A Consumer Action Publication

Put a Lock on It

Protecting your online privacy

The Internet gives individuals and families the ability to socialize, shop, bank, work, learn and be entertained virtually anywhere, anytime using a computer or mobile device. There are huge benefits to embracing the capabilities of the Internet—and for the most part it's a safe place. That's because most companies place great importance on protecting their users' privacy and account security, making it a priority to employ the latest technology to keep consumers safe online.

But online privacy and security is a shared responsibility. To achieve the desired level of privacy and the greatest level of security, computer and mobile users should take charge of their own protection by exercising common sense and taking advantage of the security tools available to them, which include free tools offered by large tech firms such as Google and Microsoft. Playing an active role helps ensure that you enjoy a safe and sound digital life.

Locking your accounts

Technology is constantly evolving, delivering ever better ways to keep outsiders from gaining access to your accounts and personal data. From online banking to social media, websites that process sensitive personal information offer tools for keeping your data safe from prying eyes. A strong password is a good way to protect your personal data; two-factor authentication is even better.

Password protection: A password is the first line of defense and the most widely used method of securing an account. Here's what you need to do to effectively password-protect your accounts.

- Create a password that is at least eight characters long and a random mix of letters, numbers and symbols. Visit Google (bit.ly/1MoNVfk), Microsoft (bit.ly/1JnLHbp) or ConnectSafely (bit.ly/1Kyu2i2) to learn more about creating strong passwords. You can also use an online tool such as PasswordsGenerator.net for help coming up with one.
- Keep your passwords secret. Rather than writing them down, use a tool that stores all your passwords and requires you to remember only one. You can learn about password managers from PCMag.com (bit.ly/10tbirr) and Lifehacker (bit.ly/1QXEc1b).
- Use different passwords for your various accounts. Change them as often as needed—for example, when someone might have found out your password or there has been a data breach (the exposure or theft of a large amount of user data).
- Choose security questions that nobody else is likely to know the answer to. Be careful about choosing questions that others could easily discover the answers to, such as "What is your mother's maiden name?" or "What is your pet's name?" (Security questions are used by some accounts to verify your identity if you have forgotten your password or are trying to access the account from an unrecognized computer or device.)
- Log out of your account when you are finished and, if you share a device with others, don't let your browser save login information. (Click the "Not now," "Never for this site" or similar option when prompted to allow the browser to save your password, or check/uncheck the appropriate boxes in the Security, Passwords, Sync or AutoFill tabs of the browser's Settings or Preferences.)
- Require a login password to start up your computer or to "wake" it. That adds another layer of protection against anyone who tries to get into your accounts from your own computer. Learn how to do this for an Apple (Mac) (apple.co/1V9p5Yt) and a PC (abt.cm/1Wiy72s). (Set your mobile devices to require a password, PIN or thumbprint, too.)

Two-factor authentication (2FA): This is much stronger protection than just a password. It requires two pieces of information to access the account (for example, a password and confirmation of an onscreen picture/graphic you've chosen, or a password and a fingerprint scan, or a password

plus a passcode that is sent to you via text message or email)—it's like having to swipe your debit card and enter a PIN at the grocery store. Learn more about two-factor authentication from Stop.Think.Connect. (*bit.ly/1DQlzpY*).

Enable two-factor authentication wherever it's available. Not all sites offer it, but many do, including Google, Apple, Facebook, Twitter and PayPal, just to name a few. This list displays many sites that offer 2FA and many that don't: *bit.ly/1JpGz6w*. (Ask sites you use that don't support two-factor authentication to do so.) Each site has its own instructions for enabling 2FA. Check Settings, first. If you can't find it there, contact the website's Support team.

Secure online and mobile transactions

Shopping and banking online can save you both time and money—two great reasons to spend and manage your money digitally. And you can keep all your accounts safe by taking some simple and effective precautions, just like you would with your wallet. Rest assured, some strong security tools are at the ready.

Encryption: This is a technology that scrambles (encrypts) the electronic information being sent through cyberspace so that it is much more difficult for hackers to track your activities and steal your data.

To determine if a website you are visiting uses encryption to protect your information as it travels between you and the site, look for the "s," which stands for "secure," in the URL (https:// rather than just http://). You might also see a padlock, or the address bar itself might turn green when you enter a secure website. Look for one or more of these assurances before you make a purchase, access your financial accounts or conduct any type of transaction.

Be aware that some standard email and text messages are not encrypted, so never send account numbers, your Social Security number or other sensitive information this way.

If you have set up Wi-Fi at home, you have a wireless router. To prevent someone nearby from accessing the information you send over the Internet through your wireless network, you must make sure the encryption feature in your router is turned on (they often come with it turned off). At the same time, create a strong network password (at least 14 random characters) for your router to keep intruders in range of your Wi-Fi signal from accessing your Wi-Fi connection. Get details about securing your wireless network from OnGuardOnline.gov (*1.usa.gov/1G2Eiya*).

