Research Paper

Let's go Phishing

Nevaeh, Wallace

Department of Cybersecurity, Old Dominion University

CYSE280: Windows System Management and Security

Professor Malik Gladden

17 April 2025

I pledge to support Old Dominion University's honor system. I will refrain from academic dishonesty or deception, such as cheating or plagiarism. As a member of the academic community, I am responsible for turning in all suspected violations of the Honor Code.

One of the most common cybersecurity threats that target users of Microsoft programs is phishing. They are called phishing attacks because swindlers fish for random victims, anyone who will take the bait. The widespread use of Microsoft products like Word, Teams, OneDrive, and Outlook in personal, academic, and professional settings has made them appealing targets for cybercriminals looking to trick users into installing harmful software or disclosing private information. Attacks could range from malicious attachments to phony login screens that imitate Microsoft user interfaces. Once a user is tricked, attackers can distribute malware over a network, obtain illegal access to accounts, or exfiltrate data. Users and businesses must be informed and use the best security procedures available as phishing attempts get more complex.

This paper will cover different types of phishing attacks, signs of phishing, the damage a phishing attack could do, the history of data breaches at Microsoft, how Microsoft lowers its risk to threats, and suggestions on other things they could do to help reduce their risk.

Since phishing attacks are becoming more complex, the type of phishing has advanced from just one type to almost 20 different variations. Spear phishing would be the most common type, it is called this because the attacker targets one individual in an organization to try to steal credentials. Another type of attack, similar to spear phishing, is something called Whaling. Whaling is when the attacker targets a senior executive, in a sense, trying to catch the big fish. This is different because these individuals have more access than the normal employee. Vishing is voice vishing, an attacker uses the phone to

try to steal information from targets. Smishing is another type of phishing that deals with using the phone, but instead of their voice, they try to trick you through text messages. A type of phishing I have never heard of is Angler phishing. Fake social media posts are used by anglers to trick users into downloading malware or providing login credentials.

Phishing has evolved and has taken so many different forms that it has become difficult to know what is real and what is fake. The most obvious indicator would be language mistakes. Spell browsing has been added to most organizations' email platforms for active messages. Therefore, misspellings or grammatical errors should trigger red flags because they are unlikely to originate from the verified source. Additionally, it may be a sign that an email is unsafe if it asks you to act unusually or ask for unusual interest, such as payment, identification, or other sensitive information. Lastly, you should always verify the web address. The email could be a space off from the original, and they could take all your money. You always have to check these little things before you do anything on your end.

As we all know, all companies experience cyber attacks and data breaches, and Microsoft is no exception. Microsoft has been experiencing breaches since 2010, with 2024 being the most recent attack. In April of 2019, it was announced that a hacker obtained a customer support agent's credentials, allowing access to some webmail accounts. This would be an example of Spear phishing, attacking an individual to gain access to a company's data. Later that same year, a misconfigured Microsoft internal customer support database left records on 250 customers exposed. Anyone with a web browser who was able to connect to the database could see the details because the

database was not adequately password-protected for around a month. In March 2013, after taking part in a survey and joining a prize draw, the login credentials of around 3,000 Xbox Live users were made public. Information such as gamer tags, names, birthdays, and emails was posted online, not via a hack. It is not clear if this information was used maliciously.

Because of their long history of data breaches, Microsoft has added additional protection to different programs. Hyper-V virtualization technology from Microsoft is used in Windows Defender Application Guard and Microsoft Edge to provide defense against the growing threat of targeted assaults. To prevent access to your company data, the Hyper-V container separates the device from the rest of your network if a website is judged untrusted. Email access is preserved during and after emergencies with Microsoft Exchange Online security (EOP), which provides dependability and security against spam and viruses. EOP can strengthen your protection by offering numerous spam filtering measures, including bulk mail controls and foreign spam, through many layers of filtering. To help defend your files, online storage, and email against viruses, use Microsoft Defender for Office 365. Microsoft Teams, Word, Excel, PowerPoint, Visio, SharePoint Online, and OneDrive for Business provide comprehensive protection. It enhances Exchange Online Protection's security features to offer superior zero-day protection by guarding against malicious links and preventing dangerous attachments.

Microsoft has added things to beef up its security to prevent phishing attacks, but there's always room for improvement. You should always start with educating users, permitting in-line instruction, and reporting. They could take it a step further and, when

questionable activity is noticed, incorporate interactive anti-phishing tests or alarms straight into Outlook. They could also add real-time visual alerts such as “Unusual sender” or “Urgent request”. Microsoft could also integrate the Red team tool, add phishing chatbot scenarios, bespoke payload testing, and real-time risk scoring for staff members to Microsoft Attack Simulator.

Just like there are several types of phishing attacks, there are also many ways that you could be negatively impacted if you fall victim to an attack. The most common would be financial losses; individuals could suffer from immediate or ongoing financial difficulties. Identity theft is another big one. If an attacker gains your information, they could open fraudulent accounts, commit tax fraud, and access private information. Phishing attacks can also lead to damage to the reputation of businesses and individuals. When an individual or company's information is compromised, it can lead to a loss of trust.

If you think you have been a victim of a phishing attack, here are a few things you should do. Contact your IT admin if you're working on a work computer, immediately change all passwords associated with the accounts, and notify your bank and credit card company of any fraudulent activity. Another important step you should take is to jot down as many specifics of the attack as you can remember while it's still fresh in your mind. Try to keep track of any information you may have shared, including usernames, account numbers, and passwords, as well as the location of the attack, such as Teams or Outlook.

One of the most persistent and dynamic risks in the cybersecurity space is still phishing attacks, particularly for users of popular platforms like Microsoft. As demonstrated in this research, the proliferation of phishing types, ranging from spear phishing and whaling to smishing and angler phishing, indicates the increasing sophistication and targeting of these assaults. Because Microsoft products are so ingrained in academic, professional, and personal settings, users need to be on the lookout for strategies that aim to compromise confidential data and interfere with daily operations. Even while Microsoft has strengthened its defenses with products like Exchange Online Protection, Microsoft Defender, and Hyper-V technologies, proactive security measures and user awareness are still crucial. Individuals and organizations may be further empowered to combat phishing attacks through interactive safety features, enhanced detection systems, and ongoing education. To protect digital assets and preserve confidence in the platforms we use daily, technology, training, and prompt reactions must all be used in concert to prevent phishing.

References

https://firewalltimes.com/microsoft-data-breach-timeline/

https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

https://www.hipaajournal.com/microsoft-issues-advice-on-defending-against-spear-phishing-attacks/

https://www.kiteworks.com/secure-file-sharing/microsoft-is-a-magnet-for-phishing-attacks/

How to protect against phishing attacks - Microsoft Defender for Endpoint | Microsoft Learn

https://teckpath.com/the-rise-of-microsoft-teams-attacks-a-deep-dive-into-recent-phishing-threats/

https://trustifi.com/blog/microsoft-365-phishing-email-examples/

What is a Phishing Attack? Types and Examples