International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Research Paper on Spreading Awareness About Phishing Attack Is Effective In Reducing The Attacks?

Bhakti Ulhas Desai, Guide: Asst. Prof. Gauri Ansurkar

Student, M. Sc IT, Keraleeya Samajam (Regd.) Dombivli's Model College, Maharashtra, India

---

Abstract – As a result, an infinite amount of private information and financial transactions become prone to cybercriminals. Phishing is an example of a highly effective sort of cybercrime that allows criminals to deceive users and steal important data. Since the primary reported phishing attack in 1990, it's been evolved into a more sophisticated attack vector. At present, phishing is taken into account one in every of the foremost frequent samples of fraud activity on the web. Phishing attacks can cause severe losses for his or her victims including sensitive information, fraud, companies, and government secrets. this text aims to guage these attacks by identifying this state of phishing and reviewing existing phishing techniques. Studies have classified phishing attacks in line with fundamental phishing mechanisms and countermeasures discarding the importance of the end-to-end lifecycle of phishing.

From this research we understand that phishing attacks are increasing day by day and people are not able to identify such type of phishing attack. Giving phishing awareness training is one way by which we can reduce the number of attacks.

1. INTRODUCTION

Phishing is variety of attack during which an attacker sends a fraudulent message designed to trick an individual into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransom ware. Phishing attacks became increasingly sophisticated and sometimes transparently mirror the location being targeted, allowing the attacker or hacker to look at everything while the victim is navigating the positioning, and transverse any additional security boundaries with the victim.

There are differing kinds of phishing like Spear Phishing, Whaling, Vishing and Email Phishing. Spear Phishing-Spear phishing is an electronic or email communications scam targeted towards a selected individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals might also will install malware on a targeted user's computer.

Whaling -Whaling is style of attack during which attacker mainly aimed position persons to steal or access the sensitive and steer.

Vishing - Vishing is that the combination of voice and phishing. In vishing attack attacker try and get sensitive and lead through call.

Vishing is that the phone scam where scammer get your financial information like account number and password. Email Phishing -Email phishing could be a form of attack within which attacker send false mail to user and trick them to falling for a scam.

2. ADVANTAGES OF PHISHING AWARENESS TRAINING.

- Empower your employees to become your first layer of cyber security

In a Web root 2019 study, it absolutely was found that 67% of employees received a minimum of one phishing email at work; and 49% of employees admitted they clicked links in messages from unknown senders during work. Because the online world is getting more and more interconnected, cyber attacks have also become more sophisticated. This includes, but isn't limited to phishing, spear-phishing attacks, business email compromise, social engineering scams, common malware and ransom ware and faux websites to steal data or infect devices. By providing interactive and ongoing training programs to your employees, they're going to have the knowledge to identify phishing emails and avoid risks online, and eventually will become your first layer of protection to cut back the quantity of security incidents.

- Meet regulatory compliance requirement

Many businesses have specific compliance requirements. as an example, if your business takes mastercard payments from customers, you want to follow PCI compliance. Or if your company stores or processes personal information about EU citizens, you need to accommodates the GDPR. Corporate compliance covers both industry policies and procedures in addition as federal, provincial and native compliance laws. Regulatory compliance is when a corporation abides by those laws and regulations. If an organization is found to be out of compliance with certain laws per their industry, this could lead to fines and/or legal

punishment. for several industries, like financial, healthcare, education, government, and retail, Cyber Security Training may be a common growing need as technology plays a bigger role in information and data handling. This training is intended to guard users and corporations from outside digital attack through better end-user practices.

3. WHAT IS THE NEED OF PHISHING AWARENESS TRAINING

Phishing may be a kind of attack during which a attacker attempt to gather personal information by impersonating a legitimate brand and sending users to a malicious website Phishing awareness training educates persons on a way to identify and report suspected phishing attempts, to safeguard themselves from cybercriminals and hackers. With help of phishing awareness we will identify the bad actors who want to disrupt and steal from your organization. Phishing awareness training refers to a training campaign or session that educates, train end users on specific phishing threats they'll encounter in their daily lives.

Effective phishing awareness training initiatives reduce phishing simulations to reinforce employee understanding, allowing them to detect and avoid phishing attacks. Simulating phishing attacks on your workforce also allows you to test your organization's maturity regarding its security awareness posture. Many businesses conduct regular phishing awareness training to stop employee from compromising their credentials, downloading malicious attachments or sending sensitive information to an impersonator. There's a typical misconception that phishing scams are easy to identify which only those that are non-technical would fall victim. There's also the false security of over-relying on technology to forestall phishing.

4. MINIMIZING PHISHING ATTACK IS IMPORTANT:

According to CISCO's 2021 Cyber security Threat Trends report, about 90% of information breaches occur thanks to phishing. Spear phishing is that the foremost typical sort of phishing attack, comprising 65% of all phishing attacks. The 2021 Tessian research revealed that employees receive a median of 14 malicious emails once a year.

