Protecting Your Money

Three Fraud Prevention Tips

(NAPS)—Since government pandemic assistance programs have largely come to an end, fraudsters have turned their attention back to developing increasingly clever ways to trick you into giving them your money—but you can protect yourself and your assets.

Here are two confidence schemes that have been trending in recent months:

- **Malicious Links:** Bad actors text a link that appears to be from a legitimate company. Even if you don't provide any information, clicking on the link can lead to malicious software or viruses on your phone.
- **Spoofing:** Fraudsters attempt to steal personal information by pretending to be someone with an urgent request—these bad actors often pose as government agents or fraud investigators from your bank.

In both scenarios, the goal of the bad actors is to trick the customer into providing personal information as well as bank account and login details that will let the fraudster take over the account and empty it using various peer-to-peer payment services or wires. Since the bad actors have personal information and the bank account login details, they are able to pose as the customer and confirm that they want to send money. In the case of the impostor phone call, the scammer will often trick the customer into sending them money to "resolve fraudulent activity" while speaking with them on the phone.

The experts at Citi suggest the Top 3 Tips to help you avoid these types of fraud:

1. Scammers Have Learned How to Spell: Don't assume that all scammers misspell or use obvious email addresses and URLs, or make requests that you send money to a faraway land to claim a lost fortune. Today's fraudsters send emails and text links that closely imitate those from real companies or other trusted individuals and that may appear to be legitimate.

2. Be Skeptical of Unsolicited Messages: Be aware of seemingly real emails, texts and phone calls that ask you to urgently provide personal or account information. These tricks are especially successful when people are distracted by their busy lives. Don't click on a link from any email or text that you receive unexpectedly and delete unsolicited incoming emails and texts. Additionally, don't provide any personal identifying or account information to any inbound communication by phone, email or text. Contact your bank or the merchant directly via known and trusted communication channels if you are concerned about an account that is the subject of an unsolicited or suspicious message.

You can outsmart scammers and protect your money.

3. Don't Take the Call—Make the Call: If you get a call from an unknown number, don't answer it or return it. Instead, reach out directly to your bank by logging in to its secure website or by calling the known customer service number from the back of your card to review account activity and information. Even if you get a call from a number which appears on caller ID as your bank's name and number, do not provide personal information on that inbound call as fraudsters can easily spoof the incoming caller ID information.

Cyber-enabled fraud is very lucrative and bad actors work around the clock, using sophisticated algorithms that enable them to set up convincing confidence schemes that will trick you into giving away your credentials, your identity, even your life savings. Be vigilant to avoid taking the bait.

Learn More

For further information about fraud and how to fight it, visit: www.citi.com/fraudprevention.