What is Multi-Factor Authentication?

Multi-Factor Authentication (MFA) is a security measure that can help protect your online accounts in the event your login credentials are compromised. MFA is a multi-step verification process that requires two or more verifying factors during authentication to validate users and can vary for each account. The most common factors are passwords, a one-time passcode (OTP), the answer to a secret question, biometrics, or a known device.

Why is MFA Important?

MFA makes it more difficult for bad actors to gain access. With MFA enforced, they will need more than just your username and password to gain access to your accounts.

Did you know login credentials such as usernames and passwords that were part of a data breach can be purchased by bad actors via the dark web or that Artificial Intelligence (AI) can be used to automate guessing various password combinations until the correct password is found?

Although MFA can help make you safer online, bad actors may still be able to gain unauthorized access to your accounts if you aren't careful. Cybercriminals use a variety of techniques to bypass MFA, such as SIM swapping, social engineering, email account takeover, man-in-the-middle attacks, and malware.

MFA Bypass Techniques Explained

SIM swapping is when impersonators convince a mobile carrier to activate a new SIM card on a new device. Once the new SIM card is activated, the criminal now has access to any new text messages or phone calls sent to your phone number, including your OTPs that are sent as SMS texts.

Social engineering is when individuals are manipulated into giving bad actors access to private information. Bad actors convince victims they are from the entity whose system they are attempting to gain access to so that victims disclose confidential information or allow criminals access to their account. Actors are known for calling, sending emails or text messages, asking for user's OTP or sending them to a spoofed website that prompts for user's login credentials and OTP.

Email account takeover is when a criminal gains unauthorized access to an email account, in some cases locking the owner out by changing the password and other identifying factors. Once the criminal is in the email account, all new and past activity is monitored. They then impersonate the account owner to take over accounts on other systems. Email account takeover is very useful for criminals when users enroll for email authentication as their form of MFA.

Man-in-the-middle (MITM) attack is when the criminal places themselves between two parties to intercept data being exchanged. This type of attack is common on public WiFi because the networks are unencrypted and allow criminals to see any connected internet traffic. Verification factors such as login credentials and OTPs transmitted over the unencrypted network are then used by criminal to access victim's account.

Malware is a malicious software that is installed to infect devices as a way to steal sensitive information. Once a device is infected it allows criminals to take control and access 2FA (Two-Factor Authentication).

Tips to help prevent MFA from being bypassed

Use an authenticator app that is stored on a device other than the device used to access systems.

Authenticator apps generate unique Time-Based One-Time Passwords (TOTP) that expire usually every 30-60 seconds. This password is not transmitted over the internet making it harder to steal. However, when the authenticator app is stored on the same device used to access accounts online, if the device is compromised then the bad actors will have access to TOTP and be able to bypass security measure.

Avoid sharing OTP codes.

Bad actors will try to trick victims into revealing their OTP by utilizing social engineering. By sharing your OTP code, you are giving access to your accounts.

Use security keys.

A security key is a physical object that must either be inserted or tapped to a device to authenticate the user. Because security keys authenticate the user by something they physically possess, it makes it harder for the bad actors to steal. It is important once you have authenticated yourself that you remove the security key from the device and store it in a secure area to avoid unauthorized access. If the physical security key is left in the device when not being used the criminal will be able to bypass this security measure if the device is compromised.

Use strong passwords.

A strong password is difficult to guess which can prevent criminals from attempting to bypass MFA. Never use the same password for multiple apps, so that if one app is compromised, the criminals will not have the password to another.

Stay educated.

Staying educated on the latest cyber threats and scams will help prevent you from becoming a victim. Additionally, help your friends and family by sharing your knowledge so that they don't become victims of scams.

The Evangeline
BANK AND TRUST COMPANY

Member FDIC
EQUAL HOUSING LENDER