Cybersecurity Safety Tips for Consumers

TN Department of Financial Institutions

September 2022

Table Of Contents

Security Best Practices

The following tips are considered best practices regardless of the media you are using to connect to the internet:

Update your software. Software updates are important for all your devices, as they fix flaws (vulnerabilities) within the software code that hackers can potentially exploit to gain access or steal personal and/or financial information. Therefore, when the vendor issues an update, it should be installed as soon as possible. Additionally, adjust settings on your personal device to permit automatic updates to the software. This includes apps, web browsers, and operating systems (OSs).

Install and use antivirus software. Installing an antivirus software program and keeping it up to date is a critical step in protecting your computer. Many types of antivirus software can detect the presence of malware by searching for patterns in your computer's files or memory. Antivirus software uses signatures provided by software vendors to identify malware. Vendors frequently create new signatures to ensure their software is effective against newly discovered malware.

Remove unnecessary software. Intruders can attack your computer by exploiting software vulnerabilities, so the fewer software programs you have installed, the fewer avenues there are for potential attack. Review the software installed on all your devices. If you do not know what a software program does, research the program to determine whether or not the program is necessary. Remove any software you feel is not necessary after confirming it is safe to remove. This includes apps on your mobile devices.

Back up important files and data before removing unnecessary software to prevent accidentally removing programs that turn out to be essential to your OS. If possible, locate the installation media (e.g., CD) for the software in case you need to reinstall it.

Backup your files. Creating backup files offline for all your devices to an external hard drive or to the cloud can help prevent loss of personal or business information due to theft, loss, or destruction of a device.

Use strong passwords. Use strong passwords or passphrases for laptops, desktops, tablets, and smartphones. Instead of using just a password, passphrases allow more variation and are less likely to be guessed by unauthorized users. Passphrases are typically at least 16 characters long, separated with spaces or dashes and are somewhat complex. Not only are passphrases much more secure, they are typically easier to remember. An example of a passphrase is: "***I own 2 cars and 1 truck!***" Use the strongest, longest password or passphrase permitted. Do not use passwords that can be easily guessed, like your own birthday (or those close to you) or names of children or pets. Additionally, it is good practice to change your passwords every 90 days. This is especially important for passwords linked to financial accounts.

Do not use the same password. Use different passwords for different accounts. By using the same password for multiple accounts, you run the risk of an attacker compromising multiple accounts, not just one. If you have several passwords and have trouble remembering which password goes with which account, consider using a password manager to securely store and remember your passwords. (What is a password manager?)

Encrypt devices. Encrypting files on your devices (e.g., smartphones, tablets, laptops, desktops) that have sensitive or personal information ensures that unauthorized parties cannot read your files, even if they physically possess the device. (What is data encryption?)

Use multi-factor authentication. When available, use multi-factor authentication as an additional security safeguard for protecting your personal information. Most financial, email, and social media websites/applications offer this additional security feature. (Why aren't passwords sufficient?)

In addition to the above security best practices, the following tips are specific to the topics addressed below.

Home Network

Secure your router. Change the default password and name; turn off remote management, and logout as the administrator.

Enable and configure your firewall. A firewall is a device that controls the flow of information between your computer and the internet. Most modern operating systems include a software firewall. The majority of home routers also have a built-in firewall. Refer to your router's user guide for instructions on how to enable your firewall and configure the security settings. Set a strong password/passphrase to protect your firewall against unwanted changes.

Secure your wireless network. When setting up a wireless network connection, ensure you are using at least WPA2 encryption. Other wireless encryption standards, such as WEP and WPA, are known to be less secure and vulnerable to several different known attacks. (Securing Wireless Networks).

Modify unnecessary default features. Removing unnecessary software, modifying and/or deleting unnecessary default features reduces attackers' opportunities. Review the features that are enabled by default on your computer and disable or customize those you do not need or do not plan on using. As with removing unnecessary software, be sure to research features before modifying or disabling them.

Operate under the principle of least privilege. In most instances of malware infection, the malware can operate only using the privileges of the logged-in user. To minimize the impact of a malware infection, consider using a standard or restricted user account (i.e., a non-administrator account) for day-to-day activities. Only log in with an administrator account—which has full operating privileges on the system—when you need to install or remove software or change your computer's system settings.

Mobile Devices

Avoid Using Public Wi-Fi Networks. If possible, avoid using public Wi-Fi hotspots at airports, restaurants, hotels, and other public locations, as these networks can be opportunities for cyber criminals to steal personal or financial information. This is especially true when conducting business or personal transactions involving financial and/or sensitive information.

If you must use a public Wi-Fi hotspot, then consider using a virtual private network (VPN) app that encrypts your information from potential eaves dropping.

Do not leave your mobile device unattended. When in public areas, do not leave your mobile device unattended. This makes access to your device easier for cyber criminals.

