As more daily tasks, from shopping and banking to working and socializing, get done on a computer or mobile device, the opportunities to expose your personal data increase.

While many security measures enhance the safety of digital transactions, online and mobile consumers may still face privacy risks. An open Wi-Fi connection, a lost smartphone or an accidentally revealed password are just a few of the ways your information could get out without your permission. Fortunately, there are many tips and tools to help you make safe and secure transactions online and on the go.

Why is online and mobile security important?
While the internet and mobile technology have improved our lives in many ways, they also have created new ways for consumers’ personal information to be stolen, unintentionally revealed, or misused. For example, an identity thief anywhere in the world could steal your identity by luring you to a fraudulent website that tricks you into revealing your password. A lost or stolen smartphone full of stored passwords and account information could pose more risk than a missing wallet.

If your information is given to third parties by a website you’ve visited, you could receive frequent (and perhaps annoying) marketing emails (spam), or even unauthorized charges. The good news is, you can avoid these and other potential problems by being cautious and staying informed.

Tips for protecting your privacy
One of the best ways to protect your personal data is to deal only with financial institutions, merchants, app developers and others who work hard to protect the security and privacy of their customers and website visitors. When considering a company, product, or service, look for:

- **Legitimacy:** A fancy website doesn’t make a business legitimate. If you or someone you know is not familiar with a company’s reputation, check its authenticity, customer satisfaction rating and complaint history through an online search. Verify information and claims (for example, call the phone number listed).

- **Encryption:** A closed padlock or unbroken key in the browser frame and an “s” after “http” (“https://”) in the website address indicate that the site is secure and encrypted. (This means the information is being sent in a format that only the intended recipient can read.) Logos from companies such as VeriSign and McAfee signify that a website uses encryption or other security technology to protect your data. Click on the logos for more information about the site.

- **Manage your cookies.** Cookies are small files stored on your computer by websites you visit. They track your activity while online and are used to target marketing efforts, but it also is used for things like remembering items in your shopping cart and recognizing you as a repeat visitor. You can set your browser to delete cookies automatically whenever you exit, or to not accept cookies at all. Instead, consider enabling or disabling cookies on a site-by-site basis. Check the Help section of your browser for more.

- **A zero liability policy:** This guarantees you won’t owe anything as a result of unauthorized activity, and that any money taken from your account will be replaced.

- **A privacy policy:** This explains how customers’ personal information is collected, used and stored, should be clearly posted on the company’s website. Ideally, it should state that the company won’t share your information with third parties (unaffiliated individuals or organizations). If not, you should be able to easily “opt out” of having your information shared. Logos from organizations such as TRUSTe or BBBOnline signify a trustworthy or reasonably strong privacy policy. (Click on the seal to verify that it’s legitimate—the address that appears should match the address of the official certifying company website.) Look for a privacy policy if you are not satisfied that your privacy will be protected.

- **A privacy policy:** A site that automatically ends your session or when stepping away from the computer without logging off or closing the browser window. Another good sign is a login that requires authentication, such as a code sent to your phone that you must enter or a question you must answer in addition to your username and password. An app should require either a passcode or a biometric scan (your fingerprint or facial recognition).

- ** axlewrap:** A site that automatically ends your session or when stepping away from the computer without logging off or closing the browser window. Another good sign is a login that requires authentication, such as a code sent to your phone that you must enter or a question you must answer in addition to your username and password. An app should require either a passcode or a biometric scan (your fingerprint or facial recognition).

- **Protect your passwords.** Create strong passwords for your computer, mobile device, accounts and apps and don’t reveal them to anyone. Never save your password on sites with your login information or include it in email messages with your credit card on file. While it’s a hassle, consider entering your payment card number each time you make a purchase instead of allowing the merchant to save it. Instead, consider enabling or disabling cookies on a site-by-site basis. Check the Help section of your browser for more.

- **Log out.** Never leave your computer or mobile device unattended while logged on to a banking or payment site or app. Sign out and close the app or browser window when finished. Do not leave your computer or mobile device sitting on top of a desk, away from your screen. If using a shared or public computer, clear your browsing history by clicking on the Tools menu (in most browsers) and selecting “Delete Browsing History” or “Clear Private Data.”

- **Extra security features:** A site that automatically ends your session or after a certain period of inactivity is an example of an extra measure of security. This prevents someone from accessing your account if you walk away from the computer without logging off or closing the browser window. Another good sign is a login that requires authentication, such as a code sent to your phone that you must enter or a question you must answer in addition to your username and password. An app should require either a passcode or a biometric scan (your fingerprint or facial recognition).

- **Managing online transactions.** As more daily tasks, from shopping and banking to working and socializing, get done on a computer or mobile device, the opportunities to expose your personal data increase.
Don’t send sensitive data by email. Don’t send personal information such as credit card numbers, passwords, your birth date or your Social Security number by email. Instead, log in to the company’s website. Most companies that deal with sensitive information allow logged-in users to send secure mail to customer service and to receive an answer via the site.

