Phishing Attacks in using Microsoft Programs

Madelene McFarlane

Old Dominion University

Everyone is different in terms of knowledge and skills. Some people find themselves very keen with the arts and others are gifted with athletic talents. Similarly, some people are skillful in the way of detecting potential cyberattacks and others find themselves to be too trusting of everything on the internet. Those who act as human vulnerabilities are the prime target of those that send out phishing scams or attacks. This paper will cover the prime function of phishing attacks and social engineering that takes place in order for the attack to successful exploit human vulnerabilities. Along with addressing the overall harm that can arise from a successful phishing attack being exploited properly. Then wrapping it up with how Microsoft systems are working to protect those who come face to face with a phishing attack and other measures that should be implemented in order to not fall victim to a phishing attack.

Phishing attacks, like most other methods of cyber-attacks, are not just limited to one particular system structure. Therefore, phishing attacks are not just limited to that of Microsoft systems. All systems, messages, applications, and websites are vulnerable to phishing attacks. Each system having their own proactive protocol in order to try and keep user's safe from phishing attacks. Though the focus will be directed to that of Microsoft systems within this paper for simplicity's sake. However, one factor that all phishing attack hold in common is that of the measures and methods that are taken in order to successfully deceive the system's users into exposing sensitive information to the attacker source. This common factor is that of the human vulnerability and the user not being able to identify a malicious phishing source and giving up sensitive information or even installing malware onto their own system. Exposing important data and putting a whole network at potential risk.

The most common form of phishing is found within what is known as a phishing email. A phishing email is one of the most popular ways of phishing for human error vulnerabilities within a company. Though most people are aware of this method of cybercrime there is still a good percentage of people that fall prey to this attack. Therefore, keeping this method of phishing alive and well.

This form of phishing also explains the overall framework of phishing quite well. A phishing email will often times contain a malicious link or download file that is being presented as an official or safe bit of information. Then once the prey clicks on the link or downloads the phishing attack will then download malware onto to computer and or computer systems involved. Often times the malware will be ransomware, cause sabotage to the systems, or to steal information that can be found on the attacked computer system. The key factor to phishing attack being that the human error factor succeeds and clicks on the malicious attachment and launches the attack on themselves.

The email being an excellent textbook example of what a phishing attack details as. The presentation of a safe and official means of information or link when its actuality the content being presented is that of a malicious intent. Phishing attacks can be found in more forms then just that of the email variety that has been presented. But the attacks can also be found in forms such as false advertisements, websites, as well as some may argue that generous given official usb thumb drives containing malware can be argued as a extended form of phishing and attacking a target’s system.

Even though society and companies have gained further knowledge and training for keeping themselves protected from phishing attacks there are still many cases in which phishing attacks are successful. With all the emails that are sent through a company or a busy individual there is always a chance that even a well-educated individual may fall victim to an attack. When this happens the effects of the attack varies, but none the less there is damage that will occur from clicking the given link or downloading the content that was presented to the victim and then employed the malware behind the attack.

There are three main types of damage that can occur from a launched phishing attack that was successfully activated. These three main types of damage involve: data encryption, data theft, and monetary theft. A main point that should be stressed within these three different types of damage is that all of them are equally as harmful to a system as well as the individual. The amount of damage that can be caused within these variant types differs based on the aggression of the malware that has exploited the system as well as if the proper procedure was followed in order to provide damage control.

Data encryption is a phishing damage category that is often times referred to as ransomware. Ransomware encrypts key files on a system and offers to restore them if the presented fee is paid by the user, hence the name. This can then lead to lose of access to the information files as well as system data. Depending on how long it takes for the system to be restored this damage can lead to a major business disruption.

The next form of damage that can occur from a successful phishing attack is data theft. Simply put this is when the malware that was linked to the phishing attack has the intent on stealing data that is on the user’s computer system and or the network that the computer is connected to. The result of this damage is data will either be lost from the system entirely or stolen from the system. This can then lead to an extreme level of the user’s or company’s data being extorted on the dark web.

Data theft can also be tied to the third category of damage which is monetary theft/gain. This is because data theft when extorted will often times provide economic gain for those that triggered the phishing attack and thus gained the data that was then stolen. However monetary theft has a couple of different forms along with that of data theft. If a phishing attack is successful, the malware could allow access to the hacker to modify company invoices. Thus, creating fake invoices and then cash them or selling the invoices to those that wish to cash them on their own behalf.