Use a device manager to locate, lock, and wipe a lost mobile device. Consider using an app that gives you the ability to locate, lock, and wipe a lost or stolen device. This will limit the ability of a cybercriminal to access personal information on your mobile device.

Turn Bluetooth off when not in use. Bluetooth and other wireless technologies should be turned off when not in use to prevent Bluejacking and other malicious techniques that allow unauthorized access to your device.

Think before you buy an app. Always purchase apps from reputable vendors to avoid malware that could compromise your mobile device. Additionally, when choosing an app, make sure it does not request excess permissions from your device. You may want to reconsider installing an app that requests access to your contacts, pictures, or other private information.

Online Banking

Do not use public computers to conduct online banking transactions. Public computers (e.g., hotel business centers, libraries, internet cafes, etc.) are more susceptible to tampering and increase the likelihood of exposing your financial information to undo risk. Also, default settings on public computers may save your browsing history and passwords making them accessible to the next user. If you must use a public computer, always remember to clear your browsing history, cache history, and close the browser window before ending your session.

Keep personal information personal. Do not disclose personal information to anyone. In addition, financial institutions will never call or email you and ask for personal information. If you get a call or email from someone asking for personal information and claiming to be from your financial institution, cut off communication and call or go to the bank to confirm the validity of the issue.

Use the financial institution's official online banking address when accessing your account. Never click a link in an email or text to access your online banking website, as cybercriminals have the ability to make malicious links look legitimate. Always take time to type in the official online banking address in the address bar of your web browser.

Always close out your web browser after an online banking session. Remember to close out your web browser after every online banking session to reduce session hijacking and cross-site scripting.

Set up account notifications. Most financial institutions offer some sort of notification options tied to changes in account balances and transactions made. Use these options (if available) to monitor your account for potentially fraudulent transactions and/or error.

Regularly check your online account balances. On a regular basis, consumers should check their online bank account balances and transactions for accuracy.

Person-to-Person Mobile Payments (P2P)

Research P2P payment options. Not all P2P payment apps are the same. Conduct your own research and make sure you are comfortable with the level of security employed and features offered. A simple internet search should provide enough information to make an educated decision.

Only download legitimate P2P payment apps. To ensure you are downloading a legitimate P2P app, only download from trusted sources.

Change the default security settings. Most P2P payment apps have default security settings, which may be less secure. Review default security settings and make sure you are using the highest-level security allowable.

Enable notifications. Always enable transaction and account modification notifications in the settings on the P2P app. This allows you to monitor your account for potentially fraudulent activity and/or errors.

Review the apps terms of service. Always review the P2P apps terms of service to ensure there are sufficient avenues to settle disputes and detail how your information is used.

Protect your P2P app with a PIN. Not all P2P apps have the option to set PIN, but if they do, take advantage of this option. Setting a PIN if your device is lost or stolen makes it more difficult for someone to access your payment app.

Make your account private. Several P2P apps give the user the option to link activity to social networks. Disabling this feature will prevent others from following your activity.

Only send/receive money from trusted people. Some people use P2P apps to purchase and sell items from person to person. Do not use a P2P app to purchase or sell an item with someone you do not know, as scammers can take advantage of P2P apps, resulting in fraudulent transactions.

Use a P2P app that insures your account funds. When possible, use a P2P app that ensures the funds in your account, like an FDIC insured bank or NCUA insured credit union.

Double check recipient information. When sending funds using a P2P app, make sure you double check the recipient information (e.g., username, phone number, or other identifier) as it is nearly impossible to get funds back if they are sent to the wrong recipient. In addition, use a QR code (when available) to ensure your money was sent to the correct recipient.

Online Shopping

Use recognizable and trustworthy websites. Prior to providing any personal or financial information, ensure you are doing business with a legitimate, trustworthy business. Cybercriminals can often create malicious e-commerce sites that look legitimate but are actually used to steal personal and/or financial information. (See Understanding Web Site Certificates)

Look for the "Lock" icon. To ensure the information you are sending is being encrypted look for the padlock icon 🔒 and an address that begins with "http**s**" instead of just "http." The "s" indicates the information is being encrypted using secure socket layer (SSL).

Personal information should stay personal. Online businesses only need basic payment information to complete a purchase. Never provide your social security number and/or date of birth to complete an online purchase. (See Avoiding Social Engineering and Phishing Attacks and Recognizing and Avoiding Email Scams)

Use a credit card for online purchases. Laws limit your liability regarding fraudulent purchases when using a credit card. Typically, debit cards do not offer the same level of protection and can result in nonsufficient fund fees and other charges if the fraudulent purchase results in an overdrawn bank account.

Keep records. Always keep records of your online transactions and compare them to your monthly statements. If a discrepancy exists, then report it immediately. (See Identity Theft Reporting)

Social Media

Think before you post. Status updates, comments, and pictures can divulge more information than you might intend. For example, posting vacation pictures while on vacation could let a criminal know you are not home and they could break in your house.

