

12 tips for protecting your data and internet-connected devices

Here are 12 tips for keeping your email, personal accounts, and internet-connected devices safer from cyberattacks:

1

Be skeptical of messages with links, especially those asking for personal information

[Fake links and websites](#) can be very convincing. Rather than trusting links, hover over the link to check the URL, go directly to the official website to verify, or find a phone number on the sender's official website so you can call them directly to confirm the message is legitimate.

2

Be on guard against messages with attached files

Never open unexpected attachments or embedded items, even if they seem to come from people or organizations you trust. If you are concerned that the message may be important, call the sender to verify.

3

Keep your digital workspace clean and simple

Remove unnecessary apps and browser extensions. Your IT team can help identify and remove potential security risks through regular device health checks.



4

Install software updates immediately

App, browser, and operating system updates often fix security vulnerabilities that can be exploited. Enable automatic security updates, when possible, to stay protected without extra effort.

5

If you must use passwords, make them strong and unique with a password manager

Strong passwords have at least 14 random characters and symbols. Use [Microsoft Edge](#) to remember passwords and manage password changes.



6

Enable the lock feature on all your mobile devices

Require a PIN, fingerprint, or facial recognition to unlock your device.

7

Share personal information only in real time

Use your device's official app store. Your IT team can also provide approved business apps directly to your device.

8

Go passwordless with passkeys for stronger security

Passkeys let you sign in with your face, fingerprint, or device PIN—no password needed. With passkeys, there are no passwords to steal and there is no sign-in data that can be used to perpetuate attacks. [Learn how to set up a passkey for your Microsoft Account.](#)

9

Use Windows 11 and turn on tamper protection to protect security settings

Always use the latest version of [Windows](#). Tamper protection blocks unauthorized changes to your security settings, and it is recommended that IT manage these device permissions as an admin.

10

Protect system configuration files from unauthorized sharing

Avoid sharing system files, security settings, or network details through email, messaging, or with unauthorized users. These files can reveal vulnerabilities that attackers can exploit to compromise systems.



11

Use Conditional Access to enforce device compliance

[Ensure](#) only secure, managed devices connect to your organization's network and meet your requirements before you grant them access to your organization's apps and services.

12

Download apps only from official sources

Never share credentials via email or text. If you absolutely must email personal information, use Microsoft Outlook's encryption tools.

➔

Learn more about [endpoint security](#), including how it works, common risks, and best practices to help keep endpoints safe