Electronic Banking Security Tips

Whether you are banking from your mobile device, a computer, ATM, and or the telephone the following practices can protect you from fraud.

- ***Back Up Data Regularly –*** Regularly back-up your mobile devices and computers.
- ***Maintain Documentation of Transactions –*** Many people rely on their bank to provide transaction histories, but no matter what form of electronic banking you use make sure that you independently document the details of the transaction for your own records.
- ***Utilize Access Passwords –*** Make sure to use passwords/PINs and/or biometric scanning devices to access your mobile device, computer, and/or ATM or telephonic system.
- ***Don't allow automatic log in to your bank accounts.***
- ***Don't save your password, account number, or PIN on your computer and/or mobile device.***
- ***Download and install antivirus/anti-spyware software on your computers and/mobile devices.***
- ***Be careful when downloading Programs and/or Applications -*** All downloads should be from a trusted source.
- ***Avoid "free offers"-*** Emails, instant messages, texts, and or social media targeted advertisements that offers free items may contain viruses or malware. Remember the old adage: "Nothing in life is free"
- ***Be cautious of messages from unknown sources.*** Be cautious of any form of message (voicemail, email, text, etc.) asking you to update, validate or confirm personal information such as your account information or password. Legitimate sources like banks, mortgage lenders, and even internet email and social media sites will NEVER contact you to update this type of information. It is your responsibility to contact them if an information updated is required.
- ***Check your account often –*** At least once per day review your banking transactions to catch fraudulent activity quickly.
- ***Do not use Public Wi-Fi*** - When accessing sensitive information from a mobile device or computer ensure that the network is properly protected. If a network doesn't ask for a password it is Public and you should not use it for sensitive transactions.
- ***Make sure you log out of social networking sites and online banking when you are finished using them.***

- ***Install operating systems updates for all computers and mobile devices as they become available as they often include security updates.***
- ***Before you dispose of, upgrade, or recycle your computer or mobile device backup your data, remove/de-authorize any licensed services, and reinstall the operating system or factory reset.***
- Use a secure browser and trusted computer for sensitive transactions.
- Log off when you're done using Web sites that require a user ID and password.
- Disconnect and shut down when you're not using your computer.

Social Engineering

Social Engineering is a non-technical method of intrusion hackers utilize. It relies heavily on human interactions and behaviors. The most prevalent type of Social Engineering attack that occurs to customers is a phishing attack. Phishing is the attempt to acquire sensitive information such as usernames, passwords, credit card details, financial information, and sometimes money for malicious reasons by masquerading as a trustworthy source.

Phishing attacks can occur by email, text, instant messaging, social media, and/or by phone.

Here are a few ways you can prevent yourself from falling victim to social engineering techniques:

- Don't respond to ANY email or social networking post or message that advertises free items, asks for money or to utilize your account for a monetary transaction, requests you to reveal user names and passwords, asks for your phone number and/or address, or other confidential information.
- Don't assume that an unsolicited phone call or message is actually from a trusted source. Thieves can research your purchases or donations, then pose as a business or charity.
- Verify. If someone on the phone or a message is telling you there is a problem with your online banking account don't give them additional information to "fix" the problem. Hang up or delete the email and check those accounts directly by logging in normally or calling a published customer service number.
- Be conscious of what can be learned about you. Thieves are very good at digging out the basic security questions such as mother's maiden name or the model of your first car.

- Even the most innocent attachments can be infected with malware. If you aren't certain the message came from a legitimate source DO NOT OPEN it without verifying. Call the source and ask if they sent an email with an attachment.