With the damages that are listed there is not one that seems any bit pleasant to someone that stores valued data on their computer system. Luckily along with better one’s own knowledge about how to proactively protect themselves from phishing attack. There is also pre-built-in protection on Microsoft systems to better help prevent the success of a phishing attack. These additions help create a barrier between the human error that phishing attacks rely on and the caution that every computer systems user should have and continue to grow throughout time. These measures given through Microsoft systems are an automatic protection that are pre-enable on Microsoft systems and therefore are already at work when the user logs in for the day.

These measures that Microsoft systems use come in a variety of different types. Most of which being different levels of scans on different areas that the system uses. This is to help prevent any suspicious activity that may slip by the user. An example of this is that of the Microsoft system will scan emails that are being sent to the user and match the sender and contents of the email for a couple of resources.

The resources that are commonly looked at are the sender that is sending the initial email. This is scanned due to the fact of sometimes hackers will create an email similar to one that commonly messages the victim but carries a slight off spelling in order to blend it with the regularly contacted email. The system will then in turn alert the user that they have never sent emails to or from this email before and thus can cause the user to take a closer look at who the sender really is and the contents in which the email holds. Thus, possibly preventing a phishing attack.

Another factor that is commonly scanned is that of the contents of the sent email. If the email contains a suspicious link or a non-official download attachment a similar alert will be issued to the user. This alert in regards of the emails content will then prompt a similar effect as for the sender scan. Additionally, the email may be hidden altogether in order to prevent an accidental click and therefore an accidently activation of the malicious phishing email attack on the user’s system.

Every system’s user is different just like how each person in society is different. Every user has different strength and weaknesses. The strengths are important but also identifying the weak points is what a cybercriminal is looking for when deploying a phishing attack onto a system’s user. The phishing attack being a malicious code hidden as a link or download that is presented to a user as an official and safe resource.

Commonly phishing attacks are known as being present in primarily in emails, which is correct. If a successful phishing email is activated onto a user’s system a range of damage can be presented. These main three types of damages are ransomware, data theft, and monetary theft. All of these different damages ranging in effect and all of which causing harm to the user and to potentially a company that the system that has been hacked is connected to as well.

Though Microsoft system have built in measures to try and keep systems safe from phishing attacks no matter the form they may take. The most common measure is that of the scans that automatically read each email that the user may receive. Scanning for unknown and new emails that are being sent along with any out of the normal content that the emails may contain. Raising awareness to the user that there is potentially something harmful being sent within the email and to take a further look. These measures deployed by Microsoft systems along with the continuing growing knowledge that the user has to face in order to keep their systems and information safe from phishing attacks.

References

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021, January 18). *Phishing attacks: A recent comprehensive study and a new anatomy*. Frontiers. Retrieved January 23, 2023, from https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

Chen, J., & Guo, C. (2007). *Online detection and prevention of phishing attacks | IEEE conference ...* ieeexplore.ieee.org/. Retrieved January 23, 2023, from https://ieeexplore.ieee.org/abstract/document/4149954

Issac, B., Chiong, R., & Jacob, S. M. (2014, October 17). *Analysis of phishing attacks and countermeasures*. arXiv.org. Retrieved January 23, 2023, from https://arxiv.org/abs/1410.4672

Jackson, C., Simon, D. R., Tan, D. S., & Barth, A. (1970, January 1). *An evaluation of extended validation and picture-in-picture phishing attacks*. SpringerLink. Retrieved January 23, 2023, from https://link.springer.com/chapter/10.1007/978-3-540-77366-5_27#Bib1

Milletary, J. (2005). *Technical Trends in Phishing Attacks*. ftp.unpad.ac.id. Retrieved January 23, 2023, from http://ftp.unpad.ac.id/orari/library/library-ref-eng/ref-eng-3/network/network-security/cert/techtips/Phishing_trends.pdf

Rains, T. (2020). *Cybersecurity threats, malware trends, and Strategies*. Google Books. Retrieved January 23, 2023, from https://books.google.com/books?hl=en&lr=&id=8YLoDwAAQBAJ&oi=fnd&pg=PP1&dq=Phishing%2BAttacks%2Bin%2Busing%2BMicrosoft%2BPrograms&ots=q12sS__azl&sig=MfB7ee4YsCuM2mEJR2Egz5dtPu0#v=onepage&q=Phishing%20Attacks%20in%20using%20Microsoft%20Programs&f=false