Phishing Attacks and Various Anti Phishing Techniques

[1] Kadheejath Azmeena O P, [2] Mariyammath Thabsira G, [3] Zulaikath Fahmida
[1,2,3] Student, *Dept. of Computer Science and Engineering, Bearys Institute of Technology Mangalore*

***Abstract*-- Phishing is a form of cybercrime where an attacker imitates a real person / institution by promoting them as an official person or entity through e-mail or other communication mediums. In this type of cyber attack, the attacker sends malicious links or files through phishing emails that can perform various functions, consisting capturing the login credentials or account details of the victim. These e-mails affect victims because of money loss and identity theft. This paper presents an overview about various phishing attacks, characteristics of phishing and various techniques to protect the information.**

***Keywords*— Phishing attack, Security, Anti Phishing**

I. INTRODUCTION

Phishing is a false attempt, generally made via email, to lure personal information of any user. It point to the act that the attacker make users to visit phishing website by sending them faked e-mails, and without a sound get user's personal details such as user name, passwords, etc. The main goal of the attacker is always to attract notion into giving up confidential information. Phishing is also known as "Brand Spoofing". The statement has its own birth from two words-Password harvesting or- fishing for passwords. One of the most important point of phishing is to fraudulently carry out economic transaction on behalf of users using a spam email that consists a URL link pointing to a fraudulent website concealed as an online bank or a government entity. Phishing is a rising struggling for the internet users. The most effective clarification to phishing attack is, training and education users not to unknowingly go behind the fraud links to websites where they have to give personal information. Phishing is a crucial impact on Web. Section – II discusses characteristics of phishing attack. Section III discusses about types of phishing attack. Section IV discusses prevention of phishing attack. Section V describes techniques used to detect phishing attack. Section VI discuss on the survey on phishing detection techniques and Section VII describes the conclusion part of the paper.

II. CHARACTERSTICS OF PHISHING ATTACK

i. *Absence of recipients name*: The group who sends fraudulent emails which do have links but depend on the user's reply for continue the attack usually find the email record from websites or use web write off. This particular type of email is always remark to be coming without the name of the receiver mentioned somewhere in the email.

ii. *The Mention of Money*: The simple way a attacker can get stranger to reply to emails seems to be promising a fine amount of money. Once the users starts to believe that he/she is going to get the word total of money and that the people making the promise are true, then the attacker ask them for confidential information or ask to transfer a amount of money to an account and then they disappear.

iii. *Reply Inducing Sentence:* The attacker fake as the institution they mention in the email, and then do whatever they can to convince the victim into belief so that people may respond and provide with private information. If anyone does reply, the real mind of attacker starts attractive.

iv. *Poor Spelling and Grammar:* Majority of phishing fraud emerge from areas of the world where English is not normally spoken. One more sure indication of a phishing attack is strange formatting, including misplaced punctuation and capital letters. Many attacks also tend to trade meaninglessly hyperbolic language and a origin of exclamation marks.

III. TYPES OF PHISHING ATTACK

A. Deceptive Phishing:

An attacker sends bulk email with a message. Where peoples are requested to tick on a link. The majority of familiar type of phishing attack, deceptive phishing point out to any attack through which fraudsters presume as a valid team and attempt to steal people's private information or login credentials.

