IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 6, June 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106100|

Review on Phishing Attack Detection using Recurrent Neural Network

Mr.Harish Kadam [1], Prof.Sneha Tirth [2]

P.G. Student, Department of Computer Engineering, Trinity College of Engineering and Research Pune, India [1]

Associate Professor, Department of Computer Engineering, Trinity College of Engineering and Research Pune, India [2]

ABSTRACT: Phishing is a crime that involves the stealing of personal information from users. Individuals, organisations, cloud storage, and government websites are all targets for the phishing websites. Anti-phishing technologies based on hardware are often deployed, whereas software-based ones are favoured due to cost and operational reasons. Current phishing detection technologies have no solution for challenges like zero-day phishing assaults. To overcome these challenges, a three-phase attack detection method dubbed the Phishing Attack Detector based on Web Crawler was suggested, which uses a recurrent neural network to precisely detect phishing instances. Based on the classification of phishing and non-phishing pages, it covers the input features Web traffic, web content, and Uniform Resource Locator (URL).

KEYWORDS: Attack detection, Recurrent Neural Network, Deep Learning.

I. INTRODUCTION

Fraudulent emailing, phone calls, and text messages are all examples of phishing, which is when someone pretends to be someone else from a legitimate organisation contacts a victim or target and entices them to divulge personal information, banking and credit card information, or passwords. Phishing is a severe crime that must be taken seriously. Usernames, passwords, bank information, account details, national security identifiers, and other personal information are obtained by an attacker by inviting them to visit a fake website that mimics the appearance of a legitimate website in order to gain personal information from them. A new concept that was coined from the word 'fishing,' phishing is short for "fishing for information." The information acquired is used for prospective target advertisements or, in the case of identity theft and attacks (such as money transfers from one's bank account), for identity theft and assaults. Sending e-mails, messages that have the potential to lead to data theft or the collection of personal information, is a typical method of attack. Create a profile on a social networking website. They obtain upgrades to their websites through the use of passwords, credit cards, or attackers who entice you to comply with your personal information and alter it through the use of a fictitious website. The attackers will be able to successfully capture your personal information on your server if you submit it to them. This will allow them to carry out the following step with your information and use it for their malicious purposes.

Phishing is a term that refers to a website that impersonates a well-known company's website in order to obtain personal information from clients such as usernames, passwords, or structured savings numbers. Mail spammers can be divided into two categories based on who they are attempting to contact. Some telemarketers are spammers, who send a few hundred or a large number of spontaneous e-mail messages to clients in order to gain their business. Spammers are classified as follows: they continue to send messages at random intervals but are not really excited about what they are doing. They frequently spam or push resources that are completely unrelated to the problem. Some examples include: sightings, knowing news, and remarks about meetings, among other things. In fact, while the concept of "phishing" is not new, criminals, sometimes known as "phishers," have become increasingly adept at employing it in recent years to steal personal information and perpetrate economic and social crimes. Increases in the amount of phishing attacks have been seen considerably over the last four to five years. Phishing is a frequent practise that is simple to carry out when travelling to a foreign country. Phishing is a form of social engineering that is used to trick a target into visiting a bogus website by sending them a spoof link. The victim may get an email containing the forged connection or it may be located on a public website. It is possible to construct a fraudulent website in the same way that a legal website is built. Consequently, rather of forwarding the victim's request to the appropriate web server, the request is forwarded to the attacker's website.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106100|

II. RELATED WORK

Our research [1] describes a thorough investigation of the security issues created by mobile phishing attacks, which includes web page phishing attacks among other things, and the conclusions we reached. MobiFish, a novel automated lightweight anti-phishing technique for mobile platforms, is proposed by the author. MobiFish is both automated and lightweight, and it is both revolutionary and lightweight. MobiFish is used to verify the legitimacy of web pages, programmes, and permanent accounts. MobiFish compares the actual Identity to the claimed Identity in real time, and the results are displayed on the screen. The many different types of phishing attempts on mobile devices are not well addressed by the existing systems, which are designed to counteract web-based phishing attacks on PCs.

In order[2] to deceive an online user into giving personal information, the following steps must be taken: The major objective of this review is to provide a literature survey on social engineering assaults, including phishing attacks, as well as detection measures for these types of attacks. Different types of Phishing attacks, including tab-napping, fake emails, Trojan horses, and hacking, are discussed in detail in the paper, as well as the best approaches to avoid them in the future. Every firm has security issues in order to protect personal information from this type of social engineering attack. These worries have been a source of substantial concern for users, website developers, and security specialists for a very long time.

Financial institutions of all sizes are being targeted by cyber thieves who are intelligent, well-organized, and well-funded. They are primarily targeting commercial and retail account [3] holders, but they are also attacking other financial institutions. The availability of anomaly detection technologies that can be installed quickly and immediately ensures that everyone who has an online banking account is automatically safeguarded against all types of fraud attempts with the least amount of disruption to legitimate online banking activities. According to the Federal Financial Institutions Examination Council, employing anomaly detection will minimise the total cost of fraud while enhancing consumer loyalty and trust.

