IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 21, Issue 3, Ser. V (May - June 2019), PP 40-44
www.iosrjournals.org

Review on Phishing

Trupti V. Kantale, Mr. Lovely. S. Mutneja, Pooja W. Pawar,
Mr. Shoeb A. Khan
Department Of Computer Science And Engineering
Sant Gadge Baba Amravati University
Amravati, Maharashtra, India.

***Abstract**: The word PHISHING was discovered around 1996 by the hackers of America stealing online accounts and passwords which was the origin of phishing. Phishing is well known example of Social Engineering. Accessing personal information as well as financial credential by using malware or any social engineering platforms and which may then use by the 'phishers' for their personal gain is the primary goal of phishing technique. Email Spoofing and Instant Messaging are the two most relevant techniques used for phishing. In Email Spoofing and Instant Messaging techniques, unknowingly user enter their personal information and financial credential at a fake website which may look like real websites. This paper presents an overview about phishing origin in the first section and various techniques to avoid phishing in second section.*

***Key Words:** Malware, Phishing, Anti-Phishing, Security Email Spoofing, Instant Messaging.*

Date of Submission: 12-06-2019 Date of acceptance: 28-06-2019

I. Introduction

The 'Phishing' is the integration of two words ‘Phishing’ and ‘Phreaking’. Phishing is defined as the act of manipulating user through various craving technique like sending emails from suspicious websites which seems to be similar to the real ones, websites maneuvering and so on. Phishing emails are just another category of spam. Phisher’s represent themselves as the respected companies (target) just to access customer account and personal information in tricky manner. There are different techniques to access user’s personal as well as financial information like fraud websites, fraud mail, and phishing. Among all these techniques phishing is the most compatible technique for the phishers to steal the user’s personal and credential information in silly manner. Phisher’s steal the user’s personal information by applying techniques like sending emails which seems to be come from legitimate websites. It seems to be like that “there’s been problem is occurred while visiting the page please reload the page by clicking the website given below” or “enter your password in correct manner.” Usually the strategy to access the personal and financial credential information is fixed and it seems to be like in the form of text messages, emails and messages format look alike Your mobile number has won prize money from amaz0n company please fill your personal details and account number to the given website. This type of local phishing attacks can be prevented by restricting the sources from where it comes. Phishing is ever-growing process it will remain exist as there are several greedy ways to fool the user but it is our duty to verify the provided information is correct or not. Scarcity of knowledge and awareness about phishing makes it profitable. Sufficient Knowledge about phishing and security tools avoid phishing threats and can reduce the phishing technique. Phishing is defined as the form of fraud by which a cyber-attacker is able to steal personal information of user by using social platforms and resources like Facebook, Instagram and twitter According to COLIN WHITTAKER definition, "Phishing page as any webpage that without permission, alleges to act on the behalf of a brand with the intention of confusing viewers into performing an action with which viewer would only trust a true agent of the brand."

The cyber attackers may use the most common method for attacking such as email sending which may look like original emails from banks, online organizations or any trusted agencies. In these emails they make some certain required changes according to their facility as well as user’s convenience to make the user fool. Now a days Credit card fraud is the panoramic term use for the phishing attacks. Credit card fraud initialization starts with theft of the actual card or stealing the data bounded with the bank account, including bank details along with the three or four-digit card verification number. As the transaction becomes digital, so there is the greater impact on the credit card fraud and the percentage of phishing attacks is raising day by day. It is our duty to verify debit card details along with it’s Personal Identification Number(PIN) which is known only to you and keep updating it within every three months. Based on the phishing attack there are several reason behind compatible phishing, but there are mainly three reasons why phishing is so popular and successful they are as follows.

In this paper, in the first section we discuss what is phishing and in the second section we discovered some anti-phishing tools.

II. Literature Review

Venkata Prasad Reddy, V. Radha, Manik Jindal [5] introduces two methods to secure from phishing attack. First method is built on spoof alert and Second method is a browser extension. In the first method whitelist are involved which contains data as per user's requirement and in the second method use of trusted windows which specially use for to show the password entry along with photographic representation.

Aanchal Jain and Prof. Vineet Richariya [6] implement a pattern for web browser, which is used as an agent and processes the data from phishing attacks. When the user uses the web browser and open the email and if any attack is detected the user will be notified about the fraud email. The pattern which is mention in the paper will prevent help the user from opening the suspicious websites.

V. Suganya [7] has stated details about phishing and given idea about all kind of attacks and protective measures regarding phishing attacks.

Nilkesh Surana, Prabhjot Singh, Umesh Warade, Neha Sabe [8] implement a new algorithm defined as the 'Link guard algorithm' to remove phishing attacks. The features of hyperlink are used in this algorithm to minimize the attacks. Link guard algorithm identify the difference between the visual link and actual link.

