# PHISHING - UNVIELLING ITS TECHNIQUES

**Rahul R G**
**Student,**
**School of Computer Science and IT,**
**Jain (Deemed-to-be University), Bangalore,**
**23mcar0135@jainuniversity.ac.in**

**Murugan R,**
**Professor,**
**School of Computer Science and IT,**
**Jain (Deemed-to-be University), Bangalore,**
**murugan@jainuniversity.ac.in**

***Abstract*—This study offers a detailed investigation of phishing attacks, a common cybersecurity danger aimed at individuals and organizations globally. It explores the reasons behind phishing attacks, which vary from making money to taking advantage of people's psychology. The research underscores the necessity for thorough detection systems and protective measures in order to effectively combat phishing.**
**A study among knowledgeable individuals in the cybersecurity sector provides information on their awareness and vulnerability to phishing attempts. The results highlight how common phishing attacks are and the significance of grasping various attack vectors**.

**KEYWORDS : Cyber Threat, Cyber Security, Phishing, Social Engineering, Identity Theft**.

## I. INTRODUCTION

Cyberthreat or cybersecurity threat is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, denial of services(dos) and other attacking vectors. It also directs to the possibility of a successful attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property, or any other form of cyber data.

Phishing attacks, a common type of online fraud, involve sending deceptive links to steal sensitive information. The article explores machine learning techniques for accurately categorizing phishing attacks. [1]

Cyber threats include various dangers from cyber-attacks such as cyberbullying, online predator contact, data theft, misinformation, and breaches in national security. These dangers aim at a range of industries including healthcare, government, military, finance, entertainment, and businesses, resulting in financial losses, data breaches, and societal consequences.[2]Phishing attacks often rely on social engineering tactics to manipulate victim into actions that compromise security. Researchers have developed various anti-phishing methods in recent years and still other methods are being developed. Anti-phishing software and techniques are circumvented by the phishers for dodging tactics. Though threat intelligence and behavioral analytics systems support organizations to spot the unusual traffic patterns, still the best practice to prevent phishing attacks is defended in depth.

## II. MOTIVATION AND THE CAUSE

Phishing attacks are driven by different reasons like acquiring unauthorized data, inflicting financial harm, and taking advantage of human behavior. Cybercriminals employ strategies of social engineering to deceive people into voluntarily disclosing sensitive information. The advancement of technology has made it easier for cybercriminals to access personal information by pretending to be trustworthy sources, leading to an increase in fraudulent activities. Phishing methods involve making counterfeit websites that look like real ones in order to trick users into giving away personal information such as credit card numbers and passwords. Even with anti-phishing tools in place, scammers still take advantage of people's weaknesses, underscoring the need to comprehend the psychological and sociological tactics scammers use in order to create successful protection measures.[3]

Phishing attacks are more common due to the motivation behind them especially the financial benefits behind them which give the cause for the attackers to commit this social engineering attack at larger extent and exploit human psychology aspect and essentially trick them into giving their personal information to these scammers.

Phishers try to obtain confidential information such as financial data through the creation of counterfeit websites or emails that seem legitimate. Certain attackers or groups focus on defense and diplomatic sectors for collecting intelligence by using phishing emails. Research indicates that people may

choose not to engage in protective behaviors against email phishing because they perceive there are advantages to not doing so and they weigh the associated costs of protective measures. [4]
Phishing attacks target private information such as financial details by pretending to be trustworthy online sources, taking advantage of users' trust and lack of internet security. The goal of various phishing techniques, like deceptive and malware-based phishing, is to trick users into sharing personal, financial, or password data through social engineering tactics, underscoring the importance of detection systems in fighting these risks.[5]

Moreover, spear phishing techniques may be utilized in phishing attacks, customizing messages to particular individuals or organizations depending on their interests, positions, or associations. Knowledge of these typical strategies can enable people to enhance their protection against phishing scams, promoting caution and doubt towards unexpected messages asking for confidential data or urging immediate response.

The motivation and the desires all accumulates into or encourages the phishers or attackers into committing the fraudulent activities and breach the personal sensitive data it may be confidential personal or financial data of individual,
if it remains unnoticed the attackers keep on doing these attacks which will help them financially and ultimately leads to the attackers going unnoticed for a longer period of time.

## III. STRATEGIES TO IMPLEMENT BETTER DETECTION SYSYEM

Different methods have been suggested in recent studies to improve phishing detection systems. One method includes using Machine Learning models to specifically detect phishing URLs by analyzing their characteristics, with the goal of evaluating and choosing the most effective model.[6]

The other methods can also be explored here such as using of Machine learning and artificial intelligence which is most prominent nowadays it helps with algorithm and analyze vast amount of data which covers most of the digital or cyber space which individuals are actively involved in order to identify and analyze different patterns and trends. The other most commonly used is Real-Time Detection Technique which helps us filtering the received emails and can be sophisticated phishing attacks, this includes analyzing suspicious URLs, emails content and also user behavior, this point is explained above citated material.

