Customer's Guide to Cybersecurity – Tips for Preventing Online Fraud and Theft

Protect Your "Cyber Home" With a Solid Foundation

Simple steps to secure your computers and mobile devices for Internet banking and shopping

Your home has locks on the doors and windows to protect your family and prevent thieves from stealing cash, electronics, jewelry and other physical possessions. But do you have deterrents to prevent the loss or theft of your electronic assets, including bank account and other information in your personal computers, at home and when banking or shopping remotely online?

"Think about all of the access points to and from your computer — such as Internet connections, email accounts and wireless networks," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "These always need to be protected. Otherwise, it's like leaving your front door wide open while you are away so that anyone could come in and take what they please."

Consider these strategies.

For Banking by Computer or Mobile Device

Take extra precautions for logging into bank and other financial accounts. These measures include using "strong" user IDs and passwords by choosing combinations of upper- and lower-case letters, numbers, and symbols that are hard for a hacker to guess. Don't use your birthdate, address or other words or numbers that can be easy for con artists to find out or guess. Don't use the same password for different accounts because a criminal who obtains one password can then log in to your other accounts. Keep your user IDs and passwords secret, and change them regularly. Make sure to log out of financial accounts when you complete your transactions or walk away from the computer.

Consider using a separate computer solely for online banking or shopping. A growing number of people are purchasing basic PCs and using them only for banking online and not Web browsing, emailing, social networking, playing games or other activities that are more susceptible to malicious software — known generally as "malware" — that can access computers and steal information. As an alternative, you can use an old PC for this limited purpose, but uninstall any software no longer needed and scan the entire PC to check for malicious software before proceeding.

Take precautions if you provide financial account information to third parties online. For example, some people use online "account aggregation" services that, from one website, can provide a convenient way to pay bills, monitor balances in deposits and investment accounts, and even keep track of your frequent flyer miles. While these websites may be beneficial, they can also present potential issues related to the security of the account information you have shared with them. If you want to use their services, thoroughly research the company behind the website, including making sure that you're dealing with a legitimate entity and not a fraudulent site. Also ask what protections the website offers if it experiences a data breach or loss of data.

Periodically check your bank accounts for signs of fraud. If you bank online, check your deposit accounts and lines of credit at regular intervals to spot and report errors or fraudulent transactions, just as you would review a paper statement. Online banking makes it easier and faster to monitor your accounts. This is important, because the sooner you can detect a problem with a transaction, the easier it should be to fix.

Federal laws generally limit your liability for unauthorized use of your debit, credit and prepaid cards, especially if you report the problem to your financial institution within specified time periods, which vary depending on the circumstances (see How Federal Laws and Industry Practices Limit Losses From Cyberattacks). A good rule of thumb is to check your accounts online once or twice a week. Also, many banks make it easier for customers to keep track of their accounts by offering email or text message alerts when balances fall below a certain level or when there is a transaction over a certain amount.

Basic Security Tips

Keep your software up to date. Software manufacturers continually update their products to fix vulnerabilities or security weaknesses when they find them. "All of your software should be checked and updated as generally recommended by the manufacturer or when flaws are found," explained Kathryn Weatherby, a fraud examination specialist for the FDIC. "This advice goes for everything from your operating system to your word processing software, Internet browsers, spreadsheet software, and even your digital photography applications. A vulnerability in one piece of software, no matter how insignificant it may seem, can be exploited by a hacker and used as a pathway into your whole computer."

Some software manufacturers may issue "patches" that you need to install to update a program. Others may simply provide you with a completely new version of the software. "Before installing any update you receive, make sure it is legitimate, especially if it is emailed to you," said Benardo. "Check the software manufacturer's website or contact the company directly to verify the update's validity. Criminals have been known to imitate software vendors providing a security update when, in fact, they are distributing malware. Once you confirm that an update is legitimate, install it as soon as possible to correct whatever security flaw might exist."

