Microsoft Security

Protect your business: Cybersecurity 101

Cybersecurity threats can shut down your business, steal sensitive data, and hold you ransom. Learn about the cybersecurity landscape and how to protect your business.

Cybersecurity threats come in two forms: external and internal.

External threats

External threats target your network. Attackers will try to overwhelm you with traffic so you cannot access the systems you need to run your business. There are two main types of network attacks:

Denial of service (DoS)

An attack where a computer sends many requests to a network service to overwhelm the target service.

Distributed denial of service (DDoS)

Similar to a DoS attack, only it uses multiple computers in several locations in a coordinated attack.

Protecting your network

Azure DDoS Protection Standard helps defend against DDoS attacks. It is automatically tuned to protect all public IP addresses in virtual networks.

Internal threats

Internal threats target people. Attackers use social engineering tactics to trick users into providing access credentials or revealing sensitive information.

Common attacks include:

Phishing and spear phishing

Scammers send emails to your employees from what appears to be a colleague, friend, or reputable person or company containing a link or attachment. If the employee clicks the link or opens the attachment, the attackers can gain access to your systems.

Vishing

Like phishing but using phone calls instead of email.

Baiting

When the attacker offers a fake prize for responding to a phishing or vishing attack.

Browser attacks

These attacks may appear as pop-up ads or suggestions to install a browser extension.

Protecting your network

1. Provide your employees with training on safe email and browsing use. Learn more.
2. Help employees understand potential risks when online. Share our other cybersecurity educational infographics: 10 easy rules to secure your personal data & protect your devices, 7 ways to protect yourself from phishing, 5 pro tips to protect yourself from tech support scams.
3. Offer attack simulation training in Microsoft Defender for Office 365.
4. Go passwordless and use multi-factor authentication.
5. Ensure all company devices use the latest version of Windows and internet browser.
6. Enforce corporate file-saving protocols. Store and encrypt company data securely in the cloud.
7. Educate employees on the importance of using secure connections such as HTTPS. Install the HTTPS Everywhere plug-in for your browser.
8. Make it a practice with employees to check website certificates to verify the website's identity.
9. Enable pop-up blockers by default.
10. Use cloud-based antivirus solutions like Microsoft Windows Defender.

Learn more about Microsoft Security's insights at www.microsoft.com/security/business/cybersecurity-awareness.

Share more about cybersecurity best practices

Microsoft