

CPF 0001-18-CID361-9H

19 January 2018

Combating Social Media Impersonation

Frequently, U.S. Army Criminal Investigation Command receives notifications from individuals stating they were scammed online by someone claiming to be a U.S. Soldier. Unbeknownst to the U.S. Soldier, an online scammer has used the Soldier's name and available social media photos to perpetrate a crime.

While the majority of U.S. Soldier social media impersonations are of officers, online scammers will impersonate enlisted personnel, Army civilians, and contractors. Scammers, using information from your profile, capitalize on the trustworthy reputation of individuals associated with the Army. By monitoring your social media identity, you can protect your Army family and your reputation.

Mitigating Fraudulent Social Media Accounts

Search for your name on social media sites. Since scammers may use your photo but change the name, you should also conduct a Google [image search](#) of your social media profile pictures.

If you find yourself or a family member being impersonated online, the links below will lead you to step by step instructions for reporting false profiles on several popular social media sites.

- [Facebook](#)
- [Instagram](#)
- [Twitter](#)
- [Google+](#)
- [LinkedIn](#)

Additional Resources

For more information about social media safety, you can review these cybercrime prevention flyers:

- [Social Networking Safety Tips](#)
- [Twitter Safety Tips](#)
- [LinkedIn Safety Tips](#)
- [Google+ Safety Tips](#)
- [Facebook Safety Tips](#)



Contact Information:

Cyber Criminal Intelligence Program
27130 Telegraph Road

Phone: 571.305.4482 IDSN 2401
Fax: 571.305.4189 IDSN 2401

Email

usarmy.cciuintel@mail.mil

CCIU Web Page

<http://www.cid.army.mil/701st.html#sec6>

CID LOOK OUT
ON POINT FOR THE ARMY

DISTRIBUTION:

**This document is authorized for the
widest release without restriction.**

ICE

CCIU uses the Interactive Customer Evaluation (ICE) system. Please click on the ICE logo and take a moment to provide feedback.

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer (CPF), along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization's mission. CID does not exercise any editorial control over the information you may find at these link locations.



"DO WHAT HAS TO BE DONE"