



CPF 0007-2019-CID361-9H

30 May 2019

## Social Media Scamming — What's New?

Whether referred to as Card Popping, Cash Out, Card Flipping, or Cracking, the hustle is the same and on the rise. Scammers are using social media sites like Instagram, Snapchat or Facebook to run ads or directly private message military members to fraud them out of their hard-earned money.

The scammers pose as former or current military members, bank officials, day traders, financial consultants, debt relief agents, or even model agents offering ways to make thousands fast.

As they socialize with you, they learn your personal or emotional needs, giving them leverage to exploit. If you tell them you are financially stable, they will try to offer stock options for high-valued companies such as Apple or Amazon. Or even offer money for access to your Facebook friends.



If you take the bait, the scammer will request your personal banking information such as login and password for the supposed purpose of depositing money to your account. Once a deposit is made, you may be asked to send a bank transfer or wire cash from a money transferring service to a third party. However, what the scammer has now involved you in is the funneling of money. You may even find that loans have been issued in your name from your bank.

Never give out your account information and never transfer money to someone you do not know.

If you feel you have been a victim of Card Popping, Cash Out, Card Flipping, or Cracking, please adhere to the following guidance:

- Discontinue correspondence with the scammer.
- Notify your bank or financial institution.
- Change account passwords and seek additional security procedures for future logins.

### Contact Information:

**Cyber Criminal Intelligence Program**  
**27130 Telegraph Road**  
**Quantico, Virginia 22134**

**Phone: 571.305.4482 IDSN 2401**

**Fax: 571.305.4189 IDSN 2401**

[Email](#)

[CCIU Web Page](#)

**CID LOOK OUT**  
**ON POINT FOR THE ARMY**

### DISTRIBUTION:

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



- Consider credit monitoring or locking your credit through one or all three of the major credit bureaus.
- Notify your command, CID office, or law enforcement authorities.

## Resources

[Social Media Scam: Card Cracking](#) – USAA

[8 Social Media Scams to Avoid](#) – Navy Federal Credit Union

[American Banking Association Card Cracking Infographic](#) – ABA

[What are the Biggest Social Media Scams of 2018?](#) – IBM Security Intelligence

[Military Scams on Instagram: Why Cybercriminals Target the Armed Forces](#) – ZeroFox

## In the News

[Twenty-nine charged in Chicago with 'Cracking cards' bank fraud scheme](#) – Reuters

[Hip-Hop group indicted in \\$1.2M fraud scheme](#) – Atlanta Journal-Constitution

To receive future CCIU Cybercrime Prevention Flyers, send an email to: [usarmy.cciuintel@mail.mil](mailto:usarmy.cciuintel@mail.mil) with "SUBSCRIBE: CPF" in the subject line.

The logo for the Interactive Customer Evaluation (ICE) system, featuring the letters 'ICE' in a stylized, blue, blocky font with a slight 3D effect.

**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.