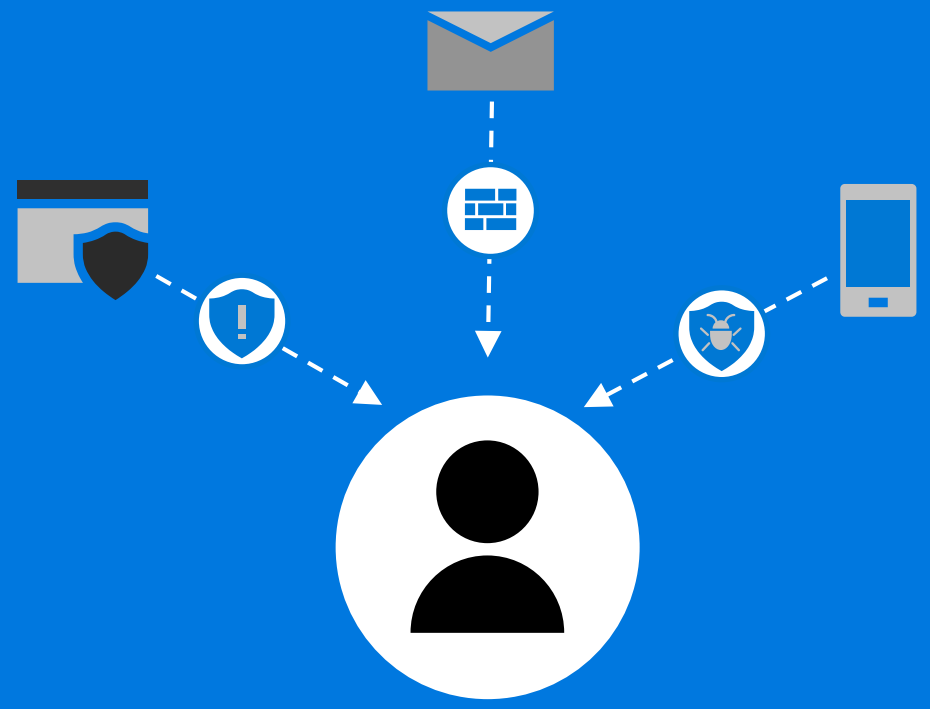


Help protect yourself and your campaign from digital threats



Your account and your campaign 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 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>.

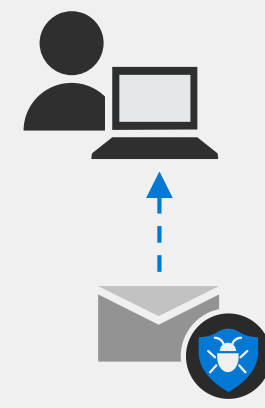
Encrypt and use labels for sensitive or confidential emails

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. Office 365 Message Encryption works with Outlook.com, Yahoo!, Gmail, and other email services.

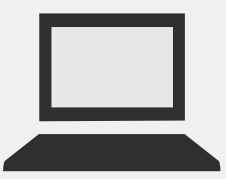
You can also use labels to identify email that contains sensitive or confidential information so that your users know not to share it. Your admin configures the labels.

TIP: In Outlook, choose **Options > Permissions** to set encryption and labels – set sensitive or important email to **Encrypt** or **Do Not Forward**. For more information, see <https://aka.ms/UseEncryption>.

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.

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 following: <https://aka.ms/reportspammal>.

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

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 use Microsoft 365 Business or Enterprise, set up ATP anti-phishing by following <https://aka.ms/ATPantiphis>.

Spot spoofer and impersonators by checking the full email address or speak directly with the sender you know. Find out more and follow these instructions: <https://aka.ms/SpotSpoofing>.

Malicious Sites

Malicious sites host viruses and malware – your company can be at risk if someone clicks on a link that goes to a malicious site. Links to malicious sites are sent via email and included in social media posts or website adverts. Each of these might include a 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.

If your business uses Microsoft 365 Business or Enterprise, set up ATP safe links by following: <https://aka.ms/SetATPSafeLinks>.

