IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

Challenge Related to Phishing Attacks and Associated Countermeasures Present on the Internet

Pradeep Kumar Shah, Assistant Professor,
Department of CCSIT, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India
Email Id- pradeep.rdndj@gmail.com

ABSTRACT: ***Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware. Phishing attacks have become increasingly sophisticated and often transparently mirror the site being targeted, allowing the attacker to observe everything while the victim is navigating the site, and transverse any additional security boundaries with the victim. Now-a-days most of the people were familiar with the internet and its applications. Along with the internet usage, the attacks also have increased. Phishing is the one the most possible attacks in internet and through this the Phisher will get the confidential information like passwords. So that the users will not be able to access their own information. In this paper, an overview of phishing its techniques and anti-phishing methods are discussed.***

KEYWORDS: ***phisher, phishing, blacklist, anti-phishing***

1. INTRODUCTION

Phishing is the act of attempting to attain user's information by masquerading as a legal entity in an electronic communication. The act of sending an e-mail to a user arguing to be an established legitimate enterprise in an effort to scam the user's private information that will be used for theft[1]. phishing is by far the most common attack performed by cyber-criminals, with the FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime. The first recorded use of the term "phishing" was in the cracking toolkit AOHell created by Koceilah Rekouche in 1995, however it is possible that the term was used before this in a print edition of the hacker magazine 2600[2]. The word is a leetspeak variant of fishing, probably influenced by phreaking, and alludes to the use of increasingly sophisticated lures to "fish" for users' sensitive information.

The e-mail directs the user to visit a web site where they are asked to update the personal data like bank account numbers, credit card and passwords and that the legal organization already has. The effects of phishing are theft of identity and users' confidential details. This results in financial losses for users and prevents them from accessing their own accounts, loss of productivity and extreme resource consumption on corporate networks.

1.1. Phishing Methodology

Most phishing attacks are of a spoofed email that appears to have been sent from a bank or any legitimate enterprise and whose aim is to deceive its client. This message contains links to Web

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

pages that will be similar to the company's website, where victims are incited to enter their personal details. These types of crimes are not just made through email but phishing can also be launched through smashing (SMS) or vishing (Voice over IP). With smashing the users receive a text message asking them to access a link which leads to the deceitful website. In the case of vishing, users receive a call from someone claiming to represent their bank and asking them to verify a series of data.

1.2. Types of Phishing Attacks

There are several types of phishing attacks[4]. They are listed below:

a. Deceptive Phishing or Instant Messaging:

Phishing is referred to account theft using instant messaging but the most common method today is a deceptive email message. The messages may be about the verification of account information, system failure that asks the users to re-enter their information, undesirable account changes, new free services requiring quick action and many other scams are sent to a large group of recipients with the hope that they will respond by clicking a link to or signing onto a false site where their confidential information can be collected.

b. Malware-Based Phishing

It refers to scams runs malicious software on users' PCs. Malware can be launched as an email attachment or as a downloadable file from a web site who are not able to keep their software applications up to date always.

c. Keyloggers and Screenloggers

These are varieties of malware that tracks keyboard input and sends the relevant information to the hacker through the Internet. They can be embedded into user's browser known as helper objects that runs automatically when the browser is started.

d. Session Hijacking

it refers to an attack where the users' activities are monitored until they sign out from the target account or transaction. The malicious software can undertake unauthorized actions such as transferring funds without the user's knowledge.

e. Web Trojans or Trojan

Hosts pop up invisibly when user is attempting to log in. They collect the user's details and transmit them to the phisher.

f. Hosts File

Poisoning is that when a user types a URL it must translated into an IP address before it is transmitted over the Internet. By poisoning the hackers have a fake address transmitted which takes the user to a fake "look alike" website where their information can be stolen.

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

g. System Reconfiguration

Attacks modifies the settings on a user's PC for malicious purposes. For example: a bank website URL may be changed from "ticketbook.com" to "tikketbook.com".

h. Data Theft.

