Phishing Attacks and its Detection

Bhumika P Patel[1], Ghanshyam I Prajapati[2]

[1]*Department of Information Technology, Shri S'ad Vidya Mandal Institute of Technology, Bharuch, India*
[2]*Department of Computer and Information Technology, Shri S'ad Vidya Mandal Institute of Technology, Bharuch, India*

***Abstract*— Phishing is a procedure of fraud in which the attacker tries to get data within cybercriminals. It is a procedure of texting in which an attacker pretends to be someone else in order to obtain sensitive information. The attacker creates a situation where people believe that they are dealing with an extreme change. Phishing is considered as a planning attack rather than targeted one. This paper surveys the literature on the detection of phishing attacks. Various types of phishing attacks such as Deceptive Phishing, E-mail spoofing, Malware Based Phishing, Tab nabbing, Session Hijacking, Search Engine Phishing, DNS-based Phishing, Phone Phishing, etc. are described. The mechanics of phishing, various techniques used in attack of phishing, characteristics of phishing attack, how to prevent phishing attack and also provide the advantages and disadvantage of the phishing attack. With increase in number of trusting users of internet the chances of getting enclosed in phishing attacks is quite a possible thing.**

***Index Terms* - Phishing, Phishing Attack, Phishing emails, URL-Based.**

I. INTRODUCTION

Phishing is a false attempt, usually made through email, to steal personal information of any customers. It point to the act that the attacker demand users to visit a faked web site by sending them faked e-mails or instant messages, and without a sound get victim's personal information such as user name, password, national security ID, etc [1]. Phishing, The main goal of the phishers is always to attract nation into giving up important information. Phishing is also identified as ''Brand Spoofing". The statement has its origin from two words - Password harvesting or-fishing for passwords [15]. One of the most important aims of phishing is to dishonestly carry out fraudulent economic transactions on behalf of users using a fake email that contains a URL pointing to a fake web site concealed as an online bank or a government entity. Phishing is a rising difficulty for internet users [5]. Phishers aim the users who have no knowledge on internet safety and make them believe that the emails come from trusted organizations [6]. The most effective explanation to phishing attack is training and education users not to blindly go behind the fake links to websites where they have to give personal information [2]. Phishing is considered as a planning attack rather than targeted one [3]. Phishing websites looks like to valid website therefore people cannot make difference among them [9]. With increase in number of trusting users of internet the chances of getting enclosed in phishing attacks is quite a possible thing [14]. Phishing is a major problem on the Web [16]. Section-II describes types of Phishing Attack. Section-III describes Characteristics and Prevention of Phishing Attack. Section IV describes various techniques for Phishing Attack. Section V describes a survey on phishing attack and its detection and Section VI describes the conclusion of the paper.

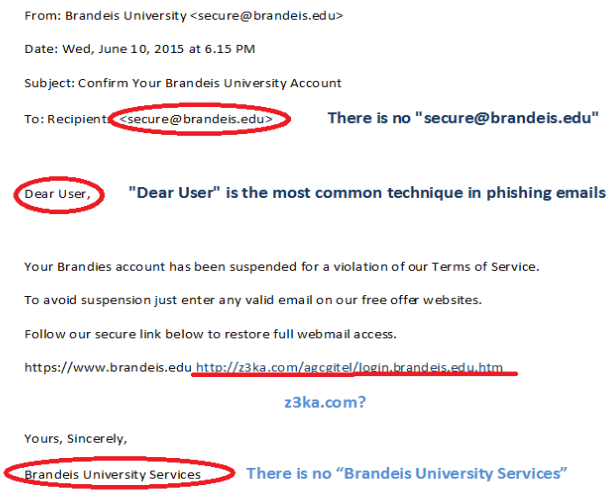

Fig.1. Example of Fake E-mail Phishing Page

II. TYPES OF PHISHING ATTACKS

A. Deceptive Phishing: A phisher sends large email with a message. Users are requested to click on a link. The most common type of phishing scam, deceptive phishing refers to any attack through which fraudsters assuming a valid groups and attempt to steal people's personal information or login credentials [8].

B. Data Theft Phishing: Information can contain activation keys to software, passwords, sensitive and personal email and any other data that is stored on the user's computer are lift by the phishers, known as the data theft phishing [8].

