IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

RISING PHISHING ATTACKS AND ITS COUNTER MEASURES

Ashwini KR
Research Scholar ,
Department of PG Studies in Commerce
St Agnes College,Mangalore

Abstract: With the significant growth of internet usage, people share their personal information and financial transactions which becomes defenceless against cyber criminals. Phishing is one such example of a highly effective form of cyber crime that allow fraudsters to mislead online users and hack most important information. As of now, phishing is viewed as perhaps the most continuous fraudulent activities on the internet. Phishing attacks can lead to severe losses for the victims including confidential information. These attacks may occur through malicious mails, text messages and telephone calls. After getting the information , the attacker could commit crimes like hacking bank accounts, passwords and financial losses. This paper provides an explanation on phishing attacks to create awareness and also some counter measures to overcome phishing attacks.

***Index Terms* - Phishing attacks, Cyber Criminals, Awareness ,Counter measures**

I. INTRODUCTION

The digital world is rapidly extending and developing and likewise. Cyber criminals are also increasing who depend on illegal use of digital assets especially personal information for dispensing harm to people. Cyber criminals has also developed their methods for stealing their information. One of the social engineering crimes that allows the attacker to perform identity theft is called phishing attack. Phishing involves sending fraudulent emails to a target that appear to come from a creditable source. The goal of phishing is to gather sensitive data such as bank account details or install malware into target system.

Cyber criminals have taken advantage during pandemic by using widespread awareness of the subject to trick users into revealing information or clicking on malicious links or attachments downloading malware to their computers. They even impersonate government organisations, ministries of health centers for public health or important figures in a relevant country in order to disguise themselves as reliable sources. The corona virus pandemic has created new challenges for business as they adapt to an operating model in which working from home has become normal.

For this study secondary data has been collected which is available on internet and in the literature. Various annual reports of RBI was also taken for the study.

II. LITERATURE REVIEW

Neha Sharma,Dhiraj Sharma(2018) observed the different types of frauds and its prevention system in the Indian banking sector and also the role of employees as well as customers with regard to banking fraud. The study is based on secondary data. Research method adopted for the study was content analysis. From the findings it is clear that indepth knowledge and understanding of frauds is very important and valuable for government, bankers, acamedicians,auditors, bank customers etc.. in order to prevent frauds.

Alhuseen O Alsayed,Anwar L.Biligrami investigated on how hackers try to steal data's of customers and conduct financial fraud. Users can prevent phishing attacks through security solutions such as E-mail and web page Personalization, Protection software, two factor authentication and customer awareness. Phishing is growing rapidly and will cause damage to both users and banks if precautions is not taken against these kinds of attacks.

Soni RR & Soni Neena(2013) observed that as there is tremendous development in the usage of online transactions the number of banking scams also has increased which has affected more and more people. Most of the customers and institutions lost their money due to cyber frauds. According to their findings it was observed that private sector banks had the largest number of online frauds in comparison to public sector banks. Most of the banks were found to be involved in fraudulent practices even after giving tight security measures in online transactions.

John Thompson Okpa,Benjamin Okorie Ajah, Joseph Egidi Igbe (2020) examined the increasing incidence of phishing and also its impact on the survival of corporate organisations in Nigeria. Total of 1074 respondents were selected for the study, which includes financial institutions, telecommunication network providers, manufacturing companies. From the findings it was suggested that corporate organisations should spend more time in educating their staffs and customers as how they can prevent attacks from cyber criminals. Customers should be very careful when they conduct business transactions ,responding to any mails, sharing sensitive information with others.

3.1 *RESEARCH OBJECTIVES:*

1. To study the different types of phishing frauds.
2. To analyse on the phishing process and phishing counter measures.

3.2 PHISHING FRAUDS:

Phishing is a type of a social engineering where a hacker sends a fraudulent message with intention to trick a human victim to reveal sensitive information to the attacker or to deploy malicious software on the victims infrastructure like ransomware. At present phishing is the most common attack performed by fraudsters. Some of them are:

- Deceptive Phishing: it involves imitating a legitimate website and sending an email to the target which appears to be real. The email sent would contain a malicious URL or link. It would instruct the target to click on the address. After following the instructions, the phishing website gathers all the login credentials and alternative sensitive information regarding the target and forwards it to the attacker.
- Spear phishing: the attacker aims at one person and lures him or her into providing confidential information. The fraudsters customise the email consistent with the individual. The email would consist some of the targets information like persons name, companies name etc... spear phishing can happen even in social media like Linkedln where they find it very easy to obtain information on the individuals profession.
- Whaling: occurs once the phisher targets an individual at an executive position like CEO. The attacker would be identifying the victim for a substantial amount before performing the attack. The attacker similar to other types, would send an email to the target and manipulates him or her into providing information. Whaling is considered as a very dangerous attack.
- Pharming: The attack will victimize a wide range of people without having to be targeted on an individual basis. First technique involves a code that is sent to the target via email that modifies all local host files within the system. This causes target to be redirected to the malicious site in spite of getting into the proper URL. Second technique is DNS Poisoning. Here the victim will be redirected to malicious websites without their knowledge.

