Computer Security

Scammers, hackers, and identity thieves are looking to steal your personal information – and your money. But there are steps you can take to protect yourself, like keeping your computer software up-to-date and giving out your personal information only when you have a good reason.

Use Security Software That Updates Automatically

The bad guys constantly develop new ways to attack your computer, so your security software must be up-to-date to protect against the latest threats. Most security software can update automatically; set yours to do so. You can find free security software from well-known companies. Also, set your operating system and web browser to update automatically.

If you let your operating system, web browser, or security software get out-of-date, criminals could sneak their bad programs – malware – onto your computer and use it to secretly break into other computers, send spam, or spy on your online activities. There are steps you can take to detect and get rid of **malware**.

Don't buy security software in response to unexpected pop-up messages or emails, especially messages that claim to have scanned your computer and found malware. Scammers send messages like these to try to get you to buy worthless software, or worse, to "break and enter" your computer.

Treat Your Personal Information Like Cash

Don't hand it out to just anyone. Your Social Security number, credit card numbers, and bank and utility account numbers can be used to steal your money or open new accounts in your name. So **every time** you are asked for your personal information – whether in a web form, an email, a text, or a phone message – think about whether you can really trust the request. In an effort to steal your information, scammers will do everything they can to appear trustworthy.

Check Out Companies to Find out Who You're *Really* Dealing With

When you're online, a little research can save you a lot of money. If you see an ad or an offer that looks good to you, take a moment to check out the company behind it. Type the company or product name into your favorite search engine with terms like "review," "complaint," or "scam." If you find bad reviews, you'll have to decide if the offer is worth the risk. If you can't find contact information for the company, take your business elsewhere.

Don't assume that an ad you see on a reputable site is trustworthy. The fact that a site features an ad for another site doesn't mean that it endorses the advertised site, or is even familiar with it.

Give Personal Information Over Encrypted Websites Only

If you're shopping or banking online, stick to sites that use encryption to protect your information as it travels from your computer to their server. To determine if a website is encrypted, look for **https** at the beginning of the web address (the "s" is for secure).

Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, the entire account could be vulnerable. Look for https on every page of the site you're on, not just where you sign in.

Protect Your Passwords

Here are a few principles for creating strong passwords and keeping them safe:

- The longer the password, the tougher it is to crack. Use at least 10 characters; 12 is ideal for most home users.
- Mix letters, numbers, and special characters. Try to be unpredictable – don't use your name, birthdate, or common words.
- Don't use the same password for many accounts. If it's stolen from you – or from one of the companies with which you do business – it can be used to take over all your accounts.
- Don't share passwords on the phone, in texts or by email. Legitimate companies will not send you messages asking for your password. If you get such a message, it's probably a scam.
- Keep your passwords in a secure place, out of plain sight.

Back Up Your Files

No system is completely secure. Copy important files onto a removable disc or an external hard drive, and store it in a safe place. If your computer is compromised, you'll still have access to your files.

Malware

Avoid Malware

Scam artists try to trick people into clicking on links that will download malware and spyware to their computers, especially computers that don't use adequate security software. To reduce your risk of downloading unwanted malware and spyware:

- **Keep your security software updated.** At a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. Set your security software, internet browser, and operating system (like Windows or Mac OS) to update automatically.
- **Don't click on any links or open any attachments in emails unless you know who sent it and what it is.** Clicking on links and opening attachments – even in emails that seem to be from friends or family – can install malware on your computer.
- **Download and install software only from websites you know and trust.** Downloading free games, file-sharing programs, and customized toolbars may sound appealing, but free software can come with malware.
- **Minimize "drive-by" downloads**. Make sure your browser security setting is high enough to detect unauthorized downloads. For Internet Explorer, for example, use the "medium" setting at a minimum.
- **Use a pop-up blocker and don't click on any links within pop-ups**. If you do, you may install malware on your computer. Close pop-up windows by clicking on the "X" in the title bar.
- **Resist buying software in response to unexpected pop-up messages or emails**, especially ads that claim to have scanned your computer and detected malware. That's a tactic scammers use to spread malware.
- **Talk about safe computing.** Tell your kids that some online actions can put the computer at risk: clicking on pop-ups, downloading "free" games or programs, opening chain emails, or posting personal information.
- **Back up your data regularly**. Whether it's text files or photos that are important to you, back up any data that you'd want to keep in case your computer crashes.

