FACT SHEET
U.S. Army Cyber Command

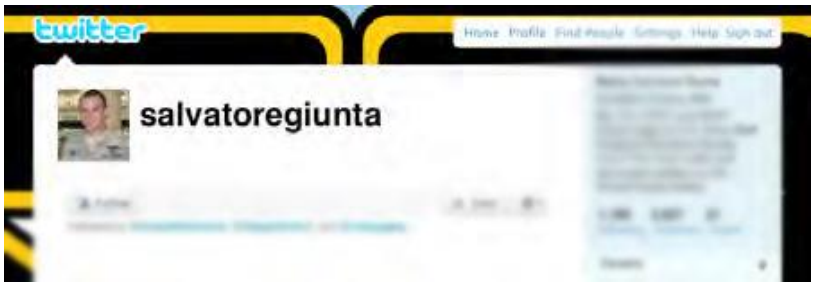
The Nation's Army in Cyberspace

www.arcyber.army.mil • www.army.mil/armycyber • @ARCYBER

THE FACTS: SOCIAL MEDIA IMPOSTERS

What are social media imposters?

Imposters are social media users who claim to be someone they are not, including U.S. Army officials or Soldiers. Some impersonate others for recognition, and some do it for financial gain. An imposter will set up an account, profile or page that looks real, but is in fact a phony. Even those who do not have social media accounts are still at risk, because imposters may steal their personal identification and set up accounts using that information and the victim's likeness. Imposters and scammers can damage an individual's finances and reputation, and the reputation of the Army.



Anyone can be affected by imposters, from Soldiers to senior leaders. Former Staff Sgt. Salvatore Giunta was impersonated on Twitter before he was awarded the Medal of Honor. Twitter does allow for imposter accounts, if they indicate that they are "unofficial" or "fan" accounts. The Army's Online and Social Media Division contacted the Twitter account manager to make sure the account was identified as a "fan" or "tribute" account.

How do I know if a social media account is an imposter?

If you are looking to identify an official U.S. Army social media presence, you can start by searching the Army's official social media directory at: www.army.mil/media/socialmedia.

Imposters can be clever, using different user names, spellings that are close to correct, and personal or official photos. There are some warning signs of a scam or common identifiers associated with imposter accounts:

-- The account is not registered
-- The account has very few photos
-- Photos that are very new and reflect the same date range are a red flag
-- The account has very few followers and comments
-- Official accounts will not send friend requests
-- The account name and photos do not match
-- There are obvious grammatical or spelling errors
-- Key information is missing

ABOUT US: United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

As of 17 April 2017

What can I do if I suspect someone is a social media imposter?

When imposter accounts are identified, it is important to report the accounts to the host platforms. The major social media platforms have reporting systems in place. Here are a few:

Facebook: https://www.facebook.com/help/174210519303259
Twitter: https://support.twitter.com/forms/impersonation
Instagram: https://help.instagram.com/contact/636276399721841
Google and Google+: https://support.google.com/mail/contact/abuse
Flickr: https://help.yahoo.com/kb/SLN7389.html/
Skype: Email fraud@skype.net

If you receive a request from an account claiming to be a senior leader, have issues with accounts listed in the official Army directory, or need assistance reporting imposters, contact the Army Office of the Chief of Public Affairs' Online and Social Media Division at usarmy.pentagon.hqda-ocpa.mbx.osmd-inquiry@mail.mil. The email must contain the URL any other proof of imposter or fake accounts. For requests regarding problems removing imposter accounts after they have been reported, the subject line should read "Request: imposter reporting assistance". For requests regarding accounts listed in the Army directory the subject line should read "Request: special priority reporting portal access".

How can I reduce my vulnerability to social media impersonation?

-- Conduct routine searches across social media platforms for your name. Include like or close spellings, as imposters often use similar spellings to remain undetected.
-- Set up a Google search alert for your name and like or close spellings.
-- Ensure privacy settings on all professional and personal accounts are set to the maximum.

Sources:
U.S. Army Social Media Handbook, April 2016
Army Imposter Reporting fact sheet
Army Social Media Imposters fact sheet

Follow ARCYBER on
(click the images to visit our pages)

ABOUT US: United States Army Cyber Command directs and conducts integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries.

As of 17 April 2017