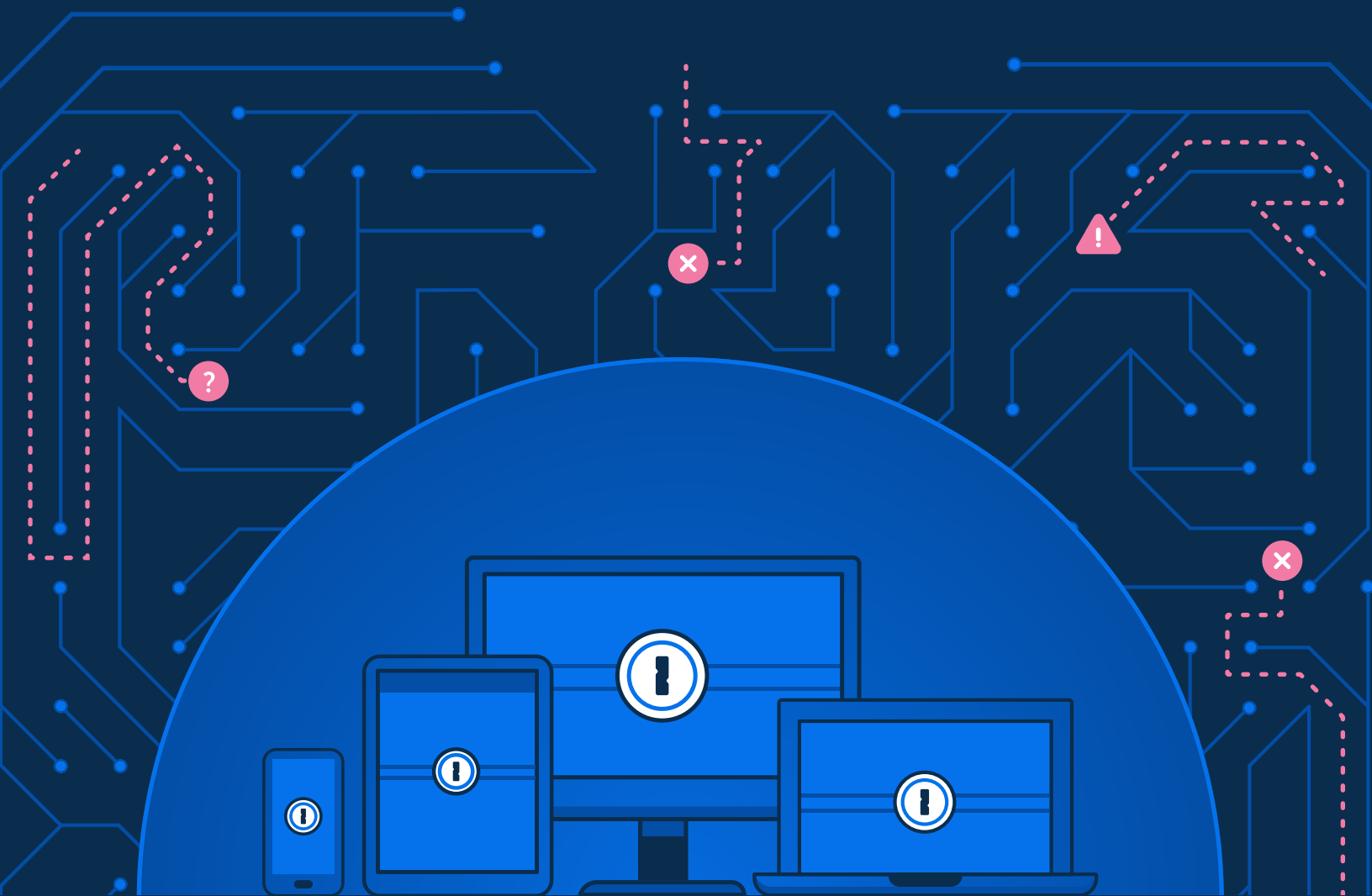


# A beginner's guide to cybersecurity

15 tips to protect your data  
and stay safe online



The internet is littered with stories about data breaches and people who have lost their accounts to cybercriminals. But don't be alarmed! It doesn't take much to protect yourself from the vast majority of attacks. For Cybersecurity Awareness Month, we've put together a list that anyone can follow to improve their digital defenses – both at home and in the office. By the end, you'll enjoy more peace of mind while using your favorite devices and services, knowing that you're following best practices to keep your logins and personal data safe.

