The best Internet security:

Layers of protection and good habits

After the on-line review site Wirecutter interviewed information security experts and experienced online-security journalists, they learned that no single app can protect you from an ever-changing array of new malware. The best protection consists of setting up and maintaining layers of security on your devices: keeping your operating system, browsers, and software updated, paying for decent but not overbearing virus and malware protection, installing browser extensions for Web privacy and security, and getting into smart security habits.

These tips aren't just for the tech-averse, or those starting over after a malware event—this guide is for everyone who uses a computer. The Wirecutter editors and writers working on this guide realized which layers they had neglected in their own setups. Sometimes the person who is confident in their setup—too confident—still ends up clicking the wrong link, or downloading the wrong PDF, and infecting their system with malware.

First layer:

Keeping your OS, browser, and other software up to date

Computers, browsers, and important apps receive updates more frequently now than in the late-1990s/early-2000s heyday of viruses, and the updates are often automatic and hard to avoid. That's a good thing—don't delay these updates, because they often contain important security fixes.

Operating systems

Windows 10 automatically installs updates, unless you go to some lengths to delay them. MacOS can install system updates automatically, and even automatically applies updates to apps you've downloaded through the official App Store. Chromebooks automatically update when you restart them (so you have to shut them down sometimes, instead of just putting them to sleep by closing them). If you haven't updated to the latest version of your OS—particularly if you're still on Windows 7 or 8 and haven't updated to Windows 10—you should do so as soon as possible.

It's frustrating to turn on your computer to do something and then wait while a large, slow update installs, and it's annoying when that update breaks a driver or messes up your software, as sometimes happens. But system updates are usually smaller, faster, and less disruptive than the big overnight-download updates that came to earlier Windows and Mac versions, and they're important for keeping your computer secure.

Browsers

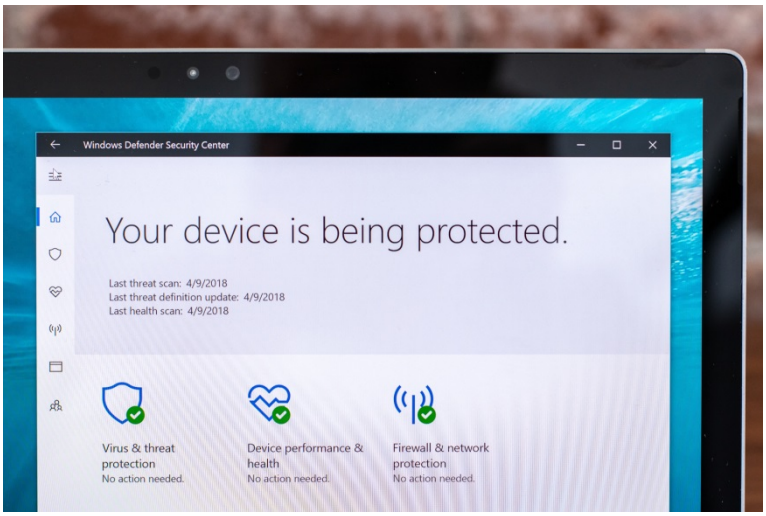
Most major Web browsers update automatically: Google's Chrome browser and Mozilla Firefox automatically download updates and install them the next time you launch the browser. But if you tend to leave huge collections of tabs open for days, you should restart when you see an available update and allow the browser to restore your tabs (or close them and be free). Microsoft's Edge browser updates along with Windows updates, and Safari receives updates through Apple's App Store. Extensions installed in Chrome, Firefox, Safari, and Edge also update automatically.

Important apps

Some apps bug you incessantly about tiny updates, while others never let you know about important fixes. If you use a program often, and especially if it connects to the Web (and most of them do), enable any "check for update" options in its settings.

Second layer:

Windows Defender



"If you have an up-to-date operating system, like Windows 10 or (macOS) High Sierra, there is no reason for a consumer to install any additional antivirus," said Rich Mogull, CEO and analyst at independent security research firm Securosis. "Operating systems have come an extremely long way since the days of Windows XP and rampant infections."

