**Globus** An International Journal of Management & IT
A Refereed Research Journal
Vol 10 / No 2 / Jan-Jun 2019 ISSN: 0975-721X

# A REVIEW STUDY ON PHISHING ATTACK TECHNIQUES FOR PROTECTING THE ATTACKS

*Km Sakshi Gupta
**Dr. K.P. Jayant

## Abstract

Phishing is a type of network attack or a form of criminal activity attempt to obtain the sensitive information such as username, password etc. online. It creates duplicate web pages to fool users. Email Phishing contains the messages like ask the users to enter the personal information so that it is easy for hackers to access the information. This concept is based on the Link Guard Algorithm also known as End Host Anti-Phishing Attack. This algorithm is used for finding the phishing emails sent by the phisher to grasp the information of the end user. Link Guard Algorithm is totally based on the characteristics of the phishing hyperlinks. Each and every user is implemented with this algorithm. After that the user can recognizes the phishing emails and avoid responding to such mails. This paper presents an overview about phishing attacks and various techniques to protect the information.

**Keywords**: Phishing, Anti-phishing, Information security and Privacy.

## Introduction

The term “phishing” derived from the word “fishing” for catching the passwords and documentations in the web. The expression “ph” comes from “phone phreaking”, which was very general technique that bothered telephone systems during 1970s. In 1996, for the first time, the phrase “phishing” was used by a group of hackers, who shawl/access **America Online (AOL)** accounts by trapping unaware AOL users into disclosing their password [9]. A complete phishing attack involves the roles of phisher. The main objective of phishing attack is to clearly steal the sensitive information such as-

- User account number
- User passwords and user name
- Credit card information
- Internet banking information

Some of the phishing emails also contain the malicious or unwanted software that can track your activities and slow down the computer. The one of the effective solutions to prevent a phishing attack is to integrate the security features with the web browser which can raise the alerts whenever a phishing site is accessed by an internet user. The most effective explanation to the phishing attack is training and the education users not to blindly go behind the fake links to the websites where they have to give personal information[1].

With increase in number of trusting users of the Internet the chances of getting enclosed in phishing attacks is quite a possible thing[2].

This paper is organized in Six sections. Section II of this paper gives the phishing life cycle. Section III gives the Classification of phishing attack. Section IV gives some approaches to prevent phishing attacks. Section V gives the phishing techniques to protect the phishing attack and section VI concludes the paper.

## Phishing Life Cycle

A duplicate webpage generally contains a login form, and when a end user opens the duplicate webpage and enter the personal information, this information is accessed by the attacker, then the attackers use this information for some personal and financial gain.

**M.Tech Scholar, Department of CSE, IIMT University, Meerut, India*
*** Associate Professor, Department of CSE, IIMT University, Meerut, India*

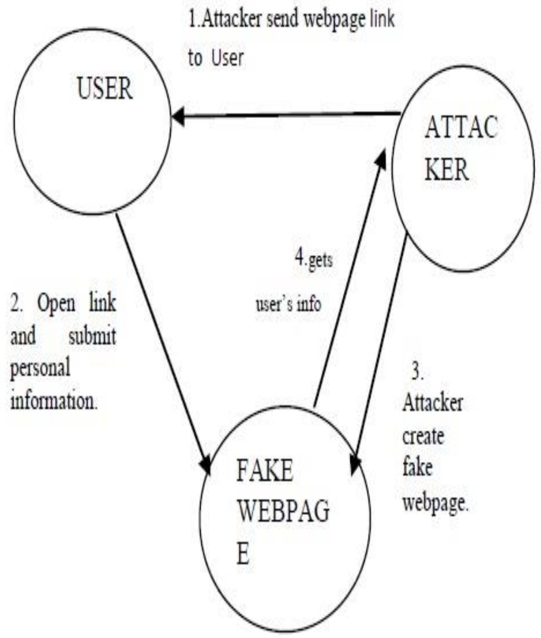
The following steps are involved in a phishing attack [3]:

**Step 1:** The attacker copies the content from the website of a well-known company or a bank and creates a phishing website. The attacker keeps a visual similarity of the phishing website similar to the corresponding legal website to attract more users.

**Step 2:** The attacker writes an email and includes the link of the phishing website and sends it to the target users and trying to convince the targeted user to visit their websites.

**Step 3:** The receivers opens the email and visits the phishing website. The phishing website asks the user to enter personal information, for example, if the attacker copying the phishing website of a well-known bank, then the users of bank are very likely to give up their credentials to the fake website.