## Passwords

### 1. Use strong, unique passwords

That means no common passwords like "123456," "qwerty" and "password," or anything that includes your name or date of birth. They should also be long – we recommend at least 16 characters.

All of your passwords should be unique, too. You might use Single-Sign On (SSO) at work, which lets you log into multiple apps and services with the same credentials. It doesn't matter, however, whether you need to remember 10 or 10,000 passwords – all of them still need to be strong and unique. If you use the same set of characters for everything, you're putting your company at risk.

?

#### But why?

Imagine you signed up for a new social network. Then, six months later, it was breached and every user's password was leaked onto the internet. If you use the same password for everything, a criminal could use your leaked credentials to access other accounts you own.

Of course, no one can remember 100 different passwords – especially if they're random strings like "UmxT9t4s8B6sVhr6mvSo." The solution? Adopt a password manager that can do the creating and remembering for you.

## 2. Share passwords securely.

Everyone has passwords that they need to share from time to time. At home, it could be the Wi-Fi password or the credentials for a video streaming service. At work, you might need to share a subscription to a trade publication, or the license key for a particular piece of software.

Don't rely on post-it notes, insecure text messages, emails, spreadsheets, or random text documents for these – switch to a password manager like 1Password. It's secure and convenient because everyone will know exactly where to find and access your shared credentials.

## 3. Use two-factor authentication everywhere it's offered.

Two-factor authentication (2FA) is an extra layer of security that protects your accounts from thieves who have managed to find or deduce one of your passwords.

?

### How it works:

You can ask for a time-based one-time password (TOTP) to be sent any time someone tries to sign into your account – it could be via email, a dedicated authentication app, or text message (though we don't recommend using SMS as it's vulnerable to interception). Whoever is trying to sign-in will then be asked to submit the TOTP along with your password. It's a great system because an attacker is unlikely to have access to both the password and the place where you retrieve your TOTP.

You can even use 1Password to store and deliver these special codes. It's not quite the same as 2FA because your passwords and TOTP are stored in the same place, but this approach still offers plenty of security benefits and reduces the friction of using 2FA. If a criminal found one of your passwords in a leak, for example, they wouldn't be able to log in without the TOTP code that you have stored inside 1Password.



## Hardware

### 4. Keep your devices up to date.

Most operating systems give you the option to apply security updates automatically. As a general rule, you should only use hardware that can run the latest version of Windows, macOS, Linux, iOS, or Android. And don't use an operating system that is no longer receiving security updates, like Windows 7 – especially if you're planning to use the internet.

### 5. Protect your devices with a strong password or PIN.

That means your PIN can't be "1111" or the year you were born (they're simply too easy for a criminal to guess). Alternatively, use a biometric unlock method like Windows Hello or Face ID. Both are convenient without compromising your device's overall security.

### 6. Consider encrypting your hard drives.

Full-disk encryption (FDE) protects your system's entire hard drive, including the operating system. If an attacker stole your device, they would be asked to provide the encryption key – which typically comes in the form of a password – to complete the boot up process and access any data on the drive. To get started, follow the guides provided by [Apple](#), [Microsoft](#) and the [Linux community](#).

## 7. Don't leave your devices alone in public places.

Now that the world is opening back up again, don't forget that you should be on your guard in cafes, hotel lobbies and other public spaces. You should never leave your devices unattended, and if you need to get up momentarily – to greet someone or retrieve a coffee order, for example – you should lock them or take them with you, just in case.



*One for the office!*

### **Adopt the same mentality at work.**

Your office should be safe from criminals. Nevertheless, it's important to lock your devices whenever you leave your desk. You don't want to give anyone the chance to read your emails, steal sensitive company data, or take a picture of the top-secret project you're working on.

