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 personal information 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. And if your information is sold 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.

Risks for online and mobile consumers

Everyone runs the risk of having a piece of mail intercepted or a confidential conversation overheard. But if you bank or make payments online or by mobile device, you should be aware of some other ways your privacy could be violated.

- Someone who ends up with your lost or stolen computer or phone could be able to access your personal data, account numbers and payment information.
- Someone could intercept the information you send and receive over a wireless network.
- A scammer could trick you into entering your private information on a spoof (copycat) website or responding to a bogus email request (phishing).
- A data breach (the theft or unintentional release of information held in an institution's database) could result in your and other customers' information landing in the hands of an identity thief.
- Someone you know could access your accounts by guessing or discovering your password. Or, your saved usernames and passwords on a shared computer or unprotected mobile device could give a key to intruders.
- Your computer or mobile device could be infected by spyware or other malware capable of stealing your data.
- Your information, gathered by a business, could be sold or given to one or more third parties for marketing or other purposes. (There even have been cases of sharing payment card information between businesses, resulting in unauthorized charges.)

What to look for in providers and products

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 or trustworthy. If you're 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 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.
- ***Extra security features:*** A site that automatically ends your banking session 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 out or closing the browser window. Another good sign is a login that requires two-factor authentication, such as a code sent to you 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 thumbprint or facial recognition).
- ***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 strong privacy policy:*** A privacy policy, which 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.) Leave the site if you are not satisfied that your privacy will be protected.

The collection of consumer information is not necessarily a bad thing. Many reputable companies and merchants use the information they gather to improve customer service and efficiency, making your online or mobile experience more pleasant and productive. However, some companies use consumer information for aggressive marketing efforts, sell the data to one or more third parties, or fail to protect the data from hackers, dishonest employees or others who would misuse it. Caution is the best policy when deciding who to give your business to and how much personal information to reveal.

Tips for protecting your privacy

- ***Reveal only what is necessary.*** When registering for an online service or account, fill out only those fields in the registration form that are required to use the service or open an account. (These are usually marked with an asterisk.) If given a choice, select options that result in less of your personal information being shared, at least in the beginning. Entering online contests and filling out forms for free trials or coupons may result in your information being sold or shared for marketing and promotions.
- ***Update operating systems and apps.*** The makers of computers, tablets and smartphones regularly update their software, often with important security upgrades. Apps, too, require that you install the latest update to ensure you have the most secure version available.
- ***Take advantage of browser capabilities.*** Newer internet browsers have built-in features that, when enabled, can help protect your privacy. For example, some browsers warn you when you are about to navigate to a site that may be fraudulent. Read the Help section of your browser for more information, and update your browser software regularly to take full advantage of new privacy features as they become available.
- ***Manage your cookies.*** Cookies are small files stored on your computer by websites you visit. They track your activity while at the site. This information often is 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 instructions.
- ***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 financial or personal information—including retailers who have 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.
- ***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 with the session or when stepping away from the 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."

- ***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 pre-registered account.
- ***Do business only with individuals and companies you trust.*** Check the reputation (complaint history and customer 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.
- ***Vet your apps.*** Don't download an unfamiliar app until you've read user reviews and made sure the developer is legitimate. Read the developer's privacy policy for the app, which might be found under the "Settings" or "About This App" tab. TRUSTe certifies the privacy practices of mobile app developers as well as website owners, so look for the logo. If necessary, reset the app's privacy settings to a level you are comfortable with. Be aware that some apps need to track your location to be effective.
- ***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.
- ***Be on guard for fraudulent communications.*** If you question 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.
- ***Erase 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.

Assistance and information

Federal Trade Commission *www.ftc.gov*

The FTC educates the public about how to protect themselves in the marketplace and takes complaints about businesses that violate consumers' rights and privacy.

OnGuardOnline.gov *www.onguardonline.gov*

The U.S. federal government and the technology industry provide information and tips to promote online safety and security.

Privacy Rights Clearinghouse *www.privacyrights.org*

The Privacy Rights Clearinghouse provides information on a wide range of privacy issues.

CNET *https://www.cnet.com/how-to/strong-passwords-9-rules-to-help-you-make-and-remember-your-login-credentials/*

Learn how to create strong passwords and manage them securely.

AnnualCreditReport.com *www.annualcreditreport.com*

Review your credit reports regularly for signs of identity theft. You are entitled to receive three free credit reports a year.

Consumer Action

www.consumer-action.org
Consumer advice and referral hotline:
https://complaints.consumer-action.org/forms/english-form or 415-777-9635
Chinese, English and Spanish spoken

Consumer Action created the Digital Dollar series with funding from Visa Inc.

VISA consumeraction

Visit Visa's financial education program, Practical Money Skills, at: ***https://www.practicalmoneyskills.com***

Find tips and practical know-how for protecting account information, avoiding payment card scams, and resolving unauthorized card use in English and Spanish at: ***www.visasecuritysense.com***

Rev. 3/20

Your Digital Dollars

Safety and privacy in online and mobile transactions

Protect your identity and data while banking or paying digitally

Financial education from *Consumer Action* and *Visa Inc.*