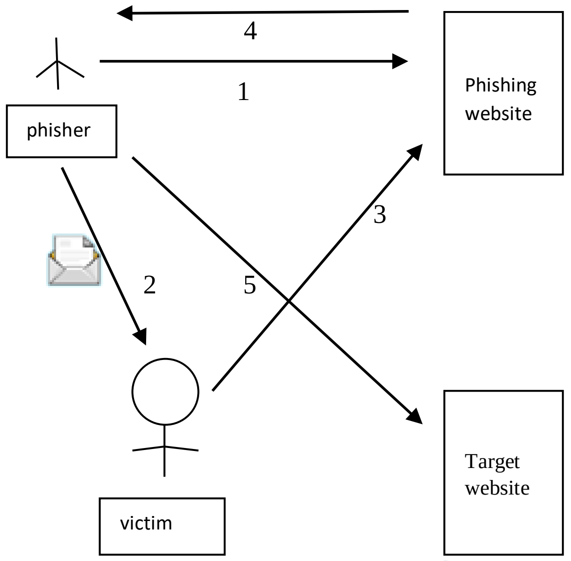


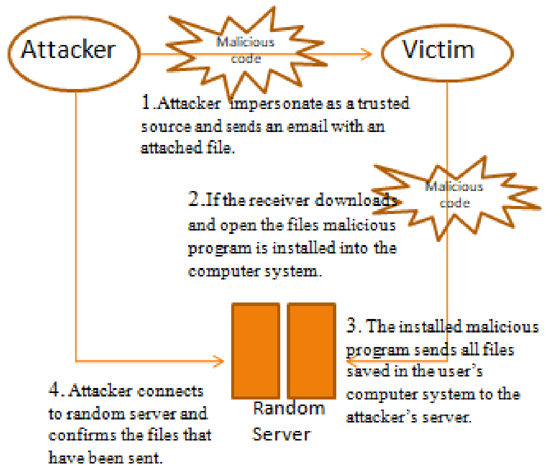
Fig 1: Deceptive Phishing

B. *Phone Phishing:*

This kind of phishing occurs when the people are requested to dial a phone, assuming from a valid bank, to query the information for their bank account details. Involvement of caller ID is one of the new method of Phone Phishing.

C. Spear phishing:

It is an kind of e-mail spoofing fraud try that selects a particular organization, seeking legal access to private data also type of phishing attack that focuses on a single user or section within an company.



1.Attacker impersonate as a trusted source and sends an email with an attached file.

2.If the receiver downloads and open the files malicious program is installed into the computer system.

3. The installed malicious program sends all files saved in the user's computer system to the attacker's server.

4. Attacker connects to random server and confirms the files that have been sent.

Fig 2: Spear Phishing.

D. Clone Phishing:

A type of phishing attack whereby a authentic, and recently delivered, email having an addition or link had its satisfaction and receiver address taken and used to generate an almost same or cloned email is known as clone phishing.

E. *Whaling:*

This kind of attack points mostly at the higher profiles or any of the high level posts in a work firm. The phishing email is emailed to the people in the form of legitimate subpoenas, customer complaint or any notification that require high profiler's attention. The destination is dissimilar from the URL text in the e-mail.

IV. PREVENTION OF PHISHING ATTACK

1. Give training to the users to understand how phishing attacks work and to be aware when phishing like e-mails are received.
2. Identify and block the phishing websites in time.
3. Increase the security of the websites.
4. Block the phishing e-mails by different frauds clarify.
5. Never email private or confidential information, even if people are known to the recipient.
6. Do not click on the links, download files or open documents attached in emails from unknown senders.
7. Keep systems or laptop with a firewall, spam filters, anti-virus and anti-spyware software.
8. Verify online accounts and bank details regularly to make sure that no unauthorized transaction has been made.

V. Phishing Detection

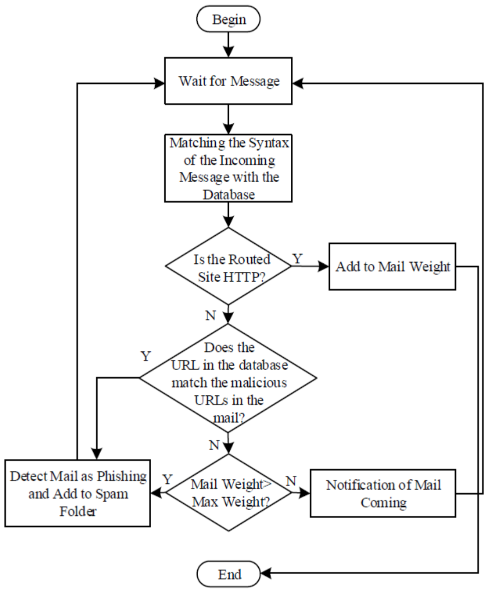

Begin
Wait for Message
Matching the Syntax of the Incoming Message with the Database
Is the Routed Site HTTP?
Y
Add to Mail Weight
N
Does the URL in the database match the malicious URLs in the mail?
Y
N
Detect Mail as Phishing and Add to Spam Folder
Y
Mail Weight> Max Weight?
N
Notification of Mail Coming
End

Fig. 3: Flowchart of the application

To check the text content and determine whether the related message contained phishing elements, an application called "Anti Phishing Simulator" was developed. Figure 3 shows the simple flowchart of the implemented application. To check whether it is a phishing message or not an e-mail can be found in primitive ways. For this observe whether a link with the message similar to the actual website, if the sent mail or referrer web site is using some emotional or exciting words to get a response, whether it is spelling mistakes in the email or on the website. However, many people pay attention to this point unconsciously entering the links given to others accounts.

