CYBERSECURITY - EMAIL PHISHING PRECAUTIONS

Email remains mission critical business function for many organizations, and for this reason, it has also become the primary mechanism used by cybercriminals to gain access to protected systems. One of the primary methods used by cybercriminals is a technique called “Phishing,” which is an attempt to acquire sensitive information by masquerading as a trustworthy source. Phishing continues to evolve in sophistication and scale everyday making even trained personnel second guess themselves.

The term phishing was coined by hackers in the 1990s in reference to their process of using email to convince recipients into giving up their passwords or financial data. Phishing attempts have become widespread and extremely sophisticated over time. For cybercriminals wanting to reach the largest number of people electronically, email remains the favored approach.

In 2024 phishing messages increased by 202%, with credential based phishing attacks surging by 703% (SlashNext, 2024) approximately 347.3 billion emails were in circulation each day (Paubox, 2024)

Nearly 1.2% of all emails sent daily are malicious, which means about 3.4 billion emails daily (Paubox, 2024).

Malicious components of Phishing Email

Attachments

A file (Microsoft Office document, pdf or image file) attached to the email will contain malicious software called malware. Upon opening the attachment, the malware attempts to infect the machine or reach out to the Internet to download additional malware to the system.

Embedded links to websites

The embedded link will appear to take recipients to a legitimate website. However, they will be redirected to a fake site that attempts to collect credentials and then pass recipients to the legitimate site. Many times, these fake sites also attempt to install malware onto the system.

Malware can be used to provide remote access to your system, steal information or even encrypt (make unreadable) the files on your computer and hold them for ransom (called ransomware).

Tips for identifying a Phishing Email

Not all phishing emails can be easily identified, but there are some basic attributes that can be used to raise the suspicion level of an email. If any of the statements below are true, delete the email or use extra caution before opening it.

Not recognizing the sender of the email.

The email is asking for personal or financial information.

The email wants the recipient to respond immediately or makes an urgent request for information.

The email includes upsetting or exciting statements, which are usually false, that want the recipient to act quickly.

The email wants the recipient to open an attachment or click on a website link that was not expected. This could be to view an article or video pertaining to any number of intriguing topics such as current social events, news tragedies or holiday sales. Other forms include a notification of fraudulent charges on a credit card, or that a cell phone or email account has been locked out.

Email safety tips

The easiest way to avoid falling victim is to delete any emails that can be identified as suspicious. If the email looks legitimate or is from a valid sender, consider the following safety tips.

- Never send financial or personal information (account numbers, social security numbers, credit card numbers, ID's and passwords, tax identifier numbers, etc.) via email unless a form of email encryption is being used. This is a special type of email that scrambles the information so only the recipients can read it.
- Verify that website links embedded in emails are being directed to the correct website. Do this by placing the cursor over the link (do not click on the link). Hovering over the link will show you the real website in a pop-up window, or if using a web browser, it will be in the lower left hand corner.
- Contact the sender to verify that the email was legitimately sent to you. Instead of clicking on the link provided in the email, contact the sending party to obtain their legitimate website then manually type it in to the web browser.
- Consider using separate email accounts, one for business, one for financial institutions, one for friends and family and one for subscriptions and registrations.
- Run firewall and anti-virus/anti-malware detection programs on computer systems. These are subscription-based services and it is important to keep them up-to-date.
- Use different and complex passwords for each account that utilizes email addresses.
- Avoid using the same password across accounts, using the same password will compromise the accounts if the credential is stolen.
- Never reply to a suspicious email as this will validate your email address as active.
- When using hosted email services (Yahoo mail, Gmail, Outlook online, etc.) enable two-step verification. Once the password is entered, a prompt will ask to enter a randomly generated code that is sent to a mobile device.

Phishing emails can be very sophisticated and convincing. Those who fall victim to a phishing email, should take action immediately.

Phishing victim action plan

- Notify the IT department or vendor of the organization to enact any Incident Response Plans (IRP) that may be in place.
- Scan the system with an anti-virus or anti-malware product.
- Change any account passwords that utilized the compromised credentials.
- Monitor any compromised accounts for suspicious activity or fraudulent charges.
- If financial account credentials were compromised, notify the appropriate financial institution or organizational representative.

Conclusion

The cybersecurity landscape in 2024 has been marked by a significant increase in phishing and ransomware attacks. The commoditization of cyberattack tools, such as Phishing-as-a-Service (PhaaS) platforms, has contributed to this surge (The Wall Street Journal, 2025), making it imperative for individuals and organizations to adopt robust security practices. By staying informed and implementing the strategies outlined above, you can significantly reduce the risk of falling victim to cyber threats.

REFRENCES

[i] Symantec Corporation. (2016, April). 2016 Internet Security Threat Report. Retrieved from https://www.symantec.com/security-center/threat-report

[ii] Gudkova, D., Vergelis, M., Demidova, N., & Shcherbakova, T. (2017, February 20). Spam and Phishing in 2016. Securelist. Retrieved from https://securelist.com/analysis/kaspersky-security-bulletin/77483/kaspersky-security-bulletin-spam-and-phishing-in-2016/

[iii]Hoxhunt. (2024). Phishing trends report 2024. https://hoxhunt.com/guide/phishing-trends-report [hoxhunt.com]

[iv]Paubox. (2024, February 2). 2024 phishing statistics: Latest figures and trends. https://www.paubox.com/blog/2024-phishing-statistics-latest-figures-and-trends [paubox.com]

[v]SlashNext. (2024, April 5). Phishing attacks double in 2024. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/2024-phishing-attacks-double/ [infosecurity-magazine.com]

[vi]The Wall Street Journal. (2025, January 16). Do-it-yourself cyberattack tools are booming. https://www.wsj.com/articles/do-it-yourself-cyberattack-tools-are-booming-7ce1445d [wsj.com]