SCAM REPORT
MILTON TOWNSHIP S.A.L.T. COUNCIL MEETING 9-11-23

Prepared by Arnold H. Shifrin

Two-Factor Authentication Scam

The two-factor authentication (2FA) scam is one in which criminals convince victims to divulge the codes required to access online bank accounts. Once criminals have an individual's login credentials and the 2FA code, they can access an account and drain money from it.

Background: Two-factor authentication adds a second layer of protection to your online bank accounts. After entering your user name and password to access an account (first layer of protection), a multi-digit code (the 2FA code) is sent by text to your cell phone (second layer of protection). You are required to input the code before you can fully access the account. Thus, a criminal would need both your account login information and 2FA code to break into your account.

How the scam works: You receive a call from someone claiming to be from your bank. The caller states there has been suspicious activity associated with your account recently and that immediate action is required to keep your account from being compromised. The caller is professional and persuasive and convinces you the bank's IT personnel can secure your account. All they require is the 2FA code you receive when you login to the account. You trust the bank and wish to protect your holdings, so you comply with the caller's request and disclose the code.

Though unknown to you at the time of the call, the scammer has the login credentials for your account. This information was obtained in one of the following ways: 1) your user name and password were weak and easily hacked, 2) malware was installed on your computer and your login credentials were stolen, or 3) your bank experienced a data breach and your personal information was exposed. Armed with your user name, password, and recently-disclosed 2FA code, the scammer logs in to your account, changes the login credentials to lock you out, and transfers the funds to another account. Your money is gone.

How to protect yourself

- If you receive a "fraud alert" from your bank, do not provide any information to the caller. Hang up the phone and contact your bank to determine if your account is in jeopardy. Use a telephone number you know is correct, not one that was given to you by someone else. If the "alert" is verified, change the password for each account you have at the bank.
- Do not trust phone numbers appearing on your caller ID. Those may be "spoofed" calls and the call from your bank may have been placed by a cybercriminal.
- Legitimate callers will not ask for your 2FA code. If a caller claiming to be from your bank asks for the code, you are dealing with a scammer. Hang up the phone. Do not divulge your code to anyone.
- To help secure your online accounts, always enable 2FA when it is offered. If available, consider enabling biometric authentication (e.g., facial or fingerprint recognition) to further protect you.
- To prevent your login credentials from being hacked, create strong, long, unique passwords for all your online financial accounts. Do not use the same password across multiple accounts. Consider using a password manager to securely store your passwords.
- Regularly monitor your online financial accounts, including monthly statements, for suspicious or unauthorized activity. Report any discrepancies to your bank.
- If you are a victim of this scam, notify the following: your bank, the Federal Trade Commission, the Illinois Attorney General Senior Citizens Consumer Fraud Hotline, the FBI's Internet Crime Complaint Center, and your local police department.

[Source: Wells Fargo]