PROTECT YOUR DATA

Wireless providers and the broader wireless ecosystem work relentlessly to protect networks and devices and to stay ahead of constantly evolving cyber dangers.

However, there are risks associated with any action online and your risk assessment may be different based on your preferences and the contents of the account. For example, the risks associated with a bank or social media account being compromised may be different to different people depending on how they use or value the account. Since you are most knowledgeable about what is in your accounts, it is important to secure your information in the way that makes the most sense to you for the accounts you have.

By making a few simple changes to your devices and accounts you can maintain security against outside parties' unwanted attempts to access your dat. This will also protect your privacy from those you don't consent to sharing your information with. Getting started is easy. Here's a guide to a few simple changes you can make to protect yourself and your information online.

Protect Your Accounts

In the past decade, data breaches and password leaks have struck companies such as Equifax, Facebook, Home Depot, Marriott, Target, Yahoo, and countless others. If you have online accounts, hackers have leaked data from at least one of them. Want to know which of your accounts have been compromised? Search for your email address on Have I Been Pwned? to cross-reference your email address with hundreds of data breaches.

- Require PINs/passwords whenever possible and use multi-factor authentication to prevent unauthorized access to your accounts.
- Do not jailbreak, root, or otherwise override the native settings on your phone.
- Keep your operating system updated to protect against cyber vulnerabilities.
- Use additional layers of security like Virtual Private Networks (VPNs) and encryption applications to further protect your sensitive information, especially on open networks.
- Watch out for phishing scams where a source that seems trusted asks for your SSN, bank account number, driver’s license number, etc. Always use publicly available contact information for the source to verify if the data they are requesting is needed.

Protect Your Web Browser

Companies and websites track everything you do online. Every ad, social network button, and website collects information about your location, browsing habits, and more. The data collected reveals more about you than you might expect. You might think yourself clever for never tweeting your medical problems or sharing all your religious beliefs on Facebook. Chances are good that the websites you visit regularly provides all the data advertisers need to pinpoint the type of person you are. This is part of how targeted ads remain one of the internet's most unsettling innovations.

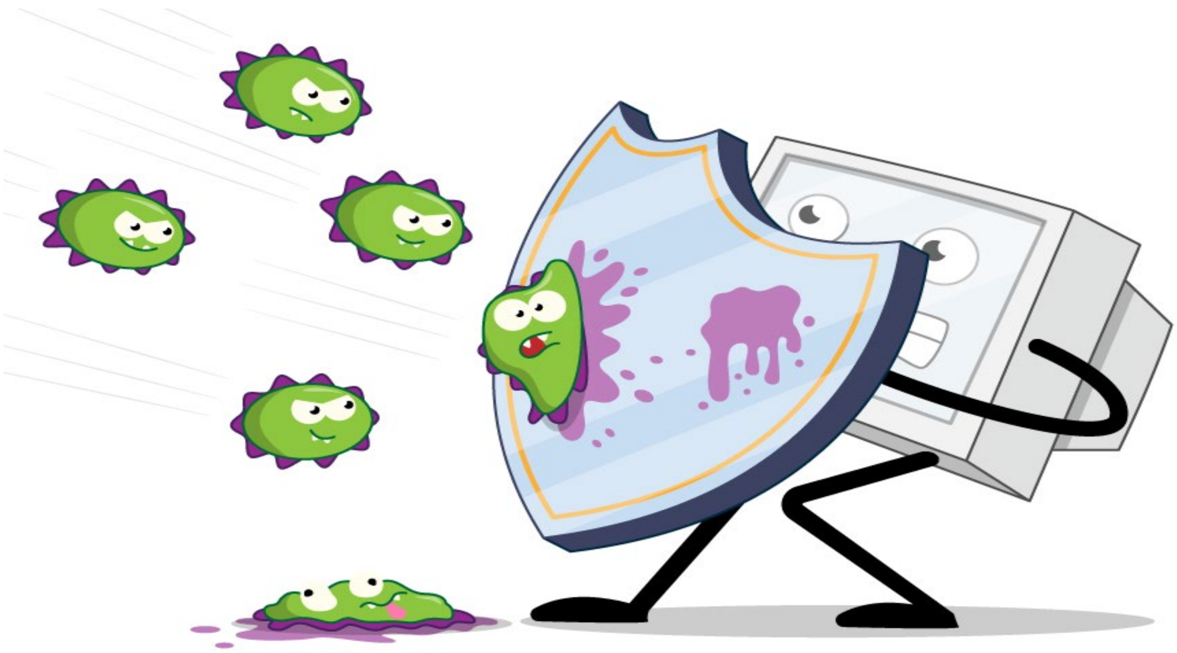
You should also install the HTTPS Everywhere extension. HTTPS Everywhere automatically directs you to the secure version of a site when the site supports that. This makes it difficult for an attacker, especially if you're on a public Wi-Fi at a coffee shop, airport, or hotel, to digitally eavesdrop on what you're doing. Some people may want to use a VPN but it's not necessary for everyone. If you frequently connect to a public Wi-Fi, a VPN is useful because it adds a layer of security to your browsing when HTTPS isn't available.

Use Antivirus Software on Your Computer

Viruses might not seem as common as they were a decade ago, but they still exist. Malicious software on your computer can wreak all kinds of havoc, from annoying pop-ups, covert bitcoin mining, to scanning for personal information. If you're at risk for clicking perilous links, or if you share a computer with multiple people in a household, it's worthwhile to set up antivirus software, especially on Windows computers.

If your computer runs Windows 10 or 11, you should use Microsoft's built-in software, Windows Defender. Windows Defender offers plenty of security for most people, and it's the main antivirus option that Wirecutter recommends; we reached that conclusion after speaking with several experts. If you run an older version of Windows (even though we recommend updating to Windows 11) or use a shared computer, a second layer of protection might be necessary. For this purpose, Malwarebytes Premium is your best bet. Malwarebytes is unintrusive, it works well with Windows Defender, and it doesn't push out dozens of annoying notifications like most antivirus utilities tend to do.

Mac users are typically okay with the protections included in macOS, especially if you download software only from Apple's App Store and stick to well-known browser extensions. If you do want a second layer of security, Malwarebytes Premium is also available for Mac. You should avoid antivirus applications on your phone altogether and stick to downloading trusted apps from official stores.



Update Your Software and Devices

Phone and computer operating systems, Web browsers, popular apps, and even smart-home devices receive frequent updates with new features and security improvements. These security updates are typically far better at thwarting hackers than antivirus software.

All three major operating systems can update automatically, but you should take a moment to double-check that you have automatic updates enabled for your OS of choice: Windows, macOS, or Chrome OS. Although it is frustrating to turn your computer on and have to wait out an update the security benefits are worth the trouble.

For third-party software and apps, you may need to find and enable a *Check for updates* option in the software's settings. Smart-home devices such as cameras, thermostats, and light bulbs can receive updates to the app as well as to the hardware itself. Check the settings using the device's app to make sure these updates happen automatically; if you don't find an automatic-update option, you may have to manually reboot the device on occasion (a monthly calendar reminder might help).

The Importance of Paranoia

Security and privacy are linked, so you need to get in the habit of protecting both. It might seem like a time-consuming and overwhelming headache, but once you follow these steps all that’s left is to cultivate your judgment and establish good online behaviors.

Be suspicious of links in emails and on social media. Make your accounts private and don’t share anything you wouldn’t mind getting out anyway.

Once you settle into a low-key, distrustful paranoia about new apps and services, you’re well on your way to avoiding many privacy-invading practices.