e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

TECHNIQUES TO PREVENT THE USERS FROM PHISHING ATTACKS

R.Sathya[1,] J.Vijayaraj[2], Dr.K.Purushotaman[3]
[1,2,3]*Dept. Of IT ,SKP Engineering College,Tiruvannamalai*

Abstract-Phishing is web-based attack causes the most vital problem for the internet users, which uses fraudulent emails and websites mainly aimed to obtain the private information of the users such as bank details, credit card details, social security details, online sijaet paper templatehopping account details, passwords of various important accounts etc., The phishing website differs from the legitimate website by some distinct characteristics and the w3c standards also will be violated in the phishing web sites.

Keywords: Phishing, Antiphishing techniques, Intrusion, Security

I. INTRODUCTION

Phishing is an attempt done by the phishers, mainly used to gain the user's sensitive information through email or websites or URL redirection. Phishing attacks are continuously growing and one of the technique is to use login screen in a pop window. While the user browses the website that seems to be the legitimate website, the mail that contains an hyperlink to open a new window will be sent by the phishers. The pop up window, which looks like an organizational website will ask the users to validate or update the account.

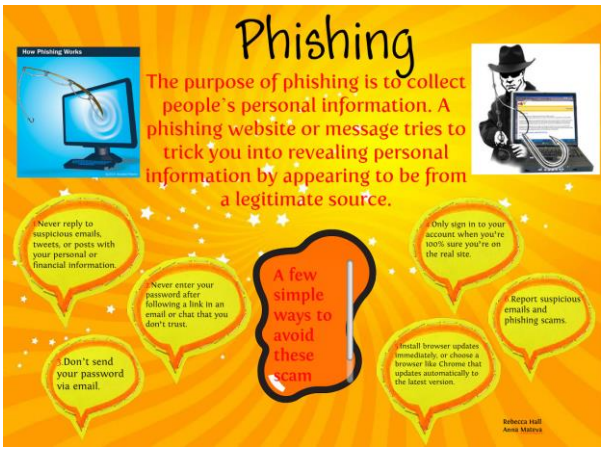
The people who trust the information which they obtain through email will provide their private details like passwords of online account, banking details, instead of knowing that the mails are from the phishers, which enables the users to lose their private content to the attackers.

Phishing is a type of deception designed to steal user's valuable data,con artists may send millions of fradulent email messages that appear come from your trusted websites.

Phreaking+phishing=Phishing.

Phreaking-Making phone calls for free back in 70's.
Fishing-Use bait to lure the target.

As scam artists become more sophisticated,so do their phishing email messages and popup windws.The impact of phishing are both domestical and international that are concern with their commercial and financial sectors.



II. CHARACTERISTICS OF PHISHING ATTACKS

Business email phishing is kind of spearphishing, in which phishers are professional, globally distributed, and team-worked. This type of phishing is characterized as targeted, well-planned, multi-staged, and difficult to protect against. They are financial transaction oriented, twin phishing along supply chain, and can the most potent negative impact to victims.

A. Request URL:

Images,CSS,External Scripts in webpages are loaded from other URLs.Large percent of RURLs are in its own domain.

B. URL of Anchor:

The portion of anchor URL in a legitimate webpage, points to the same domain as the page itself.webpage name should be meaningful to the users and should be in lowercase letters.The anchor URL should be made easy to understand for users.

C. Server Form Handler:

Generally,most of the e-business based webportals uses username and password for authenticating the e-business users.Thus the e-business based webpages contains server form handler.

D. Logos:

The phishing websites uses logos found on the legitimate website to appear like the real website.So phishers can load it from their legitimate website domain to their phishing websites.

III. BASIC IDEAS TO PREVENT FROM PHISHING ATTACKS

Softwares that detects intrusion and provides malware security must be installed and updated regularly. The firewall should be maintained properly.

The most sensitive/private financial and personal information should not be mailed to unauthorized web sites.

The links on suspicious links should not be clicked. The latest version of browser which contains integrated antiphishing techniques and security patches should be installed.The awareness on phising should be made by the user himself by studying the latest news regarding phising

Email attachments from trusted authorities must be opened. If the email comes from the new websites, it has to be checked properly.

Prevent posting sensitive information from suspicious website.The advantages of this idea is

to prevent all possible attacks and lets the user to knows the website is malicious.

