



Issue: January 19, 2012

Army stresses caution, education to combat social media scammers

(Source: Social Media Division, U.S. Army Office of the Chief of Public Affairs)

You just signed up for a Facebook profile and a four-star general already wants to be your friend.

Good thing right? Not likely.

Fake profiles, impostors and online scams litter the social media landscape, and as social media evolves, so do the tactics of online crooks.

As social media use becomes more prevalent in today's Army, many Army leaders and Soldiers recognize that effective social media education is the best way to keep Soldiers from falling into the traps set by social media scam artists.

"It's still the wild west out there," said Staff Sgt. Dale Sweetnam, the noncommissioned officer in charge of the Online and Social Media Division, or OSMD, in the Office of the Chief of Public Affairs.

"You have to stay vigilant, protect your information and always be on the lookout for social media scams."

The Army authorizes the use of social media in both official and personal capacities, but Sweetnam said the threats are always present so education is key. Social media scam artists work tirelessly to steal personal information, impersonate Soldiers and try to acquire sensitive information.

"We are all familiar with the Nigerian money scam emails that used to plague our email accounts a few years ago, right? Well now that our online use has evolved, so have scammers," said Maj. Juanita Chang, the Army's director of OSMD.

"If you are a scammer who wants to build someone's trust and then con them into sending you money, doesn't it make sense to steal the identity of someone America trusts – and nobody is held in higher esteem than our military members, so they make a lucrative case to impersonate. People inherently trust the military and wouldn't imagine being conned by a Soldier or a general with a chest full of medals," said Chang.

In 2009, the Robin Sage Experiment effectively demonstrated how people respond to social media scams. In December of 2009, Provide Security, a cyber security company, created fake Facebook, Twitter and LinkedIn profiles for a person they named "Robin Sage." Sage claimed to be "Cyber Threat Analyst."

Over the next few months, the fake persona collected hundreds of friends and over time, slowly extracted sensitive information from those in the intelligence and cyber communities. Not only does the Robin Sage Experiment demonstrate how easy it is for someone to penetrate social media circles, it shows that even some of the most security-minded individuals are still susceptible to attacks.

Not every social media scam is as complex and thought out as the Robin Sage experiment. In many cases, people will simply go online, become “friends” with a Soldier in uniform, steal the photo and use it as their own profile photo. Some individuals have actually taken the identity of a deceased Soldier and used as to solicit money from unsuspecting victims.

One such incident was reported by the New York Post in 2011. It happens to deceased Soldiers, active Soldiers and even Army leaders.

“I spend a few hours a week searching social media platforms for people posing as Army leaders,” Sweetnam said. “We work hard to protect the digital integrity of our Army leaders. It’s disappointing to find that there are so many scam artists out there, but for now, that’s just the way it is.”

Sweetnam said that fake Pages also exist for Army organizations, so he suggested that those interested in finding official Army social media presences should check out the Army’s Social Media Directory.

Sweetnam said that regardless of how involved you are with social media, it’s important to always be on the lookout for scams. He said that you should never “friend” someone you don’t actually know in person on Facebook. You should also do periodic Google searches for your name to make sure nobody is using your name and likeness for personal gain. And, of course, always keep Operations Security in mind.

“OPSEC should always be the paramount concern,” said Sweetnam. “Throughout our Army career, we are trained on the importance of OPSEC. Maintaining information security should apply not only during deployments, but each time you sign on to Facebook or Tweet.” To stay safe, the Online and Social Media Division suggests that social media users take several precautions when using social media.

- It’s important to not share information that users don’t want to become public.
- 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.
- Take a close look at all privacy settings. Set security options to allow visibility to “friends only.”
- Users should be careful about what they post about their lives on social media platforms. Once something is out there, users can’t control where it goes.
- Be cautious when listing job, military organization, education and contact information.
- 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.

- 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.
- Create different, strong passwords for each online account. Never give password information away.

“Social media is an exciting space,” Sweetnam said. “There is a lot the Army can achieve using social media and there are endless benefits for Soldiers and their families. But we have to be safe and we have to be on the lookout for those who wish to ruin a good thing.”