Literature Survey

Date 13 October 2022

Project Name Project -Web Phishing Detection

1)A Survey of Phishing Website Detection Systems:

Abstract :

Phishing URL is a widely used and common technique for cybersecurity attacks. Phishing is a cybercrime that tries to trick the targeted users into exposing their private and sensitive information to the attacker. The motive of the attacker is to gain access to personal information such as usernames, login credentials, passwords, financial account details, social networking data, and personal addresses. These private credentials are then often used for malicious activities such as identity theft, notoriety, financial gain, reputation damage, and many more illegal activities. This paper aims to provide a comprehensive and comparative study of various existing free service systems and researchbased systems used for phishing website detection. The systems in this survey range from different detection techniques and tools used by many researchers. The approach included in these researched papers ranges from Blacklist and Heuristic features to visual and content-based features. The studies presented here use advanced machine learning and deep learning algorithms to achieve better precision and higher accuracy while categorizing websites as phishing or benign. This article would provide a better understanding of the current trends and existing systems in the phishing detection domain.

REFERENCES

(Prachit Raut1, Harshal Vengurlekar2, Rishikesh Shete3 1,2,3Department of Computer Engineering, Vasantdada Patil Pratishthan's College of Engineering and Visual Arts, Mumbai, Maharashtra, India.)

2)Phishing Detection using Machine Learning based URL Analysis:

Abstract:

As we have moved most of our financial, work related and other daily activities to the internet, we are exposed to greater risks in the form of cybercrimes. URL based phishing attacks are one of the most common threats to the internet users. In this type of attack, the attacker exploits the human vulnerability rather than software flaws. It targets both individuals and organizations, induces them to click on URLs that look secure, and steal confidential information or inject malware on our system. Different machine learning algorithms are being used for the detection of phishing URLs, that is, to classify a URL as phishing or legitimate. Researchers are constantly trying to improve the performance of existing models and increase their accuracy. In this work we aim to review various machine learning methods used for this purpose, along with datasets and URL features used to train the machine learning models. The performance of different machine learning algorithms and the methods used to increase their accuracy measures are discussed and analysed. The goal is to create a survey resource for researchers to learn the current developments in the field and contribute in making phishing detection models that yield more accurate results.

REFERENCES

(Arathi Krishna V, Anusree A, Blessy Jose, Karthika Anilkumar, Ojus Thomas Lee,Department of Computer Science and Engineering, College of Engineering Kidangoor,Kottayam, India.)

3)A survey on anti-phishing in websites:

Abstract :

Phishing and fraud sites have been widespread on the internet in recent times, which's become a source of great concern and a serious cybersecurity problem, as internet fraudsters target sensitive data and personal information of users, especially the username and password. Numerous approaches have been proposed and used to prevent and reduce these phishing websites and attacks, and protect users and their privacy. In this paper, we categorized the present anti-phishing approaches into two main classes: Content-based and Non-content-based. The content-based approach is also classified into URL content analysis and webpage content analysis. This helps in finding out numerous anti-phishing techniques and algorithms to choose the best approach in future contributions.

REFERENCES:

(Robat D., Mukhter H., Shariful I., Abujarr S.2019. Learning a Deep Neural Network for Predicting Phishing Website. PhD Thesis, Brac University, Bangladesh.)

4)A Survey of Phishing Attack Technique:

Abstract:

It is a crime to practice phishing by employing technical tricks and social engineering to exploit the innocence of unaware users. This methodology usually covers up a trustworthy entity so as to influence a consumer to execute an action if asked by the imitated entity. Most of the times, phishing attacks are being noticed by the practiced users but security is a main motive for the basic users as they are not aware of such circumstances. However, some methodologies are limited to look after the phishing attacks only and the delay in detection is mandatory. In this paper

we emphasize the various techniques used for the detection of phishing attacks. We have also discovered various techniques for detection and prevention of phishing. Apart from that, we have introduced a new model for detection and prevention of phishing attacks.

REFERENCES:

(Pratik Patil , Prof. P.R. Devale M Tech Student, Information Technology, BVUCOE, Pune, India1 Professor, Information Technology, BVUCOE, Pune, India.)

5)Phishing Detection: A Literature Survey

Abstract:

This article surveys the literature on the detection of phishing attacks. Phishing attacks target vulnerabilities that exist in systems due to the human factor. Many cyber-attacks are spread via mechanisms that exploit weaknesses found in end-users, which makes users the weakest element in the security chain. The phishing problem is broad and no single silver-bullet solution exists to mitigate all the vulnerabilities effectively, thus multiple techniques are often implemented to mitigate specific attacks. This paper aims at surveying many of the recently proposed phishing mitigation techniques. A high-level overview of various categories of phishing mitigation techniques is also presented, such as: detection, offensive defense, correction, and prevention, which we belief is critical to present where the phishing detection techniques fit in the overall mitigation process.

REFERENCES:

(Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones.)

Problem Solution

To overcome the problem of phishing website whenever we are clicking on one website it must show an alert box like it is a secure website or it is not a secure website. Then another way is that we can scan the website in order to prevent our system or mobile from the phishing attack. Even though technologies are there we as the user have to be aware of the websites whether it is secure or not. We should not click any unwanted websites.

Problem Identification

There are many users who purchase products through online platform and the payment is done through e-banking. There are some fake banking websites in which they collect the more sensitive information like username, password, credit card details etc , for illegal purpose. This type of websites are called phishing website. Here web phishing is one of the security threat to web services on the internet.

CONCLUSION

This paper aims to enhance detection method to detect phishing website using machine learning technology. Also , classifiers generated by machine learning algorithms identify legitimate phishing websites.The proposed technique can detect new temporary phishing sites and reduce the damage caused by phishing attacks. The performance of the proposed technique based on machine learning is more effective that previous phishing detection technologies. In the future, it will be useful to investigate the impact of feature selection using various algorithms.