An Important Scam Notification from USAA

Social media scam targeting service members

Jun 24, 2015
DO NOT provide your personal banking information through social media.

There is a social media scam, predominately seen in Instagram, which is targeting military service members. This scam has been around for over a year, but has picked up steam over the past few months and more and more people in and out of the military are falling prey to fraudsters. Please review the following items and stay alert.

The fraudsters are targeting military, veterans and their families. In exchange for their personal banking information, they are promised the ability to make easy money. The victim provides their log in/password information and the fraudster gains the ability to deposit fraudulent funds directly into their account. They immediately pull out their fee, before the institution can identify the credibility of the deposit, and the victim is left responsible for the used funds. The amounts range from $2K to $20K, growing the debt of the victims in a matter of minutes.

The consequences are very unpleasant - you are responsible to pay back the entire amount. Funds are transferred to collections, impacting the victim's credit score and could even result in criminal charges.

Take a moment and think about offers that seem too good to be true. If you have to question if it is legit, walk away. Many victims thought the most they could lose was the balance in their account – they were wrong.

To the people who influence the potential victims, take time to be an advocate and help us educate. They are being taken advantage of and it is our obligation to protect them.

Here are some tips. Make sure to read, follow and share, regardless of where you bank.

1. Offers of free money. USAA (and no other legitimate financial institution) is NOT going to

post offers of easy money on social media.

2. Odd phone numbers. A credible USAA number is either a 210 area code or 800 number.

3. Requests for your information. Fraudsters ask for things USAA or any other legitimate institution would never ask for, such as personal identifiers, debit card information and account numbers — USAA and legitimate banks already have all that.

4. Unprofessional pictures. The pictures (fraudsters use) on Instagram might show cash or risqué images of women. They are not images representative of legitimate bankers, investors or USAA employees. That's not USAA's image.

5. Directions to send money back. USAA recently had a conversation with a fraudster posing as a USAA official. The scam was an offer to deposit unclaimed insurance money into the member's account but required a 50% fee to be sent back to the fraudster after the deposit was made. USAA or any other legitimate financial institution would not deposit funds into a member's account and ask them to send half back.