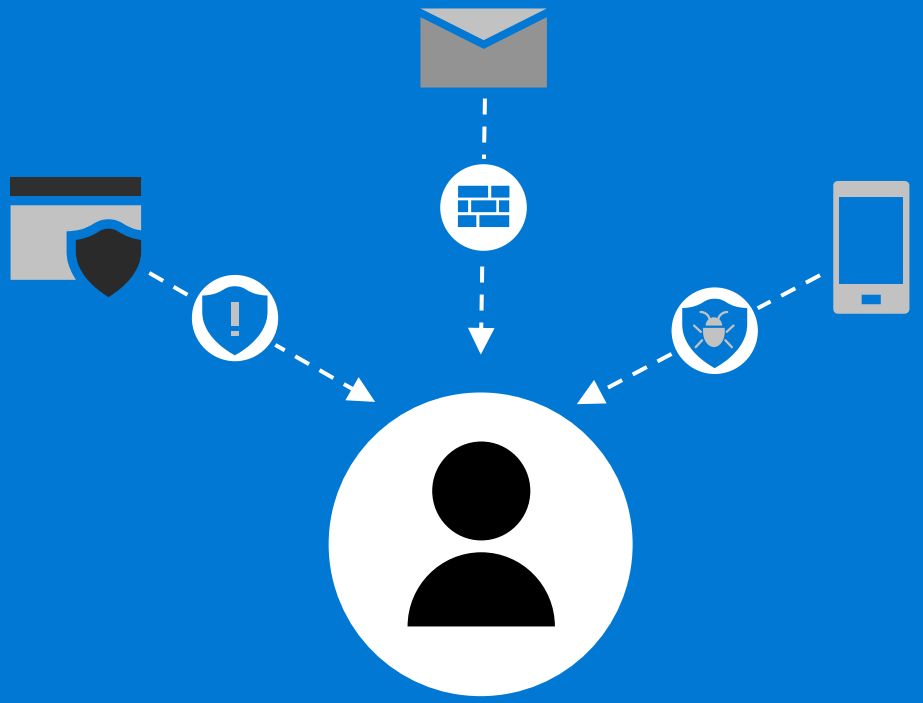
Microsoft

Help protect yourself and your business from digital threats



Your account and your business face serious threats to data, accounts, and devices. Knowing what to look for is your first line of defense. Use this guidance to help protect yourself, your information, and your business or campaign from cyber criminals and hackers.

Control your information

Stay in control by taking these actions

Use secure links instead of attaching documents

Email attachments can be forwarded to anyone or saved and redistributed. Make sure you know who can access your documents by sending a secure link from SharePoint or OneDrive instead. That way, you can specify the permissions for that file – restricting it to your organization, to people you invite, or as read-only so it can't be modified.

TIP: Never send documents as attachments - send a secure link instead.
For more information, see https://aka.ms/SendSecureLink.

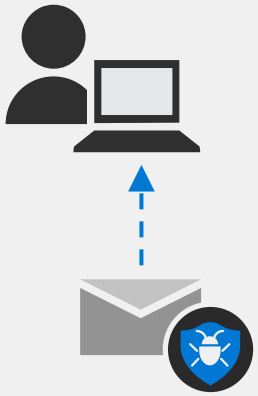
Encrypt and use labels for sensitive or confidential emails

Help ensure that only intended recipients can view message content by encrypting important email. You can send and receive encrypted email messages between people inside and outside your organization.

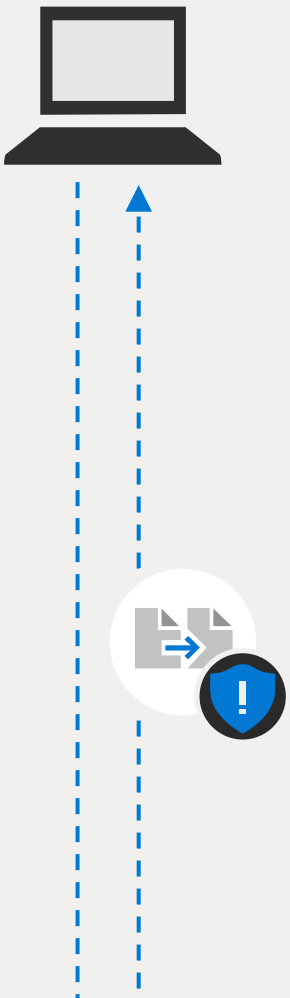
You can also use labels to identify email that contains sensitive or confidential information so that your users know not to share it. Your admin configures the labels. For more information, see https://aka.ms/sensitivity-labels.

