MODEL TECHNOLOGY SOLUTIONS

Cybersecurity Simplified: Phishing

Phishing is a form of fraud in which an attacker masquerades as a reputable person or company in email or other electronic communication channels. A common phishing tactic is to send an email with a forged return address, so that the message appears to have originated from a legitimate source, making it more likely that the recipient will open it.

Phishing attacks are popular with cybercriminals, because it is easier to trick someone into clicking a malicious link in a seemingly legitimate email than it is to break through a computer's defenses.

Examples of phishing schemes:

- An employee receives an email from her company's CEO, asking her to buy electronic gift cards for a customer recognition event. The request is time sensitive so she quickly purchases these online and sends the gift card numbers to the CEO. Weeks later she discovers the CEO never made the request
- An employee receives an email with a link to a secure document. They enter their credentials to view the document, but the document fails to load. They move on to other work and forget about the glitch. In reality, they have delivered their username and password to hackers, who can now use it to access their email and other online accounts, including systems and data used by your company.

Microsoft 365 Business Premium helps protect you against phishing attacks.

Most cloud email services include endpoint threat protection against phishing through basic spam filtering. Microsoft 365 Business Premium adds sophisticated technologies that provide an additional level of protection:

- **Time of click protection against malicious links:** Cybercriminals sometimes redirect seemingly safe links to unsafe sites using a forwarding service hours or days after a message is delivered. To help ensure continuous protection, clicked links are checked in real time. The destination is blocked if it is known to be malicious.
- **URL detonation:** When a user clicks a link that has an unknown reputation, the system checks the destination for patterns of suspicious behavior in a secure "sandbox." While this scanning is happening, users see the message "this link is being scanned." If the link is identified as malicious after the scan, the user is warned against opening it.
- **Anti-spoofing technology** uses machine learning and advanced analysis techniques to identify signs than an email sender may not be who they appear to be. If impersonation is detected the email is blocked or moved to junk mail.
- **Multi-factor authentication** helps keep attackers out of your environment even if a phishing attack results in a compromised password. Advanced multi-factor authentication with Conditional Access gives you the ability to configure trusted locations such as an office network and block access from countries where you aren't conducting business.

Microsoft's Commitment to Enhancing Security Technology

The anti-phishing and anti-malware capabilities included in Microsoft 365 Business Premium is called Microsoft Defender for Office 365 (previously Office 365 Advanced Threat Protection). This is the same technology used to protect many of the world's largest companies.

Threats rapidly evolve, so we continue to invest in expanding capabilities to help secure mailboxes from attacks. Microsoft uses artificial intelligence to identify and protect against emerging threats in real time. Our machine learning models leverage Microsoft's wide network of threat intelligence. Additionally, our team of seasoned security professionals provide expertise in the latest ways to combat malware, cyberattacks, and attacker motivation.

Microsoft Defender for Office 365 also shares threat signals with other defenses and sensors within Microsoft. Connecting security data and systems allows Microsoft security technologies to continuously improve endpoint threat protection.

Healthcare

Healthcare organizations are often targeted by hackers for the valuable medical records and health insurance data they hold. Phishing remains a common tactic used by cybercriminals to trick employees with clever email messages. Scams could involve harvesting login credentials or launching a malware attack.

Having a layered defense system like Defender in place to intercept and block malicious emails before they reach users' inboxes is essential for protecting data. Organizations should also provide awareness training to employees to help them spot and avoid suspicious emails that manage to get through. Both are important elements of effective endpoint threat management.