We think Windows Defender is good enough for most people using Windows. It receives regular updates from a dedicated security team, it doesn't monopolize resources, it doesn't bug you about upgrades or install unwanted programs, and the company behind it, Microsoft, would have a lot to lose if its built-in security app were to do something underhanded.

In Windows 10, Defender is set up to update itself automatically, run in the background, and bug you only if it hasn't been able to do a systemwide scan in a long while because you've been busy. Don't disable it, and don't stop its updates.

Apple's built-in protections are good enough that Mac owners don't need an all-in-one security suite like Norton or McAfee either, especially if they stick to good security habits, such as downloading apps from the App Store whenever possible. Even so, they're not fail-

proof—it's still a good idea to add an anti-malware layer that doesn't slow your system as much or pester you to upgrade.

Third layer:

Malwarebytes Premium

All viruses are a kind of malware, but malware includes a lot more than just viruses. The security experts we interviewed recommended that most people install Malwarebytes Free on Windows and macOS. A real-time scanning tool that runs without interruptions, Malwarebytes scans your system diligently without hogging resources. Rather than relying on a list of known bad software, it looks for any app or process exhibiting scummy behavior. It has some overlap with Windows Defender in what it protects against, but that's smart—much malware is written to work around the security built into the most common operating systems.

Fourth layer:

Helper apps

Once you've fortified your computer with an up-to-date operating system, browser, and antivirus and/or anti-malware apps, you should work to keep the things you do on your computer private, and to keep your accounts and sensitive data protected with strong tools. Here are our recommendations, from staff and experts, of the best additions to your security scheme:

uBlock Origin (available for Chrome, Firefox, Microsoft Edge, Safari**):** Install this ad blocker and privacy tool for your browser, and the only thing you have to do is occasionally turn it off on sites that won't work with its restrictions and whitelist sites you want to receive full advertising revenue. Meanwhile, it quietly blocks known tracking cookies that follow you from site to site and build an unnamed but revealing profile of you. It also blocks the worst-behaved ads, like the kind that pop up false alerts about your system being infected. We also like the Electronic Frontier Foundation's Privacy Badger, which blocks the cookies it notices tracking you as you browse, rather than maintaining a list of known offenders like traditional ad blockers do.

Make sure to install a verified, trustworthy ad blocker from the original maker of that extension, such as from our links above. Fake, malware-installing ad blockers are common, and these similarly named impostors may insert their own ads or track you.

HTTPS Everywhere: While many sites have shifted toward using an encrypted connection by default, too many sites offer it only as an option. This extension forces as many sites as possible to encrypt the page and ensure your browsing is a more private affair. With HTTPS enabled, the owner of the Wi-Fi you're using, the network administrator at work, and your Internet service provider can see only that you're on eff.org, for instance, not eff.org/jobs.

Password Managment: Using the same password, or slight variations of it, leaves you vulnerable to identity theft and privacy violations. Use a password manager like LastPass to make all of your passwords longer, random, and more secure.

VPN: A virtual private network encrypts all the traffic between your computer and a VPN server, which means nobody can monitor or modify your browsing, messaging, or other traffic. VPNs are most useful when you're connecting to untrusted or unsecure Wi-Fi networks, such as at coffee shops, hotels, or other public places where someone could be snooping, and they can also reduce the amount of data that large websites and services can collect about your online behavior, as detailed in our guide to VPNs. We recommend a subscription based VPN to ensure speed, security and support.

