Internet safety tips

Know the dangers of the internet

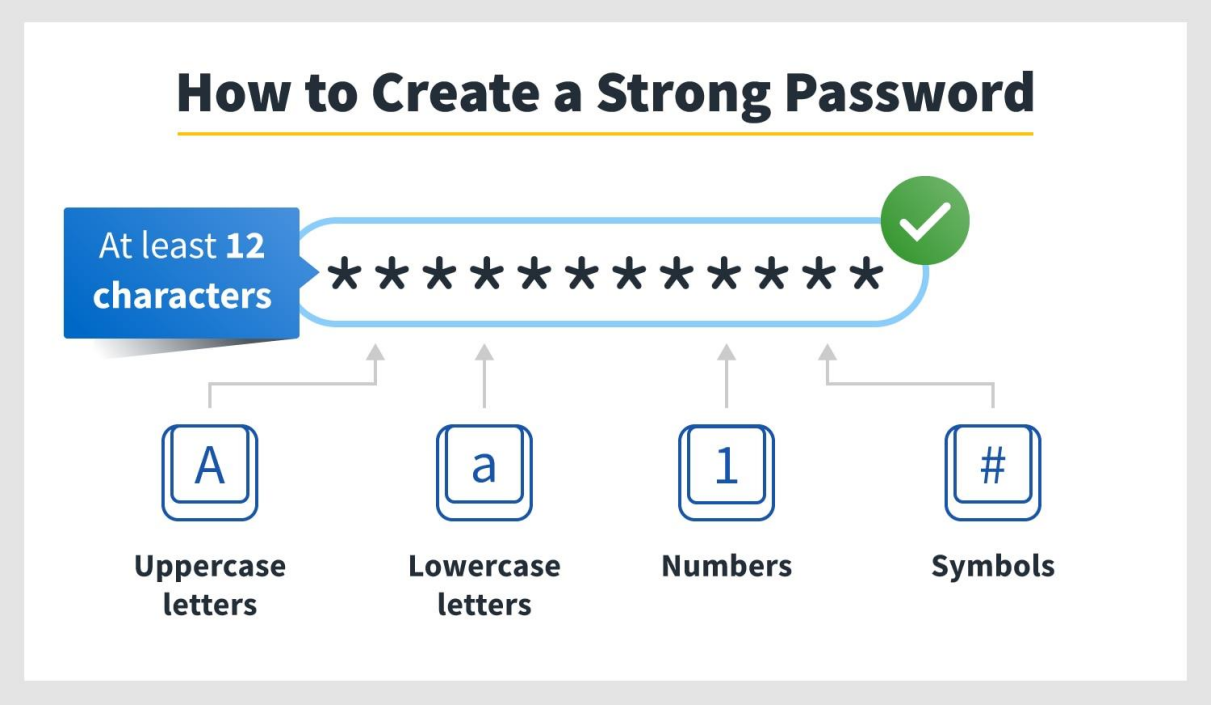
When it comes to cybersecurity, kids are often one of your family's weakest links — and that can be for lack of knowing the dangers of the internet. Teach kids about suspicious activity online and encourage them to ask for help if something seems unusual.

Remember your identity is important

Sometimes kids make themselves vulnerable to **identity theft** by disclosing personal information online because they believe they have nothing to lose. A **child's identity** can have as much value as an adult's identity, if not more. Scammers can trick kids into disclosing their Social Security number and other details that can be used to commit identity theft. Remind children not to reveal too much information about themselves. Their date of birth, address, and SSN are all examples of personal information, and they shouldn't share them freely.

Choose strong passwords

Passwords are the primary defense against hackers. Yet, many people reuse the same password for multiple accounts and use passwords that are easy to guess, because they're also easy to remember. Teach your kids to **create a hack-proof password** by selecting a combination of uppercase and lowercase letters, numbers, and symbols, and make sure it's at least 12 characters long. New password recommendations suggest length over complexity, the longer a password, the harder to hack.



Keep your social media accounts secure

There's a good chance someone in your house is on a social network. But **social media** can also attract cyber snoops and identity thieves. Keep a close eye on your social accounts. If someone messages you who hasn't done so in a while, be suspicious. Your friend's account may have been hacked. Parents should remind teens to also never meet in person with someone they met online and tell an adult if a stranger is messaging them.

