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 101

Cybersecurity vulnerability can come from internal or external threats:

**External threats:**
Network attacks aka Denial-of-Service

Network attacks overload your system, server, or network with traffic, so you cannot access the systems you need to run your business.

- **Defeat network attacks:**
  - Azure DDoS Protection Standard helps defend against DDoS attacks. It is automatically tuned to protect all public IP addresses in virtual networks. To learn more, click here.

**Internal threats:**
Attacks on users aka social engineering attacks or exploitation

Social engineering targets your employees through email or when they browse online. Common social engineering attacks are:

- 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.
- 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.

**Defeat social engineering attacks**

10 ways to protect your employees:

1. Provide your employees with training on safe email and browsing use.
2. Raise employee awareness of 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 your employees 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.
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 identity of the website.
9. Enable pop-up blockers by default.
10. Use cloud-based antivirus solutions like Microsoft Windows Defender.

- **Get the latest news from Microsoft Security, go to microsoft.com/en-us/securitynow.**

- **Share this infographic**

Read the rest of the series here:

- 10 easy rules to secure your personal data & protect your devices
- 5 pro tips to protect yourself from tech support scams
- 7 ways to protect yourself from phishing

©2021 Microsoft Corporation. All rights reserved. This document is provided “as is” information and views expressed in this document, including URLs and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.