International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Detection of Phishing Attack

*Grandhi Vanitha**

GMR Institute of Technology Razam, Kinneravada, Thogiri, Saravakota, Srikakulam, Andhra Pradesh, PIN-532427, India.

ABSTRACT

Now a days there's lots of information security issues. Hackers are now abundantly expert in using their knowledge for hack into someone else's system and grab the knowledge. Phishing may be a sort of social engineering attack often accustomed steal user data, including login credentials and Mastercard numbers. Phishing is an act of making a web site almost like a legitimate website with a motive of stealing user's lead. Phishing fraud can be the foremost popular cybercrime. Phishing is one in all the risks that originated a pair of years back but still prevailing. This paper discusses various phishing attacks, a number of the newest phishing evasion techniques utilized by attackers and anti-phishing approaches. This review raises awareness of these phishing strategies and helps the user to practice phishing prevention. Phishing are targeting payment industry and cloud services the most. We can protect them by using some protocols.

Keywords: Phishing, Phishing types, Evasion techniques, Anti-phishing approaches.

1. Introduction

Phishing could be a reasonably social engineering attack that sometimes targets to assemble confidential data like identity records and monetary account details from online users by protecting them as a truthful entity in digital communications. Phishing is disbursed by creating a special website by either copying or modifying the legitimate page a touch bit in order that the net user is unable to differentiate between the fake and legit sites. People do most of the transactions online nowadays. Paying the bills or transferring money, everything is completed through websites. Once phishers obtain these stolen credentials, they'll use these details to make a fake account of the victim, which contains a serious impact on their credentials or may deny users access to their accounts. According to the Anti-Phishing Working Group (APWG Q2 2019) report , the total number of phishing sites detected is 182,465 in 2019. In this, the most targeted industry sector is webmail and Software-as-a-Service (SaaS). 84% of phishing attacks target financial services, shipping, cloud storage services and payment services (Phishlab Phishing report 2019). The payment sector is the most attractive target for phishing. Attackers regularly use a series of software tools referred to as phishing kits to line up phishing websites . Through phishing kits, people having little technical knowledge can deploy phishing. A phishing kit contains an internet site element and a knowledge processing component. The web site element consists of images, codes, and different content material to make a phishing website. Phishing kits mainly target banking, financial institutions, retail companies and trade goods like Microsoft, PayPal, Amazon, Apple,etc. The system architecture described during this paper deals with a hybrid approach of phishing detection where a random selection of techniques is used which may detect legitimate websites accurately without moving to other phases.Random features are selected supported the principle just like the keyed Intrusion detection system There are various techniques and specific technologies that are developed to combat phishing. Phishing cannot be ceased using a single technology.There are various approaches to detect phishing attacks such as a list-based approach, machine learning, visual similarity, Heuristic-based approach

2. Literature Review

- They given a good idea of phishing attack, the kinds of phishing attack through which the attacks are performed.Focuses on developing a detection and prevention techniques.Phishing is explained step-by-step.Here the research focuses on developing a detection and prevention techniques so in future the client can take necessary actions to forestall phishing attacks.In future, focus is to check various tools for phishing attack prevention.[1]
- In this paper they explained on phishing attacks to make awareness and a number of other countermeasures to beat. Phishing types, phishing mechanism, Anti-phishing Techniques.This study provides an in-sight to phishing, the mechanism of the attack, various forms it can occur in and therefore the possible solutions to beat them.[2]
- A comparative study of the in-use anti-phishing tools was accomplished and their limitations were acknowledged.Also, a step wise procedure of designing an anti- phishing model is discussed to construct an efficient framework which adds to our contribution.They also mentioned the utmost must spread awareness regarding the phishing attacks and use of anti-phishing tools while browsing the net.They compared all the models by using 5 styles of approaches supported the quantity of features used, accuracy and size of dataset.This study provides an in-sight to phishing, the mechanism of the attack, various forms it can occur in and also the possible solutions to beat them.[3]