C. Session Hijacking: It is a type of phishing attack where customer's activities are monitored clearly until they log into a target account like the bank account, transferring funds and establish their credentials.

D. Phone Phishing: This type of phishing creates problems when the people are asked to dial a phone number, claiming to be from a valid bank, to ask the details for their bank accounts. One of the newer types of Phone Phishing is done by the involvement of Caller ID [7].

E. Spear Phishing: : It is an type of e-mail spoofing fraud attempt that targets a specific association, seeking legitimate access to confidential data also type of phishing attack that

focuses on a single user or department within an organization [7].

F. Key Loggers: Key loggers are the exacting varieties of malware that path keyboard input and throw applicable information to the hacker via the internet [8].

G. Clone Phishing: A type of phishing attack whereby a valid, and previously delivered, email containing an addition or link had its satisfaction and recipient address taken and used to create an almost identical or cloned email is known as clone phishing [7].

III. CHARACTERISTIC AND PREVENTION OF PHISHING ATTACK

A. CHARACTERISTIC OF PHISHING ATTACK

i. Absence of recipient's name: The groups who send emails which do not contain links but depend on the victims reply for moving out the attack generally find the email record from websites or use web write off [3]. This specific type of email is always remark to be coming without the name of the recipient mentioned somewhere in the email [12].

ii. The Mention of Money: The easiest way a phisher can get someone to reply to emails seems to be promising a fine sum of money [3]. Once the peoples starts to think that he/she is going to get the word total of money and that the people making the promise are real, then the phisher ask them for sensitive information or ask to transfer a sum of money to an account and then they disappear[3].

iii. Reply Inducing Sentence: The phisher fake as the entity they mention in the email, and then do everything they can to tempt the victim into confidence so that people may reply and provide with sensitive details. If anyone does reply, the actual mind of phisher gets attractive [3].

iv. Poor Spelling and Grammar: Most phishing fraud arises from areas of the world where English is not usually spoken. Another sure sign of a phishing fraud is strange formatting, including misplaced punctuation and capital letters. Many frauds also tend to quality meaninglessly hyperbolic language and a cause of exclamation marks [6].

B. PREVENTION OF PHISHING ATTACK

i. Give education to the users to understand how phishing attacks work and to be aware when phishing like e-mails are received [11].
ii. Identify and block the phishing Web sites in time.
iii. Improve the security of the web sites [11].
iv. Block the phishing e-mails by various frauds clarify [11].
v. Never email private or financial information, even if people are close with the recipient [11].
vi. Do not tick on links, download files or open attachments in emails from unknown senders [11].
vii. Keep computers or laptop with a firewall, spam filters, anti-virus and anti-spyware software [11].
viii. Verify online accounts and bank statements regularly to ensure that no unauthorized transaction has been made [11].

IV. VARIOUS TECHNIQUES USED FOR PHISHING ATTACK

i. Website Phishing Detection: The best thing to avoid phishing frauds is always go in a straight line to the web site which has to visit rather than clicking a link [6]. Google Chrome keeps track of common phishing sites and can alert when users visit ones. The causes such as click the link, urgent action required, general greeting, spelling and grammar mistake are some awareness of website phishing [13].

ii. URL Based Phishing Attack: Fake URLs are phishers device to perform phishing attacks. Defeat the actual URL from the user is one of making fake URLs techniques. If the URL contains an IP address instead of containing website's name, it is the indication of a doubtful URL [17]. Unknown Noun Presence is another technique where domain names are not created by using some random letters [5]. If URL is having @ symbol then it is recognize as phishing URL [9].

iii. Redirect Page: When user clicks on the link, user may be redirected to the phishing website. If the number of redirect page is less than 2 then it is legal site. If it is greater than 2 and less than 4 then it is considered as doubtful phishing website [9].

iv. Email Based Phishing Detection: A most wanted phishing method among cybercriminals is to spoof the display name of an email. Including attachments that contain viruses and malware is a common phishing approach. Fraudsters not only prank in the display name, but also spoof in the header from email address [6].

v. Web-based Delivery: Web based delivery is one of the most difficult phishing techniques. Also known as "man-in-the-middle," the hacker is placed in between the original website and phishing system. The phisher mark outs information during a transaction among the fraud website and the user. As the user continues to pass information, it is gathered by the phishers, without the user knowing about it [5].