Because you can't always be sure that an outside network is encrypted, it's safest to use your wireless carrier's network rather than public Wi-Fi for shopping or banking when you're away from home. If you are using a shared computer or device, always log out of a banking or shopping session when you're finished so that nobody can access your account after you leave. Learn more about using public Wi-Fi safely from the Federal Trade Commission (FTC) (*1.usa.gov/1L62Nlr*).

Firewalls: Most computer operating systems come with a built-in firewall—a barrier between the outside world and your computer. Built-in firewalls are not always set to "On." Check the computer's Security settings (often found under "Preferences") to make sure yours is. If you are having trouble finding the controls, do an online search for the word "firewall" along with the name of your computer operating system to get instructions.

Mobile device safety

A smartphone or tablet allows you to take all the Internet's capabilities with you wherever you go. While their portability and the technology that makes them work offer big advantages for users, mobile devices present unique privacy and security challenges. That doesn't mean you shouldn't use them in all the ways you like—just that taking a few additional or different steps can protect your privacy and your data.

Securing your devices: Because of their portability, there is a greater risk of a mobile device being lost or stolen than, say, a desktop computer. In addition to keeping an eye on your device, you can take advantage of tech tools designed specifically to keep your mobile device and its data safe.

Start by locking your device with a password or PIN (or thumbprint, depending on the version). Set it to lock after a few minutes of inactivity. At the same time, enroll in a remote locate/lock/erase program such as Find My iPhone (Apple) or Android Device Manager. This allows you to find your device if you've misplaced it, or remotely lock it or delete your stuff if it's been lost or stolen.

Don't forget to "wipe" the data off your device before you sell, donate or dispose of it so nobody else can access your personal information. CTIA-The Wireless Association offers tips and links to instructions for erasing the information on your particular type of mobile device (*bit.ly/1jeEDZN*).

Learn more about cyberproofing your phone from AARP (*bit.ly/1FfksoF*).

Apps: "Apps" are software applications designed specifically for mobile devices. Much of a smartphone or tablet's functionality comes from downloaded apps—they enable you to track your fitness, share a "selfie," notify friends where you're having dinner, monitor your investments, play Words With Friends and much, much more. Make sure such powerful software works **for** you, not against you.

- Vet your apps. Only download apps from trusted sources. Read user reviews and make sure the developer is legitimate before downloading.
- Set your apps for the desired

amount of privacy. Many apps depend on the ability to retrieve and share users' personal information, such as contacts, calendars and even location. To control what an app collects and shares, check the settings in the app itself (as opposed to the device settings). If the app wants to collect more personal data than you are comfortable with, don't download it. Review the app's privacy policy, if it has one. If it doesn't, consider choosing a different app.

◆ Avoid apps that announce your location to others, or disable that function if you have the option. Sharing your physical location with strangers could put you at risk of a home robbery or otherwise compromise your safety and privacy. (Some apps, such as those that provide maps and directions, use your location to provide a service but don't make it public.)

◆ Install software updates as they become available to ensure you always have the newest version of the app available.

◆ Read notifications of changes to the app's terms of use or privacy policy so that you can uninstall the app if it plans to collect or share more of your data than you want. Depending on the app and the significance of the changes, you may receive a direct notification (typically by email or from within the app, known as a "push notification"). In other cases, the only way you'll find out about a change might be to revisit these sections in the app or at its website.

Safe and sound social media

For many people, using social media is a part of everyday life. Sharing can be a good thing—**if** you're revealing only what you want with the audience you choose. To avoid the potential consequences of oversharing, think twice before you post, tweet or otherwise reveal personal information, and use the tools available to control what others see.

Preserving your privacy: Not everyone using social media has your best interests at heart. It's important to make smart choices about what to share and whom to share it with so that your personal data can't be used in unintended ways.

Start by adjusting the social media network's privacy settings to match your comfort level—from not sharing with anyone to sharing only with your circle of friends to sharing with the general public. First, log in to your account, then look for a tab or heading such as "Privacy," "Privacy Controls," "Privacy Settings," "Account Settings" or "Preferences." If you're having trouble finding it, use the site's "Help" feature or email the website's Support team.

Don't share personal information—your full name, address, phone number, mother's maiden name or year of birth, for example—that could be used for identification purposes (and ID fraud). And don't share current location and travel plans, which could put you or your property at risk.

It's a good policy not to accept invitations or "friend" requests from people you don't know.

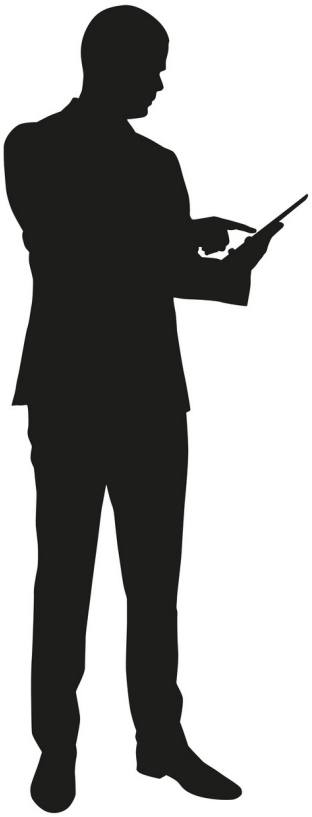
Learn more in Consumer Action's publication **Privacy and Control for Social Media Users** (*bit.ly/1xPC8PO*).