Currently phishing attacks arrive by mail, few arrives through malicious websites and very few by phone. When attack happens through telephone then it is called vishing. If its done through text message then it is smishing. Most common words used by fraudsters recently is urgent, request, important, payment, attention. Phishing frauds increased during the period of covid. Attackers exploited individuals looking for details on testing and treatment, assuring financial assistance and government stimulus packages, scams offering protective equipment etc.

3.2 *PHISHING PROCESS*

The motive of phishing attack is to control the attacker into providing confidential information about him or her. Phishing attacks can be explained in six steps. Initially Attacker starts the process by planning the attack. He will create an email that appears to be genuine for the victim in order to provide his or her data. After sending email to the target, it will be followed by gathering the information on the victim. Using the victim's information attacker commits cybercrime such as credit card fraud, theft etc… here victim is unable to differentiate between genuine and phishing emails. The victim enters his or her credentials in the webpage which will be easier for the hacker to access all the information to the victim.

3.3 COUNTER MEASURES

There is no single solution that is capable of preventing these attacks. There are few defense strategies to prevent phishing.

1. Human education: Awareness and human training is one way to avoid phishing. 95% of phishing attacks are caused due to human errors. Existing phishing detection training is not enough for preventing current sophisticated attacks. Giving Training is an effective way to protect users when they are using online services. Educating people are not useful if they ignore notification about fake websites. Most of the time phishing training focus on how to identify and avoid phishing emails and websites. Social media phishing is phishers favourite medium to deceive their victims. Certain countermeasures are taken by social networks to reduce suspicious activities on social media such as two factor authentication for logging. Moreover, basic knowledge in computer security is required among trained users.
2. Technical solutions: Technical solutions for anti-phishing are available at various levels of the delivery chain such as mail servers and clients, internet service provider etc... In email phishing, anti-spam software tools can block suspicious emails. There are certain techniques that can detect fake emails by checking the spelling and grammar correction are increasingly used which can prevent email from reaching users mailbox.

A new method has been developed which is called PILFER (PHISHING IDENTIFICATION BY LEARNING ON FEATURES OF EMAIL RECEIVED) where it classifies phishing emails depending on various features such as IP based URL's, number of links in the HTML parts of an email, number of domains, number of dots etc… this method shows high accuracy in detecting phishing emails

4.Conclusion:

Phishing attacks will be considered as one of the major threats to individuals and organisation. It's been known that age, gender, web addiction, user stress and plenty of different attributes have an effect on the susceptibleness to phishing between people. Apart from email and web phishing, new styles of phishing mediums like voice and SMS Phishing are on the rise. Moreover, the employment of social media-based phishing has exaggerated in use in parallel with the expansion of social media.

Although human education is the most effective way to avoid phishing, but it's difficult to remove the attack completely. Continuous awareness training on security and developing anti phishing techniques is the only way to avoid the risk.

.

REFERENCES

1. Mehdi Dadkhah,MSc,Glenn Borchardt,PhD,Tomasz Maliszewski,PhD.(2017). Fraud in Academic Publishing:Researchers under Cyber Attacks. *The American Journal of Medicine*,Vol 130,No 1.pp 27-30.
2. Vaishnavi Bhavsar, Aditya Kadlak, Shabnam Sharma.(2018). Study on Phishing Attacks. *International Journal of Computer Applications*(0975-8887) Volume 182-No.33.
3. Zainab Alkhalil, Chaminda Hewage,Liqaa Nawaf, Imtiaz Khan.(2021) Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Front. Comp.Sci.,09.
4. Arachchilage N.A.G.,Love S.(2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviour*,38(September), 304-312. https://doi.org/10.1016/j.chb.2014.05.046.
5. Chaudhry J.A., Chaudhry S. A., Rittenhouse R. G.(2016). Phishing attacks and defenses. *International Journal of Security and its Applications*, 10(1), 247-256. https://doi.org/10.14257/ijsia.2016.10.1.23
6. Ye Cao, Weli Han and Yueran Le.(2008) – Anti-phishing based on automated individual white-list, *Proceedings of the 4th ACM workshop on Digital Identity Management*, pp.51-60.
7. Akarshita Shankar, Ramesh Shetty, Badari Nath K(2019). A Review on Phishing Attacks. *International Journal of Applied Engineering Research* ISSN 0973-4562 Volume 14, Number 9 (2019) pp. 2171-2175.
8. John Thompson Okpa,Benjamin Okorie Ajah, Joseph Egidi Igbe (2020). Rising trend of Phishing Attacks on Corporate Organisations in Cross River State, Nigeria.International Journal of Cyber criminology;Vol. 14, Iss.2. 460-478.
9. https://www.statista.com Phishing-Statistics & Facts.