Microsoft Security

Aware and Secure:

Best practices to safeguard your business

In today's rapidly changing threat landscape, human beings, not technology, represent an organization's first and last lines of defense.

The responsibility for cybersecurity must be shared. Individual team members as well as security professionals all have important roles to play. By understanding best practices to behave safely online, everyone can do their part, and we can be cyber smart together.

Becoming cyber smart

Help everyone in your organization understand what they can do to keep themselves and their colleagues safe online with the following cybersecurity infographics.

- Devices — View infographic >
- Scams — View infographic >
- Phishing — View infographic >
- Passwords — View infographic >

Employee-facing threats

Because employee-facing threats target human beings, attackers use social engineering tactics to trick users into providing access credentials or revealing sensitive information. Some of the most common tactics are listed below.

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.

Spear phishing

A more advanced form of phishing, spear phishing targets specific individuals (those most likely to have valuable information or access) rather than random targets.

Content injection

This type of attack injects a familiar website (such as an online banking portal), with malicious links, forms, or pop-ups that direct users to a secondary website that asks for confidential information.

Link manipulation

Malicious links that appear to come from trusted sources and take users to spoofed websites, where they are prompted to enter account information.

Man-in-the-middle

When cybercriminals trick two people into sending information to each other. The scammer may send fake requests or alter the data being sent and received by each party.

Malware

Malware includes malicious applications or code that damages or disrupts the normal use of computers, tablets, phones, and other endpoint devices.

The five dimensions of basic cyber security

How to protect your organization from 99% of attacks:

1. Enable multifactor authentication (MFA)
2. Apply Zero Trust principles
3. Use modern anti-malware
4. Keep systems up to date
5. Protect data

1 Enable multifactor authentication (MFA)

With MFA enabled, you can prevent 99.9% of attacks on your accounts.[1]

MFA best practices

Make it easy

Select an MFA option with the least amount of friction (like using biometrics in devices or FIDO2 compliant factors such as Feitan or Yubico security keys) for your employees.

Be judicious

Choose MFA when extra authentication can help protect sensitive data and critical systems rather than applying it to every single interaction.

Avoid end-user toil

Use conditional access policies, pass-through authentication, and single sign on (SSO) to help users avoid multiple sign-on sequences to access non-critical file shares or calendars on the corporate network when their devices are current with the latest software updates

2 Apply Zero Trust principles

Zero Trust is the cornerstone of any resilience plan limiting the impact on an organization.

The Zero Trust principles

Assume breach

Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly. This means constantly monitoring the environment for possible attack.

Explicitly verify

Ensure users and devices are in a good state before allowing access to resources. Protect assets against attacker control by explicitly validating the fact that all trust and security decisions use relevant available information and telemetry.

Use least priviliaged access

Limit access of a potentially compromised asset with just-in-time and just-enough-access (JIT/JEA) and risk-based policies like adaptive access control. You should only allow the privilege that is needed for access to a resource and no more.

3 Use modern anti-malware

Use extended detection and response anti-malware. Implement software to detect and automatically block attacks and provide insights to the security operations.

4 Keep up to date

Unpatched and out of date systems are a key reason many organizations fall victim to an attack. Ensure all systems are kept up to date including firmware, the operating system, and applications.

3 best practices

Patch

Ensure devices are robust by swiftly applying patches and changing default passwords and default SSH ports.

Reduce

Eliminate unnecessary internet connections and open ports and restrict remote access by blocking ports, denying remote access, and using VPN services.

Segment

Segmenting networks limits an attacker's ability to move laterally after initial intrusion. IoT devices and OT networks should be isolated from corporate IT networks through firewalls.

5 Protect data

Knowing your important data, where it is located and whether the right systems are implemented, is crucial to implementing the appropriate protection.

To learn more about the cyber hygiene practices detailed above, see Basic cyber hygiene prevents 99% of attacks.

10 top-of-mind tips to protect your network

1. Provide your employees with training on safe email and browsing.
2. Offer attack simulation training in Microsoft Defender for Office 365.
3. Go passwordless and use MFA.
4. Ensure all company devices use the latest version of Windows and internet browser.
5. Enforce corporate file-saving protocols. Store and encrypt company data securely in the cloud.
6. Educate employees on secure connections. Install HTTPS Everywhere plug-in for your browser.
7. Train employees to verify website identities by checking website certificates.
8. Explore automation best practices and data governance strategies to ensure secure environments.
9. Enable pop-up blockers by default.
10. Use cloud-based antivirus solutions like Microsoft Windows Defender.

1. https://www.microsoft.com/en-us/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/

Explore more cybersecurity best practices and skilling opportunities at https://aka.ms/cybersecurity-awareness.

Microsoft Security

©2023 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL 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