**Step 4:** The attacker gets the personal information of the user via the fake website and uses this information of the user for financial or some other benefits



1.Attacker send webpage link to User
USER
ATTAC KER
4.gets user's info
2. Open link and submit personal information.
3. Attacker create fake webpage.
FAKE WEBPAG E

**Figure 1- Lifecycle of the Phishing Attack**

## Classification of Phishing Attack

Phishing attacks can be classified as follows-

### 1. Deceptive Phishing

The meaning of the "Deceptive" is misleading. In this attack the phisher will send you an email pretending from a recognized source (banks, online shopping websites) which request you to make payment, to change your existing password, Re-enter your login user name and password, verify your account information etc.[3][6]

### 2. Malware based Phishing Attack

Malware Software is used by the phisher to attack on the user, after installation of these infected software the phisher succeed in performing unauthorized actions, such as accessing the user's private data, transferring funds etc.

### 3. Man –in-Middle Phishing

This attack is hard to detect than many other forms of phishing .In this attack the phisher places himself in between the user and the system or legal websites [3]. When the user is not active on the system the phisher notes the enter information and later can use or sell the information of the user.

### 4. Search engine phishing

In this attack, the phisher creates a duplicate websites with attractive or pleasing offers and have them indexed legitimately with the search engine. The users finds the sites in normal course of searching for product and services and are fooled into giving up their information.

### 5. Key Loggers and Screen Loggers

In this attack, the phisher use different types of malwares that track keyboard input and send the relevant information to the attacker by the help of Internet [8].

### 6. Clone Phishing

Clone phishing requires the attacker tries to clone a websites that the user usually visits. The clone websites usually asks for login credentials, copying the original websites. This will allow the attackers to save these credentials in a text file, database record on his own server, then the attacker redirect his user to the original websites as a authenticated user[11].

## Approaches To Prevent Phishing Attack

There are various approaches to prevent phishing attack-

### A. Detection of Phishing Websites in Time

If we can detect and block the phishing websites then we can prevent phishing attack. It is easy to determine whether the site is phishing or not, but is difficult to find those phishing sites out in time.

### B. Enhance the Security of the Websites

The business websites like bank websites take new methods to guarantee the security of the user's personal information.

One of the method is to enhance the Security is to use Hardware devices. For Example, the Barclays bank provides hand-held card reader to the user[7]. Before shopping in the net, user need to insert their credit card into the card reader and enter their PIN code , then the card reader will produce a onetime security password, the user can perform the transactions only after the right password is entered. However, there are so many techniques [4][5] which needs the additional hardware to realize the authentication between the users and the websites.

### C. By Using Various Spam Filters, Block Phishing Email

Phishers generally use e-mails as "feed" to allure potential users. SMTP (Simple Mail Transfer Protocol) is the protocol to deliver e-mails in the Internet and also lacks necessary authentication mechanisms. Information related to sender, such as the name and email address of the sender, route of the message, etc., can be counterfeited in SMTP. Thus, the attackers can send out large amounts of spoofed e-mails which are seemed from legal organizations. The phishers hide their identities when sending the spoofed e-mails, therefore, if anti-spam systems can determine whether an e-mail is sent by the announced sender (Am I Whom I Say I Am?), the phishing attacks will be decreased dramatically.

### D. Install Online Anti-Phishing Software in User's Computers

It is possible for the users to visit the spoofed Web sites.

Users can install anti-phishing tools in their computers.

The Anti-phishing tools in use today can be divided into two categories: [6]

- Blacklist/white list based.
- Rule-based.

**Category I:** When a user visits a Web site, the anti-phishing tool searches the address of that site in a blacklist stored in the database. If the visited site is on the list, the anti-phishing tool then warns the users. Tools in this category include Scam Blocker from the EarthLink Company, Phish Guard, and Net craft, etc. Though the developers of these tools all announced that they can update the blacklist in time, they cannot prevent the attacks from the newly emerged (unknown) phishing sites.

**Category II:** This category of tools uses certain rules in their software, and checks the security of a Web site according to these rules[10]. Examples of this type of tools include Spoof Guard developed by Stanford, Trust Watch of the Geo Trust, etc. Spoof Guard checks the domain name, URL (includes the port number) of Web site, it also checks whether the browser is directed to the current URL via the links in the contents of e-mails. If it finds that the domain name of the visited Web site is similar to a well-known domain name, or if they are not using the standard port, Spoof Guard will warn the users. In Trust Watch, the security of a Web site is determined by whether it has been reviewed by an independent trusted third party organization. Both Spoof Guard and Trust Watch provide a toolbar in the browsers to notify their users whether the Web site is verified and trusted. It is easy to observe that all the above defense methods are useful and complementary to each other, but none of them are perfect at the current stage.