TIP: In Outlook, choose **File** > **Options** > **Trust Center** > **Trust Center Settings**, and then choose **Email Security** to set encryption your encryption settings. For more information, see https://aka.ms/encrypt-email-messages.

Security threats



Threats to data, accounts and devices



Malware

Malware is software that can damage your computers or network, and possibly steal data from you, including personal or customer information. For more information, see https://aka.ms/malware-problems.

TIP: Don't open email attachments that you're not expecting. If in doubt, speak directly to the sender. Don't click links in email that you can't verify. Hover over each link to verify the actual destination and use the browser to go directly to web sites instead of clicking a link in an email. This can help avoid malicious software downloading onto your computer.

Spam & Viruses

Spam is email that you don't want and can flood your inbox. A virus is malware that targets a weakness in your business' computer system and use the internet to spread itself to other systems.

TIP: if you use Outlook, report suspicious messages. See https://aka.ms/report-junk.

Phishing and spoofing

Phishing emails look like they are from a legitimate company or someone you know. For example, an email that appears to be sent from a government agency might be asking for personal information like a password, or an account number.

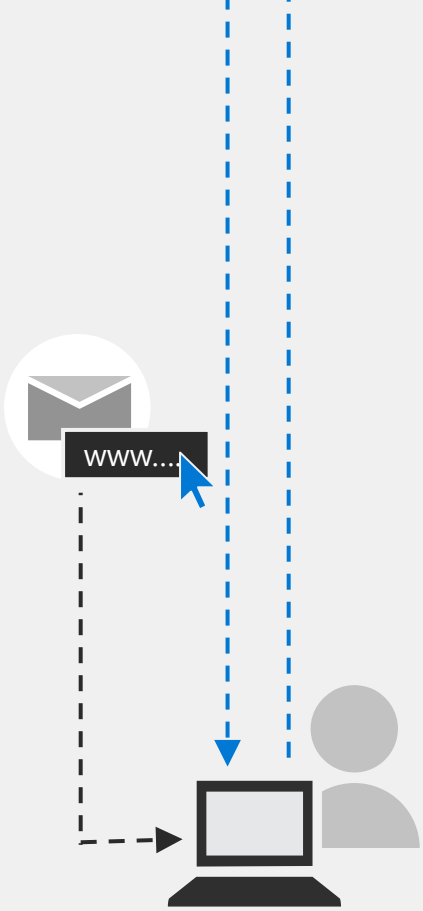
Phishing emails might include a “spoofed” email address. For example, you know Alice@contoso.com, but when you examine the email address, your message came from user@contoso1234c.com.

Impersonation is also a form of phishing; your email comes from a domain or user very similar to one that you know. For example, email from user@contosot.com at a first glance it looks like it came from user@contoso.com

Learn what to watch for with phishing attempts in email. Follow the guidance in https://aka.ms/spot-phishing.

TIP: Phishing emails often sound urgent, have spelling errors, and include requests for personal information. If an email requests information by reply or includes a link to log in to your account, ignore it. Instead, go directly to the organization’s web site or speak directly to the sender to verify.

If you’re an admin, or you want to learn more about security settings and best practices, see https://aka.ms/secure-your-data.



Malicious Sites or Files

Malicious sites host viruses and malware – your business can be at risk if you or someone else clicks on a link that goes to a malicious site. Links to malicious sites are often sent via email and included in social media posts or website adverts. Each of these might include a seemingly valid reason for visiting the site.

TIP: Never go to a financial or other web site with critically private data by clicking a link in an email.

You can also receive email that contains malicious files or content. For example, an email can look like it includes an invoice you might have been expecting, or some other attachment. Opening a malicious attachment can put your business at risk.

To help protect against malicious sites or files, Microsoft 365 includes advanced email security, such as safe attachments and safe links. For more information, see https://aka.ms/email-security.

If you're an admin, or you want to learn more about security settings and best practices, see https://aka.ms/secure-your-data.

For more information, visit aka.ms/M365BPusers