6 Things You Need to Do to Prevent Getting Hacked

wired.com/story/how-to-prevent-getting-hacked

Matt Burgess, WIRED UK August 29, 2021

There are two big reasons why people get hacked. Flaws in software and flaws in human behavior. While there's not much you can do about coding vulnerabilities, you can change your own behavior and bad habits.

Just ask former US president Donald Trump, whose Twitter password was "maga2020!" Or Boris Johnson, who revealed details of sensitive Zoom calls at the start of the pandemic in 2020. (These world leaders will have had specific security training from protection agencies too.)

The risks are just as real for the average person—even if the stakes aren't quite so high. If your accounts aren't properly protected, your credit card could be compromised or your private messages and photographs stolen and shared for all to see. Working out if your accounts have been hacked is a time-consuming and potentially frustrating process. You're better off taking some steps to mitigate the risks of getting hacked in the first place. Here's what you can do to protect yourself.

Use Multi-Factor Authentication

Arguably the most effective thing you can do to protect your online accounts is turning on multi-factor, or two-factor, authentication for as many of your accounts as possible. The method uses a secondary piece of information—often a code generated by an app or sent via

SMS—alongside a password.

This secondary piece of information helps to prove it really is you trying to log in, as the codes are often accessed on the phone in your pocket. Even if you do have a password that's easy to guess (we'll get to that shortly), an attacker is unlikely to get access to an account with multi-factor authentication turned on unless they have your phone.

There's a guide to all the accounts that support the method here, but in the first instance you should turn it on for all the accounts that hold personal information that could be abused. Like messaging apps such as WhatsApp, social media including Facebook, Instagram, and Twitter, and your email accounts.

Not all forms of multi-factor authentication are equal though. Code-generating apps are considered more secure than getting codes via SMS, and beyond that, physical security keys provide an even more robust layer of protection.

Get a Password Manager

Let's talk about passwords. It's 2021. You shouldn't be using "password" or "12345" for any of your passwords—even if it's a throwaway account.

All the passwords you use for your online accounts should be strong and unique. What this really means is they should be long, include a mixture of different character types, and not be used across multiple websites. Your Twitter password shouldn't be the same as your online banking one; your home Wi-Fi network shouldn't use the same credentials as your Amazon account.

The best way to do this is by using a password manager. Password managers create strong passwords for you and store them securely. If the fact that they can stop you getting hacked isn't enough to make you consider using one, a password manager also means you never have to struggle to remember a forgotten password again.

From our testing of the best password managers our there, we recommend trying out LastPass or KeePass.

Learn How to Spot a Phishing Attack

Quickly clicking can be your worst enemy. When a new email or text message arrives, and it includes something that can be tapped or clicked, our instincts often lead us to do it straight away. Don't.

Hackers have used the pandemic as cover to launch wave after wave of phishing attacks and dumb Google Drive scams.

Anyone can fall for these types of scams. The main thing to do is to think before you click. Scam messages try to trick people into behaving in a way they wouldn't normally—with, say, pretend instant demands from a boss or messages that say an urgent response is required.

There's no foolproof way to identify every type of phishing effort or scam—scammers are constantly upping their game—but being aware of the threat can help reduce its effectiveness. Be cautious, think before you click, and download files only from people and sources you know and trust.

Update Everything

Every piece of technology you use—from the Facebook app on your phone to the operating system that controls your smart lightbulb—is open to attack. Thankfully, companies are always finding new bugs and fixing them. That's why it's crucial you download and update the latest versions of the apps and software you're using.

Start with your phone. Navigate to your device settings and find out what operating system you're using, and update it if you're not on the latest version (iOS 14 is the latest for iPhones; Android 11 is the latest from Google). For apps and games, Apple's iOS 13 and above downloads updates automatically, although these settings can be customized. On Android, auto-updates can also be turned on by visiting the settings page in the Google Play Store.

Once you've updated your phone, you need to work out what devices to update next. Generally these should be done in order of potential impact. Any laptops and computers you own should be high up the list, and then work back through other connected devices in your life. Remember: Everything is vulnerable, including your internet-connected chastity belt.

Encrypt Everything

Protecting your communications has never been easier. Over the last half-decade, companies handling our personal data—including the messages we send and the files we upload to the cloud —have realized that encryption can help them as well as their customers. Using encrypted services means that what you're sending is better protected against surveillance and won't be accessible if your device gets lost or stolen.

There are two main end-to-end encrypted messaging services, Signal and WhatsApp. Messages (including photos and videos) plus voice calls and video calls are encrypted by default within both apps. They both also let you use disappearing messages, which remove what you've sent after a set period of time. The practice can help keep your chats private, even from those that have access to your devices. Our advice is to use Signal where possible, as it collects less metadata than WhatsApp and isn't owned by Facebook. But if you can't get your friends to move to Signal, WhatsApp offers a lot more protection than apps that don't use end-to-end encryption by default.

For your emails, encrypted provider ProtonMail can protect your messages, and there's also the option to use burner email accounts for mailing lists and purchases where you don't want to hand over your personal data.

Beyond your messages, encrypting the files on your devices can help reduce the chances of your data being compromised if you're hacked or lose your devices. Both iPhone and iOS encrypt your hard drive by default. Just make sure you use a strong password or PIN for your devices. A little more effort is needed to encrypt the hard drive on your laptop or computer. Turn on Apple's FileVault to encrypt your startup disk, and on Windows you can turn encryption on through the Settings menus or use BitLocker encryption.

Wipe Your Digital Footprint

The past can come back to haunt you. The old online accounts you no longer use and the login details that belong to them can be weaponized against you if you don't do anything about them. Hackers frequently use details from previous data breaches to access the accounts people currently use.

Reducing the amount of information that's available about your online life can help cut your risk of being hacked. A very simple step is to regularly delete your Google search history, but you can also use privacy-first Google alternatives.

Beyond this, there's a lot more you can do to reduce your digital footprint. Find the old accounts you no longer use and delete them. It'll reduce the amount of spam you get and reduce the number of ways hackers can target you. Use Have I Been Pwned? to find your information in old data breaches, use a VPN to boost browsing privacy, and download Tor if you really want to boost your online anonymity.

This story originally appeared on WIRED UK.