Microsoft

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, thereby 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.

Phishing email detections increased 250% from January to December 2018 worldwide.

Source: Microsoft Security Intelligence Report Volume 24, February 28, 2019

Microsoft 365 Business helps protect you against phishing attacks

Most cloud email services include some protections against phishing through basic spam filtering. Microsoft 365 Business 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, each time a link is clicked, it is checked in real-time, and 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 examines emails to identify forged "From" headers. When Microsoft has a high confidence that the header is forged (or "spoofed") the user is warned that the sender may not be who they appear to be.

Microsoft's commitment to enhancing security technology

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

Threats rapidly evolve and become increasingly complex, so we continue to invest in expanding capabilities to help secure mailboxes from attacks. Microsoft uses artificial intelligence and machine learning to identify and protect against emerging threats in real-time. Our machine learning models leverage Microsoft's wide network of threat intelligence, plus seasoned threat experts who have deep understanding of malware, cyberattacks, and attacker motivation, to combat a wide range of attacks.

Office 365 ATP also shares threat signals with other defenses and sensors within Microsoft. For example, when a malicious file is detected by Windows Defender ATP, that threat can also be blocked by Office 365 ATP. Connecting security data and systems allows Microsoft security technologies to continuously improve threat protection, detection, and response.

Get started:

Learn more about Microsoft 365 Business at www.microsoft.com/microsoft365/business