"Anti Phishing Simulator" determines whether a message is phishing thanks to the Bayesian classification algorithm and the scores added to the database. It is instantly perceived as a spam message by the words that are exciting, phrases that increase the desire for shopping, and which contain unwanted content. In addition, these spam mails can be viewed from the spam section. At the same time, it is possible to add an unwanted site URL address or an unwanted word to the database with the "add spam" feature. The page's html code is displayed with the "URL control" feature for those who have mastered the computer programming language. In this way, it can be checked whether the links in the page are valid or not. Although the database is very large, there is "add spam" feature to manage it on demand. In this way, the user can filter out messages that are not really spam, but that he does not want to see. Figure 4 shows the logical operation of the life cycle of a phishing attack and the detection operation performed.

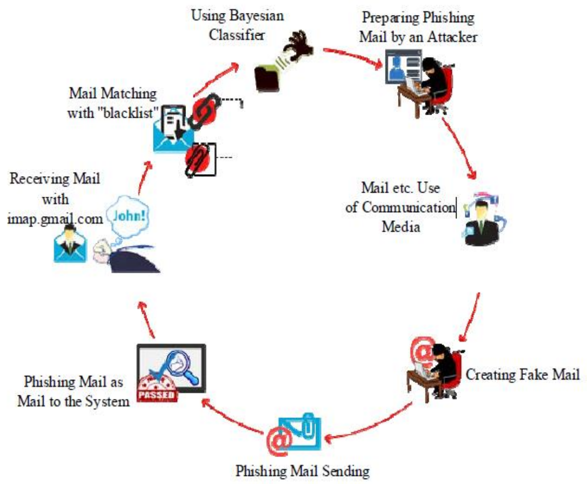
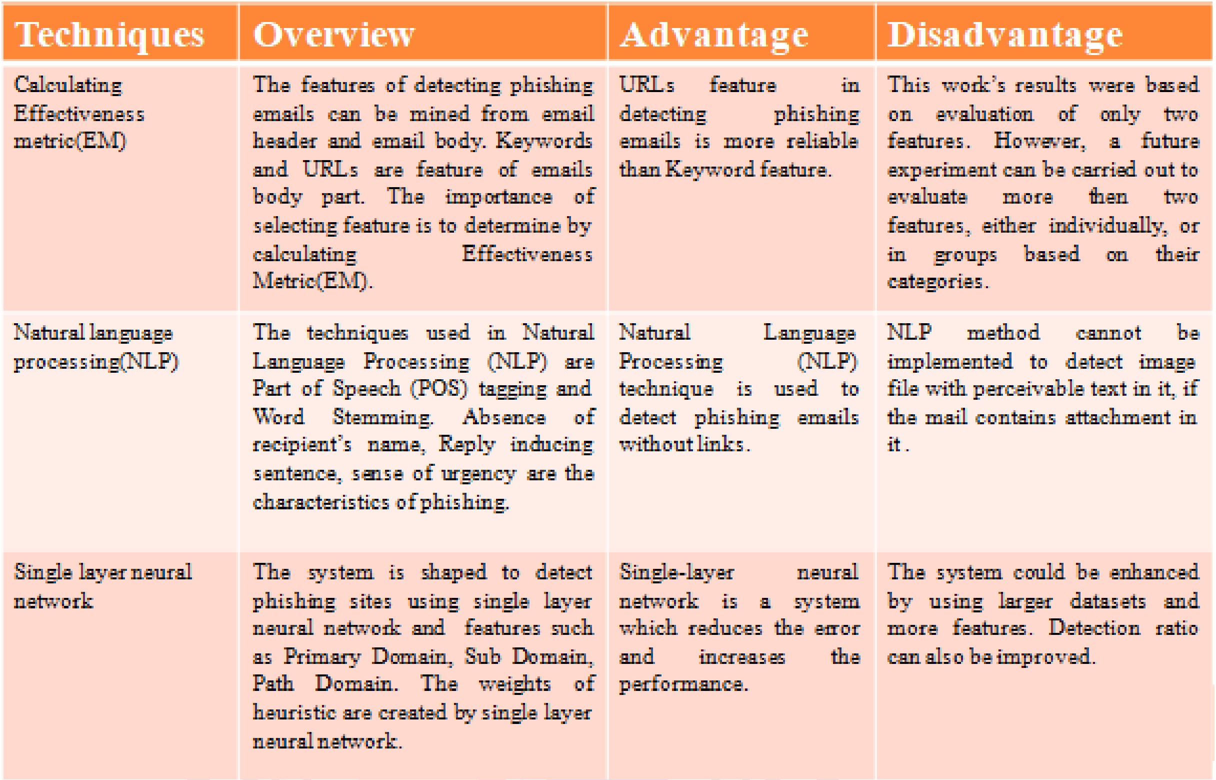

