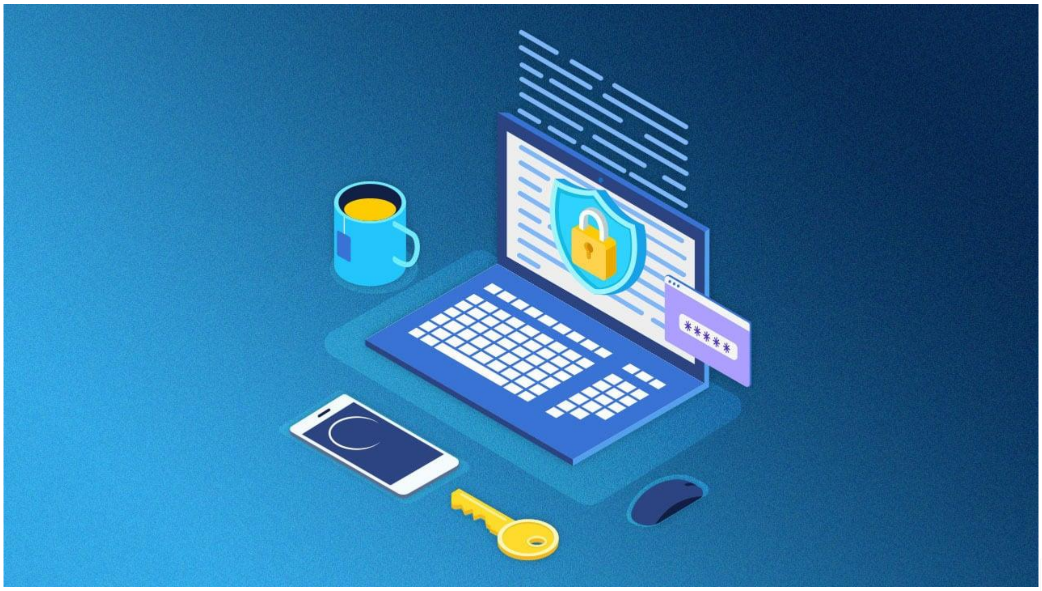
12 Simple Things You Can Do to Be More Secure Online

Follow these easy tips to protect the security of your devices, your data, your internet traffic, and your identity.

By Neil J. Rubenking & Jill Duffy

Updated April 17, 2023



(Image: Getty Images/Nadezhda Buravleva)

Every week brings news of yet another data breach. Schools, factories, websites, and even government agencies get caught with their protection down, and we all suffer. There's nothing you can do to prevent these faraway breaches, but rather than bemoan that fact, get busy! There's plenty you can do to protect your own devices, data, and privacy.

Making your devices, online identity, and activities more secure doesn't take much effort. Several of the following tips boil down to little more than common sense, yet they'll help keep you safer online.

1. Install Antivirus Software and Keep It Updated

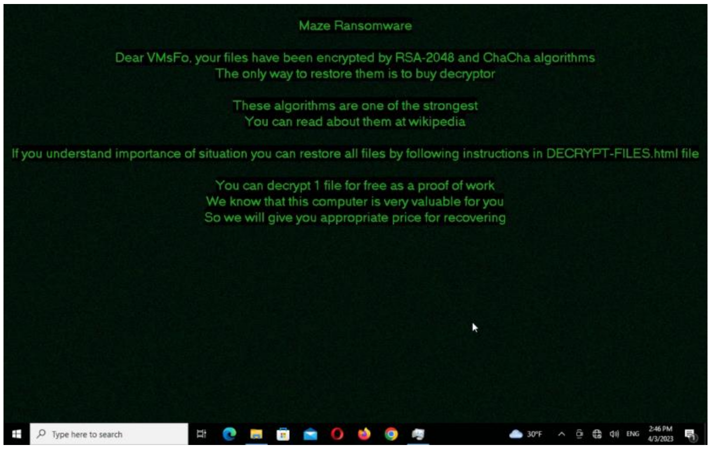
We call this type of software antivirus, but fending off actual computer viruses is just one small part of what they do. Ransomware encrypts your files and demands payment to restore them. Trojan horse programs seem like valid programs, but behind the scenes, they steal your private information. Bots turn your computer into a soldier in a zombie army, ready to engage in a denial-of-service attack, spew spam, or whatever the bot herder commands. An effective antivirus protects against these and many other kinds of malware.

