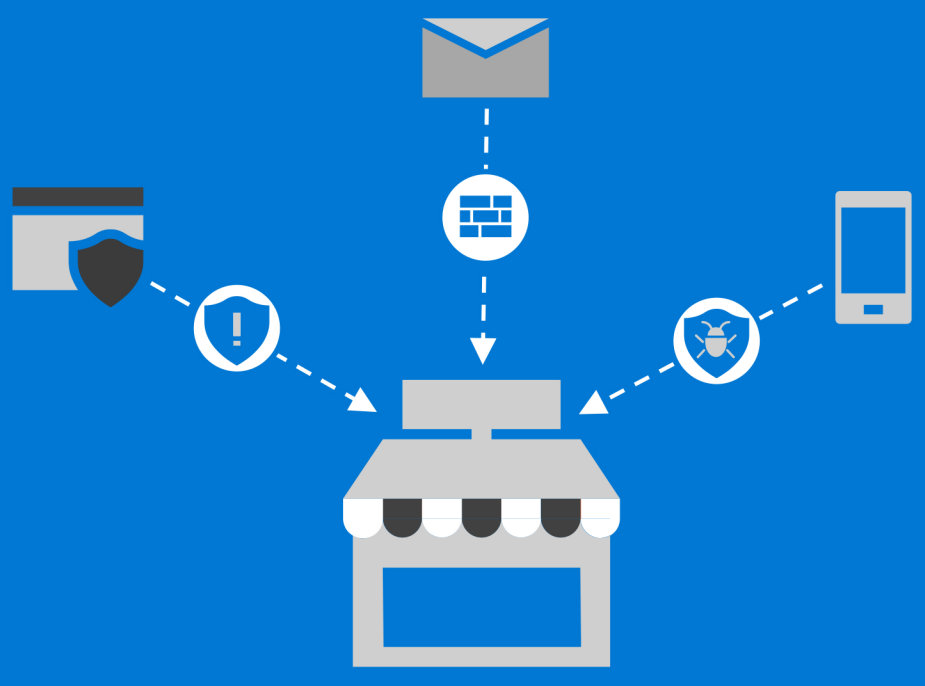
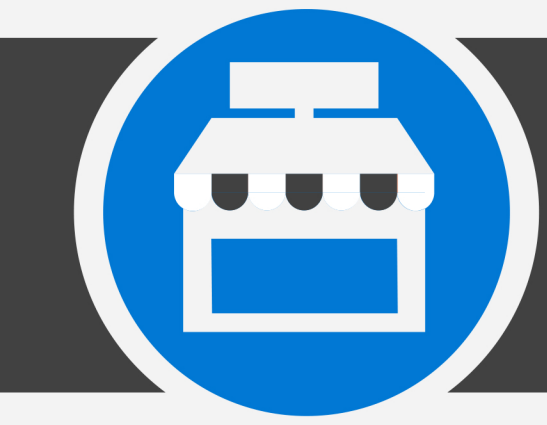
Microsoft

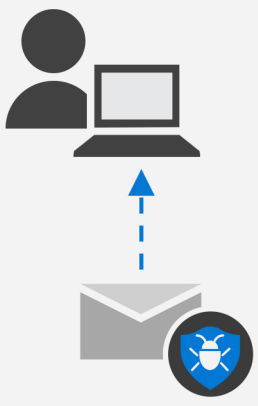
Help protect your small business from threats to data, accounts, and devices



Every business faces serious threats to data, accounts, and devices. Knowing what to look for is your first line of defense. Use this guidance to help protect your organization from cyber criminals and hackers.



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.

Phishing

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

Spoofing (Form of phishing)

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: Spot spoofers 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 your banks web site 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.

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/reportspammail.

For more information, visit aka.ms/SecureO365M365