Computer Crime Investigative Unit
U.S. Army Criminal Investigation Command

Cyber Crime Alert Notice

Contact Information:
Cyber Criminal Intelligence Program
27130 Telegraph Road
Quantico, Virginia 22134

Phone: 571.305.4482 [DSN 240]
Fax: 571.305.4189 [DSN 240]

E-mail

CCIU Web Page

2CAN 0003-15-CID361-9H **02 February 2015**

Cybercriminals Target USAA Members

Overview:

Recent crime reports reveal a social media fraud scheme targeting USAA members. The scheme may target other groups or financial institutions because the techniques can be easily adapted.

Background:

The scammer, pretending to be an official representative of USAA, contacts a USAA member on social media (e.g., Facebook, Twitter, Instagram) claiming the member has won an award or is eligible for a customer incentive. In order to receive the award payment, the member is asked to pay a finder's fee, commission or service charge.

Conveniently, the fee can be paid from the proceeds of the award. The scammer asks for the USAA member's mobile banking credentials (username, password and PIN) and uses USAA's mobile banking application to deposit checks into the member's account. Then, the member is asked to electronically pay the finder's fee to the purported USAA official, usually through a wire or money transfer service like Moneygram or Western Union. Wire and money transfer services are used because traceability is often limited.

Predictably, the deposited award checks are not genuine and, after several days, are returned unpaid and charged back to the USAA member's account. While the deposits are fake, the money the member wires to the scammer is very real.

Most likely, the scammers surf social media content (images and comments) randomly identifying military personnel and their family members. Once identified, they are prime targets for the USAA scam, not because the scammer has specific knowledge of any actual USAA affiliation. Rather, the scammers shotgun their messages betting (and current reporting indicates good odds of success) that at least some of the recipients actually have USAA relationships.

If you are suspicious about any social media post claiming to be from USAA or you have been approached as described in this Cybercrime Alert Notice, please contact USAA at abuse@usaa.com. For similar scams involving other financial institutions, please contact their security department, the Internet Crime Complaint Center or the United States Federal Trade Commission.

Cyber Crime Alert Notice

Reminder:

Verify through established channels the authenticity of anyone asking for your personal information, financial information, passwords, PINs and so forth, especially if you did not initiate the interaction.

Recommended Practices:

- Be suspicious when someone you do not know contacts YOU and asks for YOUR personal information.
- Never, in any social media setting, provide usernames and passwords to anyone; your bank will not ask for personal information, including debit card numbers and PINs.
- Verify, verify, verify! Contact the financial institution directly.
- Use a telephone number or email you know to be valid; look on the financial institution's website, the backs of your debit or credit cards or statements.
- DO NOT rely on the person who contacted you to provide a verification telephone number or email. Remember, you are verifying because you are skeptical of the person's reliability.

Previous CCIU Advisories related to Social Media:

Social Networking Safety Tips, CPF 0037-14-CID361-9H, 5 December 2014

"Phoney" Tech Support, 2CAN 0015 –12-CID361-9H, 24 August 2012

For more information about computer security and other computer related scams, we encourage readers to visit the CCIU website to review additional cyber crime alert notices and crime prevention flyers.

Additional Resources:

- The Latest Social Media Scam: Card Popping, USAA
- Staying Safe on Social Networking Sites, United States Computer Emergency Readiness Team
- Safe Social Networking, National Crime Prevention Council

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