It's Surprisingly Easy to Be More Secure Online

In theory, you can set and forget your antivirus protection, letting it hum along in the background, download updates, and so on. In practice, you should look it over every now and then. Most antivirus utilities display a green banner or icon when everything is hunky-dory. If you open the utility and see yellow or red, follow the instructions to get things back on track.

You may be thinking, wait, isn't antivirus built into Windows? Not only is Microsoft Defender Antivirus baked into the operating system, it automatically takes over protection when it detects no other antivirus, and it just as automatically steps aside when you install third-party protection. The thing is, this built-in antivirus just doesn't compare with the best third-party solutions. Even the best free ones are way better than Defender. Don't rely on it; you can do better.

Whether you've chosen a simple antivirus or a full security suite, you'll need to renew it every year. Your best bet is to enroll in automatic renewal. With some security products, doing so enables a malware-free guarantee. You can always opt out later if you get the urge to switch to a different product.



Maze Ransomware

Dear VMsFo, your files have been encrypted by RSA-2048 and ChaCha algorithms
The only way to restore them is to buy decryptor

These algorithms are one of the strongest
You can read about them at wikipedia

If you understand importance of situation you can restore all files by following instructions in DECRYPT-FILES.html file

You can decrypt 1 file for free as a proof of work
We know that this computer is very valuable for you
So we will give you appropriate price for recovering

(Credit: PCMag)

One more thing. If your antivirus or security suite doesn't have ransomware protection, consider adding a separate layer of protection. Many ransomware-specific utilities are entirely free, so there's no reason not to try a few of them and select the one that suits you best.

---

2. Explore the Security Tools You Install

Many excellent apps and settings help protect your devices and your identity, but they're only valuable if you know how to use them properly. To get the maximum protective power from these tools, you must understand their features and settings. For example, your smartphone almost certainly includes an option to find it if lost, and you may have even turned it on. But did you actively try it out, so you'll know how to use it if needed?

Most antivirus tools have the power to fend off Potentially Unwanted Applications (PUAs), troublesome apps that aren't exactly malware but don't do anything beneficial. But not all of them enable PUA detection by default. Check the detection settings and make sure yours are configured to block these annoyances. Likewise, your security suite may have components that aren't active until you turn them on. When you install a new security product, flip through all the pages of the main window, and at least take a glance at the settings. If it offers an initial onboarding tour, don’t skip it—rather, go through the tour methodically, paying attention to all the features.

Antivirus tools usually include some form of browsing protection, typically in the form of a browser extension. If you accidentally try to visit a dangerous page or a phishing fraud, they divert the browser to a safe warning page. Many of them mark up search results so you don't even click on a dangerous link. And all this helps you not at all if you don't have the browser extension installed and working. Check each browser you use to make sure it's protected.

To be extra sure your antivirus is configured and working correctly, you can turn to the AMTSO's (Anti-Malware Testing Standards Organization) security features check. If your antivirus doesn't pass, it's time to contact tech support and find out why.

---

3. Use Unique Passwords for Every Login

One of the easiest ways hackers steal information is by getting a batch of username and password combinations from one source and trying those same combinations elsewhere. For example, let's say hackers got your username and password by hacking an email provider. They might try to log into banking sites or major online stores using the same username and password combination. The single best way to prevent one data breach from having a domino effect is to use a strong, unique password for every single online account you have.

Our Top Password Manager Picks

Keeper Password Manager & Digital Vault Review

Creating a unique and strong password for every account is not a job for a human. That is why you use the random password generator built into your password manager. Several very good password managers are free, and it takes little time to start using one. For-pay password managers generally offer more features, however.

When you use a password manager, the only password you need to remember is the master password that locks the password manager itself. When unlocked, the password manager logs you into your online accounts automatically. That not only helps keep you safer but also increases your efficiency and productivity. You no longer spend time typing your logins or dealing with the time-consuming frustration of resetting a forgotten password.

One more thing to consider. If you get creamed by a self-driving car tomorrow, how will your heirs manage to access your accounts? The most advanced password managers let you identify a password heir, someone who will receive access to your account after you shuffle off this mortal coil.

