Microsoft Security

12 tips for protecting your data and internet-connected devices

Here are 12 tips for keeping your email, accounts, and devices—including those that are connected to your organization's network—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, find a phone number on the sender's official website so you can call them directly to confirm the message is legit.

2

Be on guard against messages with attached files

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

3

Only share personal information in real time

It's always best to share personal information in person or by phone. If you absolutely must email personal information, use Microsoft Outlook's encryption tools.

4

Go passwordless and use an authenticator app for stronger security

Your password can't be stolen if you don't have a password. Turn on passwordless for your Microsoft account to sign in with your phone or Windows Hello instead.

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

Install software updates immediately

Many app, browser, and operating system updates contain security fixes for currently active issues, so install them promptly to maintain the latest security standards.

8

Ensure all the apps on your device are legitimate

Only install apps from the official app store for your device.

9

Use Windows 11 and turn on Tamper Protection to protect your security settings

Always use the latest version of Windows. Tamper Protection blocks unauthorized changes to your security settings.

10

Reduce your attack surface

Eliminate unnecessary internet connections, restrict open ports, and use scanning tools to check your digital environment for potential weaknesses, so you can take action and mitigate risks.

11

Use your firmware scanning tools

Check your work environment for potential weaknesses so you can take action and mitigate risks.

12

Don't transfer files that contain system definitions

Sending system definitions through insecure channels or for non-essential personnel can enable attacks to your digital landscape, corrupting your processes and making your environment vulnerable.

Explore more cybersecurity awareness topics and skilling opportunities at https://aka.ms/cybersecurity-awareness.

Microsoft Security