IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 1, May 2023

Detection Prevention and Proactive Prevention of Phishing Website

Shambhavi[1], Vivek Anil Bhujbal[2], Sourabh Kumar Singh[3]
Students, Department of Computer Engineering[1,2,3]
Sinhgad College of Engineering, Pune, Maharashtra, India

Abstract: *Phishing is frequently a routine attack on people when fake websites are used to trick individuals into divulging all of their personal information. Phishing records process tool URLs are used to steal personal data, including user names, passwords, and online banking activity. Attackers that utilize phishing techniques use websites with rectangular diplomas as a visual and semantic spoof of the real websites. Phishing strategies have advanced swiftly as the age has progressed; however, this may be avoided by using anti-phishing tools to spot phishing. A potent tool frequently utilized in the direction of phishing assaults is the machine planning to apprehend. The suggested system has also investigated the capabilities and methods of machine learning for detection.*

Keywords: Phishing, Phishing Websites, Detection, Machine Learning

I. INTRODUCTION

Phishing imitates the features and options of emails and makes them seem identical to the real thing. It resembles the real supply quite closely. The customer believes that this email is from a legitimate job or business. This forces the user to click on the links provided in the phishing email and visit the phishing website. These phishing websites were developed to imitate the design of a clever website. The phishers coerce people into listing up their private information by sending false messages, asking them to confirm their account, and other means so that they may list up the information they want to use against them. They come up with strategies that prevent users from constantly having an option but to visit their fake website. The most dangerous criminal activity in the online world is phishing. Since the majority of users log on to access the services offered by governmental and financial institutions, phishing attempts have significantly increased over the past several years. Phishers started using this as a lucrative business to make money. Phishing may be illegal, but those that engage in it do so because they find it to be incredibly trustworthy, efficient, and doesn't cost anything.The email identity of someone may actually be obtained by phishing, therefore it's extremely sincere to check for it out every day and send an email to everyone since it's publicly available everywhere. These attackers have a terrible lack of resources, making it difficult for them to quickly and effectively advance vital knowledge. The phishing scams have an impact on fraud, statistics loss, malware infections, etc. The vital information of a user, such as their password, one-time password, credit/debit card numbers, CVV, sensitive company information, medical knowledge, secret information, etc., is information in which those cybercriminals are interested. These thieves frequently also gather information that will give them direct access to social media. There are several programs, methods, and algorithms that are used to identify phishing. These comprise utilized at the academic and corporate levels. Take for instance that to cover the original domain selection the phishing assaulter would feel horribly long and complicated name of the domain. A phishing address and also the parallel internet page have numerous characteristics that may be unique from the address. This is frequently horribly obvious

II. LITERATURE SURVEY

In [1] Various machine learning algorithms logistic regression, decision tree classifier, random forest classifier, AdaBoost, gradient boosting classifier for the phishing detection.

In this paper logistic regression [2], Gaussian Naïve Bayes and Random Forest were been Proposed Proposed[3], a machine learning-based phishing detection system by using eight different algorithms to analyze the URLs, and three different datasets to com pare the results with other works.

DOI: 10.48175/IJARSCT-9710

In [4] Review was made With the huge number of phishing emails or messages received every day, companies or individuals are not able to detect all of them, where different reviews were given for detection of phishing attack, by using machine learning.

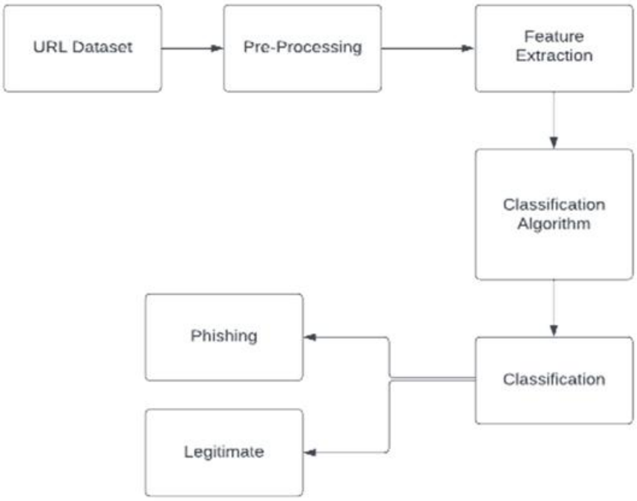
Proposed [5] three approaches for detecting phishing websites. First is by analyzing various features of URL , second is by checking legitimacy of website by knowing where the website is being hosted and who are managing it, the third approach uses visual appearance based analysis for checking genuineness of website.

