Computer Security Tips for Bank Customers

Computer-related crimes affecting businesses or consumers are frequently in the news. While federally insured financial institutions are required to have vigorous information security programs to safeguard financial data, consumers also need to know how to protect and maintain their computer systems so they can steer clear of fraudsters. Here is a short checklist.

1. Protect your computer. Install anti-virus software that scans your computer for malicious software ("malware") that can steal login IDs, passwords and account information (including credit or debit card numbers). Also use a firewall program to guard against unauthorized access to your computer. Anti-virus protection and firewall options vary, and some are free. Choose one, install it, and then set the software to update automatically.

2. Safeguard your smartphone, tablet and similar mobile devices, especially when using them for banking or shopping. Reduce your risk of downloading "apps" (applications) that contain malware by using well-known app stores, such as those established by your phone manufacturer or cellular service provider, or from the official Web site of the bank.
Also, to ensure that you have the latest fixes to software problems affecting mobile devices, opt for automatic updates for your operating system and apps or manually download updates as soon as you receive notice that they are available. Some banks provide customers with anti-malware software that can be loaded on a smartphone. You can also purchase the software from a reputable vendor.
And, don't leave your mobile device unattended. In case your device does get lost or stolen, use a password or other security feature to restrict access. You should enable the "time-out" or "auto-lock" feature on your mobile device to secure it when it's not used for a period of time. "Some phones have a remote feature that will allow you to erase all the personal information on your phone or disable it in the event that your phone is lost or stolen.

3. Understand your Internet safety features. When you are buying something online or filling out an application that contains sensitive personal information, you can have greater confidence in a Web site that encrypts or scrambles the information as it travels to and from your computer. Look for a padlock symbol on the page and a Web address that starts with "https://." The "s" stands for "secure."

4. Be careful where and how you connect to the Internet. A public computer, such as at an Internet café or hotel business center, may not have up-to-date security software and could be infected with malware. Also, for online banking or shopping, avoid connecting your computer, tablet or smartphone to a wireless network at a public "hotspot" (such as a coffee shop, hotel or airport).

5. Be suspicious of unsolicited e-mails and text messages asking you to click on a link or download an attachment. It's easy for fraudsters to copy corporate or government logos into fake e-mails that can install malware on your computer.
Ignore any unsolicited request for immediate action or personal information, no matter how genuine it looks. If you decide to validate the request by contacting the party that it is supposedly from, use a phone number or e-mail address that you have used before or otherwise know to be correct. Don't rely on the one provided in the e-mail.

6. Use "strong" IDs and passwords and keep them secret. Choose combinations of upper- and lower-case letters, numbers and symbols that are hard for a hacker to guess. Don't, for example, use your birthdate or address. Also don't use the same password for different accounts because a criminal who obtains one password can log in to other accounts. Finally, make sure to change your passwords on a regular basis.

7. Take precautions on social networking sites. Criminals can go there to gather details such as someone's date or place of birth, mother's maiden name or favorite pet and use that information to figure out and reset passwords. Fraudsters also may pretend to be your "friend" to persuade you to send money or divulge personal information.