Unsecured PCs often contains sensitive information stored on secured servers. Such servers can be accessed using PCs and can be easily compromised. Data theft is widely used in business scrutiny. Thieves profit from selling the stolen confidential details such as communication details, legal opinions, design documents, employee related records, etc., who may want to cause economic damage.

i. DNS-Based Phishing

This Pharming is one dangerous form of phishing is pharming. This involves modifying the domain name resolution system (DNS) to redirect the users to false web pages. The process of converting an address into a numeric IP address is known as domain name resolution and is performed by DNS servers. There are types of malware to modify the system for resolving domain names on the local computer located in a file called HOSTS which stores IP addresses that can be accessed by the user. When a user enters the name of a trustworthy website, the computer first checks the HOSTS file to see if there is an IP address associated with this name. If it doesn't exit, it will check with the DNS server of the service provider.

Pharming authenticates the HOSTS file to redirect the domain name of trusted organizations so that hackers can collect the confidential information entered in these websites by users.

j. Content-Injection

Phishing hackers can replace part of the content of a trustworthy site with false content to mislead or misdirect the user into giving up their confidential information to the hacker.

k. Man-in-the-Middle Phishing

Web Based Delivery in this attack hackers position themselves between the user and the trustworthy website or system. They record the information that is being entered without affecting the transactions[5]. Then the collected information can be sold when the user is not active on the system. This type is harder to detect.

l. Search Engine Phishing

This occurs when phishers create websites with attractive offers and indexes legitimately with search engines. Users find the sites in the regular course of searching for products or services and are fooled into giving up their information.

m. System Reconfiguration Phishers

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

It may send a message where the user is asked to reconfigure the settings of the computer. The message may be from a web address which resembles a reliable source.

1.3. Detection Techniques

a. Content Based Filtering:

This technique detects phishing attack on email which was implemented by J. W. Yoon, et al with challenge-response scheme. The combinations of these techniques are needed to improve the traditional spam filtering detection technique on mobile device since the content-based filtering alone is less efficient. Content-Based filtering can be divided into rule based and statistic based.

b. Blacklist:

Blacklist is a method that needs human for the verification. This technique has very low False Positive (FP) and is widely applied in the industries as anti-phishing in toolbar. If user enters the blacklist website, a warning will be appeared. However, this method is not suitable to detect the new phishing attacks. This technique has fewer capabilities to protect users. It has also been implemented in fraud telephony and SMS filtering[6].

c. Whitelist:

Whitelisting method is different from blacklist-based. This technique needs to maintain all website in the cyber world. The limitation is that it is impossible to cover the entire website it has also been implemented to detect SMS phishing.

1.4. Preventing Phishing Scams

Phishing cannot be avoided but it can be prevented[6]. Here are some methods which can be used by the users to prevent from phishing attacks.

a. Check the email Carefully:

A phishing email claims to be from a trustworthy company and when the link is clicked, the website may look exactly like the real website. The email may ask to fill in the information but the email may not contain the users' name. Most phishing emails will start with "Dear Customer" so the user should know that a legitimate company will not send such spam emails. The email may contain the names of imaginary personnel who work in the legitimate company. For example, the user may have received an email from Mr. Green who is the Head of Human Resources at some big company telling that the user has won $4 million. To verify that mail the user can contact the real company directly not by calling the number which is provided in the email.

b. Never Enter Financial or Personal Information:

Most of the phishing emails will direct the user to the pages where entries for financial or personal information are required. An Internet user should never give confidential entries through the links that are provided in the emails.

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

c. Identify a Fake Phone Call:

Phone phishing is the method in which a phone call is made to steal the user's personal information. The user may be asked to provide financial details for the refund of money. The phone call can be from a number which appears legitimate but the area code in the phone call can be altered using VOIP technology.

d. Protection through Software:

Anti-spyware and firewall settings should be used to prevent phishing attacks and users should update their programs regularly. Antivirus software scans each and every file which comes through the Internet to the computer.

e. Never Send Personal Information through emails:

users should never send an email with sensitive information to anyone. It is a good habit to check the address of the website. And a secure website always starts with "https".

f. Check Bank Details Regularly:

To prevent bank phishing and credit card phishing scams it is a must that the users should personally check the statements regularly.

g. Never Download Files from Unreliable Sources:

If the user gets a message stating a certain website may contain malicious files do not open the website. Web browsers offer settings which gives an alert message when the user tries to access a malicious site. Never download files from suspicious emails or websites.