In [6] Proposed System provides an approach to detecting phishing email attacks using an analysis of linguistic communication and machine learning. It is accustomed search the text's syntax to detect malicious intent. A natural language processing (NLP) technique is employed in conjunction with a predicate to decode each sentence and identifies the semantic jobs of words within the sentence. Computer supervised learning is employed to come up with the blacklist of malicious pairs.

III. OBJECTIVE OF SYSTEM

The main purpose of the proposed system is to detect the phishing websites who are trying to get access to sensitive data or by creating the fake website and trying to get access of user's personal credentials. We are using machine learning algorithm to safe guard the sensitive data and detect the phishing website who are trying to gain access on sensitive data.

IV. IMPLENTATION OF MODULE



The Figure a: Block Diagram

The proposed system provides a dataset of legal and phishing URLs, which is pre-processed to put the data in a functional format for analysis. The features revolve on several characteristics of phishing websites that have been utilized to separate them from genuine ones. The characteristics and values of each type of phishing are clearly stated. For each URL, the desired features are retrieved, and valid stages of inputs are located. Each risk associated with a phishing website is then given one of these values. The double no 0 and 1 that appears the characteristic is present or not is used to address the phishing features

V. CONCLUSION

The education and knowledge of phishing attacks is the most crucial step in protecting the user. Internet users must be familiar with any security recommendations provided by experts. Additionally, users should be taught not to heedlessly click on links that direct them to websites where they must submit sensitive data. It is crucial to verify the URL before to visiting the website. It has developed into a significant network security issue, resulting in billions of dollars in losses for both customers and e-commerce businesses. Phishing has also, and probably more importantly, contributed to the mistrust and allure of e-commerce among regular consumers. The education and knowledge of phishing attacks is the

DOI: 10.48175/IJARSCT-9710

most crucial step in protecting the user. Internet users need to be mindful of any security advice provided by professionals. Additionally, users should be taught not to heedlessly click on links that direct them to websites where they must submit sensitive data. Before entering the website in the suggested system, it is important to check the URL

ACKNOWLEDGMENT

I am using this opportunity to express my gratitude to everyone who supported me throughout the course of research project report. I am thankful for their aspiring guidance, invaluably constructive criticism and friendly advice during the project work. I am sincerely grateful to them for sharing their truthful and illuminating views on a number of issues related to the project. I am also thankful to Principal Dr. S.D. Lokhande and management of SCOE for their support and encouragement. I am highly indebted to my Head of Department Prof. M. P. Wankhade and guide Prof. P. D. Bendale for their guidance and constant supervision as well as for providing necessary information regarding the project& also for their support in completing the project. I am thankful to the review committee for their valuable suggestionand feedback. I also thank laboratory staff for their valuable support. Last but not the least, I sincerely thank to thosefromteachingandnon-teachingstafffromSCOEwhoweresomehowattachedwithmyendeavor.

REFERENCES

[1]. Lakshmanarao and P.SuryaPrabhakara Rao, “Phishing website detectionusing novel machine learning fusion approach ”, IEEE 2021

[2]. Jitendra Kumar and A. Santhanavijayan , “Phishing Website Classification andDetection Using Machine Learning ”, International Conference on ComputerCommunication and Informatics, 2020

[3]. Mehmet Korkmaz and Ozgur KoraySahingoz, “Detection of Phishing Websites by Using Machine Learning-Based URL Analysis”, IEEE 2020 Charu

[4]. Singh , “Phishing Website Detection Based on Machine Learning: A Survey”,IEEE 2020

[5]. Vaibhav Patil and Pritesh Thakkar , “Detection and Prevention of PhishingWebsites using Machine Learning Approach”, IEEE 2018

[6]. T. Peng, I. Harris, and Y. Sawa, “Detecting Phishing Attacks Using NaturalLanguage Processing and Machine Learning,” Proc. - 12th IEEE Int. Conf.Semant. Comput. ICSC 2018, vol. 2018–Janua, pp. 300–301, 2018