## 8. Turn on any 'Find My' feature that's available.

You might work for a company that uses Mobile Device Management (MDM) software to help them track down lost hardware. If not, consider enabling any 'Find My' service that's available on your devices. As the name implies, it will help you pinpoint your laptop, tablet or phone if it ever goes missing. If you're particularly forgetful, consider investing in some Bluetooth trackers – like the ones made by Tile, or Apple's AirTags – for other belongings that don't have a Find My service built-in.





*One for the office!*

### **Keep your work and personal life separate.**

If you've been given a work computer, remember that it's just that: a device for work. Don't give it to your children to play Fortnite, or to an older relative who is desperate to check their emails. If you have permission to use your device outside of work, take special care to ensure your personal and corporate data is kept separate.

## **9. Protect your router.**

Your home router needs to be patched and updated occasionally, just like your smartphone and computer. You should opt into automatic updates or periodically check for new security patches. You should also protect your router with strong, unique passwords. That includes the router password – which is required to change various settings – and the Wi-Fi network password.

## **10. Be careful when connecting to public Wi-Fi networks.**

If you've updated your router and set a strong password, you can be confident that your home Wi-Fi network is pretty secure. And if you work in an office, you should be able to trust the building's Wi-Fi. In public, however, it's a different story. Some public Wi-Fi networks are secure, but a large number are not. Attackers can use the latter to snoop on your web traffic and use that information for any number of unsavory things ranging from account stealing to identity theft.

But that doesn't mean you should never use a public Wi-Fi network. Connect through a VPN where possible and avoid Wi-Fi networks with suspicious names (it doesn't take a security expert to know that "REALFreeAirportWIFI" probably isn't legitimate). If you're not sure, check with a nearby member of staff, or simply wait and connect somewhere else.

# Software



*One for the office!*

## **Think about segmentation when using apps like Slack and Microsoft Teams.**

The pandemic has forced more companies to experiment with apps like Slack, Microsoft Teams, and Discord. They're incredibly powerful but need to be used responsibly. Stop and think before inviting someone into a new chat room, group, or channel. Do they really need access to a management-level discussion? And should that access be revoked after a period of time?

It's important to use groups and rooms, each with their own privacy settings, to keep information on a need-to-know basis. Otherwise, it's more likely that sensitive information will leak or be accidentally shared with someone outside of your organization.

## **11. Switch to an end-to-end encrypted messaging app.**

End-to-end encryption ensures that no-one can read your messages. That includes the company who developed the app and any government who might be interested in reading your messages. It might seem like overkill – especially if you think that you have nothing to hide – but it's important to protect your privacy and that of the people you talk to.

Many cybersecurity experts recommend Signal, which is powered by the open-source Signal Protocol and offers end-to-end encryption by default. Other options include WhatsApp, Apple iMessage, Telegram, Viber, and Wire.

## 12. Ensure strangers can't join your video calls.

You don't want a random person sneaking into your family quiz night, or your company's quarterly review meeting. If you're using a platform like Zoom, make sure the call is private and invite-only. And if you have a shareable link, be careful where you post it.

## 13. Take care with files stored in the cloud.

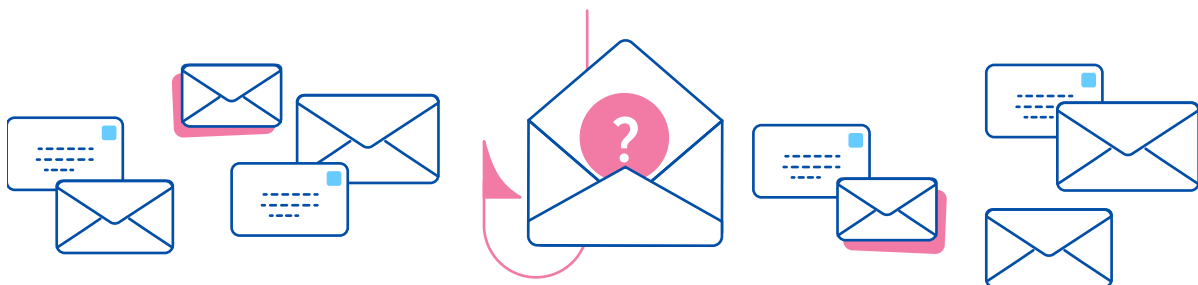
Many people use cloud-based platforms like Google Docs and Microsoft Office Online at work, or to complete school assignments and passion projects at home. If you need to share a project with someone else, be mindful of the privacy and permission settings you've chosen. If the file is sensitive, make sure that only invited people – rather than anyone with the correct link – can open it.

