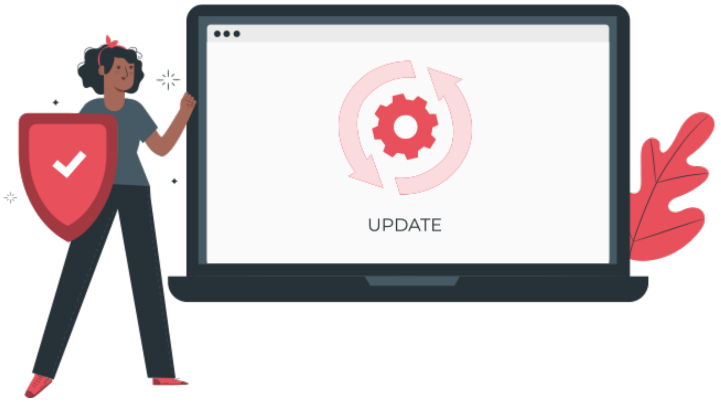
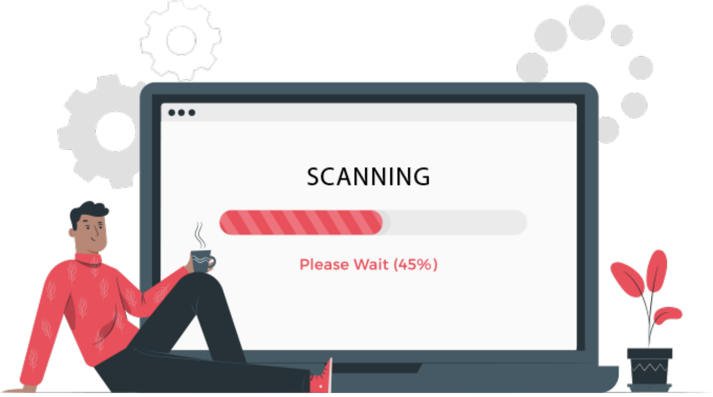
Data privacy tips

Install anti-virus/malware software. There are many home computers that do not have anti-virus/malware protection. This protection is a must-have first step in keeping your computer virus free.



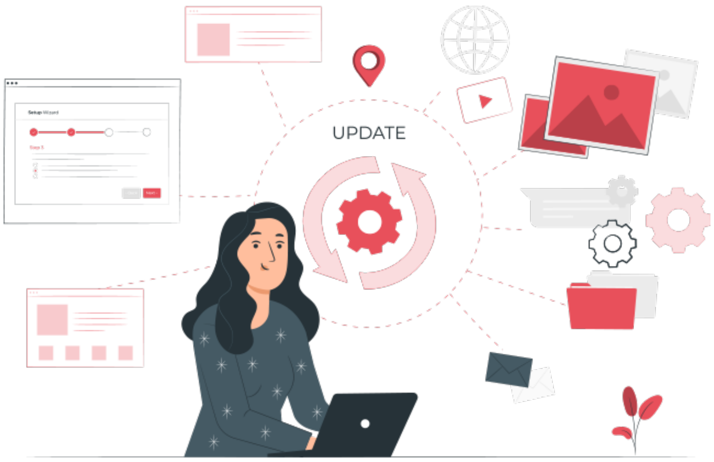
Keep your anti-virus software up to date. Having protection is the first step; maintaining it is the second. Free anti-virus software is better than nothing, but keep in mind it's not the best solution.

Run regularly scheduled scans with your anti-virus software. Set up your software of choice to run at regular intervals, overnight if your computer does not shut off automatically or go into hibernation mode. Once a week is preferred, but do not wait much longer between scans.



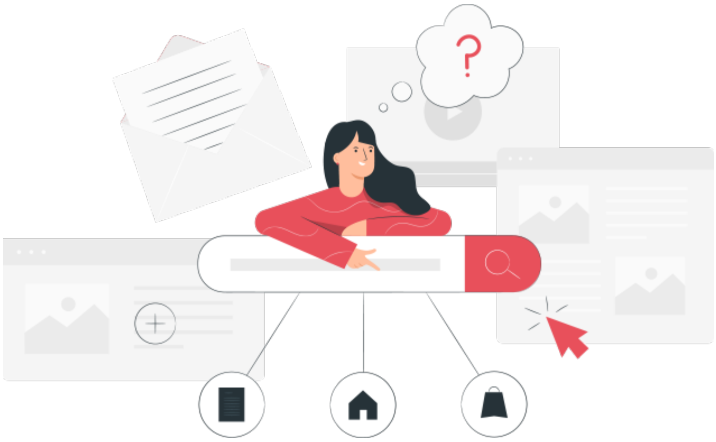
Keep your operating system current. Regardless the operating system (*Windows, Mac OS, etc)*, keep it up to date. OS developers are always issuing security patches that fix and plug security leaks. These patches will help to keep your system secure.

Keep your software current. Not only do you need to keep your operating system up to date, but all software running on your computer. PDF viewers, office applications, photo editors, all will have routine security updates sent; apply them as they come to keep your software secure.



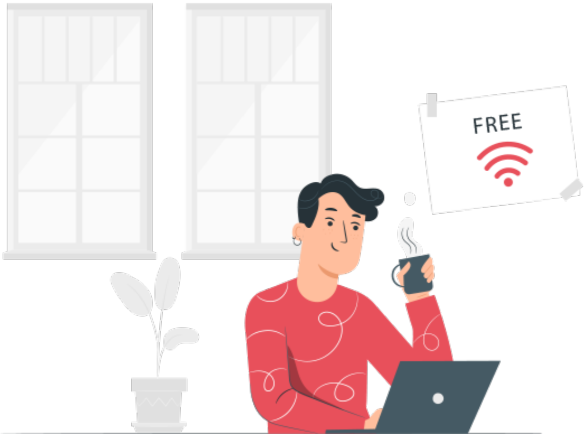
Secure your home network. Make sure your Wi-Fi requires a strong password for access. Never broadcast an open Wi-Fi connection. Use WPA or WPA2 encryption. Do not broadcast your SSID or Wi-Fi name; instead manually type in the SSID and password on each authorized device. If you have guests who use your internet, provide a guest SSID that uses a different password.

