

Three Types of Fraud: Phishing, Vishing and Smishing

Fraud continues to evolve as consumer's knowledge and awareness of fraud techniques increase. The purpose of e-mail fraud is to get the consumer to provide confidential information, such as account numbers, passwords and social security numbers. The perpetrator then uses this information to gain access to the consumer's bank and credit card accounts.

To keep you informed, below is information on the three common forms of e-mail fraud – phishing, vishing and smishing.

Phishing was the earliest form of the e-mail scam.

- An e-mail is sent to the consumer, which appears to be from a legitimate company or financial institution.
- The e-mail generally states an urgent response is necessary to keep an account from being blocked.
- The e-mail asks the user to verify personal information, such as account number, SSN, card number or personal identification number (PIN), card expiration date, or card security code.

Vishing soon followed phishing. This term is a combination of "phishing" with "voice," because the fraud is initiated via telephone and/or e-mail. A vishing request can be received in two ways:

- The consumer receives a telephone call claiming to be from a financial institution or other legitimate company, calling to verify personal information (just as in phishing scams).
- The consumer receives an e-mail or automated telephone call, requesting an urgent response or their account will be blocked. The notification refers to a phone number that when called, asks for personal information (card number, account number, PIN, etc.). Many members are accustomed to entering this information in MATTI (Members' Automated Teller Transaction Inquiry), so they aren't alarmed when asked in this situation.

Smishing is the newest form of this scam. This term is a combination of "phishing" with "short message service (SMS)" and is initiated via text message. Smishing can occur when:

- The consumer receives a text message on a cell phone or other mobile access device, confirming enrollment in a dating service (or other company) and stating the user will be charged \$2 per day unless the order is cancelled. Once the recipient clicks to cancel the order, a Trojan horse virus is downloaded that allows the criminal access to the mobile device. This enables the criminal to listen to calls and access information stored on the phone.
- The consumer receives a text message stating an account is in danger and prompts the recipient to respond by verifying personal information.

As these scams gain media attention, fewer people are willing to respond. Unfortunately, the criminals continue to use technology to find new ways to attempt to steal personal information.

Tips to Avoid Becoming a Victim of These Scams

- Never release personal or account information to unsolicited emails, telephone calls or text messages.
- Protect your personal information. Be cautious of who you give this information to.
- Don't click on links embedded in unsolicited e-mails or text messages. They can contain viruses or Trojan horses.
- If you receive a call or e-mail directing you to act immediately to avoid your account from being blocked, do not respond. Instead, call the customer service number on the back of your credit card, debit card, account statement. Or if it is a CommunityAmerica card, contact us directly at 913.905.7000 or 800.892.7957.
- Report any suspicious/vishing scam telephone number **or e-mail address** to your local or federal law enforcement agencies.
- If you receive a phishing, vishing or smishing scam claiming to be from CommunityAmerica Credit Union, contact us immediately at 913.905.7000 or 800.892.7957, or e-mail the information to: abuse@cacu.com.