Cybersecurity Guide for Financial Institution Customers

Protect your computer

Install software that protects against malware (malicious software), which can access a computer system without your consent to steal passwords or account numbers. Also, use a firewall program to prevent unauthorized access to your PC. While protection options vary, make sure settings allow for automatic updates.

Use strong authentication

Use the strongest authentication offered, especially for high-risk transactions. Use passwords that are difficult to guess and keep them secret. Create "strong" user IDs and passwords for your computers, mobile devices, and online accounts by using a combination of upper and lower-case letters, numbers, and symbols that are hard to guess and then change them regularly. Although using the same password or PIN for several accounts can be tempting, doing so means a criminal who obtains one password or PIN can log into other accounts.

Understand internet safety features

You can have greater confidence that a website is authentic and that it encrypts your information during transmission if the web address starts with "https://." Also, ensure that you are logged out of financial accounts when you complete your transactions or walk away from the computer. To learn about additional safety steps, review your browser's user instructions.

Be suspicious of unsolicited emails

It is easy for cyber criminals to copy the logo of a reputable company or organization into a phishing email. When responding to a simple request, you may be installing malware. Your safest strategy is to ignore unsolicited requests, no matter how legitimate or enticing they appear.

Be careful how you connect to the internet

Only access the internet for banking or for other activities that involve personal information using your own devices through a known, trusted, and secure connection. A public computer like those found in hotels or a library, and free WiFi networks are not necessarily secure. It can be relatively easy for cyber criminals to intercept the internet traffic in these locations.

Be careful when using social networking sites

Cyber criminals use social networking sites to gather details about individuals, such as their place or date of birth, a pet's name, their mothers maiden name, and other information that can help them figure out passwords, or how to reset them. Don't share your 'page' or access to your information with anyone you don't trust or know. Cyber criminals may pretend to be your 'friend' to convince you to send money or divulge personal information.

Take precautions with your tablet or smartphone

Consider opting for automatic updates for your device's operating system and applications as soon as they become available to reduce software vulnerabilities. Never leave your device unattended and use a password or other security feature to restrict access if your device is lost or stolen. Make sure to enable an auto-lock or "time-out" feature that locks the device if left unused for a certain period of time. Research any 'app' before downloading it. Consult your financial institution's website to confirm where to download its official application.