience
- Home Computer Security
- OPSEC on the Cyber Home Front