Fifth layer:

Good habits

Having a finely tuned car with the latest safety features isn't as important as having good driving habits. Similarly, the decisions you make while using your devices are the last thing you should address after setting up a secure system but are no less important. Based on our research and on experts' advice, here's what we recommend:

- **Enable two-factor authentication (2FA) on everything you can:** Two-factor authentication adds a second check after your password entry when you're logging in to accounts, so even someone who gets your password can't automatically gain access to your important accounts. Usually 2FA consists of a code texted to you or, even better, generated on an app like Google Authenticator or Authy. Sometimes it's a button prompt on a phone app, as with a Google account. Enable 2FA on your accounts at Google, Apple, Microsoft, Facebook and Twitter; on your password manager (LastPass or 1Password); and anywhere else you can. Your banks and medical accounts should offer two-factor authentication, and you should use it.
- **Encrypt your devices:** Encrypting the storage on your laptop, tablet, or phone protects against other people viewing or copying your personal data (even without your password) should your device get lost or stolen. Chromebooks are encrypted by default. Modern iOS and Android devices are also encrypted by default if you're using a screen lock—you can check if your Android device is encrypted by going to *Settings*, *Security & location*, *Encryption & credentials*(this path may differ slightly on different manufacturers' phones). If your Android device has a microSD card, you'll have to enable encryption for that external storage manually.
- **Use strong passcodes or biometric locks:** If your device offers a way to lock it with your fingerprint or face, use that as the primary unlocking method, in addition to a strong backup password or passcode. Avoid swiping patterns and easily guessed four-digit PINs, especially on touchscreen devices where your recent finger taps could be visible.
- **Get your software from official app stores:** Whenever possible, avoid downloading software from websites you found on Google. Instead, get that software, or something similar, in the Microsoft Store, the Mac or iOS App Store, Android's Google Play, the Chrome Web Store, Firefox Add-ons, Safari Extensions, or Extensions for Microsoft Edge. Numerous experts recommended this step as a significant shield against installing malware, and a way to ensure your apps get updates when security vulnerabilities arise. Official app stores aren't foolproof, but they are much safer than websites you find through search.
- **Pay for software that's regularly updated:** If you need software that isn't in an app store, look for apps that are frequently updated. That usually means software you pay

for—when people pay for software, the author has incentive to maintain it, update it, and not seek payment through underhanded means, like search hijacking or the sale of customer data.

- **Don't download free things you know cost money:** Software cracks, free MP3s, illegal live streams, video files with cryptic file names—you're paying for these things somehow, and often it's by opening up access to your computer or your browsing habits.
- **Treat links and files in email and social media as guilty until proven innocent:** If you weren't expecting an email or a direct message—even if it appears to be from someone you know and trust—be particularly cautious about clicking its links or opening its files. Hover over links in emails and on social networks, and look at your browser's status bar to see where they actually go. If it's a shortened link, use GetLinkInfo.com to see what it expands to. *No site should ever ask you, in an email or a direct message, to enter your existing password to deal with an account or security issue.* If you're ever uncertain, just the slightest bit, about whether a link or an email is really from the site it claims to be from, head directly to the site to deal with the issue instead of clicking the link in the message.
- **Back up your computer:** If you follow the above advice, you're unlikely to get ransomware—malware that encrypts important files on your computer and then offers to sell you the encryption key so you can get them back—but no security is flawless. Everyone should back up their data, and here's our step-by-step guide to backing up your computer. If your machine is infected, you can remove the ransomware, restore your files, and go about your day without worrying about how to get Bitcoin to a dark-web address.

What about phones?

Almost everything we've written above about computers applies to modern smartphones as well, but you should especially focus on keeping your apps updated, using strong biometric logins and passcodes, sticking to official app stores, avoiding suspicious links, and setting up accounts with two-factor authentication and strong passwords stored in a password manager.

As for keeping your phone updated and secure, that's trickier, at least for Android phones. Manufacturers are bad at updating Android phones, even their expensive "flagship" models. Although Google updates its own apps frequently, independent of manufacturers, operating system upgrades and security updates don't reach most Android phones. The exceptions are Google's own phones: the high-end Pixel phones, and the more affordable Android One models. These phones receive regular security updates, and should get operating system upgrades for three years.

Apple does a lot better at getting updates out to iPhone owners, even iPhones that are four to five years old. That said, if your iPhone is no longer receiving iOS updates, or if important apps are showing notifications that they're no longer supported on your OS version, it's time to upgrade.

This article may have been updated by Wirecutter. To see the current content, please go here.