- This study conducted a profiling analysis of the Kimsuky phishing mail attack group to determine its phishing mail attack types and the purpose of their attacks. In addition, it was shown that these attacking organizations are continuously advancing phishing e-mail attack techniques to collect important information such as that related to defense, security, and diplomacy.It was difficult for ordinary e-mail users to respond only with their interest because it used advanced attack techniques such as exploiting large attachment spoofing vulnerabilities.[4]
- This paper hopes to shed light on the recent phishing attacks using QR code and the countermeasures proposed to tackle these attacks.It is also found that, current countermeasures are insufficient and face challenges like barcode-in-barcode attacks, high overhead solutions and limited data space in the code. In comparison to the amount of work done in web and email phishing , QR code phishing detection still inadequate.This is because there are a lot of existing QR scanners without the anti-phishing feature and imposing secure QR with security feature like digital signature to every QR scanner is impractical.[5]

3. Methodologies

ANTI PHISHING: Anti-phishing refers to efforts to dam phishing attacks. Phishing could be a reasonably cybercrime where attackers pose as known or trusted entities and call individuals through email, text or telephone and ask them to share sensitive information.

ANTI PHISHING SOLUTIONS:

Phishing prevention :In order to stop phishing attack, the phishing prevention is introduced by providing an additional layer of security when the user login into the web site. the additional layer of security is via two-factor authentication, which could be a process to substantiate the user identity before the user is granted to access its login account within the website. An example of two-factor authentication via SMS. When the user has entered username and password to login into the web site, a verification code are going to be sent to the user's registered movable number via SMS. Then, the user must enter the verification code before the user can login into the web site. The verification code only are often employed in a brief time before it's expired.

Phishing detection :There are two categories for phishing detection which are user awareness and software detection. The user awareness is for to coach users so they're ready to identify phishing attempts targeted at them. The users have to use caution when visiting the online page, for instance by checking at the net page URL first. Although the user has being careful, there's an opportunity that the user may be deceived by the phisher to go to the phishing online page . Therefore, software detection is introduced to use for distinguish whether the web site is legitimate or phishing. The software detection is differentiating into two methods which are traditional and automatic method.

For **traditional method** of software detection, the blacklist is employed to manage the list of phishing websites, which are manually entered and updated within the system. The advantage of blacklist is it's high accuracy. the disadvantage of blacklist is it lacking to spot the phishing website that has short lifetime. Furthermore, if nobody report about the phishing website, then the blacklist cannot detect the phishing website.

For **automatic method** of software detection, it are often classified into two categories which are public phishing detection toolbars and academic phishing detection / classification schemes. The automated method of software detection use combinations of heuristic and blacklist based approach. The heuristic based approach examines contents of the web site. There are three varieties of heuristic based approach which are surface level content, textual content and visual content. The heuristic of surface level content means by examine at the URL of website. The heuristic of textual content means by examine the terms or words within the website. Lastly, the heuristic of visual content means by examine the layout of website.The aim of the general public phishing detection toolbars is to detect and blocking the phishing website. The user can see these toolbars as an internet browser extension. A security warning is flaunted to alert the web user when the user visits the phishing website. There are two styles of security warning which are passive warning and active warning. For passive warning, it doesn't block the content of the web site and just show the warning to notify the user about the phishing attack. While for active warning, it block the content of the web site, thus make the user unable to look at the website.

The purpose of **the academic phishing detection / classification** schemes is to identify and classify whether the website is legitimate or phishing. It utilizes Artificial Intelligence (AI) method which uses supervised learning classification algorithms to do binary classification of website whether it is legitimate or phishing.

