2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT) | 979-8-3503-8681-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICITIIT61487.2024.10580446

# A Comprehensive Survey of Recent Phishing Attacks Detection Techniques

1st S. Priya
*Dept. of Information Technology*
*Manipal Institute of Technology Bengaluru*
Manipal Academy of Higher Education, Manipal, India
s.priya@manipal.edu

2ndDanat Gutema
*Dept. of CSE*
*Vel Tech Rangarajan Dr Sagunthala R & D Institute of Technology*
vtu21463@veltech.edu.in

3rdShweta Singh*
*Dept. of ECE*
*Manipal Institute of Technology Bengaluru*
Manipal Academy of Higher Education, Manipal, India
shweta.s@manipal.edu

***Abstract*—Phishing attacks lead to fraudulent acquisition of user credentials, which is turn result in potential harm to reputation and financial security of individuals and organization. The initial instances of phishing attacks emerged in mid of 1990, when a group of hackers impersonated AOL employees through instant messages and emails, aiming to steal passwords and hijack accounts. Over the past two decades, the number of internet users has consistently grown, which has consequently led to an increase in attackers employing various technologies, software, and malicious tools. The proliferation of devices such as computers and smartphones has further contributed to the rapid rise of phishing attacks. These attacks can lead to severe financial theft and pose a significant risk to the reputation of organizations. To counter this threat, numerous techniques and algorithms have been developed and implemented. This paper explores the different detection methods, providing an analysis of their strengths and limitations.**

***Index Terms*—Website Phishing, Feature Selection, Identity Theft, Online Security, and Neural Network.**

## I. Introduction

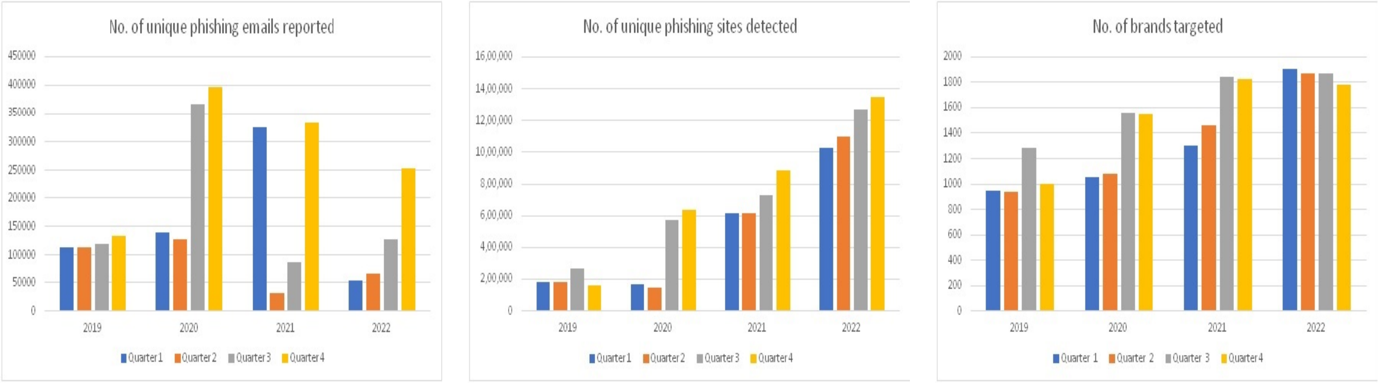
The internet is used to connect people from different parts of the world and help to facilitate the business and communication around the world. Nowadays, the tremendous growth of electronic devices such as computers and smartphones increases the usage of the internet. During 1990s, America online (AOL) emerged as one of the leading internet service provider, boasting a substantial subscriber base. The immense popularity of AOL caught the attention of hackers to form the Warez community. Despite the positive use of the internet, it becomes very vulnerable to steal the credentials of users and increasing the risk of insecurity. Day by day hackers have become more experts to break victim's account and grab information. Phishing is one type of attacks which targets users' information such as email credentials, telephone number, personal information, details of ATM cards, credit card numbers, card verification value, and bank details. It is a well-known cybersecurity attack which can be done by sending fraudulent links through the email. When the user clicks the link the user will be redirected to the phishing web pages to disclose their confidential information [1].

