IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

PHISHING ATTACK AND ITS TYPES

RAJNANDNI PATIL

RAJAT KUMAWAT

VAIBHAV BHASME

B.TECH. DEPARTMENT OF COMPUTER SCIENCE ENGINEERING, SOET, D Y PATIL UNIVERSITY PUNE, AMBI.

ABSTRACT:

As the technology is getting advance cybercrimes are increasing with the same speed. cyber-crime is nothing but getting an unauthorised access to someone's computer, networked devices or a network to steal, copy, manipulate their data or recourses. there are many cyber-attacks present some of them are man in the middle attack, phishing attack, ransomware attack, dos (denial of services), ddos (distributed denial of services) etc. one of the most commonly used and dangerous attack is phishing attack.

This research paper explores the various aspects of phishing attacks, including their definition, types, techniques, and impacts on individuals and organizations.

Phishing is a major problem because there really is no patch on human stupidity. In fact, phishing attack is so cleverly executed by the attacker that most smart person is also tricked by it.

Phishing attack is a type of cyber-attack which is mainly done to steal your information which may include credit card details, bank account information, password, login details and much more.

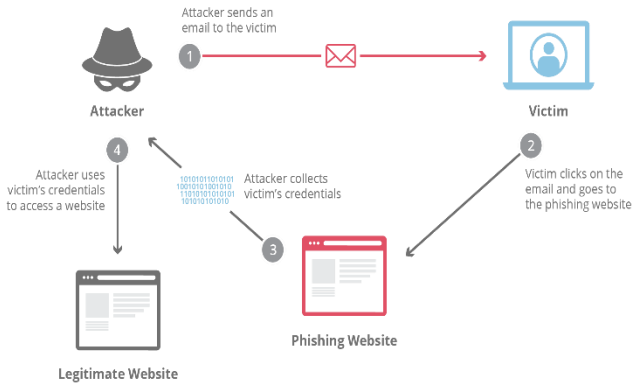
• ***INTRODUCTION:***

Phishing attacks are cunning cyber scams designed to deceive unsuspecting individuals and trick them into revealing sensitive information like passwords, credit card details, or personal data. These attacks typically occur through emails, text messages, or fake websites that appear legitimate at first glance.

once a received a mail where I was asked to fill some details about my bank account and the reason provided was it is a bank survey so, please kindly corporate and fill the form urgently, and the mail was same as the original one. So, I started filly all my information and submitted it. and by submitting this form the phishing attack was successfully executed by the attacker.

Phishing attacks are successful because they rely on our trust in familiar brands or urgent situations. By using clever tactics and manipulating our emotions, scammers try to bypass our scepticism and make us act quickly without thinking twice.

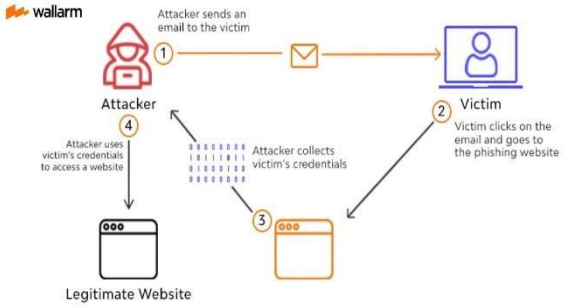
O Types of Phishing Attack: -



Phishing attack is only one cyber-attack which has many ways to be executed. There are many types of Phishing attack

O Certain Terminologies in Phishing Attack:

1. **Attacker: -** They are also called as hackers. They are people with lot of knowledge of computer technologies and networks. as the name attacker suggests that attacker is a person who attacks someone or something, so in cyber world attacker is a person who tries to get unauthorized access to a system for stealing the information or to modify the information present.
2. **User: -** Here user plays a role of a victim. user is a person whose information is being illegal accessed by the attacker.
3. **Phishing Website: -** It is a duplicate website made by the user to collect all the information entered by the user. This phishing website looks exactly same as the original website.



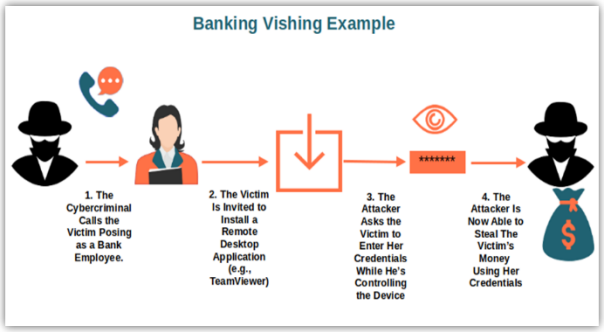
1. *Smishing Attack: -*

Smishing attack uses a SMS or a text message to be executed. Here attacker sends a SMS message or text message to the user, some of the examples of their attack are part time jobs available just click on the link below, you have just credited a bonus on your rummy account, home loans available etc. and as the user clicks on the link he enters the phishing website where he provides all asked information which is then collected by the attacker and then the attacker used all the information on the official or original website and gets access to the account of the user .

2. *Vishing Attack: -*

Vishing attack uses voice call to get execute. in vishing attack the attacker directly calls the user or victim and starts convincing the user about his fake organisation and asks the user to tell all the required information.

as the user gives the information, the attacker enters all provided information on the original website and gets access to the account of the user. example of vishing attack is you getting a call from bank to update your kyc, a person calling you to give loans etc.