---

4. Get a VPN and Use It

Any time you connect to the Internet using a Wi-Fi network that you don't own, you should use a virtual private network or VPN. Say you go to a coffee shop and connect to a free Wi-Fi network. You don't know anything about the security of that connection. It's possible that someone else on that network, without you knowing, could start looking through or stealing the files and data sent from your laptop or mobile device. The hotspot owner might be a crook, sniffing out secrets from all Wi-Fi connections. A VPN encrypts your internet traffic, routing it through a server owned by the VPN company. That means nobody, not even the owner of the free Wi-Fi network, can snoop on your data.

Using a VPN also hides your IP address. Advertisers and trackers looking to identify or geolocate you via that IP address will instead see the VPN company's address. Spoofing your location using a VPN server in another country can also serve to unlock content that's not available in your own region. On a more serious note, journalists and activists in repressive countries have long used VPN technology to communicate securely.

The upshot is that if you connect via Wi-Fi—whether it's on a laptop, phone, or tablet—you really need a VPN. If you've never used one before, or the technology sounds a bit beyond your internet savvy, don't worry, we've got covered with our feature on how to set up and use a VPN.

---

5. Use Multi-Factor Authentication

Multi-factor authentication can be a pain, but it absolutely makes your accounts more secure. Multi-factor authentication means you need to pass another layer of authentication, not just a username and password, to get into your accounts. If the data or personal information in an account is sensitive or valuable, and the account offers multi-factor authentication, you should enable it. Gmail, Evernote, and Dropbox are a few examples of online services that offer multi-factor authentication.

What Is Two-Factor Authentication?

Multi-factor authentication verifies your identity using at least two out of three different forms of authentication: something you are, something you have, or something you know. Something you know is the password, naturally. Something you are could mean authentication using a fingerprint, or facial recognition. Something you have could be your mobile phone. You might be asked to enter a code sent via text or tap a confirmation button on a mobile app. Something you have could also be a physical Security Key; Google and Microsoft have announced a push toward this kind of authentication.

If you just use a password for authentication, anyone who learns that password owns your account. With multi-factor authentication enabled, the password alone is useless. Most password managers support multi-factor, though some only require it when they detect a connection from a new device. Enabling Multi-factor authentication for your password manager is a must.

Our feature on who has multi-factor authentication and how to set it up can help you get started.

---

6. Use Passcodes Even When They Are Optional

Apply a passcode lock wherever available, even if it's optional. Think of all the personal data and connections on your smartphone. Going without a passcode lock is unthinkable.

Many smartphones offer a four-digit PIN by default. Don't settle for that. Use biometric authentication when available, and set a strong passcode, not a stupid four-digit PIN. Remember, even when you use Touch ID or equivalent, you can still authenticate with the passcode, so it needs to be strong.

Modern iOS devices offer a six-digit option; ignore it. Go to Settings > Touch ID & Passcode and select Change Passcode (or Add Passcode if you don't have one). Enter your old passcode, if needed. On the screen to enter the new code, choose Custom Alphanumeric Code. Enter a strong password, then record it as a secure note in your password manager.

Different Android devices offer different paths to setting a strong passcode. Find the Screen Lock settings on your device, enter your old PIN, and choose Password (if available). As with the iOS device, add a strong password and record it as a secure note.

7. Pay With Your Smartphone

The system of credit card use is outdated and not very secure at all. That's not your fault, but there is something you can do about it. Instead of whipping out the old credit card, use Apple Pay or an Android equivalent everywhere you can. There are tons of choices when it comes to apps. In fact, we have an entire roundup of mobile payment apps.

Setting up your smartphone as a payment device is typically a simple process. It usually starts with snapping a picture of the credit card that you'll use to back your app-based payments. And setup pretty much ends there; you're ready.

Point-of-sale terminals that support smartphone-based payment usually indicate the fact with an icon, from a picture of a hand holding a smartphone to a stylized representation of a radio wave. Just place your device on the terminal, authenticate with a thumbprint or face recognition, and you've paid up.

How is that better than using the credit card itself? The app generates a one-use authentication code, good for the current transaction only. Even if someone filched that code, it wouldn't do them any good. And paying with a smartphone app eliminates the possibility of data theft by a credit card skimmer.

Some smartphone payment apps let you pay online with a similar one-time code. If yours doesn't, check with your credit card provider. Typically, you get a temporary number to use in place of your real credit card, and the charges go to your regular account. The temporary card number will not work again after it expires. The next time your credit card company or bank calls you to try and sell you upgrades, ask about one-time use card numbers.