Display warning prompts for all unsafe actions which notifies user of specific dangers on a website.

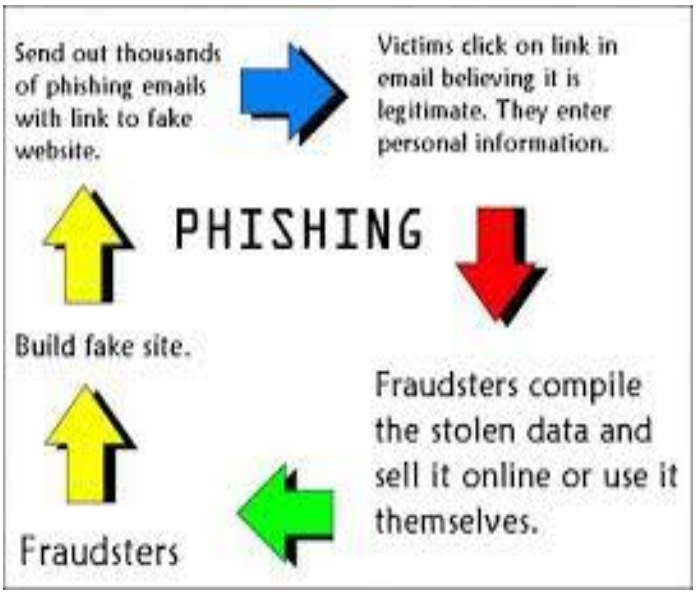


Fig 1 :Phishing Process

IV. TECHNIQUES USED IN ANTIPHISHING

Phishers use some methods to receive the sensitive information from the user. Here, some of the suggested phishing detection techniques are given.

Antiphishing techniques are mainly useful for unexperienced and technically unsophisticated users to check the trustworthiness of the websites from the user's side. The antiphishing techniques are broadly classifed into two categories namely, Server-based and client-based.

Service providers implement the server-based phishing techniques to provide security to the user those who access services from the server.

Server-based antiphishing techniques include Brand Monitoring, Behaviour Detection, Security Event Monitoring. Brand Monitoring: To identify the clonerd web pages, this technique is used. Behavioural Detection:To identify the anamolies in the user, this technique is used.

Clone phishing is a type of attack whereby a legitimate, and previously delivered, email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email (Rajkumar). The attachment or Link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender. Nowadays the popular web email system including hotmail, yahoo, and gmail allows users to specify a Reply-To address.

This function makes it possible that the users send a message from one account, but receive replies at another email address.

The phisher configured the email setting put his email address in the Reply-To part. As a result, when a user send email, the message will be replied to the phisher instead of the user-self. Then, the phisher cloned the reply and send to the user.

Controlling communications and Manipulation information. Popular email systems not only allow users to specify the Reply-To a different address, they also they also lets users send messages with another of email addresses listed as the sender. This feature helps users manage multiple accounts from one interface.

In Gmail, to use one of the alternate sender addresses, click the FROMlink when you compose a new message. After clicking FROM, you'll see a drop-down menu next to your address, where you can select the email address you'd like to send from. That means, the email can be configured and send from any address as long as that address is validated.

In this way,the receiver will see that the message comes from the real business partner's email address.

Security Event Monitoring:Security event analysis to identify anamolies, this technique is used. Client-based techniques are implemented on user side through browsers and email clients. Client-based antiphishing techniques include email analysis, blacklist, information flow, similatity of layout.

Email Analysis: It uses filters and content-analysis concepts. The most commonly used filter to find the spam and phishing mails Bayesian filter.

Nowadays, the antiphishing applications are integrated with the browsers. Another approach to detect the phishing website is to use Phishing Website Detection System using Fuzzy Techniques.

The phishing attacks can be detected using on of the following informations include images, domain, suspicious URL, https, email, iframe, popup window, script etc., The suspicious URLs contain the IP address, instead of using the real domain name. Sometimes, the phishers use the @ symbols to make the ambiguous host names. The phishing can also be detected using List-based and Heuristic-based.

