



U.S. ARMY

# Imposter Accounts, Romance Scams, and Unofficial Sites

## Identifying Imposters and Scams

## Take Immediate Action Against Imposters

## Tips To Reduce Vulnerability

If you are looking to identify an official U.S. Army social media presence start by searching on the Army's social media registry at: [www.army.mil/media/socialmedia](http://www.army.mil/media/socialmedia)

Imposters and scammers can be damaging not only to an individual's reputation, but also to the Army's. That is why it is important to know the warning signs of a scam or the common identifiers associated with an imposter account.

- The account is not registered.
- The account has very few photos.
- Photos that are very new and only in the same date range are a red flag.
- The account has very few followers and comments.
- Official accounts will not send friend requests. If you receive a request from an account claiming to be a senior leader, report it.
- The account name and photos do not match.
- There are obvious grammatical or spelling errors.
- Key information is missing.

The people establishing imposter accounts can be clever; using different user names, close spellings, personal photos, official photos, and even changing the nametape on Soldier's uniforms. Remember, anyone from Army Senior leaders to Medal Of Honor recipients, and Soldiers can be affected.

Social media platforms allow for reporting fake accounts and scams. It is the first recommended step in removing an account is to report directly on the page. Be familiar with the steps to report imposter accounts on each platform. Additional assistance can be found on the major social media platforms below.

Report an imposter on Facebook:

<https://www.facebook.com/help/174210519303259>

Report an imposter on Twitter:

<https://support.twitter.com/forms/impersonation>

Report an imposter on Instagram:

<https://help.instagram.com/contact/636276399721841>

Romance scams pose a unique challenge to identity thieves and fight against imposters because they often require you to have a dating profile in order to conduct search for fake accounts.

In addition, it is difficult to remove dating site profiles without legitimate proof of identity theft or a scam. If you suspect fraud on a dating site, take a screen shot of any advances for money or impersonations and report the account on the platform immediately.

For more tips specific to dating site scams visit the Army's Criminal Investigation Division Website at

<http://www.cid.army.mil/romancescam.html>



- Conduct routine searches across social media platforms for your name or the names of senior leaders you may represent as a public affairs professional. You should also search for like or close spellings as imposters often use similar spellings to remain undetected.
- Set up a Google search engine alert for your name and the names of any senior leaders you may represent.
- Register official accounts on the Army's social media registry at [www.army.mil/media/socialmedia](http://www.army.mil/media/socialmedia).
- Ensure privacy settings on all professional and personal accounts are set to the maximum. For tips on how to maximize your security settings and configure your social media accounts: <http://www.cid.army.mil/documents/CIU/2can/SocialNetworkingSafetyTips.pdf>.

## Online and Social Media Division

For further assistance with identifying imposter accounts and reporting fake accounts on social media or dating sites, contact Online Social Media Division at: [usarmy.pentagon.hqda-ocpa.mbx.osmd-inquiry@mail.mil](mailto:usarmy.pentagon.hqda-ocpa.mbx.osmd-inquiry@mail.mil). Note that the email must include the URL and any other proof of the imposter or fake account.