Using Bayesian Classifier
Preparing Phishing Mail by an Attacker
Mail Matching with "blacklist"
Mail etc. Use of Communication Media
Receiving Mail with imap.gmail.com
John!
Creating Fake Mail
Phishing Mail as Mail to the System
PASSED
Phishing Mail Sending

Fig. 4: Logical operation cycle of the performed work

Anti Phishing Simulator aims to control the security of information and to prevent infringements, to check whether spam is available from the current database, to enable the user to create his own spam list, and to check whether the incoming mail has dangerous content.

VI. LITERATURE SERVEY

Table.1: Various techniques used for phishing detection



Techniques	Overview	Advantage	Disadvantage
Calculating Effectiveness metric(EM)	The features of detecting phishing emails can be mined from email header and email body. Keywords and URLs are feature of emails body part. The importance of selecting feature is to determine by calculating Effectiveness Metric(EM).	URLs feature in detecting phishing emails is more reliable than Keyword feature.	This work's results were based on evaluation of only two features. However, a future experiment can be carried out to evaluate more then two features, either individually, or in groups based on their categories.
Natural language processing(NLP)	The techniques used in Natural Language Processing (NLP) are Part of Speech (POS) tagging and Word Stemming. Absence of recipient's name, Reply inducing sentence, sense of urgency are the characteristics of phishing.	Natural Language Processing (NLP) technique is used to detect phishing emails without links.	NLP method cannot be implemented to detect image file with perceivable text in it, if the mail contains attachment in it .
Single layer neural network	The system is shaped to detect phishing sites using single layer neural network and features such as Primary Domain, Sub Domain, Path Domain. The weights of heuristic are created by single layer neural network.	Single-layer neural network is a system which reduces the error and increases the performance.	The system could be enhanced by using larger datasets and more features. Detection ratio can also be improved.

VII. CONCLUSION

Phishing emails and web site attacks have provided a many opportunity for attackers to reach collection of potential victims, with small cost sum, in the hope of users supplying their private and financially sensitive information. This paper describes the different Types of Phishing Attack, Characteristic and Prevention of Phishing Attack, Different Techniques used for Phishing Attack and Survey on the Phishing Attack and its Detection.

VIII. REFERENCES

[1]. Muhammet Baykara and Zait Ziya Gurel, "Detection of phishing attacks," 978-1-5386-3449-3/18/$31.00 ©2018 IEEE.

[2]. Lakhita, Surendra Yadav, Brahmdutt Bohra, Pooja, "A review on recent phishing attack in internet," 978-1-4673-7910-6/15/$31.00c 2015 IEEE.

[3]. Melad Mohamed, Al-Daeef and Nurlida Basir and Madihah Mohd Saudi, "A Method to Measure the Efficiency of Phishing Emails Detection Features," 978-1-4799-4441-5/14/$31.00 ©2014 IEEE.

[4]. Shivam Aggarwal, Vishal Kumar and S D Sudarsan, "Identification and Detection of Phishing Emails Using Natural Language Processing Techniques," SIN '14, September 09 - 11 2014, Glasgow, Scotland Uk Copyright 2014 ACM 978-1-4503-3033-6/14/09…$15.00.

[5]. Luong Anh Tuan Nguyen, Ba Lam To, Huu Khuong Nguyen and Minh Hoang Nguyen, "An Efficient Approach for Phishing Detection Using Single-Layer Neural Network", International Conference on Advanced Technologies for Communications, 978-1-4799-6956-2/14/$31.00, 2014 IEEE.