Be wary of completing social media surveys. Many of these "fun" surveys are actually tools criminals use to find out personal information about you. They can take the answers and guess usernames, passwords, and security questions to online accounts.

Know your privacy settings. Review your privacy settings and ensure you are using the most secure options. In addition, reviewing privacy settings occasionally for changes in policies will make you aware of any changes that could leave you less secure.

Beware of links that sound suspicious or seem too good to be true. Example – "Your grandson is in jail. Please send money immediately to XXX" or "You just won $10,000! Click here to claim your prize."

Update your browser. Make sure your web browser is up to date. Older versions of website browsers can have flaws (vulnerabilities) that can allow criminals to steal your information.

Use the block button. If you are getting requests from an illegitimate profile(s), use the block button and report them to spam abuse on that social media platform.

Email Safety Tips

Use caution with email attachments and untrugsted links. Malware is commonly spread by users clicking on a malicious email attachment or a link. Do not open attachments or click on links unless you are certain they are safe, even if they come from a person you know. Be especially wary of attachments with sensational names, emails that contain misspellings or emails that try to entice you into clicking on a link or attachment (e.g., an email with a subject that reads, "You won't believe this picture of you I saw on the internet!").

Use caution when providing your information. Emails that appear to come from a legitimate source and websites that appear to be legitimate may be malicious. An example is an email claiming to be sent from a system administrator requesting your password or other sensitive information or directing you to a website that requests your information. Online services (e.g., banking, ISPs, retailers) may request that you change your password, but they will never specify what you should change it to or ask you what it is. If you receive an email asking you to change your password, visit the site yourself instead of clicking on any link provided in the email. Using your mouse, you can hover over the link (not clicking it) and it will show the actual address of the site instead of what a cybercriminal has disguised it as.

Online and Mobile Banking Account Outages

In today's world of technology, consumers are utilizing online and mobile banking applications to perform financial transactions at an ever-increasing rate. As with any technology, there may be times when an outage of some sort affects one's ability to perform day-to-day financial transactions. If this does happen, below are a few helpful hints to decrease this inconvenience.

Be prepared. Always have a small amount of cash on hand for emergency situations.

How to check your bank balance. If you cannot access your account financial institution balance online, call or drive to a branch location, as they should be able to provide you with basic information regarding your account(s) balance before the issue occurred.

Get cash. It may be possible, for tellers at your institution to accept a limited number of deposits and withdrawals, if you drive to a branch.

Watch out for fraud. Be aware of scammers or fraudsters who could contact you and claim to be from your financial institution. Never give out personal or financial information over the phone. If someone claiming to be from a financial institution contacts you, hang up and contact the institution through a published phone number.

Check your account records. After the outage is corrected, review your account information to make certain there have not been any unauthorized or fraudulent transactions.

Tips for the Elderly

Get familiar. Being educated on computer basics can greatly reduce the risk of being a victim of an online scam or fraud.

Personal information should stay personal. Online businesses only need basic payment information to complete a purchase. Never provide your financial information, social security number and/or date of birth over the phone or to complete an online transaction.

Use recognizable and trustworthy websites. Visit known and trustworthy websites and avoid unfamiliar websites, which may have programs that take personal information even without consent. Prior to providing any personal or financial information, ensure you are doing business with a legitimate, trustworthy business.

Avoid opening e-mails from unknown senders. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.

Only talk to individuals you know. Use telephones with caller identification and talk to only known individuals.

Avoid making charitable contributions over the telephone. Search online for the contact information (name, email, phone number, addresses) and the proposed offer. Other people have likely posted information online about individuals and businesses trying to run scams.

Resist the pressure to act quickly. Scammers create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.

Disconnect and shut down. Disconnect from the internet and shut down your device if you see a pop-up message or locked screen. Pop-ups are regularly used by perpetrators to spread malicious software. Enable pop-up blockers to avoid accidentally clicking on a pop-up.

Take precautions. Protect your identity if a criminal gains access to your device or account. Immediately contact your financial institutions to place protections on your accounts and monitor your accounts and personal information for suspicious activity.

Helpful Links

1. http://passfault.com/
2. https://www.ftc.gov/
3. https://www.fcc.gov/
4. https://www.us-cert.gov/
5. https://www.consumerreports.org/cro/index.htm
6. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud

TN Department of Financial Institutions

Cybersecurity Safety Tips for Consumers

The Tennessee Department of Financial Institutions has made this document available for the purpose of raising awareness regarding cyber security issues and this document should not be considered or relied upon as legal advice. The information contained in this document is compiled from various sources and the Department does not assume any responsibility for the accuracy or completeness of this information as it might pertain to specific circumstances. Readers are encouraged to conduct their own research and evaluation to assess their specific situations and needs.