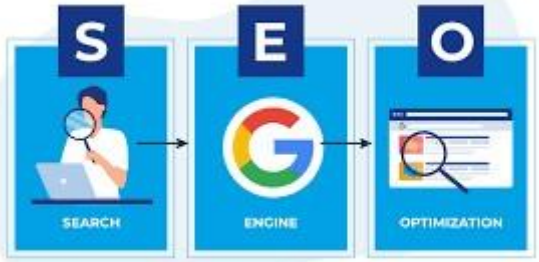


3. ***Whaling Attack: -***

Whaling attack is one of the biggest and most harmful phishing attack. Whaling attack focuses on higher authorities and not on the common users. here higher authorities are bank managers, chief executive, company owner, CEO of an organization etc. In whaling attack, the attacker can either call, message or email to the big authorities and ask them to provide the information related to their organization and then uses the same information for the phishing attack. As here whole organizations data is in risk it is a big and harmful attack. For example, a bank manager getting a call from a fake income tax office and asking to pay a tax or share the information so that the tax is updated.

4. ***Search Engine Attack: -***

Search engine attack is also called as SEO Poising or SEO trojan. in search engine attack, attacker is not attacking on a specific user. attacker shares a general link on the search engine which gets mixed with the other original links. For example, if you were searching best colleges in Pune on the google search and you get many links, one of them will be this phishing link which ones opened will ask you to login and the login page will ask you all the basic information about you and then the information will be used by the attacker in future.

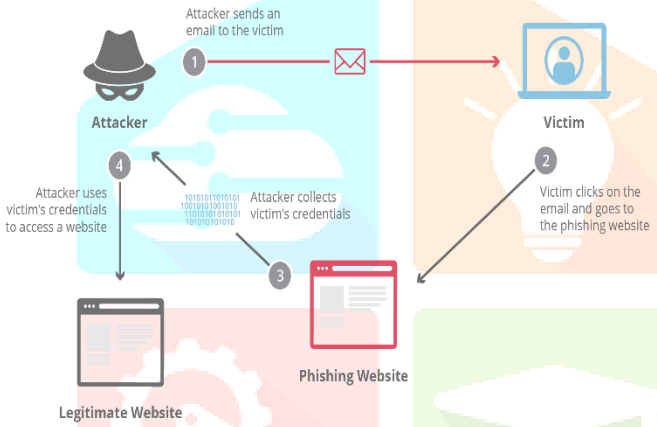


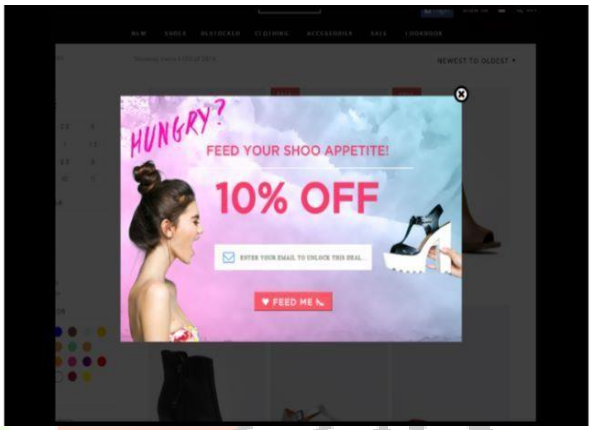
5. ***Email Phishing Attack: -***

This is the most common attack taking place nowadays. Here the user receives an email which will ask to be checked and filled on the urgent basis. Once the user clicks on the link provided will be entered in the phishing website and the information will be collected by the attacker. For example, you get an email saying congratulations you have won a lottery of one lakh rupees to claim your reward click on the below link.

6. ***Pop Attack: -***

Pop attack are the attacks that every one's system consists of pop-up attack is nothing but the attack which is done through the pop ups present on the search engines which attracts us by blinking on the top. Example of the pop ups present are khelo jeeto, best shops near you, sale buy one get two, exclusive offer on branded clothes etc.





6. Install firewalls.

• ***Preventions of Phishing Attack: -***

Preventing Phishing Attack requires a combination of good security practices and proactive measures. Here are some steps you can take to help protect yourself and your systems:

1. Get free anti phishing attack.
2. Keep changing your passwords regularly and make sure they are strong.
3. Update your browser and apps regularly.
4. Don't share personal information on unknown websites.
5. Don't click on unknown links or unauthorized links.

• ***Conclusion: -***

In conclusion, the study of phishing attacks has revealed the increasing sophistication and prevalence of this cyber threat in today's digital landscape. the research conducted by this paper puts light on the various ways through which the phishing attack can take place. These attacks involve the encryption of critical data and system by cybercriminals. phishing attack have cause financial losses, personal information going viral and the data of many organizations have been used for wrong use. Preventions of phishing attack should be spread all over and everyone should understand the need to implement those preventions and should be aware of phishing websites, links, calls and all the ways through which phishing can take place.

• References: -

1. Amija, R., Tygar, J. D., & Hearst, M. A. (2006). Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems (pp. 581-590). ACM.

2. Kobsson, M., & Myers, S. (2007). Phishing and countermeasures: understanding the increasing problem of electronic identity theft. Wiley.

3. Maraguru, P., Rhee, Y., Sheng, S., & Hasan, S. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In Proceedings of the 16th international conference on World Wide Web (pp. 51-60). ACM.

4. A.P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices (pp. 3-14). ACM.

5. Ajano, F., & Wilson, M. (2009). Understanding scam victims: seven principles for systems security. Communications of the ACM, 52(3), 134-142.