1. Keep your software, firmware and operating systems updated

- PC
- Tablet
- Phone
- Router
- TV

2. Secure your devices

Computers and smartphones hold so much information about us. They know who your contacts and friends are, they save snapshots of our lives through photos and videos, they keep track of where you are, they know your browsing habits, your financial transactions, and your shopping habits; your gadgets know virtually everything about you!

Over one-third of smartphone users don't use even the simplest 4-digit pass code

About 70 percent of users do not use any security protections for their computers

3. Use a firewall and anti-malware protection

One essential tool that keeps hackers from seeing your computer online is a firewall. A firewall keeps others from accessing your system and your network. Newer Windows and Mac systems all have built-in software firewalls for configuring your outgoing and incoming internet ports.

Another thing that will protect your system from spyware and remote access malware is security software.
Good security software will keep 99.99 percent of viruses out of your system. Whether the virus is in a download, email or coming at you online, security software can detect and block it.

There are plenty of security software programs, some free and some paid. If you're running Windows 8 or 10, you may have noticed that your system already has built-in antivirus and malware protection software called Windows Defender. It's actually a decent program for guarding your PC against virus and malware threats.

Other free options include Avast and AVG. However, while they do the basic scanning and protection well, they aren't going to have the range of extra options that a paid option might.

Norton is free to most Comcast internet users, McAfee is free to most AT&T internet users.

4. Use encryption

An extra layer of security you can employ is disk encryption. With encryption, your data will be converted into unreadable code that can only be deciphered with a specific key or password. PC users can enable Windows' built-in encryption tool BitLocker. BitLocker is available to anyone Windows 8.1 Pro, Windows 8.1 Enterprise, or Windows 10 Pro.

5. Beware of public Wi-Fi

Security risks can even be greater when you're accessing the internet using public Wi-Fi.

Crooks use public Wi-Fi to spy on unsuspecting users who join the network. Or, sometimes they even create "honeypot" networks, which are fake networks designed to steal your information.

Still, even though the risks are so high, many people use public Wi-Fi networks to check their bank accounts, purchase merchandise and complete other tasks that they'd prefer were private.

Cybercriminals can walk away with your name, address, Social Security number, email address, and even your username and password.

6. Completely wipe old devices that you're getting rid of

You don't throw away your personal files, credit card statements and tax filings in the trash for anyone to find, do you? If you don't do that to your physical files, then why shouldn't you do that to your sensitive digital files too?

Just like a physical trash can, the contents of your PC's Recycle Bin or Mac's Trash Can are only cleared out when you empty them. Using the same analogy, if it's been a while since you've emptied them, there's a treasure trove of documents and items for someone to snoop through.

If you want to get serious about your personal security, you need to erase sensitive data for good. You get can rid of that personal data by using software tools like the popular cross-platform tool CCleaner for PCs and Macs.

7. Always use strong and unique passwords

Thanks to online banking, social networking, and the cloud, much of your digital life is now online. Hackers would love to get access to any of your online accounts so they can steal the information you've uploaded.
Your password is the first line of defense against this. You want to make sure you set up a strong, unique password for every account. A password manager, such as LastPass, is a program that can store and manage your passwords for each app, service, and site that you use. It's like a locked safe (or a vault) for all your credentials, tightly secured with your own personal key.

8. Use two-factor authentication

Two-factor identification is a fancy name for adding an extra verification step to the login process of your most critical accounts.

With the 2FA setting enabled, instead of just providing your username or password to log in to an account, a secondary form of verification is required to prove your identity.

The most popular form of 2FA right now is a special one-time code that's texted to your cellphone.

The idea is that even though hackers may have figured out your credentials, without the special code, they still won't be able to access your account.

9. Secure your Wi-Fi then turn on your guest network

Friends and family always want to use your Wi-Fi. They ask politely, phone in hand because they hate to burn up their data plans when they can just use your connection. Instead of handing them your real password, use your router's "Guest Network."

This feature lets you share your internet connection with your guests while keeping them off your main network, preventing them from seeing your shared files and services.

10. Always use the right account type

When you first set up a computer, you create at least one user account. If you have several people using a computer, you can create an account for each one.

However, there are multiple types of accounts you can create. The two major ones are "administrator" and "standard." The administrator account can do whatever they want to Windows, including changing settings and installing new programs.

Someone using a standard account can't unless they put in the right password.

Everyone should be using a standard account. That way if a virus sneaks onto your system, it can't install without your permission, which makes you safer.