Be careful what you post

It's important for children, teens, and family members to know how much information is too much information. In their excitement to share milestones, teens may sometimes post their personal information online. For example, a driver's license or a travel itinerary shared online could be valuable information for identity thieves or burglars. Also personal or inappropriate photos can attract online predators, or could affect future educational or employment opportunities. **Never post vacation plans online. EX: (Status: Leaving tomorrow for a 7 day cruise!) and Never post pictures while you are still on vacation.** This is basically saying Hi, my house is empty, come on over.

Shop online only from secure sites

Whether teens are allowed to shop online is up to their parents. Whether teens will listen is another story. Teach yours how to shop safely online by acquainting them with some indicators of a secure website. One of the best indicators is whether a site is running on HTTPS, which means the site has a security certificate that safeguards visitors' personal information by encrypting their data. You can verify if a site runs on HTTPS by double-checking the beginning of a URL in the address bar and also confirming if there's a padlock next to it.

Keep privacy settings on

Web browsers, mobile operations systems, and social media channels all have settings in place to protect your privacy, and it's up to you to adjust them. Keeping them turned off means your information might be shared with marketers to help your browsing experience, but it also could be intercepted by hackers. Play it safe and keep your privacy settings on. Parents should adjust kids' devices accordingly and teach teens how to keep the settings on themselves.

Understand privacy policies ...

… and know that privacy policies may not be private. With more websites and applications collecting information and using it for advertising and marketing purposes, make sure your family knows the value of online privacy. Many apps have privacy policies that disclose that the apps collect and share their users' information. Kids and many adults often accept these policies without reading them. Even if your settings are set to private, remember nothing is private. Even the so-called **private browser is not private**. Law enforcement, website administrators, and hackers could have access to your so-called private information.

Backup data regularly

A type of malware, **ransomware** is popular among cybercriminals who can lock your computer so you can't access your valuable files, like your private photos or tax information. One of the best ways to combat the threat of ransomware is to **backup your data regularly**. Backup your kids' devices, too, and teach your teens to do the same.

Keep your internet connection secure

Almost every member of the family might access your internet connection, and each person may have devices also vying for your Wi-Fi's attention. It should come as no surprise that hackers also want to use your **home Wi-Fi** network. Cybercriminals can hack home routers and gain access to various internet-connected devices like home security systems and smart doorbells. Make sure your home Wi-Fi system has a hard-to-crack password and consider cybersecurity software that identifies "intruders" on your network. Finally, **a VPN** is one of the best ways to ensure your internet connection is secure.

Monitor online activities

Monitoring your kids offline is enough stress. Thankfully, there's some cybersecurity tools to help you monitor their online activities. Install a cybersecurity software with **parental controls** on your kids' devices to block certain features on games, track kids' location, backup their data, and manage their **screen time**.

Install a comprehensive cybersecurity suite

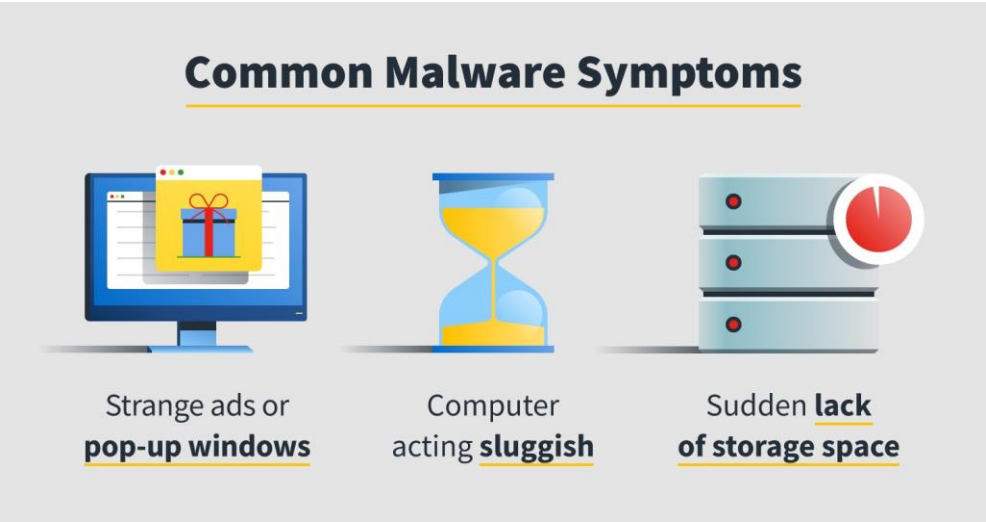
To help every family member from clicking on the wrong links and visiting the wrong sites, install a **comprehensive cyber safety solution** that provides protection for all your family members and their devices. Your **smartphone** and tablet need as much protection as your computer and laptops. So do your **thermostat, smart doorbell, home security system, and other internet-connected devices**.