Why Phishing is so popular?

Reason behind popularity of phishing

1) INSUFFICIENT KNOWELDGE:

lack of awareness/training about phishing and its fraud is the first main reason why these phishing attacks are so successful. User are unaware about how computer, operating systems, user application, web application, emails works and how to distinguish among all these application become the tedious job for users. For e.g. Some users do not understand meaning of server name, domain name, IP address and that's why they cannot distinguish between real vs fraud websites (for e.g.: they may think that www.peoplesecurity.com) similar to www.peoplesecurityy.com) Another strategy use for phishing attack may be use of email header. Users don't have sufficient or required knowledge about valid and invalid email headers.

2) VISUAL DECEPTION

Phishers may use visual tricks or methods in the form of text, images or in some another form.

a) Visual Deceptive Text: In this technique, instead of using real website they make slight (www.amazo0n.com). In this given example instead of using 'o' at the required place by replacing '0' phishing can be done this is called visual deceptive text.

b) Image hidden text: Using the image of well-known URL's which itself provide the hyperlink of fraud websites.

c)Windows hidden windows: Placingthe fraud browser window under the real browser window by making some slight change in the server address or security indicators is the frequent technique used by phishers.

For detecting phishing websites, we can use some fuzzy techniques. It is based on the fuzzy logic and there are six categories to differentiate between legitimate website and fake website. There are different number of elements included under these categories. They are as follow

Table 1: Benchmark to differentiate between legitimate website and fake website

Serial Number	Benchmark	Phishing Indication Sign
1	URL and domain name	a) Use of IP address b) Isolated or abnormal URL request c) Atypical URL d) Atypical DNS record
2	Source code and JavaScript	a) Redirected pages b) Riding or Straddling attack c) Server Form Handler(SFH)
3	Page style contents	a) Spelling error b) Use of popup notification c) Incapacitate right click d)Use of popup windows
4	Security encoding and Encryption	a) Use of Secure Sockets Layer Certificate(SSL) b) Certificate domination c)Atypical cookies
5	Web address bar	a) Extensive URL address b)Replacing-equivalent character
6	Social aspect	a) Great accent on security or response b)Procuring time for accessing accounts.

Steps included in Phishing
Diagrammatic representation of steps involved in phishing
In phishing to access the user's personal and financial information phisher's use the most common method like phone phishing, hacking, whaling and so on. In order to achieve the user's information in more sophisticated way phisher's use the simple trick to get the data in efficient and effective manner. Usually process of phishing involves six steps which further consist of Plan, Trap, Attack, Theft, Embezzlement and Post attack action.

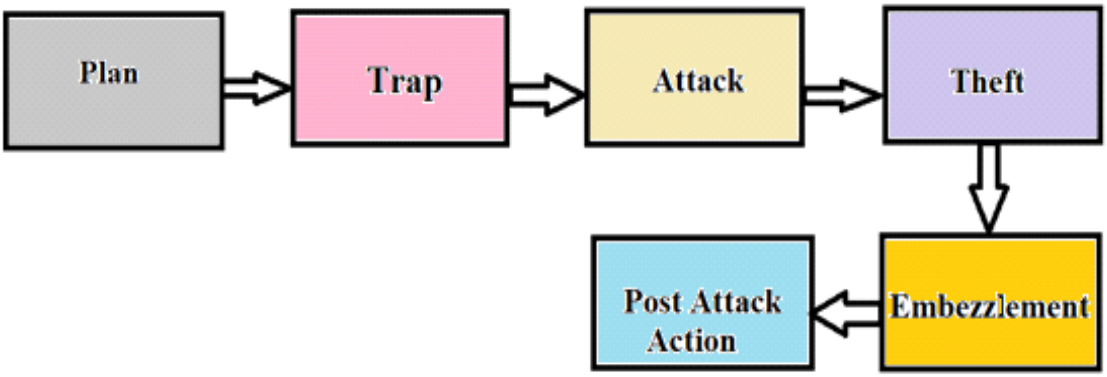


Figure 1: Steps involved in phishing

III. Phishing Types

Phishing is just wide ranging category of infraction defined as the identity stealing. Social engineering methods have great effect on phishing attacks since last decade. As the main purpose of phishing is to steal the user's personal and financial credential but still there are different ways for phishing. In order to identify category of phishing attack and provide effective and efficient security it's important to know category of phishing attacks, causes of phishing attacks and its prevention techniques are given as follows.