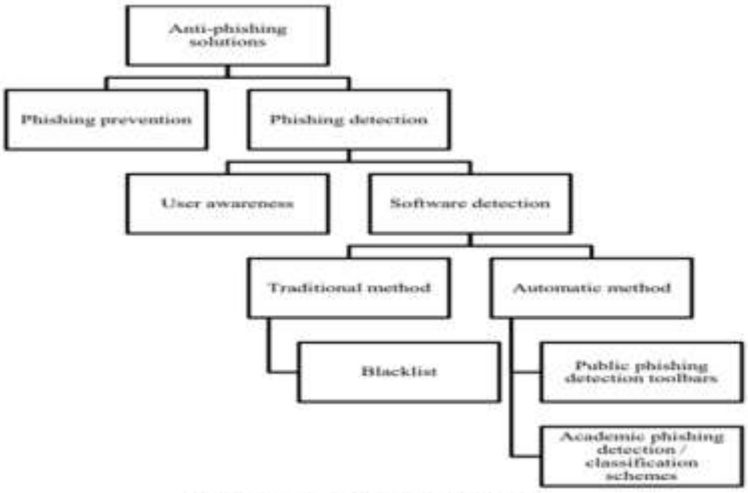

Figure 2. Types of anti-phishing solutions.

4. RESULT

PAPER	AUTHOR	METHOD	RESULT
[1]	Shabnam Sharma	Study of phishing	In this paper, the kinds of phishing attack which the attacks are performed, Focuses on developing a detection and prevention techniques.Phishing is explained step-by-step.Here the research focuses on developing a detection and prevention techniques so in future the client can take necessary actions to forestall phishing attacks.
[2]	Akarshit Shankar	A review on Phishing attack	Phishing is a technique to gather sensitive information about the target using malicious links and emails. It is one of the most dangerous cyber-attacks that occurs in organizations, personal devices, etc. It is often difficult to distinguish between genuine emails and phishing emails.
[3]	Srushti Patil	A Methodical Overview on Phishing Detection along with an Anti-Phishing Framework	we reviewed various anti-phishing approaches. All methods are discussed to give a clear idea of existing techniques, their limitations and possible improvements. Next we analyzed the in-use anti-phishing tools available for free. We found that these tools are inefficient to detect all types of phishing sites, specially the newly registered ones. We also mentioned the utmost need to spread awareness regarding the phishing attacks and use of anti-phishing tools while browsing the web.
[4]	JAEIL LEE1 , YONGJOON LEE,	Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups	An investigation of the attack techniques of the Kimsuky group since 2018 showed that the phishing pages used in the attack were not only sophisticated enough to be difficult for security experts to distinguish, but also used various disguises such as customer centers and e-mails. It pretends to be a defense and government agency using typical social engineering attack techniques. In addition, from a technical perspective, as analyzed in this paper, it was difficult for ordinary e-mail users to respond only with their interest because it used advanced attack techniques such as exploiting large attachment spoofing vulnerabilities..
[5]	Kelvin S. C. Yong	A survey of the QR code phishing: the current attacks and countermeasures	This PaperThis paper hopes to shed light on the recent phishing attacks using QR code and the countermeasures proposed to tackle these attacks.It is also found that, current countermeasures are insufficient and face challenges like

			barcode-in-barcode attacks, high overhead solutions and limited data space in the code. In comparison to the amount of work done in web and email phishing , QR code phishing detection still inadequate.

5. Discussions

In [1] analysed focuses on developing a detection and prevention techniques. In [2] provides an in-sight to phishing, the mechanism of the attack, various forms it can occur in and therefore the possible solutions to beat them.. In [3] They compared all the models by using 5 styles of approaches supported the quantity of features used, accuracy and size of dataset.In [4] , it was shown that these attacking organizations are continuously advancing phishing e-mail attack techniques to collect important information such as that related to defense, security, and diplomacy.In [5] they discussed how to shed light on the recent phishing attacks using QR code and the countermeasures proposed to tackle these attacks.

6. CONCLUSION

Phishing is one of the wide pitfalls which can not be avoided fluently. Setting up multiple authentications for dispatch networks. Any phishing attack can only succeed by clicking a link on a targeted victim. Thus, the stylish system to avoid phishing attacks is to produce mindfulness for the druggies about the types of phishing attacks within the network. Elect the stylish security software tools or operations similar asanti-phishing cybersurfer extension to avoid data security vulnerabilities of any kind. Streamlininganti-phishing tools is also another approach to help phishing to a great extent. System armature described then helps to reduce the false positive rate by assaying the content of the website. This system is effective to descry licit websites fluently. Licit website is filtered out in each phase without further moving to other phases References