When in doubt, call support

The best security software programs offer 24x7 support. If you have any suspicion you've been hacked, call for help. If you think your device is under malware, **spyware**, or ransomware attack, call for help. A good security suite will have experts to help you resolve your problem. That said, unless you are subscribed to a comprehensive (and expensive) service that actively monitors your computers, support will NEVER make an unprompted call you and ask for details or control of your computer.

Be careful what you download

There are more than 1.8 billion websites worldwide, and it's no secret that some of them have malicious intent. A malicious website is a site that attempts to install malware on your device, meaning anything that will disrupt computer operation, gather your personal information, or allow unauthorized access to your machine. This usually requires some action on your part, but there are also drive-by downloads, whereby a website will attempt to install software on your computer without asking for permission first. Downloading and running security software can help defend against these threats, but it's also worth knowing how to diagnose if your computer has malware so you can **remove malware**.



Go private on public Wi-Fi

There are a lot of **risks of connecting to public Wi-Fi** networks. In addition to keeping your kids and teens attuned to them, it's important for parents to remind themselves that hackers and cybercriminals consider public Wi-Fi, such as in malls and coffee shops, an easy access point to getting hold of your data. For this reason, always use a VPN when connecting to public Wi-Fi. Don't have a VPN? Consider if you can hold off on internet browsing until you are home.

Close unused accounts

Unused accounts can be a rich source of personal information for cybercriminals. Sometimes kids create an account with their first and last name or their birthday in the username.

Cybercriminals can patch these data points together and steal information from other sites that the individual uses. If you think you won't be revisiting the site, it's best to close the account.

Everyone should:

• Remember to logout of the accounts you've accessed before leaving the PC, even if it's a home computer.

• Never open an attachment from someone you don't know. No matter how tempting! EX: (Subject Line: Free Vacation!)

• Never share your password with anyone.

• Never upload (post) pictures of yourself onto the Internet or on-line service to people you do not personally know and NEVER upload explicit photos.

• Never download **anything** from an unknown source, ever.

• Never send money or account information to a non-validated source.

• Never give out identifying information such as your name, home address, school name, or telephone number.

Understand that whatever you are told on-line may or may not be true.

In addition to the list above, children should:

• Never buy anything online without parental permission.

• Never download or install software without parental permission.

• Print out and report mean or insulting messages to your parents or to a teacher at school.

• Never use imagines or messages that are hurtful or insulting to others.

• Never arrange a face-to-face meeting with someone you met on- line. NO MATTER WHAT!

Parents should:

• Remember that Internet technology can be mobile, so make sure to monitor cell phones, gaming devices, and laptops.

• Establish clear limits for which online sites children may visit and for how long.

• Create a favorites folder for sites your children are allowed to visit.

• Know who is connecting with your children online and set rules for social networking, instant messaging, e-mailing, online gaming, and using webcams.

• Periodically check your child's postings and internet history.

• Maintain an open dialogue with your children about their internet activities and online safety.

• In addition to yourself, identify other safe people to talk with about uncomfortable or dangerous internet incidents.

To find out the latest information on cyber safety or to report cyber incidents visit:
Federal Bureau of Investigation
http://www.fbi.gov/about-us/investigate/cyber/cyber
U.S. Department of Justice
http://www.justice.gov/criminal/cybercrime/reporting.html
U.S. Department of Homeland Security
http://www.dhs.gov/topic/cybersecurity