[4] This research study presents an in-depth assessment of phishing, including a description of what it is, the technologies and security weaknesses that it uses, and the risks that it poses to end users. [4] A thorough explanation of phishing principles and technologies will be provided in this study, which will reveal that the threat is much more than an inconvenience or a passing fad, and will analyse how organised crime groups are utilising these scams to obtain a substantial amount of money. These same technologies are being used by an increasing number of cyber-theft perpetrators to fool us and steal our personal information, which is unpleasant for us.

For the purpose of discriminating between hazardous URLs detected on websites and non-malicious URLs, the authors of this paper[6] suggest an approach referred to as optimum RT-PFL, which they describe as follows: It is necessary to encode the data set as both lexical and host functions for the URL in order to build feature components, which can then be used to construct feature components from the URL. The function extraction method is in charge of obtaining specific properties from a function. In order to discover the optimal URL functions for a given URL, the proposed selection technique, which is based on the Rough Set Theory algorithm and the Gray Wolf Optimizer, is employed. In order to maximise the effectiveness of classification systems, the attributes of the proposed algorithm will be reduced to the absolute minimum as a result of the incredibly effective data collecting. In order to assess if a URL is authentic or malicious, the URL of the authorised URL should be inserted into the classifier before running the test. In order to classify URLs, we use a newly created fuzzy logical technique to particle filtering, which is based on fuzzy logic, to classify them. The following categories have been reinforced, in addition to the detection of an exceptionally large number of suspicious URLs from malicious pages.

This research [7] provides a comprehensive empirical investigation of the problem, based on data from 1529,433 malicious URLs generated in the last two years. An examination of the tactical behaviours of attackers in connection to URLs is carried out by the author in order to find common capabilities. Following that, the author splits the data into three relevant pools, from which it is possible to establish the compromise levels of unknown URLs. In order to boost the speed of detection, the author applies a technique known as similarity matching. Because of the attackers' regular URL altering activities, the author assumes that any new URLs that they encounter will be classified by the attackers. This strategy can be used to attack a large number of malicious URLs using a limited number of functions while only requiring a small number of functions. On the basis of precision (it has the potential to reach up to 70% accuracy), the proposed method is rational, and it only requires an examination

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106100|

of the URLs' characteristics. This model can be used during preprocessing to assess whether or not input URLs are friendly, or to predict whether or not an input URL is hazardous. It can also be used as a web filter or a risk scaler.

There are two instances of the [8] objective of this study being repeated. As a starting point for this discussion, it will be necessary to review the history of phishing attacks as well as the motivations of individuals who commit them. The many different types of phishing attacks are then grouped into taxonomies to make them easier to identify. Our services will provide taxonomies of various treatments that have been proposed in the literature, which will be made available to users as a part of our services, in order to protect them from phishing assaults that are based on the attacks that were detected in our fiscalonomics. In addition, we talked about the ramifications of phishing attacks on the Internet of Things (IoTs). Finally, we address a number of literary subjects and problems that are still relevant in the fight against phishing efforts to bring our study to a close.

A new technique for guarding against phishing assaults is proposed in this study [9] by the authors, which involves automatically updating a white list of reputable websites that the user has already visited. Despite the fact that our proposed approach has a high detection rate, it has a short access time. When a user attempts to access a page that is not included in the white list, the browser notifies them that they are about to expose any personally identifiable information to the website. Aside from that, we verify the integrity of a website by examining the hyperlinks on the page in question. It is possible to prevent phishing assaults from occuring by extracting hyperlinks from your website source code and using the recommended phishing detection approach, which is described below. We found that the proposed solution to phishing has an extremely high success rate, with a true positive rate of 86.02 percent and a false negative rate of less than 1.48 percent, indicating that it is extremely effective.

Sr No	Paper Title	Paper Concept	Advantage	Disadvantage
1	LongfeiWuetal..,"Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms," IEEE 2016, pp. 6678-6691.	Author did a detailed examination into the security vulnerabilities generated by mobile phishing assaults, which included web page phishing attacks, and then presented his results in this paper.	MobiFish, a novel automated lightweight anti-phishing technique for mobile platforms, is proposed by the author. MobiFish is both automated and lightweight, and it is both revolutionary and lightweight. MobiFish is used to verify the legitimacy of web pages, programmes, and permanent accounts. MobiFish compares the actual Identity to the claimed Identity in real time, and the results are displayed on the screen.	Web phishing assaults on PCs are already being addressed with existing methods; however, these do not adequately combat the numerous different types of phishing efforts on mobile devices that are currently available.
2	Surbhi Gupta et al., ''A Literature Survey on Social Engineering Attacks: Phishing Attack,'' in International Conference	In order to deceive an online user into giving personal information, a variety of methods are employed. The major objective of this review is	Different types of Phishing attacks, including tab-napping, fake emails, Trojan horses, and hacking, are discussed in detail in the paper, as well as the best approaches to avoid them in the	Every firm has security issues in order to protect personal information from this type of social engineering attack. These worries have been a source