7. REFRENCES

1. Shabnam Sharma,” Study of phishing” International Journal of Computer Applications (0975 – 8887) Volume 182 – No. 33, December 2018.
2. Akarshit Shankar,”A review on Phishing attack” International Journal of Applied Engineering Research(2019) .
3. Srushti Patil, “A Methodical Overview on Phishing Detection along with an Anti-Phishing Framework” International Conference on Advanced Computing & Communication Systems (ICACCS**)** 2019**.**
4. JAEIL LEE1 , YONGJOON LEE,” Classification of Attack Types and Analysis of Attack Methods for Profiling Phishing Mail Attack Groups” IEEE March 30, 2021.
5. Kelvin S. C. Yong “A survey of the QR code phishing: the current attacks and countermeasures “,International Conference on Smart Computing & Communications (ICSCC)2019.
6. .K. L. Chiew, K. S. C. Yong, and C. L. Tan, ‘‘A survey of phishing attacks: Their types, vectors and technical approaches,’’ Expert Syst. Appl., vol. 106, pp. 1–20, Sep. 2018.
7. M. Adil, M. A. Almaiah, A. O. Alsayed, and O. Almomani, ‘‘An anonymous channel categorization scheme of edge nodes to detect jamming attacks in wireless sensor networks,’’ Sensors, vol. 20, no. 8, p. 2311, Apr. 2020.
8. A. K. A. Hwaitat, M. Amin, O. Almomani, M. Al-Zahrani, R. M. Al-Sayed, R. M. Asaifi, K. K. Adhim, A. Althunibat, and A. Alsaaidah, ‘‘Improved security particle swarm optimization (PSO) algorithm to detect radio jamming attacks in mobile networks,’’ Quintana, vol. 11, no. 4, pp. 614–624, 2020.
9. 9.M. A. Almaiah, Z. Dawahdeh, O. Almomani, A. Alsaaidah, A. Al-Khasawneh, and S. Khawatreh, ‘‘A new hybrid text encryption approach over mobile ad hoc network,’’ Int. J. Electr. Comput. Eng., vol. 10, no. 6, pp. 6461–6471, 2020.
10. I. Qabajeh, F. Thabtah, and F. Chiclana, ‘‘A recent review of conventional vs. automated cybersecurity anti-phishing techniques,’’ Comput. Sci. Rev., vol. 29, pp. 44–55, Aug. 2018.
11. Yi-Shin Chen, Huei-Sin Liu, Yi-Hsuan Yu and PangChieh Wang, Detect Phishing by Checking Content Consistency, IEEE, 2017.
12. Masoumeh Zareapoor, K.R. Seeja, Text Mining for Phishing E-mail Detection, Intelligent Computing, Communication and Devices: Advances in Intelligent Systems and Computing, vol. 308, pp. 65-71, August 2016.
13. Sankhwar S., Pandey D., Khan R.A - A Novel Antiphishing Effectiveness Evaluator Model, Smart Innovation, Systems and Technologies, Springer, vol 84, Cham, 2018.
14. Dr. Radha Damodaram - Study on Phishing Attacks and Anti-Phishing tools, International Research Journal of Engineering and Technology (IRJET), vol. 3, pp. 700-705, January – 2016.
15. P. Singh, N. Jain and A. Maini, “Investigating the Effect Of Feature Selection and Dimensionality Reduction On Phishing Website

Classification Problem", 2015 1st International Conference on Next Generation Computing Technologies (NGCT), Dehradun, 2015.

16. P. Barraclough and G. Sexton, "Phishing Website Detection Fuzzy System Modelling" , 2015 Science and Information Conference (SAI), London, 2015.

17. H. Shirazi, K. Haefner and I. Ray, "Fresh-Phish:A Framework for AutoDetection of Phishing Websites" , 2017 IEEE International.

18. A. Y. Daeef, R. B. Ahmad, Y. Yacob and N. Y. Phing, "Wide Scope and Fast Websites Phishing Detection Using URLs Lexical Features" , 2016 3rd International Conference on Electronic Design (ICED), Phuket, 2016.