19 AW/XP

OPSEC HOT TIP

September 2021

Service Member Impersonation Scams

Scammers love to impersonate people of authority, and that includes service members. These people often steal the identity or profile images of a service member and use them to ask for money or make claims that involve the sale of vehicles, house rentals or other big-ticket items. These scammers often send the victim bogus information about the advertised product and ask for a wire transfer through a third party to finish the purchase, but there's no product at the end of the transaction. Lately, fake profiles of high-ranking American military officials have been popping up on social media websites using photos and biographical information obtained from the internet. Scammers often replicate recent social media posts from official DOD accounts and interact with official accounts to increase the appearance of legitimacy. As an example, there are impersonator accounts on Facebook, Instagram and Twitter for Marine Corps Gen (Ret) Joe Dunford, former Chairman of the Joint Chiefs of Staff. These accounts are also interacting with Joint Staff account followers in an effort to gain trust and elicit information.

Scammers are making these profiles to defraud potential victims. They claim to be high-ranking or well-placed government/military officials or the surviving spouse of former government leaders, then they promise big profits in exchange for help in moving large sums of money, oil or some other commodity.

Here are some ways to lower the chances of you being impersonated or duped by a scammer:

• To avoid having your personal data and photos stolen from your social media pages, limit the details you provide on them and don't post photos that include your name tag, unit patch and rank.

• If an alleged official messages you with a request or demand, look closely at their social media page. Often, official accounts will be verified, meaning they have a blue circle with a checkmark right beside their Twitter, Facebook or Instagram name. General and flag officers will not message anyone directly requesting to connect or asking for money.

• Search for yourself online — both your name and images you've posted — to see if someone else is trying to use your identity. If you do find a false profile, contact that social media platform and report it.

PRACTICE GOOD OPSEC!

"SHRED, ENCRYPT, PROTECT"