Detect Malware

Monitor your computer for unusual behavior. Your computer may be infected with malware if it:

- slows down, crashes, or displays repeated error messages
- won't shut down or restart
- serves up a barrage of pop-ups
- displays web pages you didn't intend to visit, or sends emails you didn't write

Other warning signs of malware include:

- new and unexpected toolbars
- new and unexpected icons in your shortcuts or on your desktop
- a sudden or repeated change in your computer's internet home page
- a laptop battery that drains more quickly than it should

Get Rid of Malware

If you suspect there is malware is on your computer, take these steps:

- Stop shopping, banking, and doing other online activities that involve user names, passwords, or other sensitive information.
- Update your security software, and then run it to scan your computer for viruses and spyware. Delete anything it identifies as a problem. You may have to restart your computer for the changes to take effect.
- If your computer is covered by a warranty that offers free tech support, contact the manufacturer. Before you call, write down the model and serial number of your computer, the name of any software you've installed, and a short description of the problem.
- Many companies – including some affiliated with retail stores – offer tech support on the phone, online, at their store, and in your home. Decide which is most convenient for you. Telephone and online help generally are the least expensive, but you may have to do some of the work yourself. Taking your computer to a store usually is less expensive than hiring a repair person to come into your home.
- Once your computer is back up and running, think about how malware could have been downloaded to your machine, and what you could do differently to avoid it in the future.

Wireless

Understand How a Wireless Network Works

Going wireless generally requires connecting an internet "access point" – like a cable or DSL modem – to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any computer within range with a wireless card can pull the signal from the air and access the internet.

Unless you take certain precautions, anyone nearby with a wireless-ready computer or mobile device can use your network. That means your neighbors – or any hacker nearby – could "piggyback" on your network, or access information on your computer. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account.

Use Encryption

Encryption is the key to keeping your personal information secure online. Encryption scrambles the information you send over the internet into a code so that it's not accessible to others. When using wireless networks, it's best to send personal information only if it's encrypted – either by an encrypted website or a secure Wi-Fi network. An encrypted website protects **only** the information you send to and from **that site**. A secure wireless network encrypts **all** the information you send using that network.

Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. If they don't, check the company's website.

How to Tell If a Website is Encrypted

If you send email, share digital photos and videos, use social networks, or bank online, you're sending personal information over the internet. The information you share is stored on a server – a powerful computer that collects and delivers content. Many websites, such as banking sites, use encryption to protect your information as it travels from your computer to their server.

To determine if a website is encrypted, look for **https** at the beginning of the web address (the "s" is for secure). Some websites use encryption only on the sign-in page, but if any part of your session isn't encrypted, your entire account could be vulnerable. Look for **https** on every page you visit, not just when you sign in.

Secure Your Computer and Router

Use anti-virus and anti-spyware software, and a firewall. Use the same basic computer security practices that you would for any computer connected to the internet.

Change the name of your router from the default. The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know.

Change your router's pre-set password. The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. Use passwords that are at least 10 characters long: the longer the password, the tougher it is to crack.

Visit the company's website to learn how to change the password.

Limit Access to Your Network

Allow only specific computers to access your wireless network. Every computer that is able to communicate with a network is assigned a unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

Turn off your wireless network when you know you won't use it. Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

Don't Assume That Public Wi-Fi Networks Are Secure

Be cautious about the information you access or send from a public wireless network. Many cafés, hotels, airports, and other public places offer wireless networks for their customers to use. These "hot spots" are convenient, but they may not be secure.

Don't Assume a Wi-Fi Hotspot is Secure

Most Wi-Fi hotspots **don't** encrypt the information you send over the internet and are **not** secure.

If you use an unsecured network to log in to an unencrypted site – or a site that uses encryption only on the sign-in page – other users on the network can see what you see and what you send. They could hijack your session and log in as you. New hacking tools – available for free online – make this easy, even for users with limited technical know-how. Your personal information, private documents, contacts, family photos, and even your login credentials could be up for grabs.

An imposter could use your account to impersonate you and scam people you care about. In addition, a hacker could test your username and password to try to gain access to other websites – including sites that store your financial information.

Protect Yourself When Using Public Wi-Fi

So what can you do to protect your information? Here are a few tips:

- When using a Wi-Fi hotspot, only log in or send personal information to websites that you know are fully encrypted. To be secure, your entire visit to each site should be encrypted – from the time you log in to the site until you log out. If you think you're logged in to an encrypted site but find yourself on an unencrypted page, log out right away.
- Don't stay permanently signed in to accounts. When you've finished using an account, log out.
- Do not use the same password on different websites. It could give someone who gains access to **one** of your accounts access to **many** of your accounts.
- Many web browsers alert users who try to visit fraudulent websites or download malicious programs. Pay attention to these warnings, and keep your browser and security software up-to-date.
- If you regularly access online accounts through Wi-Fi hotspots, use a virtual private network (VPN). VPNs encrypt traffic between your computer and the internet, even on unsecured networks. You can obtain a personal VPN account from a VPN service provider. In addition, some organizations create VPNs to provide secure, remote access for their employees.
- Some Wi-Fi networks use encryption: WEP and WPA are the most common. WPA2 is the strongest. WPA encryption protects your information against common hacking programs. WEP may not. If you aren't certain that you are on a WPA network, use the same precautions as on an unsecured network.
- Installing browser add-ons or plug-ins can help, too. For example, Force-TLS and HTTPS-Everywhere are free Firefox add-ons that force the browser to use encryption on popular websites that usually aren't encrypted. They don't protect you on all websites – look for https in the URL to know a site is secure.