Email phishers are not just targeting consumers. They are going after high profile targets to steal proprietary information such as intellectual properties, business secrets, even national security (Hong 2012). Phishing is a hazard to E-business (Richard and Hintau). The damage caused by phishing goes beyond monetary property. Delicate bonds of trust that organization build with their constituents are eroded. People loss faith in the reliability of e-business, companies loss their customer base, reputation, andcredibility, which in turn causes significant economic loss, resources and time. However, the numbers of email phishing incidents reported for corporate and business is only very small portion of the actual number simply because victimized companies do not want to release any negative news to public so that their image can be damaged and the confidence of the investors may be undermined.

List-Based approaches are further classified into blacklist and whitelist. Blacklists contain the URL, that are considered to be phishing websites. The blacklist URLs are mainly stored in the local client or hosted at server. The URL, that is mentioned by the user will be checked with the blacklists. If the URL matches with the stored lists, then, the necessary actions will be taken or else the page will be considered as the legitimate one. The whitelist contains the list of trusted websites.

V. PHISHING ATTACK STAGES

There are several stages in phishing attack:

The email addresses of the intended users will be obtained by the attackers from various sources. The attacker generates the bogus emails which looks like legimtimate and request the recepient of the mails to perform some action and capture the true sources from the victim.

Depending on the received email, the user opens the malicious attachment and fills the form or update the details in the redirected URL, which the phisher sends and lose their private content.The attackers capture the victim's sensitive information and exploits the user details in future.

VI. CONCLUSION

Thus, Phishing is an online attack that mainly aims to obtain the users sensitive information such as online banking account passwords and credit card information. The phishing atack mainly happens due to the inexperienced web users. The major solution to avoid this problem is to train the users not to click on the links, while providing the sensitive information like passwords and online account details. The increased use of antiphishing techniques enables the users to protect from phishing websites.

REFERENCES

[1]M. Dunlop, S. Groat, and D. Shelly," GoldPhish: *Using Images for Content-Based Phishing Analysis"*, Fifth International Conference on Internet Monitoring and Protection, 2010.
[2]M. Aburrous, M.A. Hossain, F. Thabatah and K. Dahal, *"Intelligent phishing website detection system using fuzzy techniques*", 3rd International Conference on Information and Communication Technologies: From Theory to Applications (ICTTA)
[3]Cranor, L., S. Egelman, J. Hong, and Y. Zhang. Phinding Phish: *Evaluating Anti-Phishing Tools*. In Proceedings of The 14th Annual Network and Distributed System Security Symposium (NDSS '07). February 28- March 2, 2007.
[4]Y. Pan and X. Ding, "*Anomaly Based Web Phishing Page Detection"*, Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06), Computer Society, 2006.
[5]N. Chou, R. Ledesma, Y. Teraguchi, D. Boneh, and J. C. Mitchell, "*Client–side defense against web–based identity theft"*, In Proceedings of 11th Annual Network and Distributed System Security
Symposium, 2004.
[6]Blake Ross, Collin Jackson, Nick Miyake, Dan Boneh and John C. Mitchell. A Browser Plug-In Solution to the *Unique Password Problem*, 2005.
[7]3Sharp, 3Sharp Study finds Internet Explorer 7 Edges Out Netcraft As Most Accurate for *AntiPhishing Protection*. 2006.
[8]Anti-Phishing Working Group, *Phishing Activity Trends Report*. 2006 apwg_report_june_06.pdf.
[9]DOWNS, J. S., HOLBROOK, M. B.,AND CRANOR,DOWNS, J. S., HOLBROOK, M. B.,ANDCRANOR, L. F. *Decision strategies andsuscepti-bility to phishing*. InSOUPS '06: Proceedings of the second symposium on Usable privacy and security(New York, NY, USA, 2006), ACM Press, pp. 79–90.
[10]ABU-NIMEH, S., NAPPA, D., WANG, X.,AND NAIR, S. A comparison of machine learning techniques for phishing detection. In eCrime '07: Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit (New York, NY, USA, 2007), ACM,pp. 60–69.
[11]ANANDPARA, V., DINGMAN,A., JAKOBSSON, M., LIU, D.,AND ROINESTAD,H. Phishing IQ tests measure fear, not ability. Usable Security (USEC'07) (2007).
[12]CALMAN, C. Bigger phish to fry: California's antiphishing statuteand its potential imposition of secondary liability on internet service provider s.Richmond Journal of Law and Technology XIII, 1 (2006).