## 14. Check and double-check your email before pressing send.

Particularly the 'To' field. You don't want to misspell an email address and send important documents to a complete stranger.

## 15. Watch out for phishing emails.

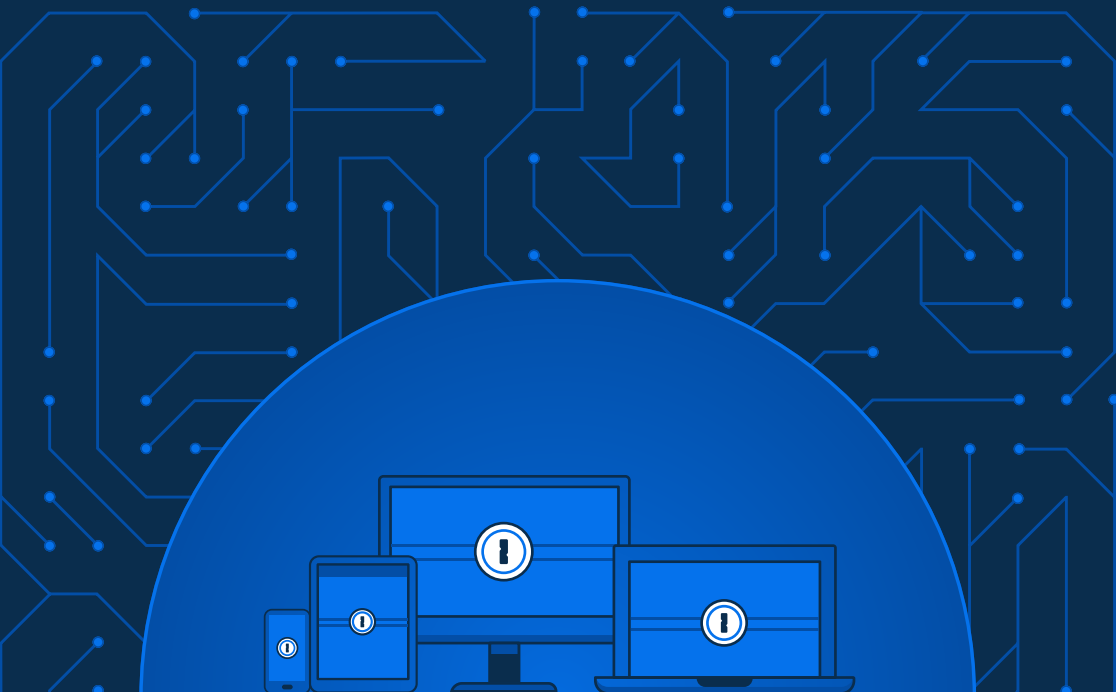
Cybercriminals will often impersonate a reputable company or person – a tactic known as phishing – and urge you to click on a link that seems legitimate, but actually sends you to a malicious site designed to steal your credentials or personal information.





Keep your eyes peeled for phishing attempts. Check the sender's email address (does it seem legitimate?) and whether you've received any messages from them before. Scan for typos and pay close attention to any language that suggests you need to take quick, drastic action. If anything seems amiss, reach out to the supposed sender another way and check the email was authentic.

Simply using a password manager can help protect you against phishing attacks. Every time you save a password, 1Password makes a note of the website URL. If you visit a scam site, the URL won't match and 1Password won't offer to autofill your account credentials. That way, you'll never be tricked into logging into a scam site like `paypa1.com` with your genuine PayPal username and password.

An illustration on a dark blue background featuring a large, lighter blue dome shape. Inside the dome, there is a desktop monitor, a laptop, a tablet, and a smartphone. Each device has a white circular icon with a black exclamation mark inside, representing a security alert or lock. The background is filled with a complex network of white circuit lines and dots, suggesting a digital or cyber environment.

**Want to learn more?**

Head to [1Password.com/resources](https://1password.com/resources) for guides, reports and white papers that will help you stay secure both at home and work.