### *A. Phishing Attacks Reports*

The Anti-Phishing Working Group (APWG) recorded a total of 1,270,883 phishing attacks in the third quarter of 2022. Moreover, the following attacks have been reported [2]:

- Phishing attacks account for approximately 36% of all security-related attacks.
- Over 80% of business organizations report being targeted by phishing attacks, primarily focusing on their employees.
- The prevalence of financial and business email compromise (BEC) attacks, which accounted for 23.2% of reported attacks, continued to be troublesome.
- Wire transfer BEC attacks make up 59%.
- Significant increase of 1000% in advanced fee fraud scams launched via email.
- The most expensive attack compromised thousands of emails and resulted in a staggering financial loss of $1.8 billion.
- A staggering volume of fraudulent emails which around 3.4 billion is being sent daily which targets a wide audience without any specific context.
- Approximately 33 million data records have been compromised due to phishing attacks in 2022.

The detailed statistics of the number of unique phishing emails reported, the number of unique phishing websites detected, and number of brands targeted are depicted in Fig. 1. From the Fig. 1 it is evident that even though the number of attacks that happened in 2021 is less than that of 2022, it affected a large number of organizations and individuals. According to APWG, the number of attacks recorded in December 2021 was 316,747, which was the highest monthly total in APWG's reporting history. In 2020, phishing against cryptocurrency targeted wallet providers and cryptocurrency exchanges were raised up to 6.5%. Among all other emails reported by



(i) (ii) (iii)

Fig. 1. APWG Report i) Number of unique phishing emails reported, ii) Number of unique phishing websites detected, and iii) Number of brands targeted

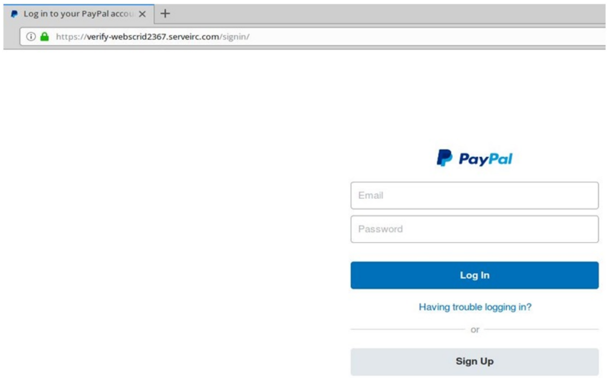
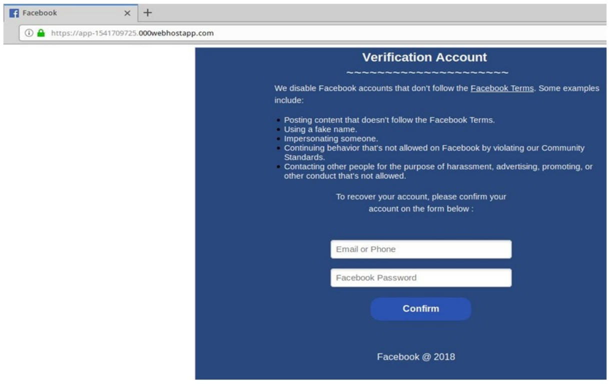

Log in to your PayPal accou
https://verify-webscrid2367.serveirc.com/signin/
PayPal
Email
Password
Log In
Having trouble logging in?
or
Sign Up

Fig. 2. A live Paypal phishing website



Verification Account

We disable Facebook accounts that don't follow the Facebook Terms. Some examples include:

- Posting content that doesn't follow the Facebook Terms.
- Using a fake name.
- Impersonating someone.
- Continuing behavior that's not allowed on Facebook by violating our Community Standards.
- Contacting other people for the purpose of harassment, advertising, promoting, or other conduct that's not allowed.