Install anti-virus software that prevents, detects and removes malicious programs. Crooks and computer hackers are always developing new malware that can access computers and steal information, such as account passwords or credit or debit card numbers. These programs also may be able to destroy data from the infected computer's hard drive.

Malware can enter your computer in a variety of ways, perhaps as an attachment to an email, a downloaded file from an infected website, or from a contaminated thumb drive or disk. Fight back by installing anti-virus software that periodically runs in the background of your computer to search for and remove malware. Also be sure to set the software to update automatically so that it can protect you from the latest malware. See Beware of Malware: Think Before You Click! for more information.

Use a firewall program to prevent unauthorized access to your PC. A firewall is a combination of hardware and software that establishes a barrier between your personal computer and an external network, such as the Internet, and then monitors and controls incoming and outgoing network traffic. In simple terms, a firewall acts as a gatekeeper that helps screen out hackers, malware and other intruders who try to access your computer from the Internet.

Only use security products from reputable companies. Some anti-virus software and firewalls can be purchased, while others are available free. Either way, it's a good idea to check out these products by reading reviews from computer and consumer publications. Look for products that have high ratings for detecting problems and for providing tech support if your computer becomes infected. Other ways to select the right protection products for your computer are to consult with the manufacturer of your computer or operating system, or to ask someone you know who is a computer expert.

Take advantage of Internet safety features. When you are banking online, shopping on the Internet or filling out an application that requests sensitive personal information such as credit card, debit card and bank account numbers, make sure you are doing business with reputable companies. You also can have greater confidence in a website that encrypts (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."

Also, current versions of most popular Internet browsers and search engines often will indicate if you are visiting a suspicious website or a page that cannot be verified as trusted. It's best not to continue on to pages with these kinds of warnings. Review your Internet browser's user instructions and explore the "tools" and "help" tabs to learn more about the security settings and alerts offered.

Be careful where and how you connect to the Internet. A public computer, such as at an Internet café or a hotel business center, may not have up-to-date security software and could be infected with malware. Similarly, if you are using a portable computer (such as a laptop or mobile device) for online banking or shopping, avoid connecting it to a wireless (Wi-Fi) network at a public "hotspot" such as a coffee shop, hotel or airport. Wi-Fi in public areas can be used by criminals to intercept your device's signals and as a collection point for personal information.

The bottom line, especially for sensitive matters such as online banking and activities that involve personal information, is to consider only accessing the Internet using your own computer with a secure, trusted connection, and to only connect laptops and mobile devices to trusted networks.

For more tips on computer and Internet security for bank customers, watch the FDIC's multimedia presentation "Don't Be an Online Victim: How to Guard Against Internet Thieves and Electronic Scams." Also, visit www.onguardonline.gov/ for information from the federal government on how to be safe online. The site includes videos from the Federal Trade Commission on what to do if your email is hacked or if malware attacks your computer.

Going Mobile: How to be Safer When Using a Smartphone or Tablet

Everywhere you look, people are using smartphones and tablets as portable, hand-held computers. "Unfortunately, cybercriminals are also interested in using or accessing these devices to steal information or commit other crimes," said Michael Benardo, manager of the FDIC's Cyber Fraud and Financial Crimes Section. "That makes it essential for users of mobile devices to take measures to secure them, just as they would a desktop computer."

Here are some basic steps you can take to secure your mobile devices.

Avoid apps that may contain malware. Buy or download from well-known app stores, such as those established by your phone manufacturer or cellular service provider. Consult your financial institution's website to confirm where to download its official app for mobile banking.

Keep your device's operating system and apps updated. Consider opting for automatic updates because doing so will ensure that you have the latest fixes for any security weaknesses the manufacturer discovers. "Cybercriminals try to take advantage of known flaws, so keeping your software up to date will help reduce your vulnerability to foul play," said Robert Brown, a senior ombudsman specialist at the FDIC.

Consider using mobile security software and apps to protect your device. For example, anti-malware software for smartphones and tablets can be purchased from a reputable vendor.