Another tactic includes utilizing advanced deep learning methods like Convolutional Neural Networks (CNN) to examine phishing emails and boost detection precision by identifying important features via feature engineering.[7] Moreover, distinctive psychological characteristics seen in phishing emails, such as creating a feeling of urgency and instilling fear, have been used to improve detection models. These traits led to notable enhancements in performance when integrated into neural network models.[8]

Training employees on phishing attack methods and how to recognize/report suspicious emails enables them to act as a strong defense against phishing attempts. Continuous training sessions, practice phishing exercises, and regular updates on new threats help employees stay alert and aware. Additionally, it is essential to keep software updated and effectively handle patches in order to address known vulnerabilities targeted in phishing attacks.

To improvise the detection system we can collobrate or utilize and share threat intelligence sharing system becomes very much crucial in the figt against phishing ,sharing threat intelligence with other security platforms and organization provide access to a wider range of attack vectors and emerging techniques. This actually allows system to stay updated on the latest phishing tactics and adapt their detection method accordingly.

Implementing multi -factor authentication system enables us to identify even if a phishing attempt succeds in obtaining login credentials this system adds another layer of deep security meaning it requires a secondary verification factor such as code sent to the phone, which reduces the risk of unauthorized access.

Overall we need to understand by implementing multiple level or different type of techniques to safeguard our data is much more necessity to stop the attackers from stealing our data, so we need to have basic understanding on what are the strategies we can implement to protect our data.

## IV. STASTICS DATA FROM THE INDEPENDENT SURVEY

When carrying out phishing studies or survey to evaluate awareness and susceptibility in individuals or organization, it is important to consider various key factors to ensure effectiveness and ethicality. To begin with it is important to clearly define the goals and limits of the study and the areas of awareness, vulnerability, or reaction patterns to be assessed and establishing the specific audience and frequency of phishing simulation. Secondly it is crucial to acquire informed consent from participants by ensuring they actually understand the surveys' purpose, characteristics, and possible risks, while also giving them the choice to opt out if they wish to do so.

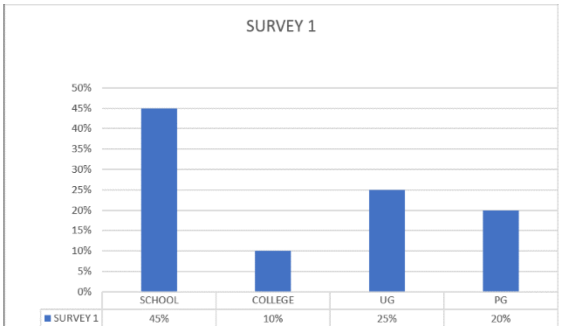
Ethical concerns are extremely important, complying with the rules and having morales, ethos and principles which should absolutely make clear of being anything near use of dishonest strategies and minimizing the risk of deviating from the questions of the survey.

The topic which we have chosen for the survey basically contains simple question relating to the understanding of the concept and its effects on the digital world and giving the insights to individuals how often they are exposed to such social engineering threats by asking them these questions so the survey can get the clear idea of what is the understanding of the individual about these topic

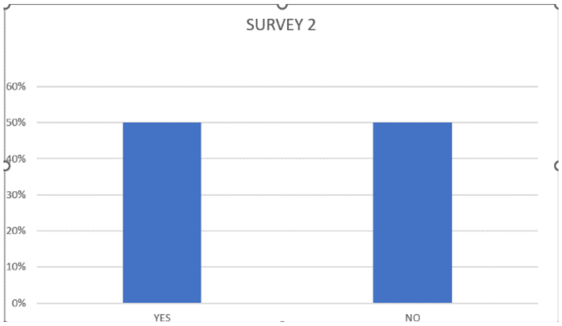
Disclaimer;
The survey was purely conducted on the academic or educated people who are currently pursuing their degree or who are they're in the current field of cyber security. This survey is also based on the findings of other research paper with the combination of our questions with current timeline to get better understanding or the grasp that people have about the topic. As these types of attacks are common and most effective in use nowadays in the current modern and digital era.

## V. SURVEY QUESTIONS WITH INTERPREATIONS

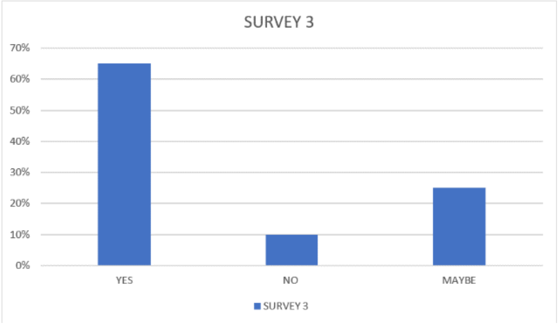
5.1. This question aims to understand when the individuals were exposed or had knowledge about the phishing attack and its types.