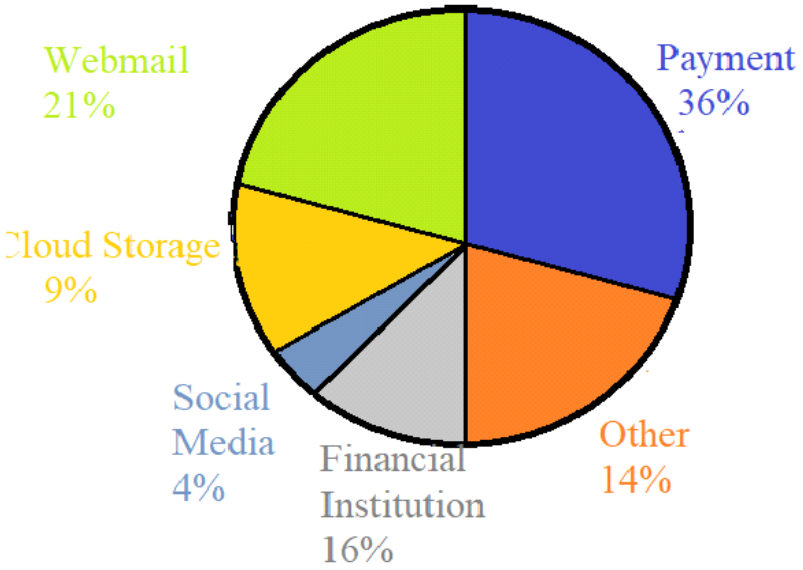
Table 2. Phishing Types

Index No.	Category of phishing	Transmission Medium	Prevention/Remedy
1)	Deceptive Phishing	a)Instant messaging b)Email messaging	a) Verify at least once suspected phishing emails b) Verify the source of information at least once c) Enhance the security of computers
2)	Malware Based Phishing	a) Sending malware as email attachment b) Popup notification of having virus in your PC's.	a) Aware of popup notification of program that are not installed in your computer b) Enter your sensitive information at sensitive websites only.
3)	Key loggers and Screen logger	a) Keyboard b) Internet	a) Use of system having inbuilt feature of detecting keylogging software b) Use of Virtual keyboard
4)	Session Hijacking	a) Use of Source Rooted IP packets. b) URL cookie	a) Use of long string as Session Key. b) Encryption of Data Traffic.
5)	Web Trojan	a) unrequested Email b) unrequested ad	a) Operating system should be always up-to-date. b) Install authentic antivirus software. .
6)	Whaling	a) Embezzlement emails similar to the real emails b) Invalid email addresses and authentic corporate logos of company.	a) Awareness about whaling attacks among people. b) Implement data protection.

Survey Report

From the last decade phishing has the abnormal growth and the main resources are social engineering platforms or malware. A survey report which was done by the Wombat security Technologies in the year 2017 concluded that there is major increase in phishing attacks more than 80 percent. According to survey which was done by ANTIPHISHING WORKING GROUP(APWG) in 2018, banking sector was the most targeted sector and there was sudden large growth of the phishing attack and it was about 36% than the others sectors like social media platforms, cloud storage, financial institution and web-mail.

Most Targeted Industry Sectors,2018[1]

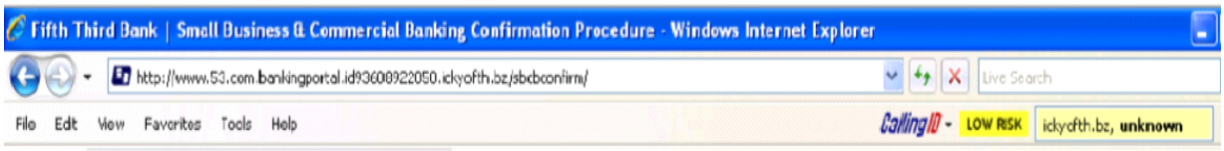


Anti-Phishing Tools

List of Anti-Phishing Tools

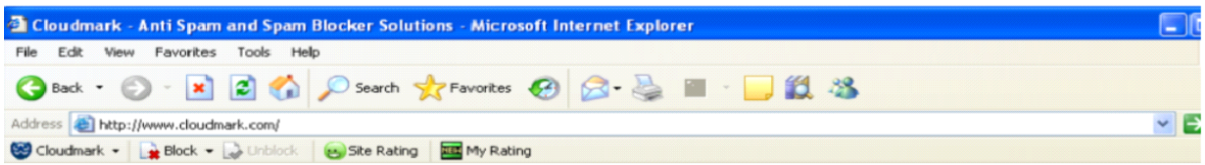
1) Calling ID Toolbar:

This toolbar is used to determine authority of given site. Calling ID is based on visual indicators. These indicators can be represented by using different colors like green represent site that is "good", Yellow color represent that site is “harmful”, Red color represent that site is "danger" and that's why it may be phishing site. The calling ID Toolbar runs on Microsoft Windows 98/NT/2000/XP with internet explorer.