Use a password or other security feature to restrict access in case your device is lost or stolen. Activate the "time out" or "auto lock" feature that secures your mobile device when it is left unused for a certain number of minutes. Set that security feature to start after a relatively brief period of inactivity. Doing so reduces the likelihood that a thief will be able to use your phone or tablet.

Back up data on your smartphone or tablet. This is good to do in case your device is lost, stolen or just stops working one day. Data can easily be backed up to a computer or to a back-up service, which may be offered by your mobile carrier.

Have the ability to remotely remove data from your device if it is lost or stolen. A "remote wipe" protects data from prying eyes. If the device has been backed up, the information can be restored on a replacement device or the original (if you get it back). A number of reputable apps can enable remote wiping.

To learn more about safely using smartphones and tablets, see the Federal Trade Commission's Computer Security Web page.

Cybersecurity for Small Businesses: Ways to Stay Protected

In today's world, it's important for small business owners to be vigilant in protecting their computer systems and data. Among the reasons: Federal consumer protections generally do not cover businesses for losses they incur from unauthorized electronic fund transfers. That means, for example, your bank may not be responsible for reimbursing losses associated with an electronic theft from your bank account — for instance, if there was negligence on the part of your business, such as unsecured computers or falling for common scams. (To learn more about the rules pertaining to electronic theft, including losses involving a business debit card, see How Federal Laws and Industry Practices Limit Losses From Cyberattacks).

Here are tips to help small business owners and their employees protect themselves and their companies from losses and other harm. Several of these tips mirror basic precautions we have suggested elsewhere in this issue for consumers.

Protect computers and Wi-Fi networks. Equip your computers with up-to-date anti-virus software and firewalls to block unwanted access. Arrange for key security software to automatically update, if possible. And if you have a Wi-Fi network for your workplace, make sure it is secure, including having the router protected by a password that is set by you (not the default password). The user manual for your device can give you instructions, which are also generally available online.

Patch software in a timely manner. Software vendors regularly provide "patches" or updates to their products to correct security flaws and improve functionality. A good practice is to download and install these software updates as soon as they are available. It may be most efficient to configure software to install such updates automatically.

Set cybersecurity procedures and training for employees. Consider reducing risks through steps such as pre-employment background checks and clearly outlined policies for personal use of computers. Limit employee access to the data systems that they need for their jobs, and require permission to install any software.

And, train employees about cybersecurity issues, such as suspicious or unsolicited emails asking them to click on a link, open an attachment or provide account information. By complying with what appears to be a simple request, your employees may be installing malware on your network. You can use training resources such as a 30-minute online course from the Small Business Administration (SBA).

Require strong authentication. Ensure that employees and other users connecting to your network use strong user IDs and passwords for computers, mobile devices and online accounts by using combinations of upper- and lower-case letters, numbers and symbols that are hard to guess and changed regularly. Consider requiring more information beyond a password to gain access to your business's network, and additional safety measures, such as requiring confirmation calls with your financial institution before certain electronic transfers are authorized.

Secure the business's tablets and smartphones. Mobile devices can be a source of security challenges, especially if they hold confidential information or can access your company's network. In the case of the latter, require employees to password-protect their devices, encrypt their data and install security apps to prevent criminals from accessing the device while it is connected to public networks. Also develop and enforce reporting procedures for lost or stolen equipment.

Back up important business systems and data. Do so at least once a week. For your backup data, remember to use the same security measures (such as encryption) that you would apply to the original data. In addition, in case your main computer becomes infected, regularly back up sensitive business data to additional, disconnected storage devices.

Use best practices for handling card payments online. Seek advice from your bank or a payment processor to select the most trusted and validated tools and anti-fraud services. This may include using just one computer or tablet for payment processing.

Be vigilant for early signs something is wrong. "Monitor bank account balances regularly to look for suspicious or unauthorized activity," suggested Luke W. Reynolds, chief of the FDIC's Outreach and Program Development Section.

Cybersecurity tips for small businesses also can be found in a new FDIC brochure. Also go to OnGuardOnline and the SBA website.