Protecting your e-reputation: The things you share—pictures, videos, activities, opinions—reveal things about you. Managing and protecting your digital reputation can save you from embarrassment and allow you to avoid the potential consequences of not putting your best foot forward. Here are some "best practices" for shielding yourself from social media fallout.

◆ Consider what an employer, recruiter, college admissions officer, lender, landlord, customer/client, government agency, insurer or other decision maker would think about what you're sharing. Realize that many people you do not know personally may turn to social media to learn something about you.

◆ Be aware that a "friend" can repost, retweet or otherwise expose what you assumed you shared only with your selected audience. And if you post something to another person's profile, you have no control over who else sees it.

◆ Backtrack if necessary. Some social media sites enable you delete posts, remove photos, change audiences, etc. so that things you shared in the past aren't visible to future viewers. (Of course, you can't do anything about everyone who has already seen what you've shared.)



◆ "Google" your name to see what pops up. Ask others to remove unflattering photos, videos or posts that include you.

◆ Make sure your accounts are secure so that they can't be hacked and used against you.

Learn more about managing your online reputation in Google's Safety Center (*bit.ly/1FunANi*).

Family-friendly Internet

The Internet offers a wealth of high-quality content not only for adults but for children of all ages, too. To ensure that your family can enjoy the best that the Internet has to offer while avoiding anything that is unwelcome, there are safeguards in place and precautions you can take.

Blocking inappropriate content: There is plenty of excellent, age-appropriate content out there for children. There is also some inappropriate content. Many companies

through which content is delivered—from broadband service providers to social media companies—enable parents to limit everything from the amount of time spent online to which sites can be visited, which videos can be seen, and which message boards and chat rooms can be visited.

Learn more about parental controls from the Family Online Safety Institute (*bit.ly/1L63Emf*) and in the Google Safety Center (*bit.ly/1G2F7XP*).

Monitoring communications: Just as not all content is appropriate for children, not everyone on social media has your child's welfare in mind. As a parent, you are the primary gatekeeper of your child's relationships in cyberspace.

Talk to your children about how to be safe and responsible online. Set clear rules about which sites they can visit and with whom they can communicate. "Friend" your children—make sure you can see what they are sharing on social media, and also what others are sharing with them. Make clear that it's not okay to go alone to see someone they "meet" on the Internet. Promise not to punish them or take away Internet access if they tell you of inappropriate communications. Check out the tips at OnGuardOnline.gov (*http://bit.ly/2eewlAl*).

Report harassment and predatory behavior to the proper authorities, which may include school officials, local police or the CyberTipline (*bit.ly/1NMiQDY* or 800-843-5678).

Avoiding unwelcome marketing: Many online companies collect users' personal information. Some companies use the data to customize and enhance user experience—such as suggesting movies and books you'd like—while others use it to tailor their marketing messages to appeal to people of similar interests. Still others—known as data brokers—collect data about consumers to sell to third-party marketing firms and other companies that use it to target ads and offers. Reputable companies are transparent about how they use your information and they offer you choices about what to share and what you want to keep private.

There are steps you can take to learn how your information will be used and how you can gain greater control over your personal data.

◆ Read the company's "Privacy Policy" or "Data Use Policy" to learn how and when the site collects, uses and shares your personal information. If you're not satisfied with its practices, look for a different site that allows you more control.

◆ If you have children, instruct them not to reveal private information at websites they visit. The Children's Online Privacy Protection Act (COPPA) requires sites to obtain parental consent for the collection or use of any personal information from children under 13. Report violations to the Federal Trade Commission (*www.ftccomplaintassistant.gov* or 877-FTC-HELP).

◆ When appropriate, activate the "Private browsing" function in your web browser, which allows you to surf the Web without the browser saving information about which sites and pages you've visited, and use a pop-up blocker to avoid the opening of unwelcome advertising windows. (Be aware that this can hinder some desirable functionality, such as a retail website remembering what is in your "cart.")

◆ Consider whether or not there is a good reason to provide more information than the minimum that is required (often indicated by an asterisk) to register for or use the service. Share the least amount of personal information possible.

◆ Understand that anytime you give up your personal information to an unvetted source—even in response to seemingly innocent quizzes or to participate in games—it can be used for unintended purposes.

Technology is constantly giving us new ways to communicate, work, learn, create, share and have fun. Don't miss out—but do be careful. Join the team effort to keep yourself and your family safe and sound online. ■

About Consumer Action

www.consumer-action.org

Through multilingual consumer education materials, community outreach and issue-focused advocacy, Consumer Action empowers underrepresented consumers nationwide to assert their consumer rights and prosper.

Consumer advice and assistance: Submit consumer complaints to our advice and referral hotline: *http://www.consumer-action.org/hotline/complaint_form* or 415-777-9635.

Chinese, English and Spanish spoken

This publication was created in partnership with Google.