What can the adversary gain from this piece of information?

They say 'The Enemy is listening', so consideration must be taken at all times when posting on social media. Major Juanita Chang, Director, Online and Social Media Division, DOA explains the role of social media in the military, common challenges, and the ways in which the Army deals with online scams and imposters.

Major Chang:
We consider operational security (OPSEC) before every post we make to a social media site, and we encourage everyone else to do the same – whether they are in the military or not. Before we post anything to a social media site, it has to have a *purpose*. We don't post things simply for the purpose of posting, we share items that have *value* and help connect the public with the Army as well as to help educate them about what we do.

For the Army, it is important for us to ask *'what can the adversary gain from this piece of information'* before we consider sharing it. And, we ensure that each item cannot be used to put any of our Soldiers at risk. We also encourage everyone to ask the same thing – if a person consistently 'checks in' to a certain bar, for example, that makes their activities predicable and sets them up to potentially be victimized.

IDGA:
How do you ensure compliance of the social media guidelines?

Major Chang:
We have published a set of guidelines for both Army organizations and individual members of the Army. As professionals, we hold everyone in the Army to a high standard and we very rarely ever have any divergence from these guidelines, and when we do, they are generally a case of simply not knowing what the guidelines are. We really don't have to do a lot to ensure compliance. *Every Soldier knows they represent the Army both on and off duty.*

IDGA:
What would you say are the greatest achievements for the Army's social media channels?

Major Chang:
This one is easy. During Hurricane Irene, the Soldiers of the 3rd Infantry Division (The Old Guard) who guard the Tomb of the Unknown at Arlington National Cemetery continued to stand watch during the hurricane. We were able to get a photo of the guard walking in humble reverence during the hurricane and we sent it out via Twitter and used the hashtag #Irene. This got the attention of the public that would not generally be following the U.S. Army. The #Irene hashtag became the source of information for hurricane updates and the story of the guard resulted in nearly every national level media outlet doing a story about this Soldier: http://abcn.ws/z2lI5Q and http://n.pr/oQlbvM for example.

IDGA:
How can scam or imposter accounts hurt an organization?

Major Chang:
The most common form of scam using imposter accounts deals with *romance scams*, but others may deal with spreading misinformation and distributing inappropriate imagery.

Unfortunately, scammers impersonate military members when trying to conduct romance scams. On one hand, this is flattering since they see the Army's service men as a trustworthy figure. But on the other hand, innocent people who think they are romantically involved with an American Soldier are in fact being cyber-robbed by perpetrators thousands of miles away. This brings down the reputation of the entire Army, especially if the victim never realizes that their scammer is not indeed a military member.

IDGA:
What ways does the army ensure authenticity of Commander's accounts?

Major Chang:
We will verify an Army official's public-facing account with one of their staff members or with them personally. Once it is verified by us, we will list it on our official registry, located at www.Army.mil/socialmedia. This is our centralized resource for all official Army social media accounts. Every account there has been verified by one of the members of our office.

IDGA:
What is the Army doing to control and mitigate unofficial pages and imposter accounts?

Major Chang:
We have public affairs officers at every Army unit or installation who will report these imposter accounts, when discovered. We have had good luck working with Facebook to remove these imposter accounts, usually the same day we report them.

Unfortunately, scammers are using other platforms, including online dating sites, etc. These sites are neither easy to find nor as cooperative at removing the imposter profiles. We cannot control every site - so what we can control is how avidly we try to educate the public about these scammers. This article, for example, gets posted to our social media sites often as a reminder:
http://www.army.mil/article/67457/Army_CID_warns_against_romance_scams/

Juanita has been an active duty Army officer since 1996 and has been an Army public affairs officer since 2003. During her deployments to Afghanistan and Iraq, Juanita produced and executed strategic communications plans to communicate the Army's story to international and local media. She was the chief of media relations for U.S. Army Hawaii in 2006. In 2009-2010, she participated in an Army work-study program with an international public relations agency in Washington D.C. where she became passionate about applying social media to all strategic communications plans and is now applying those lessons learned in her position inside the Pentagon.