Check website security. Verify that “https://” (not just “http://”) is in the browser’s address bar. All legitimate finance and retail websites use this SSL (Secure Sockets Layer) encryption to make it safe to bank or pay online.

Lock your wireless network. Leaving your wireless network “unlocked” means that anyone within range of your Wi-Fi signal can access it and possibly capture the data you send and receive on an unencrypted site. To secure your wireless network, password-protect your router.

Avoid shopping or banking in a public Wi-Fi hotspot. Wait until you’re in your home Wi-Fi network to access sensitive accounts. If that’s not possible, access your accounts using your data service rather than public Wi-Fi. If using public Wi-Fi is unavoidable, make sure you are at a secure site (https://), disable file sharing, and use a VPN (virtual private network).

Use a digital or mobile wallet. A digital wallet (e-wallet) or mobile wallet service, such as Venmo, Apple Pay, Zelle, etc., allows you to make purchases online or via an app without having to enter credit card numbers or other payment information. The purchase is charged to your secure account rather than directly to your credit card.

Do business only with individuals and companies you trust. Verify the authenticity of any business that is new to you (e.g., by checking their satisfaction ratings) of any business that is new to you before you submit personal or payment information. You can get a lot of information through a simple online search for the company’s name.

Use a pre-registered account. Some credit card issuers offer the option for you to set up an email and/or text alerts notifying you of unusual account activity. If you choose to receive such alerts, be wary of fraudulent (phishing) messages designed to look like legitimate alerts.

Be on guard for fraudulent communications. If you doubt the authenticity of an email message, text message or phone call, don’t respond. Contact the company directly to verify. Legitimate businesses never contact you to ask for your Social Security number, username, password or other sensitive data. If you fall for a “phishing” email and recognize your mistake, immediately change the password on your account and notify the institution where you have the account. Take advantage of spam and phishing filters in your email service. Always type in the web address of the site you want to visit rather than clicking on a link in an email, which could lead you to a bogus site.

Guard against malware. Use antivirus and antispyware and make sure they are updated regularly to avoid malicious software that can steal your information while you’re online. Enable your computer’s built-in firewall to create a virtual barrier between you and the internet.

Delete old banking and transaction text messages. Old text messages that contain account balance or other private information should be deleted from your phone and synced devices.

Protect your device. Since smartphones can store a great deal of sensitive information and are easily lost or stolen, it makes sense to put extra effort into protecting them. Use a password to lock the phone when it’s not in use, and set the phone to lock after a certain number of minutes of being idle.

Prevent your hard drive. Before selling, donating or disposing of your computer or mobile device, be sure to erase its hard drive. This entails more than just deleting files. Find instructions for “wiping” your smartphone at the manufacturer’s website, or contact your wireless carrier for help. If your employer provided the phone or computer, contact the person on staff who is in charge of technical issues. Be aware that your employer may have the right to access information stored on company-owned devices.

Sign up for account alerts. Most banks, credit card issuers, online payment platforms and other financial account providers offer the option for you to set up email and/or text alerts notifying you of unusual account activity. If you choose to receive such alerts, be wary of fraudulent (phishing) messages designed to look like legitimate alerts.

Enable a computer’s built-in firewall to create a virtual barrier between you and the internet.

Don’t send sensitive data by email. Don’t send personal information such as credit card numbers, passwords, your birth date or your Social Security number by email. Instead, log in to the company’s website. Most companies that deal with sensitive information allow logged-in users to send secure mail to customer service and to receive an answer via the site.

Check website security. Verify that “https://” (not just “http://”) is in the browser’s address bar. All legitimate finance and retail websites use this SSL (Secure Sockets Layer) encryption to make it safe to bank or pay online.

Lock your wireless network. Leaving your wireless network “unlocked” means that anyone within range of your Wi-Fi signal can access it and possibly capture the data you send and receive on an unencrypted site. To secure your wireless network, password-protect your router.

Avoid shopping or banking in a public Wi-Fi hotspot. Wait until you’re in your home Wi-Fi network to access sensitive accounts. If that’s not possible, access your accounts using your data service rather than public Wi-Fi. If using public Wi-Fi is unavoidable, make sure you are at a secure site (https://), disable file sharing, and use a VPN (virtual private network).

Use a digital or mobile wallet. A digital wallet (e-wallet) or mobile wallet service, such as Venmo, Apple Pay, Zelle, etc., allows you to make purchases online or via an app without having to enter credit card numbers or other payment information. The purchase is charged to your secure account rather than directly to your credit card.

Do business only with individuals and companies you trust. Verify the authenticity of any business that is new to you (e.g., by checking their satisfaction ratings) of any business that is new to you before you submit personal or payment information. You can get a lot of information through a simple online search for the company’s name.

Use a pre-registered account. Some credit card issuers offer the option for you to set up an email and/or text alerts notifying you of unusual account activity. If you choose to receive such alerts, be wary of fraudulent (phishing) messages designed to look like legitimate alerts.