1.5. Anti-Phishing Techniques

Anti-phishing technique can be considered said as an approach to counter the threats put forth by phishers[7]. This accounts to a number of techniques followed which is categorized as follows.

a. List Based Approach:

This approach is the most straightforward solution for anti-phishing. A white list contains URL's of all known legitimate sites. Many anti-phishing techniques rely on the combination of white list and blacklist[8]. The representative blacklist/white list based systems include Phish Tank Site Checker, Google Safe Browsing, Fire Phish and Calling ID Link Advisor. These anti-phishing solutions are usually deployed as toolbars or extensions of web browsers which reminds the users whether they are browsing a safe website. Blacklist suffers from a window of weakness between the time a phishing site is launched and the site's addition to the blacklist.

b. Heuristics Based Approach:

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

This technique rates the phishing possibility for a given webpage using the reputation scores either obtained from the anti- phishing community or computed from the given webpage. But the reliability of the reputation scoring is a great challenge.

c. Content Based Approach:

This method is used to measure the similarity between two given web pages by calculating the similarity between the content elements contained in the web pages. Algorithms are used to evaluate the visual similarity to detect the phishing web pages which has higher similarities to phishing targets. It also combines TFIDF retrieval algorithm to determine the probability that a given webpage is a phishing webpage. Words with highest TF-IDF weight on a given webpage can be used to classify the webpage.

1.6. Reporting Phishing

The best way of action is to report the fear to an organization that will investigate further. There are numerous such places on the Internet where the reporting can be done. One is the U.S. government-operated website which provides information where to send a copy of the email or the URL so that they may be examined by experts. It also includes the details on phishing scams and how to recognize them and to protect our information. Another website to report cyberspace scams is the Anti-Phishing Working Group (APWG): This antiphishing.org features an option where the user can copy and paste the contents of the doubtful email. There are also additional links of information to learn about phishing scams[9].

2. CONCLUSION

Most phishing messages are delivered by email, and are not personalized or targeted to a specific individual or company–this is termed "bulk" phishing. The content of a bulk phishing message varies widely depending on the goal of the attacker–common targets for impersonation include banks and financial services, email and cloud productivity providers, and streaming services. Attackers may use the credentials obtained to directly steal money from a victim, although compromised accounts are often used instead as a jumping-off point to perform other attacks, such as the theft of proprietary information, the installation of malware, or the spear phishing of other people within the target's organization. Compromised streaming service accounts are usually sold directly to consumers on dark net markets. Currently phishing attacks are so common because it can attack globally and capture and store the users' secret information. This information is used by the hackers which are indirectly involved in the phishing process. The main objective of this paper is to provide the general guidance about phishing and its techniques.

REFERENCES:

[1] A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara, "Security usability principles for vulnerability analysis and risk assessment," in *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 2007, pp. 269–278. doi: 10.1109/ACSAC.2007.14.

[2] P. S. D. Gunter Ollmann, "The Phishing Guide Understanding & Preventing Phishing Attacks," *NISR*, pp. 1–42, 2004.

Research paper UGC CARE Listed (Group -I) Journal Volume 11, Iss 11, Nov 2022

[3] F. Y. Rashid, "Types of phishing attacks and how to identify them," *www.csoonline.com*, 2017.

[4] L. J. Singh, "A Survey on Phishing and Anti-Phishing Techniques," *Int. J. Comput. Sci. Trends Technol.*, vol. 6, no. 2, pp. 62–68, 2018.

[5] X. M. Choo, K. L. Chiew, D. H. A. Ibrahim, N. Musa, S. N. Sze, and W. K. Tiong, "Feature-based phishing detection technique," *J. Theor. Appl. Inf. Technol.*, vol. 91, no. 1, pp. 101–106, 2016.

[6] Gaurav, M. Mishra, and A. Jain, "Anti-Phishing Techniques: A Review," *Int. J. Eng. Res. Appl.*, vol. 2, no. 2, pp. 350–355, 2012.

[7] Y. G. Kim and S. Cha, "Website risk assessment system for anti-phishing," in *Communications in Computer and Information Science*, 2011, vol. 185 CCIS, no. PART 2, pp. 131–138. doi: 10.1007/978-3-642-22309-9_16.

[8] P. Cain and D. Jevans, "Extensions to the IODEF-Document Class for Reporting Phishing," *RFC*, vol. 5901, pp. 1–51, 2010.