Keep Yourself Safe from New Fraud Scams

With the recent news about a few bank failures, many vendors are updating their banking information. Scammers are using this moment of change to take advantage of unsuspecting customers. By preying on common anxieties, fraudsters can trick you into sending money to a phony bank account or providing your personal banking information.

Know The Red Flags

The most common types of scams will target you through fake emails, text messages, voice calls, letters or even someone who shows up at your front door unexpectedly. No matter which technique the scammer uses, you may be:

- Contacted unexpectedly by phone, email, text, direct message or pop-up with a request for personal information or money. Never click a link or download an attachment from someone you don't know. Financial institutions will never text, email or call you asking for personal or account information.
- Pressured to act immediately with an alarming phone call, email or text that plays with your emotions. Scammers may pose as an employee from a familiar organization, such as your bank and say there's a problem that needs immediate attention. Do not act unless you have verified the person who has contacted you and the story or request is legitimate.
- Asked to pay in an unusual way, like gift cards, bitcoin, prepaid debit cards or digital currency, including Zelle® to resolve fraud. Banks will never ask you to transfer money to anyone, including yourself and will never ask you to transfer money because they detected fraud on your account.
- Asked to provide personal or account information, such as an account verification code, bank account number or PIN. When in doubt, don't give it out. Financial institutions will never text, email or call you asking for an account authorization code.
- Offered a free product or 'get rich quick' opportunity that seems too good to be true? If something sounds too good to be true, it probably is. Never cash a check for someone you don't know.

If you authorize a transfer or send money to a scammer, there's often little they can be done to help get your money back.

Tips to Keep Yourself Safe

Remember to stay calm and be skeptical of banking update requests. By following these tips, you can keep yourself safe from potential scams:

- Don’t click on anything in an unsolicited email or text message asking you to update or verify account information.
- Never send funds to a merchant until you can confirm that the request to change a payment destination is legitimate, like a statement from them or a verified customer service phone number.
- Don’t rely only on caller ID to confirm someone’s identity, as scammers can compromise that too.
- Look up the company’s phone number through a legitimate source like a statement provided by the company, and don’t use the number a potential scammer is providing.
- Take your time. A legitimate associate will never pressure you to immediately make a decision. They’ll provide you with all the necessary information and specific time frames to make your decision.

When in doubt, hang up the phone and call your financial institution directly.

Additional Resources

Here are some additional resources to learn more about avoiding potential scams and fraud:

Bank of America: How to Avoid Scams
CAPITAL ONE: Scam Education
CAPITAL ONE: Help avoid falling victim to business email compromise (BEC)
Cybersecurity and Infrastructure Security Agency (CISA) guidance

---