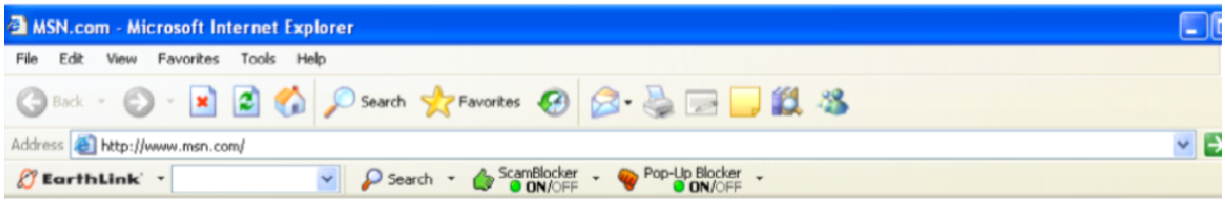


2) Cloud mark Anti-Fraud Toolbar

This toolbar is based on the user ratings. When user visits any site it asks for feedback whether it is good or bad. According to that toolbar will indicate particular colored icon for each visited site. If Green icon is appearing, then it is valid site. If Red icon is appearing, then it must be fraud site. If Yellow icon is appearing, then it has insufficient information or invalid site.



3) EarthLink Toolbar:
It is completely relying on the combination of User's ratings and user's manual verification. Small information about is given on earth link website, this toolbar allows user to report fraud phishing website. After reporting as fraud sites are added to the blacklist .



4) eBay Toolbar:
The eBay Tool uses combination of heuristics and blacklist. The account guard indicator has three modes green, red and gray. When green icon is appearing that means user visited the, and the site is operated by eBay(PayPal). When icon is displayed with red background when it is called as phishing site. When icon is displayed with gray background it may be consider as invalid.

IV. Phishing Prevention Technique

General phishing solution
1)Technological Solution
2) Change in policy
3) Identify Theft
4) Involuntary block Fraud emails.
5) Be Skeptical.
6) Avoid Email forms.
7) Check for invalid URL'S
8) Implement Anti-Phishing software
9) Enter your personal details only at trustworthy websites only.
10)Arrange Awareness program.

V. Conclusion

Phishing is an attempt to access sensitive information in tricky manner. Basically the phishing is way of identical theft. There are many different techniques to solve these issues. But due to scarcity of knowledge and security about phishing makes it successful and profitable. Due to the evolution in technique there are different anti-phishing tools and software are available to prevent phishing. In this paper, we may give the awareness about phishing problems and techniques to solve it.

References

[1]. Anti-phishing Working Group (APWG) Trends Report 2018, https://www.antiphishing.org /resources/apwg-reports / 2018
[2]. Predicting Phishing Websites Using Classification Mining Techniques with Experimental Case Studies published at IEEE explorer 176 - 181. 10.1109/ITNG.2010.117
[3]. AntiPhishing_Phil_The_design_and_evaluation_of_a_game_that_teaches_people_not_to_fall_for_phish https://www.researchgate.net/publication/221166422_
[4]. Gartner Inc. (2014). Gartner study finds significant increase in e-mail phishing attacks. [www.gartner.com/5 about/press
[5]. Venkata Prasad Reddy, V. Radha, Manik Jindal 2011," Client Side protection from Phishing attack" International Journal of Advanced Engineering Sciences and Technologies Vol No. 3, Issue No. 1, 039 – 045.
[6]. Aanchal Jain and Prof. Vineet Richariya 2011," Implementing a Web Browser with Phishing Detection Techniques" World of Computer Science and Information Technology Journal, Vol. 1, No. 7, 289-291.
[7]. V. Suganya," A review on phishing attacks and various phishing techniques", International Journal of Computer Applications (0975 – 8887) Volume 139 – No.1, April 2016
[8]. Nilkesh Surana, Prabhjot Singh, Umesh Warade, Neha Sabe 2015," Detection and Prevention of Phishing Attacks in Web" International Journal of Scientific Engineering and Technology Research, ISSN 2319-8885 Vol.04, Issue.08, April-2015, Pages:1595-1598
[9]. Computer Economics (2007), Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets and other malicious code, reference available at: http://www.computereconomics.com/page.cfm?name=Malware%20Report

Trupti V. Kantale. " Review on Phishing." IOSR Journal of Computer Engineering (IOSR-JCE) 21.3 (2019): 40-44.