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106100|

	on Computing, Communication and Automation. (ICCCA2016), 2016, pp. 537-540.	to provide a literature survey on social engineering assaults, including phishing attacks, as well as detection measures for these types of attacks.	future.	of substantial concern for users, website developers, and security specialists for a very long time.
3	Guardian Analytics. "A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectations for layered security". [Accessed: 08 Jan 2015].	Cyber criminals of all sizes are targeting commercial and retail account holders at financial institutions of all kinds, and they are using sophisticated, well-organized, and well-funded tactics to carry out their attacks.	The availability of anomaly detection technologies that can be installed quickly and immediately ensures that everyone who has an online banking account is automatically safeguarded against all types of fraud attempts with the least amount of disruption to legitimate online banking activities.	According to the Federal Financial Institutions Examination Council, employing anomaly detection will minimise the total cost of fraud while enhancing consumer loyalty and trust.
4	SANS Institute, "Phishing: An Analysis of a Growing Problem",2007. 1417 [Accessed: 23 May 2017]	An in-depth investigation of phishing is provided in this article, including an explanation of what it is, the technologies and security weaknesses that it uses, and the risks that it poses to end users and their information.	Over the course of this examination, the author describes the concepts and technology behind phishing, illustrating that the threat is much more than an irritation or a fleeting trend, and addressing how organised crime groups are employing these schemes to generate a large amount of money.	These same technologies are being used by an increasing number of cyber-theft perpetrators to fool us and steal our personal information, which is unpleasant for us.

III. OPEN ISSUES

Because of its broad use and applications, a significant amount of research has been conducted in this field. Throughout this section, it is discussed how many different strategies have been used to achieve the same aim over time in the past. Comparing this research to techniques for Phishing systems, it is clear that they are essentially distinguishable.

Customers' financial information is protected, and as a result, banks and other financial institutions put in place a number of security measures to prevent the possibility of unauthorized access to their online accounts. As the majority of online banking transactions are now carried out through a variety of applications, it is vital that this online banking activity is kept safe and secure at all times.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 6, June 2022||

| DOI:10.15680/IJIRSET.2022.1106100|

IV. CONCLUSION

Phishing is one of the most destructive sorts of web security hazards available today, and it is one of the most difficult to detect. We have built a prediction model for the identification of Phishing websites, which is based on an examination of the attributes of the assault, as a result of our research. Prediction performance of the deep recurrent neural network's deep-seated learning model beats that of other machine learning models, and its precision is the highest of any other machine learning model.

REFERENCES

[1] Surbhi Gupta et al., "A Literature Survey on Social Engineering Attacks: Phishing Attack," in International Conference on Computing, Communi- cationandAutomation(ICCCA2016),2017,pp.537-540.

[2] Jian Mao, WenqianTian, Pei Li, Tao Wei, Zhenkai Liang, "Phishing- Alarm: Robust and Efficient Phishing Detection via Page Component Similarity".Marcelo Bertalmio, Luminita Vese, Guillermo Sapiro, Stanley Osher, "Simultaneous Structure and Texture Image Inpainting", IEEE Transactions On Image Processing, vol. 12, No. 8, 2003.

[3] ZouFutai, Gang Yuxiang, Pei Bei, Pan Li, Li Linsen, "Web Phishing De- tection Based on Graph Mining", Guardian Analytics,"A Practical Guide to Anomaly Detection Implications of meeting new FFIEC minimum expectationsforlayeredsecurity".Accessed:08Jan2018.

[4] Ibrahim Waziri Jr., "Website Forgery: Understanding Phishing Attacks Nontechnical Countermeasures," in IEEE 2nd International Conference onCyberSecurityandCloudComputing,2015,IEEE.

[5] LongfeiWu et al,"Effective Defense Schemes for Phishing Attacks on MobileComputingPlatforms,"IEEE2016,pp.6678-6691.

[6] K. Rajitha and D. Vijayalakshmi, "Suspicious urls filtering using optimal rt-pfl: A novel feature selection based web url detection," in Smart Computing and Informatics, S. C. Satapathy, V. Bhateja, and S. Das, Eds.Singapore:SpringerSingapore,2018,pp.227–235.

[7] S. Kim, J. Kim, and B. B. Kang, "Malicious url protection based on attackers' habitual behavioral analysis," Computers Security, vol. 77, pp. 790 – 806,2018.

[8] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions,"TelecommunicationSystems,vol.67,no.2,pp.247–267,Feb 2018.

[9] A. K. Jain and B. B. Gupta, "A novel approach to protect against phishing attacks at client side using auto-updated white-list," EURASIP Journal on InformationSecurity,vol.2016,no.1,p.9,May2016

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details