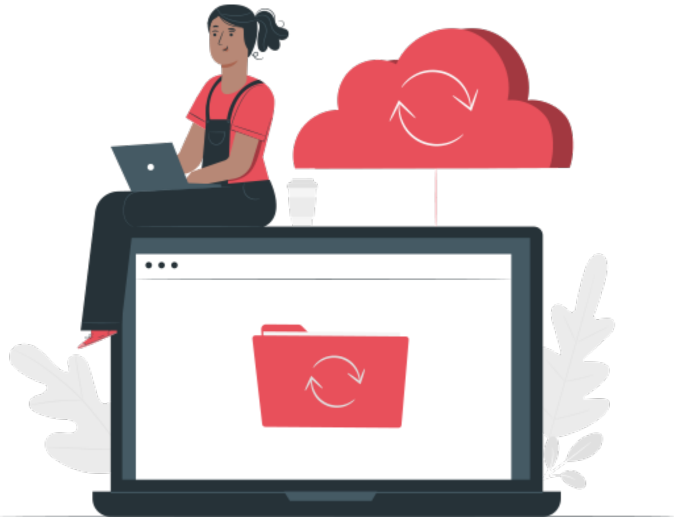
Think before you click. Avoid websites that provide pirated material. Do not open an email attachment from somebody or a company that you do not know. Do not click on a link in an unsolicited email. Always hover over a link *(especially one with a URL shortener)* before you click to see where the link is really taking you.



Keep your personal information safe. This is likely the most difficult thing to do on the Internet. Many hackers will access your files not by brute force, but through social engineering. They will get enough of your information to gain access to your online accounts and will glean more of your personal data. They will continue from account to account until they have enough of your info that they can access your banking data or just steal your identity altogether. Be cautious on message boards and social media. Lock down all of your privacy settings, and avoid using your real name or identity on discussion boards.

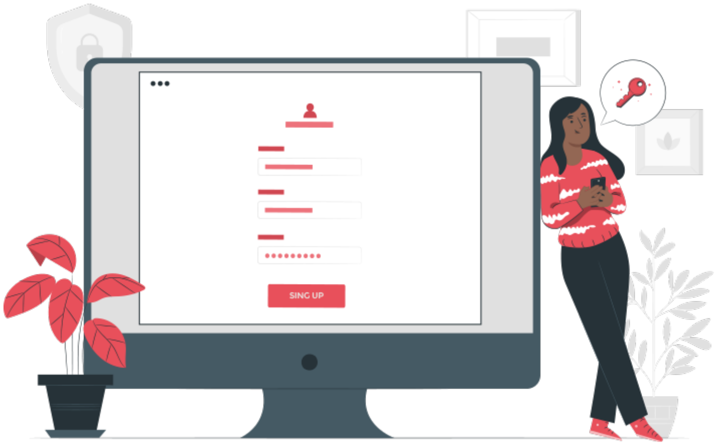
Do not use open Wi-Fi. When you are at the local coffee shop, library, and especially the airport, don’t use the “free” open *(non-password, non-encrypted)* Wi-Fi. Think about it. If you can access it with no issues, what can a trained malicious individual do?

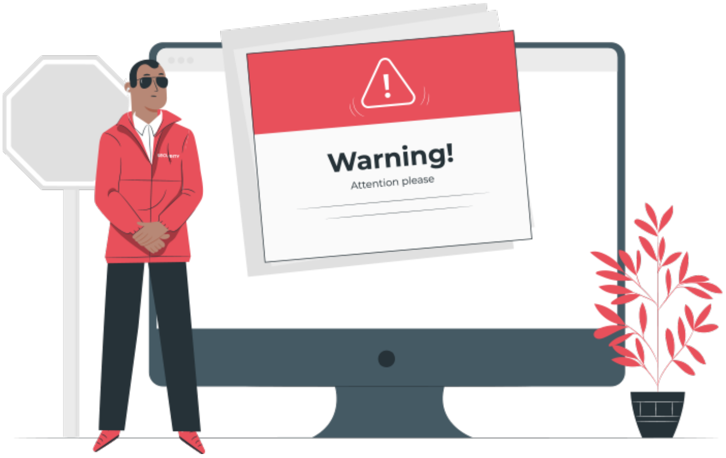




Back up your files. The best thing you can do is back up your files—all of them. Ideally you will have your files *(your data)* in at least three places: the place where you work on them, on a separate storage device, and off-site. Keep your files on your computer, back them up to an external hard drive, then back them up in a different location. You can use a backup service or simply get two external hard drives and keep one at work, at a friend’s house, at a family member’s house, or in a safe deposit box.

Use multiple strong passwords. Never use the same password, especially on your bank account. Typically, we use the same email address or username for all of our accounts. Those are easy to see and steal. If you use the same password for everything, or on many things, and it is discovered, then it takes only seconds to hack your account. Use a strong password. Use lower case, upper case, numbers, and symbols in your password. Keep it easy to remember but difficult to guess. Do not use dates or pet names.





Use a pop-up blocker. Web browsers have the ability to stop pop-up windows and allow you to set security for accepting pop-ups. Be wary of clicking on links within the pop-up screens. Never click on a pop-up window that prompts you to download software.