In step with research from the FBI, BEC attacks accounted for 1/2 the cyber-crime losses which happened in 2019.

By clearly observing both the instance we are ready to understand that phishing attack may result in huge loss. Therefore we have to try and do to scale back the phishing attack.

5. HOW CAN WE PREVENT IT

There are some way using which we can prevent the phishing attacks. After doing the survey we find some ways by which we can reduce the phishing attacks.

Know what a phishing scam looks like

Don't click on suspicious link.

Change password regularly.

Don't be tempted by pop-ups

Have a Data security platform to spot signs of an attack.

Don't give out important and sensitive information with any other.

6. REVIEW

Central issue of the present study is phishing attack that is rising as a new challenge for twenty first century.

The rapid growth of phishing attacks lead to increase the economic loss for an organization

Phishing attack cause the release of confidential information by which attacker can get the access to the victim's accounts. Every year number of phishing attacks is increasing so we need to put mechanism to control it. Phishing awareness training is one of the solution by which we can reduce the phishing attacks by training and spreading awareness about these attacks.

7. DATA & RESULTS

After creating our data collection form, we sent it to various people and collected data on various aspects of what they think about the Phishing and what idea they have about this topic.

Questionnaire

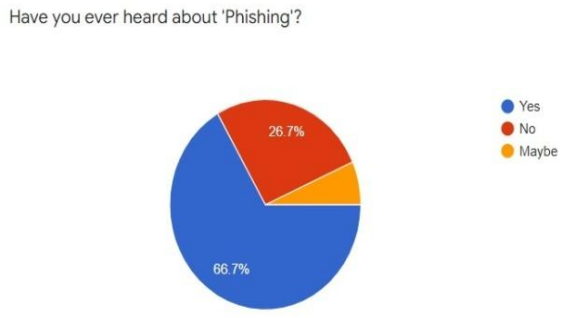
- Have you ever heard about 'Phishing'?
- Which type of URL do you use often?
- Do you know the difference between http and https?
- Do you check email address before opening the mail?
- Do you report spam or suspicious mails?
- Have you ever attended phishing awareness session?

These are some of the Questionnaire from the survey which has been helpful for me in searching for the result

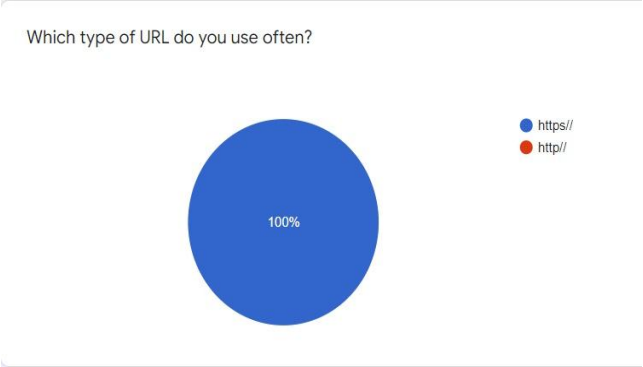
of what and how people know about Phishing and how they deal with Phishing attack.

When people were asked if they knew about phishing or phishing attack , all of the people were aware about this. In today's 21st century everyone is aware about this cyber related words. When people were asked about how much they were aware about Phishing attack the results were impressive as nearly everyone was aware of it. We rolled out the survey in such a way that whole family would be able to answer the question and it was found that all generation people knew about e-waste management.

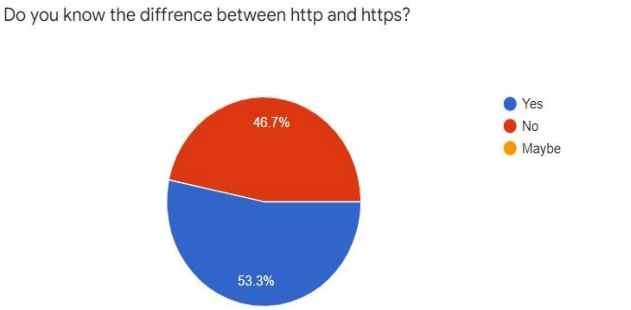
1. We reviewed this result and found about that not everybody knows about the phishing as a result we can see only 66.7% person knows about phishing.



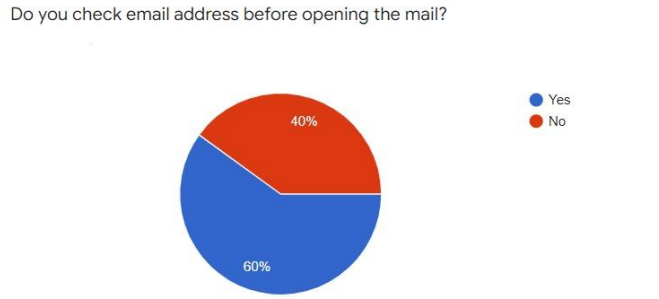
2. As we can see in the pie chart 100% of the people use https URL for safe browsing. Most of the people are aware about how to safely browse and search.