Be on guard for fraudulent communications. If you doubt the authenticity of an email message, text message or phone call, don’t respond. Contact the company directly to verify. Legitimate businesses never contact you to ask for your Social Security number, username, password or other sensitive data. If you fall for a “phishing” email and recognize your mistake, immediately change the password on your account and notify the institution where you have the account. Take advantage of spam and phishing filters in your email service. Always type in the web address of the site you want to visit rather than clicking on a link in an email, which could lead you to a bogus site.

Guard against malware. Use antivirus and antispyware and make sure they are updated regularly to avoid malicious software that can steal your information while you’re online. Enable your computer’s built-in firewall to create a virtual barrier between you and the internet.

Delete old banking and transaction text messages. Old text messages that contain account balance or other private information should be deleted from your phone and synced devices.

Protect your device. Since smartphones can store a great deal of sensitive information and are easily lost or stolen, it makes sense to put extra effort into protecting them. Use a password to lock the phone when it’s not in use, and set the phone to lock after a certain number of minutes of being idle.

Prevent your hard drive. Before selling, donating or disposing of your computer or mobile device, be sure to erase its hard drive. This entails more than just deleting files. Find instructions for “wiping” your smartphone at the manufacturer’s website, or contact your wireless carrier for help. If your employer provided the phone or computer, contact the person on staff who is in charge of technical issues. Be aware that your employer may have the right to access information stored on company-owned devices.

Sign up for account alerts. Most banks, credit card issuers, online payment platforms and other financial account providers offer the option for you to set up email and/or text alerts notifying you of unusual account activity. If you choose to receive such alerts, be wary of fraudulent (phishing) messages designed to look like legitimate alerts.

Enable a computer’s built-in firewall to create a virtual barrier between you and the internet.

Don’t send sensitive data by email. Don’t send personal information such as credit card numbers, passwords, your birth date or your Social Security number by email. Instead, log in to the company’s website. Most companies that deal with sensitive information allow logged-in users to send secure mail to customer service and to receive an answer via the site.

Check website security. Verify that “https://” (not just “http://”) is in the browser’s address bar. All legitimate finance and retail websites use this SSL (Secure Sockets Layer) encryption to make it safe to bank or pay online.

Lock your wireless network. Leaving your wireless network “unlocked” means that anyone within range of your Wi-Fi signal can access it and possibly capture the data you send and receive on an unencrypted site. To secure your wireless network, password-protect your router.

Avoid shopping or banking in a public Wi-Fi hotspot. Wait until you’re in your home Wi-Fi network to access sensitive accounts. If that’s not possible, access your accounts using your data service rather than public Wi-Fi. If using public Wi-Fi is unavoidable, make sure you are at a secure site (https://), disable file sharing, and use a VPN (virtual private network).

Use a digital or mobile wallet. A digital wallet (e-wallet) or mobile wallet service, such as Venmo, Apple Pay, Zelle, etc., allows you to make purchases online or via an app without having to enter credit card numbers or other payment information. The purchase is charged to your secure account rather than directly to your credit card.

Do business only with individuals and companies you trust. Verify the authenticity of any business that is new to you (e.g., by checking their satisfaction ratings) of any business that is new to you before you submit personal or payment information. You can get a lot of information through a simple online search for the company’s name.

Use a pre-registered account. Some credit card issuers offer the option for you to set up an email and/or text alerts notifying you of unusual account activity. If you choose to receive such alerts, be wary of fraudulent (phishing) messages designed to look like legitimate alerts.

Be on guard for fraudulent communications. If you doubt the authenticity of an email message, text message or phone call, don’t respond. Contact the company directly to verify. Legitimate businesses never contact you to ask for your Social Security number, username, password or other sensitive data. If you fall for a “phishing” email and recognize your mistake, immediately change the password on your account and notify the institution where you have the account. Take advantage of spam and phishing filters in your email service. Always type in the web address of the site you want to visit rather than clicking on a link in an email, which could lead you to a bogus site.

Guard against malware. Use antivirus and antispyware and make sure they are updated regularly to avoid malicious software that can steal your information while you’re online. Enable your computer’s built-in firewall to create a virtual barrier between you and the internet.

Delete old banking and transaction text messages. Old text messages that contain account balance or other private information should be deleted from your phone and synced devices.

Protect your device. Since smartphones can store a great deal of sensitive information and are easily lost or stolen, it makes sense to put extra effort into protecting them. Use a password to lock the phone when it’s not in use, and set the phone to lock after a certain number of minutes of being idle.

Prevent your hard drive. Before selling, donating or disposing of your computer or mobile device, be sure to erase its hard drive. This entails more than just deleting files. Find instructions for “wiping” your smartphone at the manufacturer’s website, or contact your wireless carrier for help. If your employer provided the phone or computer, contact the person on staff who is in charge of technical issues. Be aware that your employer may have the right to access information stored on company-owned devices.