

Tech Tuesday: Cybercriminals using a reverse instant payment scam

May 17, 2022



TECH TUESDAY: Reverse Instant Payment Scam

- Be wary of unsolicited requests to verify account information. Cyber actors can use email addresses and phone numbers which appear to come from a legitimate financial institution.
- Contact your bank's fraud department directly through verified phone numbers and email addresses on official bank websites or from the back of your credit or debit card.
- Be wary of callers that provide personally identifiable information, including social security numbers.
- Enable Multi Factor Authentication for all financial accounts, and do not provide those codes to anyone.
- Report fraud to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

The FBI's Internet Crime Complaint Center recently issued a warning about a rise in payment scams. Victims appear to get a text message from a bank's fraud alert department. The text asks if the customer initiated an instant money transfer using digital payment apps connected to a bank.

For example, a text may say- Bank Fraud Alert- Did you attempt an instant payment in the amount of \$5,000? Reply, Yes or No, or 1 to stop alerts.

The payment amount and financial institution may vary from victim to victim. You may even receive different texts claiming to be from different banks because the crooks are hoping to guess your financial institution.

If the victim responds, they receive a phone call that appears to be from the bank's legitimate 1-800 support number. The criminals may know a past address, your social security number, and the last four digits of your bank account. This information is used to convince you that the steps being requested are the financial institution's legitimate process to stop that money transfer.

Once the fraudsters have you on the hook, here is how they steal your money. Using the bank's legitimate website or application, the crook will instruct victims to remove your email address from their digital payment app and replace it with an email address controlled by the fraudsters. After the email address has been changed, the cyber crook tells the victim to start another instant payment transaction to themselves that will cancel or reverse the original fraudulent payment attempt. Unfortunately, victims are in fact sending instant payment transactions from their bank account to an account controlled by the criminals. Victims often only realize they've been scammed after checking their bank account balance.

The FBI recommends the following precautions:

Be wary of unsolicited requests to verify account information. Cyber actors can use email addresses and phone numbers which appear to come from a legitimate financial institution. If a call or text is received regarding possible fraud or unauthorized transfers, do not respond directly.

Instead, contact your bank's fraud department through verified phone numbers and email addresses on official bank websites or from the back of your credit or debit card, never through a text or email you receive.

Be wary of callers that provide personally identifiable information, including social security numbers. Unfortunately, there have been so many large-scale data breaches over the last decade, criminals may know some of your personal data.

Your best protection, Enable Multi Factor Authentication for all financial accounts, and do not provide those codes to anyone.

If you've been a victim of an online fraud, report it to the FBI's Internet Crime Complaint Center at www.ic3.gov.