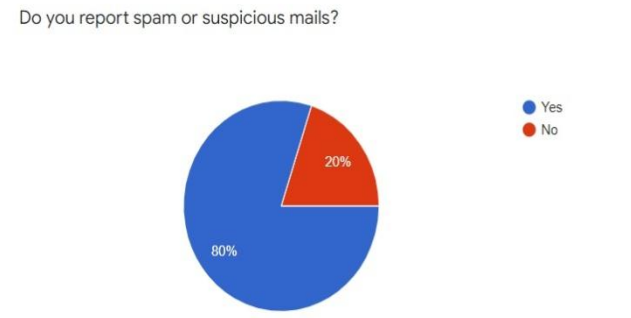
3. As we can see people don't know have idea about what is http and https. But in previous pie chart mostly people use https URL for browsing. May be they don't know the difference but they use safe way to browser. Here half of the peoples don't have idea about the URL type.



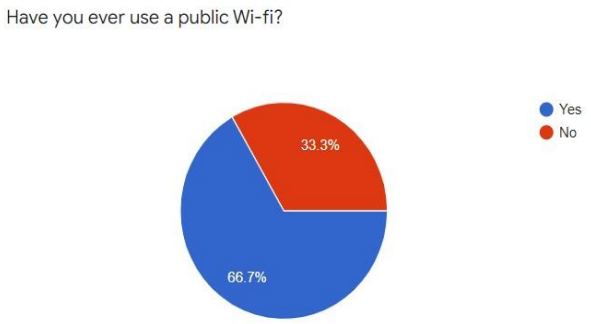
4. In today's world everyone uses Email for sending information. Most of the company or sites or offices use email to communicate with their client. According to survey 60% people check the sender name before opening the mail. So chances of getting phishing attack is less but on the other side 40% people don't check email address so it's a main threat for occurring phishing attack.



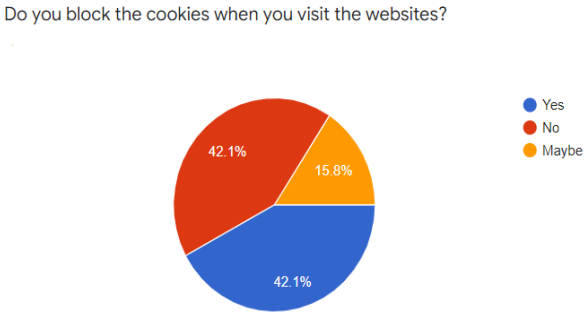
5. Email spam, also known as junk email, refers to unsolicited email messages, usually sent in bulk to a large list of recipients.As we can see in the pie chart nearly 20% people don't report spam mail,



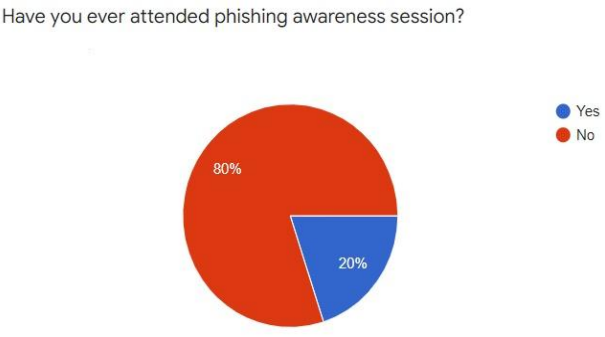
6. As we can see from below pie chart is 66.7 % people use public Wi-Fi. Public Wi-Fi is sometimes not safe so occurrence of phishing attack is high.



7. As we can see from the below chat that 42.1% people don't block the cookies when they visit the websites.
   Allowing cookies can help websites owner to streamline your surfing.



8. As we see from below pie chart 80% people didn't attend the phishing awareness session. From first pie chart we can see that everyone has heard about phishing but they don't have clear idea about phishing attack.



8. CONCLUSION

Phishing attacks are a constant threat to campus and are becoming increasingly sophisticated. Successful Phishing attacks can: Cause financial loss for victims. Put their personal information at risk. As from this research we understand that everyone is having idea about what is phishing attack but they don't pay that much attention to the phishing attack.

Phishing has a list of negative effects on a business, including loss of money, loss of intellectual property, damage to reputation, and disruption of operational activities. We face huge loss because of phishing attack. From the above survey we can see that phishing awareness training is important to train people how to deal with this type of attacks.

9. ACKNOWLEDGEMENT

I would like to thank Keraleeya Samajam's Model College for providing me with an opportunity to present this research paper. And also, I would also like to thank Divya Ma'am and teaching staff for assistance and comments that greatly improved the manuscript.

10. REFERENCES

1]Phishing Dark Waters: The Offensive and Defensive side of malicious Emails.

2]Cyber security Threats, Malware Trends and Strategies: Learn to mitigate exploits, malware, phishing and other social engineering attacks

3]Wikipedia for Phishing attacks

4]Figure, charts and survey results

https://forms.gle/o5FtC34crWVngnX18