



# New Windows PC? Start with These Security Basics

A brand-new Windows PC gives you a fresh start. Before you fill it with apps, files, and saved passwords, take a few minutes to put security basics in place.

You don't need to be a computer expert. A secure home network, a few built-in protections, and sensible browsing habits can go a long way toward keeping your new computer—and your personal information—safe.

## Start at the Front Door: Your Wi-Fi Router

Your router connects your home network to the internet. Securing it is an important first step.

Change the router's default administrator password and use a strong, separate password for your Wi-Fi network. These passwords serve different purposes: one controls the router's settings; the other lets devices join your network.

Keep the router's software updated and enable WPA3 encryption when supported, or WPA2 at a minimum. The [Federal Trade Commission's cybersecurity guidance](#) explains these basic network protections.

## Understand What a VPN Can—and Cannot—Do

A virtual private network, or VPN, encrypts traffic between your device and the VPN provider. It can also mask your public IP address from the websites you visit.

Some routers support a VPN connection for connected devices. You can also install a VPN application directly on your PC.

But a VPN does not make you untraceable, prevent every kind of tracking, or protect you from malicious downloads and phishing scams. You are also placing trust in the VPN provider.

Before choosing a service, review its privacy policy, data collection practices, and reputation. A subscription fee or a “no logs” promise alone does not guarantee privacy. The [FTC’s guide to VPN apps](#) explains what to consider.

## Keep Your Firewall on Guard

Windows includes a firewall that helps block unauthorized network connections. Make sure it is enabled, and be cautious when an unfamiliar application asks you to let it through. You can review its status in Windows Security under **Firewall & network protection**. See [Microsoft’s home computer security guidance](#).

## Give Your Browser a Security Check

Use a supported browser, keep it updated, and review its security and privacy settings. Install browser extensions sparingly, and remove those you no longer use. Pay attention to HTTPS, which encrypts the connection between your browser and a website. However, encryption does not prove that the website itself is legitimate. Scammers can use HTTPS, too.

Check the website address carefully before entering passwords or payment information. The [FTC cautions against trusting a site simply because it uses encryption](#).

## Check Your Built-In Malware Protection

Windows includes Microsoft Defender Antivirus, so a new PC does not automatically need a separate antivirus purchase. Open Windows Security and check **Virus & threat protection**. Confirm that protection is active and security updates are current. If you use another antivirus product, make sure it is supported and functioning correctly.

[Microsoft’s Windows Security guide](#) explains how these protections work.

## Keep Unnecessary Software off Your PC

Every application you install becomes something else to maintain. Be selective about downloads, especially unfamiliar utilities and browser extensions. Download software from trusted sources. Every few months, review your installed applications and remove programs you recognize and no longer need. If you are unsure what a program does, check before uninstalling it.

## Let Security Updates Do Their Job

Enable automatic updates for Windows, your browser, and other applications. Install updates promptly and complete any required restart.

Updates fix vulnerabilities that attackers may exploit. Use a supported version of Windows so your computer continues receiving the protections it needs. [Microsoft explains how Windows updates work](#).

## **Pause Before You Click**

An unexpected attachment or urgent email deserves a second look—even when it appears to come from someone you know. Criminals can impersonate trusted contacts or send messages from compromised accounts. If an attachment or request seems unusual, verify it through another channel before opening it.

When a message claims that an account is locked or a payment has failed, open the company's app or visit its website independently. Avoid using the message's link to investigate. The [FTC's phishing guide](#) describes common warning signs.

## **Keep Your Login Details to Yourself**

Be suspicious of anyone who asks you to send a password or share a verification code. A convincing logo, familiar name, or urgent warning does not establish someone's identity. If a supposed administrator contacts you, verify the request using contact information you already trust. Taking a moment to check is easier than recovering a stolen account.

## **Make Every Password Count**

Use a long, unique password for each account. Reusing passwords means that one stolen login can expose several accounts.

A password manager can help you create and store strong passwords. Enable multifactor authentication whenever it is available to add another layer of protection. [CISA's cybersecurity guidance](#) explains these account security basics.

## **Build Good Habits From Day One**

A safer computer starts with a few practical choices: secure your network, keep protections enabled, install updates, and think before you click.

Make those habits part of your routine, and your new Windows PC will be better prepared for everyday use.