### Algorithm to Protect Phishing Attack

There are various Algorithms to protect the phishing attack such as-

1. Attribute based Anti-phishing Algorithm.
2. Genetic Algorithm based Anti Phishing Algorithm.
3. An Identify based Anti phishing Algorithm.
4. Content based Anti- phishing Algorithm.
5. End-Host based Anti- phishing Algorithm. but in this paper we discuss only the LinkGuard Algorithm.

By Analysing the difference between the visual link and the actual link, the LinkGuard algorithm works. It calculates the similarities of URI with a known trusted sites.

It contains some important systems:

- **Communication:** Input process can be collected and send all the information to analyzer.
- **Database:** It stores the user input URL"S, blacklist and whitelist.
- **Analyzer:** All the data is provided by Communication and Database, and sends the results to the Alerter and then to Logger modules. It also send the warning message to the Alerter
- **Alerter:** When receiving warning messages from Analyzer, it shows the related information to alert the users and send back the reactions of the user back to the Analyzer.
- **Logger:** All the related information is store.

We believe that Link Guard is not only useful for detecting phishing attacks, but also can shield users from malicious or unsolicited links in Web pages and Instant messages.

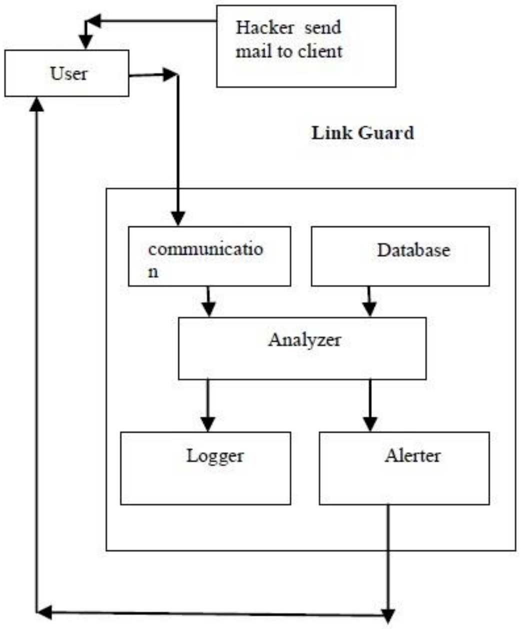


**Figure 2. Component of Link Guard Algorithm**

## Conclusions

In this paper, we proposed a review on phishing attack and techniques for protecting those attacks. Furthermore, our approach is Educate users to understand how phishing attacks work and be alert when phishing-alike e-mails are received; Use legal methods to punish phishing attackers and also use technical methods to stop phishing attackers.

The Security and Privacy are two main and most important concepts to be considered whenever there is a phishing attack. Phishing attacks are successful because of many inexperienced internet users. This paper provides a broad survey of various phishing techniques enables the attackers to steal the sensitive information. Our future work is to compare various types of anti-phishing technique and choose best one for further research.

## Acknowledgment

This research paper is supported by IIMT University, Meerut (UP). I would like to thank my guide Dr. KP Jayant (Head of Department) who provided insights and expertise that greatly guided the research. I would also like to show my gratitude to all the authors of below reference for sharing their pearls of wisdom through their papers.

## References

1. Melad Mohamed, Al- Daeef and Nurlida Basir and Madihah Mohd Saudi,” A Method to measure the Efficiency of Phishing Emails Detection Features”, IEEE , 2014.
2. 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.
3. V. Suganya, “A Review on phishing Attacks and Various Anti phishing Techniques”, IJCA, Volume 139-No.1, April 2014.
4. Anti-phishing working group http://www.antiphishing.org/.
5. Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, and John C.Mitchell. Client-side defense against web-based identity theft. In Proc.NDSS 2004, 2004.
6. U.Naresh, U.Vidya Sagar, and C.V.Madhusudan Reddy, ”Intelligent Phishing Website Detection and Prevention System by using Link Guard Algorithm” IOSR-JCE, Volume 14, Sep-Oct 2013.
7. Arpan Chandel, Prashant Kumar, and Dinesh Kumar Yadav “Phishing Attack and its Countermeasures,” IEEE Electron Device Lett., vol. 7, pp. 569–571, Nov. 1999.
8. Bhumika P Patel, Ghanshyam I Prajapati, “Phishing Attack and its Detection”, IJRSI, Volume 4, June-2017.
9. Himani Thakur, Dr. Surpreet Kaur,”A Survey Paper on Phishing Detection”, IJARCS, Volume7-No.4, July- August 2016.
10. Kalpana, Naveen Kumar, Parul Saharavat, “Email Security System using for phishing attack-Using LinkGuard Algorithm”, IJSRCSEIT , Volume 3, Issue 6, 2018.
11. Dr. M. Najreen Banu, S. Munawara Banu, “Comprehensive Study of Phishing Attack”, IJCSIT, Volume- 4, 2013.