V. LITERATURE SURVEY

TABLE I: A SURVEY ON PHISHING ATTACK

Publication/ Year	Title	Overview	Positive Aspects	Disadvantage
IEEE/2013	Profiling Phishing Email Based on Clustering Approach [1]	A method for profiling email- born phishing (ProEP) attack is used. Clustering method such as Kmeans and Two step clustering algorithm is used. ProEP stage is based on clustering algorithm predictions and classification of emails.	Kmeans and clustering algorithm consist of continuous and categorical data. The classification accuracy is improved by ProEP algorithm for selecting number of cluster.	Ham and phishing emails can be varied because of continuous and categorical data.
IEEE/2014	A Method to Measure the Efficiency of Phishing Emails Detection Features [2]	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 selected feature is to determine by calculating Effectiveness Metric (EM).	URLs feature in detecting phishing emails is more reliable than Keyword feature.	Here in proposed method can be used to evaluate other types and categories of phishing email detection features.
ACM/2014	Identification and Detection of Phishing Emails using Natural Language Processing Techniques [3]	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 can be implemented in such a way that it can detect both the text part of the email and also the attachment.
IEEE/2014	An Efficient Approach for Phishing Detection using Single Layer Neural Network [4]	The system is shaped to detect phishing sites using single layer neural network and six features such as Primary Domain, Sub Domain, Path Domain, Page Rank, Alexa Rank, and Alex Reputation. The weights of heuristic are created by single layer neural network.	Neural Network provide a solution for classification or pattern recognition problems.	The system could be enhanced by using larger datasets and more features. Detection ratio can also be improved.
IEEE/2014	Performance Study of Classification Techniques for Phishing URL Detection [5]	The data are classified using the algorithms such as Naïve Bayes, Multi-layer Perceptron, Tree-based classifier, Random Forest, K- Nearest Neighbor. Features such as lexical, URL based, Network based and Domain based features are being classified.	Tree-based classifiers are the best giving performance for the phishing URL classification.	The improvement of accuracy of the system is needed for performance.
IEEE/2015	A Computer Vision Technique to Detect Phishing Attacks [6]	Using Computer vision technique SURF (Speed Up Robust Features) detector to extract valid and suspicious web page. SURF detection technique reduces computation cost. Suspicious site undertakes SURF detection.	For comparison of suspicious website with image database, SURF detector is used. Zero- day phishing attack is used as solution.	SURF methods fails when phishing websites is replaced with advertisements or style of image is changed. Accuracy can be improved by calculating not only of image but also of CSS style.
IEEE/2015	A Review on Recent Phishing Attacks in Internet [7]	The techniques used for phishing attack are Heuristics and Blacklisted. Types of phishing attacks are Spear, Clone, Phone phishing.	Recent phishing attacks are Bioazih Attack, Dyre malware email, Heart bleed phishing attack and Tab napping attack.	Phishing is used for unauthorized access of data and concept of hackers.
IEEE/2015	Detection of Phishing Attack using Visual Cryptography in Ad hoc Network [8]	The proposed Anti-phishing approach is based Visual Cryptography. A user generates two shares of image using (2,2) visual cryptography. visual cryptography scheme does not suffer from false positive.	Pixel expansion is an important parameter for Visual Cryptography Schemes. Using two share of image one share is stored at client side and other share is uploaded to web site at time of user registration.	Future work can be done on centralized approach.

IEEE/2015	Phishing Websites Detection through Supervised Learning Networks [9]	Two algorithm of Supervised Learning such as Adaline and Back propagation network along with support vector machine is used to detection rate and classification.	Support Vector Machine is used for applications such as pattern recognition and regression analysis. Adaline network with SVM gives better results.	Back propagation algorithm along with SVM in java can be used in future for getting the cure on phishing attack on sites.
IEEE/2016	Use of HOG Descriptors in Phishing Detection [10]	Histogram of Oriented Gradients (HOG) descriptor method is used for characterizing and capturing object appearance or shape. Two modules such as "Wrapper" and "Hogger" are used for HOG descriptors.	HOG method is aimed to detect zero-day attacks for web pages in phishing attacks.	By using HOG method, it is not necessary that we can get accurate results using the different descriptors.