You can also get the protection of one-use credit card numbers using third-party apps. IronVest, for example, can mask credit card numbers, email addresses, and phone numbers. You shop and communicate as always, but the merchant doesn't receive your actual information.

---

8. Use Different Email Addresses for Different Kinds of Accounts

People who are both highly organized and methodical about their security often use different email addresses for different purposes, to keep the online identities associated with them separate. If a phishing email claiming to be from your bank comes to the account you use only for social media, you know it's fake.

Is Your Security Software Even Working? Here's How to Check

What Really Happens In a Data Breach (and What You Can Do About It)

Don't Be Caught by Email Scams: How to Avoid Phishing

Consider maintaining one email address dedicated to signing up for apps that you want to try, but which might have questionable security, or which might spam you with promotional messages. After you've vetted a service or app, sign up using one of your permanent email accounts. If the dedicated account starts to get spam, close it, and create a new one. This is a do-it-yourself version of the masked emails you get from IronVest and other disposable email account services.

Many sites equate your email address with your username, but some let you select your own username. Consider using a different username every time—hey, your password manager remembers it! Now anyone trying to get into your account must guess both the username and the password.

---

9. Clear Your Cache

Never underestimate how much your browser's cache knows about you. Saved cookies, saved searches, and Web history could point to home address, family information, and other personal data.

To better protect that information that may be lurking in your Web history, be sure to delete browser cookies and clear your browser history on a regular basis. It's easy. In Chrome, Edge, Firefox, Internet Explorer, or Opera, simply press Ctrl+Shift+Del to bring up a dialog that lets you choose which elements of browser data you want to clear. If you use a different browser, try that key combo regardless; it might work. Otherwise, search the menu.

Deleting cookies may cause trouble for some websites—you may lose any personalization you've applied. Most browsers let you list favorite websites whose cookies shouldn't be tossed.

For a complete guide to getting started, you can read our feature on how to clear your cache in any browser.

---

10. Turn Off the 'Save Password' Feature in Browsers

Speaking of what your browser may know about you, most browsers include a built-in password management solution. We at PCMag don't recommend them, however. We feel it's best to leave password protection to the experts who make password managers.

Think about this. When you install a third-party password manager, it typically offers to import your password from the browser's storage. If the password manager can do that, you can be sure some malicious software can do the same. In addition, keeping your passwords in a single, central password manager lets you use them across all browsers and devices.

---

11. Don't Fall Prey to Click Bait or Phishing Scams

Part of securing your online life is being smart about what you click. Clickbait doesn't just refer to cat compilation videos and catchy headlines. It can also comprise links in email, messaging apps, and Facebook. Phishing links masquerade as secure websites, hoping to trick you into giving them your credentials. Drive-by download pages can cause malware to automatically download and infect your device.

Don't click links in emails or text messages, unless they come from a source you trust. Even then, be cautious; your trusted source might have been compromised, or the message might be fake. The same goes for links on social media sites, even in posts that seem to be from your friends. If a post seems unlike the style of your social media buddy, it could be a hack.

For more, read our story on how to avoid phishing scams.

---

12. Protect Your Social Media Privacy

There’s a common saying: if you’re not paying for a service, you’re not a customer; you’re the product. Social media sites make it easy for you to share your thoughts and pictures with friends, but it’s easy to wind up sharing too much.

You can download your Facebook data to see just what the social media giant knows about you. It may be quite an eye-opener, especially if you're the kind of person who routinely clicks on quizzes that require access to your social media account. Really, you don't need to know which Disney princess or dog breed you are.

Beware, too, of hackers posing as your social media friends. A common scam starts with a private message and ends with hackers taking over your account and using it to continue the scam. If you get an odd or unexpected private message from a friend, ask about it using email or some other type of communication. Your friend may have been scammed.

You can drastically reduce the amount of data going to Facebook by disabling the sharing platform entirely. Once you do, your friends can no longer leak your personal data. You can't lose data to apps, because you can't use apps. And you can't use your Facebook credentials to log into other websites (which was always a bad idea).

Of course, other social media sites need attention too. Google probably knows more about you than Facebook, so take steps to manage your Google privacy, too. Make sure you've configured each social media site so that your posts aren't public (well, all except Twitter and other broadcast media services). Think twice before revealing too much in a post, since your friends might share it with others. With care, you can retain your privacy without losing the entertainment and connections of social media.