



Army: Soldiers Must Consider OPSEC When Using Social Media

By Lisa Ferdinando

Army News Service

It's as easy as a click of a mouse or a tap on a smartphone. And in a few seconds, sensitive Army information might be shared that could get Soldiers killed.

With social media's ease, in any part of the globe, at any time, a Soldier, Army civilian or family member can post pictures from a deployment or talk about an Army mission. But these seemingly innocent posts could actually contain sensitive information that endangers Soldiers by revealing locations, security measures, mission operations or troop movements, said the Army's social media experts.

Soldiers, Army civilians and family members need to be mindful of what they put online, with operations security at the forefront of their considerations, said Staff Sgt. Dale Sweetnam, with the Online and Social Media Division of the Army's Office of the Chief of Public Affairs. He said this applies to whether the person is a Soldier or Army civilian communicating as an organization or as an individual on social media sites.

"Once it's out there, it's out there," Sweetnam said. "You can delete it, but if the wrong person took a screen shot, that's actionable intelligence and you can't get that back."

Sweetnam compiled the Army's Social Media Handbook and conducts training for Soldiers about the do's and don'ts of posting on social media. The do's include using social media to get out the messages of your command, inform the public of Army activities or stay connected with loved ones. The don'ts include not revealing sensitive information about missions, units or Soldiers, Sweetnam said.

Besides considering opsec, Soldiers must maintain their professionalism at all times, even when off-duty, Sweetnam said. They are subject to the Uniform Code of Military Justice and could face corrective or disciplinary action if they violate the rules of conduct at any time, he said.

Those violations would include a Soldier releasing sensitive information, insulting his or her chain of command, posting discriminatory statements, or sharing or linking to inappropriate material.

How to protect the Army family

Sweetnam said the Army encourages Soldiers to share with their families the lessons of operations security and using social media.

“The spouse, when the Soldier is deployed, may post something about his or her return, and that could be considered opsec,” Sweetnam said. “It even goes an additional level, to not only police yourself but make sure your family knows what it can and cannot do.”

The Army’s social media experts tell Soldiers not to use location-based social networking services when deployed or in classified areas; for Soldiers and families not to post specific dates or locations of deployments; and recommend setting privacy settings to “friends only” on personal accounts to prevent personal information from ending up in the wrong hands.

The Army suggests that users consider turning off the geotagging feature that is automatically turned on in some smartphones and digital cameras. Geotagging is the equivalent to adding a 10-digit grid coordinate to a photograph telling where it was taken, which could reveal sensitive information about a location.

Sweetnam said for the most part, Soldiers understand the importance of being vigilant at all times when using social media.

“The majority of the Soldiers who are in uniform now have grown up with social media. This is the way they communicate,” he said. “They are more aware of the do’s and don’ts, and we don’t necessarily have to constantly drive it into them. But occasionally, we have to send out those reminders.”

‘Professional at all times’

A post by a Soldier or Army civilian could be potentially taken by a member of the public as an official post, said Brittany Brown with the Online and Social

Media Division. That is why it is important for everyone in the Army family to always be professional, she said.

“Ultimately what we tell Soldiers and civilians is that you are responsible for anything that you put on social media sites, whether it is a Facebook page you’ve created in an official capacity as a Soldier or Army employee, or it’s your personal page that you’ve only connected to your loved ones,” said Brown.

Brown recommends that if it isn’t something you wouldn’t say in formation or in a public setting, then don’t post it on social media, no matter how locked down your page is. You just never know who ultimately ends up seeing the information you post, she said.

“These things can have long-term effects,” she said. “In the 20 seconds it took you to post the photo, you may have put lives at stake. Of course you wouldn’t do that intentionally, but if that photo has that metadata embedded in it, then you are putting Army operations and more importantly lives at stake by posting that.”

She said family members should be careful when posting information, such as if their spouse is deployed and they are now home alone. They should also think about the “trickle-down effect” before they post, and how the information could impact their Soldier and others, she said.

“At the end of the day, it keeps all of us safe,” Brown said. “It’s better to be safe than sorry.”

Resources

Army Social Media Handbook, version 3.1 (January 2013) ■



<https://www.armyupress.army.mil/Journals/NCO-Journal/>
<https://www.facebook.com/NCOJournal>
<https://twitter.com/NCOJournal>
<https://www.instagram.com/ncojournalofficial/>

Disclaimer: The views expressed in this article are those of the authors and do not necessarily reflect the opinions of the NCO Journal, the U.S. Army, or the Department of Defense.

