Take precautions with your tablet or smartphone. Consider opting for automatic updates for your device's operating system and "apps" (applications) when they become available to help reduce your vulnerability to software problems. Never leave your mobile device unattended and use a password or other security feature to restrict access in case your device is lost or stolen. Make sure you enable the "time-out" or "auto-lock" feature that secures your mobile device when it is 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 mobile application.

Educate yourself. To learn more about cybersecurity, visit the "Stop. Think. Connect. Resource Guide" at www.stcguide.com/resource-index.

A message from the
Federal Deposit Insurance Corporation

FDIC-018-2016

A CYBERSECURITY GUIDE for Financial Institution Customers

Computer-related crimes affecting businesses and consumers are frequently in the news. While federally insured financial institutions are required to have vigorous information security programs to safeguard financial data, **financial institution customers also need to know how to steer clear of fraudsters.**

This guide, developed by the Federal Deposit Insurance Corporation, provides cybersecurity information for financial institutions' customers on how to protect and maintain their own computer systems.

Protect your computer. Install software that protects against malware, or 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 the settings allow for automatic updates.

Use the strongest method available to log into financial accounts. 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 combinations 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 in to other accounts.

Understand Internet safety features. You can have greater confidence that a website is authentic and that it encrypts (scrambles) 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 web browser's user instructions.

Be suspicious of unsolicited e-mails asking you to click on a link, download an attachment, or provide account information. It's 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 where and how you connect to the Internet. Only access the Internet for banking or for other activities that involve personal information using your own laptop or mobile device through a known, trusted, and secure connection. A public computer, such as at a hotel business center or public library, and free Wi-Fi 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 mother's 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 know and trust. Cyber criminals may pretend to be your 'friend' to convince you to send money or divulge personal information.