VI. CONCULSION

Phishing emails and web site attacks have provided a nameless opportunity for scammer to reach collection of potential victims, with little cost sum, in the hope of victims supplying their personal and financially sensitive information. Most web browsers support plugging to protect users from phishing websites. It point to the act that the attacker demand users to visit a faked web site by sending them faked e-mails or instant messages, and without a sound get victim's personal information such as user name, password, national security ID, etc. Phishing attack is one of the key threats of network which stole the user's top secret or confidential information. User education or preparation is an effort to increase the procedural understanding level of users to reduce their affected to phishing attacks. The disadvantage of phishing attack in sending an email to a user incorrectly claiming to be a fraud company to cheat the user into providing personal information on a bogus website. The details will then be used for identity phishing theft. However, numerical study release how phishing is still a big fraud to today's world as the online era reports. Thus paper describes the various Types of Phishing Attack, Characteristic and Prevention of Phishing Attack, Various Techniques used for Phishing Attack and Survey on the Phishing Attack and its Detection.

REFERENCES

[1]. IsredzaRahmi, A Hamid and Jemal H. Abawajy, "Profiling Phishing Email Based on Clustering Approach," IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.

[2]. Melad Mohamed, Al-Daeef and Nurlida Basir and Madihah Mohd Saudi, "A Method to Measure the Efficiency of Phishing Emails Detection Features", IEEE, 2014.

[3]. Shivam Aggarwal, Vishal Kumar and S D Sudarsan, "Identification and Detection of Phishing Emails Using Natural Language Processing Techniques", ACM, 2014.

[4]. 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, IEEE, 2014.

[5]. Pradeepthi. K V and Kannan. A, "Performance Study of Classification Techniques for Phishing URL Detection", Sixth International Conference on Advanced Computing (ICoAC), IEEE, 2014.

[6]. Routhu Srinivasa Rao and Syed Taqi Ali, "A Computer Vision Technique to Detect Phishing Attacks", Fifth International Conference on Communication Systems and Network Technologies, IEEE, 2015.

[7]. Lakhita, Surendra Yadav, Brahmdutt Bohra and Pooja, "A Review on Recent Phishing Attacks in Internet", IEEE, 2015.

[8]. Vimal Kumar and Rakesh Kumar, "Detection of Phishing Attack Using Visual Cryptography in Ad hoc Network", peer-reviewed, IEEE ICCSP, 2015.

[9]. Priyanka Singh, Yogendra P.S. Maravi and Sanjeev Sharma, "Phishing Websites Detection through Supervised Learning Networks", IEEE, 2015.

[10]. Ahmet Selman Bozkir and Ebru Akcapinar Sezer, "Use of HOG Descriptor in Phishing Detection", International Symposium on Digital Forensics and security, IEEE, 2016.

[11]. Mahmoud Khonji, Youssef Iraqi, Andrew Jones, "Phishing Detection: A Literature Survey", IEEE Communications Surveys & Tutorials, VOL-15, IEEE-2013.

[12]. Xing Fang, Nicholas Koceja, Justin Zhan, Gerry Dozier, Dasgupta Dipankar, "An Artificial Immune System for Phishing Detection", IEEE World Congress on Computational Intelligence, Brisbane, Australia, June, 2012.

[13]. Samuel Marchal, Kalle Saari, Nidhi Singh, N. Asokan, "Know Your Phish: Novel Techniques for Detecting Phishing Sites and their Targets", IEEE 36th International Conference on Distributed Computing Systems, 2016.

[14]. Zheng Dong, Apu Kapadia, Jim Blyth, L. Jean Camp, Beyond the Lock Icon: Real-time Detection of Phishing Websites Using Public Key Certificates, IEEE, 2015.

[15]. Weibo Chu, Bin B. Zhu, Feng Xue, Xiaohong Guan, Zhongmin Cai, "Protect Sensitive Sites from Phishing Attacks Using Features Extractable from Inaccessible Phishing URLs", IEEE Communication and Information Systems Security Symposium (IEEE ICC), 2013.

[16]. Yanhui Du, Fu Xue, "Research of the Anti-Phishing Technology Based on E-mail Extraction and Analysis", International Conference on Information Science and Cloud Computing Companion, IEEE, 2014.

[17]. K. Nirmal, B. Janet, R. Kumar, "Phishing - The threat that still exists", IEEE, 2015.