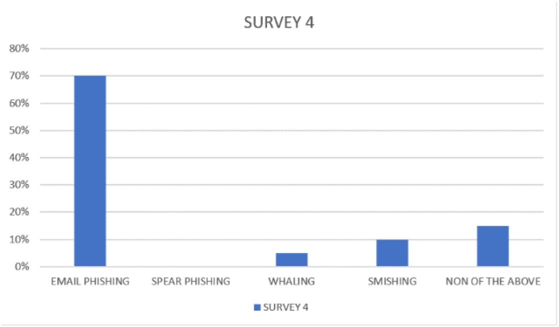
5.2. This survey question helped us to know if the individuals received an email or message asking for your login credentials or personal information unexpected.



5.3 This question was helpful in understanding if individual knows what is phishing is and how it differs from other types of cyberattacks.



5.4 This question was helpful in understanding if individual if they know other type of phishing attacks.



To summarize or put in the context most people are aware the phishing attacks when they were mostly in college or while doing their undergraduate program and it also enables us to understand whether they have received an email or any other type of message or calls to which the response overwhelming and it was recorded in fifty-fifty range. Some of them were victim of the phishing scam and some of them were aware and tried to avoid to as many as scam and stay vigilant. It also gave an idea if the individuals knew any other type of phishing attacks and how is their knowledge about them in which the response was somewhat mixed which shows their understanding about the different types of attack also.

## I. CONCLUSION

The survey that has been carried out regarding the topic of the phishing attack has shed some light on how the phishing attacks are done and revealed to us in the various aspects and capacity on how they impact both individuals and the organization or the companies and what are the ways it can have severe consequences on a day-to-day basics. Phishing attacks continue to pose a significant threat to cybersecurity, We have also seen some of the motivation behind the attacks and mainly what are the causes for this type of attack that are being carried out firstly we understood its for the greater good of the individual and as well as the financial gains that maybe they are gaining from and secondly to exploit to exploit an individual and organization and defame them or paly with the human psychology aspect of it. We've framed the movement of cautious techniques against phishing, displaying the use of cutting-edge innovations like AI, information mining, and interesting ways to deal with reinforce recognition exactness. Notwithstanding, regardless of these progressions, challenges endure in really alleviating phishing dangers. Issues, for exploiting human personal and sensitive information these prevalent cybercrimes where attackers deceive individuals into revealing sensitive information, these attacks involve sending fraudulent links and messages to manipulate victims into disclosing personal data like login credentials and financial information.[1]

example, keeping up with low misleading positive rates, the development of party time assaults, and the need for consistent observing and reaction procedures feature the complex idea of the phishing scene.
This paper also gives the solution that by implementing a sophisticated techniques we can avoid phishing attacks and protect the sensitive information with techniques like anti-phishing tools in place, scammers still take advantage of people's weaknesses, underscoring the need to comprehend the psychological and sociological tactics scammers use in order to create successful protection measures.[3]

## REFERENCES

[1] Sidra, Aslam., Ali, Bou, Nassif. (2023). Phish-identifier: Machine Learning based classification of Phishing attacks. doi: 10.1109/ASET56582.2023.10180869Rola, Al, Halaseh., Ja'far, Alqatawna. (2016). Analyzing CyberCrimes Strategies: The Case of Phishing Attack. doi: 10.1109/CCC.2016.25M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.

[2] Jaeil, Lee., Yong-joon, Lee., Donghwan, Lee., Hyukjin, Kwon., Dongkyoo, Shin. (2021). Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups. IEEE Access, doi: 10.1109/ACCESS.2021.3084897

[3] Soumya., T. (2017). Phishing Attack Techniques. Imperial journal of interdisciplinary research

[4] Jaeil, Lee., Yong-joon, Lee., Donghwan, Lee., Hyukjin, Kwon., Dongkyoo, Shin. (2021). Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups. IEEE Access, doi: 10.1109/ACCESS.2021.3084897

[5] Thakur, Pooja, Prakash., Gaikwad, Nandini, N.., Thakur, Vrushali, M. (2022). Study and Analysis of Phishing Attack. International Journal of Advanced Research in Science, Communication and Technology, doi: 10.48175/ijarsct-3087

[6] Shakirat, Aderonke, Salihu., Idowu, Dauda, Oladipo., Abdul, Afeez, Wojuade., Muyideen, Abdulraheem., Abdulrauph, O., Babatunde., Adeleke, Raheem, Ajiboye., Ghaniyyat, Bolanle, Balogun. (2022). Detection of Phishing URLs Using Heuristics-Based Approach. doi: 10.1109/ITED56637.2022.10051199

[7] (2023). Phishing Attack Detection Using Convolutional Neural Networks. doi: 10.1109/ICACCS57279.2023.10113077

[8] (2022). Phishing Detection Based on Multi-Feature Neural Network. doi: 10.1109/ipccc55026.2022.9894337