To recover your account, please confirm your account on the form below :

Fig. 3. Facebook phishing website

corporate users, a significant portion were categorized into different types of phishing attacks. Specifically, 51.8% of these reported emails were identified as credential theft phishing attacks, aimed at illicitly acquiring user credentials. Another 38.6% of the reported emails were consisted of response-based attacks, including methods such as Business Email Compromise (BEC), scams, and gift card scams, which aimed to exploit recipients into providing sensitive information or making fraudulent transactions. Additionally, 9.6% of the reported emails were associated with malware delivery, whereby malicious software is distributed to compromise the security of the recipient's system [3]. The recent attack scenarios are depicted in Fig. 2 and 3.

### B. Recommendations and Solutions

In the literature, different technologies and algorithms have been developed by the research community for detecting the phishing attacks in a efficient manner. Basically, the phishing website detection techniques can be classified into following categories: list based detection, heuristic-based detection, machine learning-based detection and deep learning based detection. These categories represent different approaches to identify and flag the phishing websites [4]. Though, the list based techniques and heuristic based detection techniques have shown the prominent results, the intelligent techniques like Machine Learning (ML) and Deep Learning (DL) have undergone rapid evolution within the field of Artificial Intelligence (AI). These techniques play a crucial role in ensuring the security and efficient management of computing operations and cybersecurity. ML and DL algorithms can analyze vast amounts of data and identify hidden patterns or anomalies that may indicate potential security threats. By continuously learning and adapting, these techniques can enhance security measures by staying ahead of emerging risks and evolving attack methods [5]. This paper presents the extensive survey about the recent and future challenges involved in detecting phishing attacks.

## II. Existing Literature

In this section, the detailed classification of phishing detection techniques have been discussed. Fig. 2 depicts the classification of different phishing detection approaches.

### A. Blacklist Techniques

Blacklist approach is one type of list-based phishing detection methods in which a list of identified phishing sites

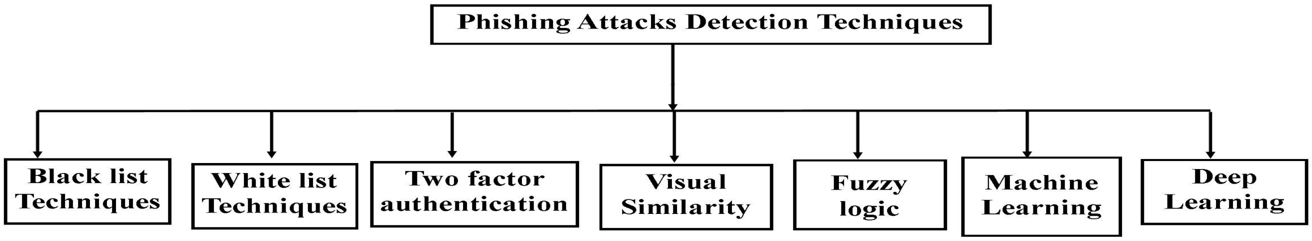


Fig. 4. Classification of Phishing Detection Techniques

is maintained, and the website being examined is cross-verified against the list. The blacklist method uses a source like spam traps or spam filters. The user posts are used to collect multiple information regarding the phishing campaign. The collected information are compiled by the third parties such as PhishTank, APWG, etc. This technique requires low resources on the host machine and effective when minimal FP rates are required. However, the list based approaches suffers from inability to identify zero-hour phishing assaults and creating excessive queries with heavily loaded servers [6]. The blacklists have shown the prominent results in designing various toolbars which are listed in Table I.

### *B. White-list Techniques*

An alternative approach to black list based phishing detection is the white list based method. Unlike the blacklist approach, white list approach maintains a comprehensive list of known safe websites and their relevant information. Most of the white list approaches adopt a universal approach, aiming to encompass all legitimate websites globally. However, it is challenging to maintain an all-inclusive catalog of legitimate websites, as it requires centralized information for assessing webpage legitimacy. Few research efforts have been dedicated to enhance white list approaches, making it an area with limited focus [7].

### *C. Two Factor Authentication*

In two factor authentication two level of security is involved. The first level authentication done by user name and password whereas, second level authentication done by biometrics, or different tokens generations method such as OTP(One Time Password). Though it adds extra security over password mechanism, there will be a possibility of denial of service if server goes down. Moreover, since the security is mainly rely on user and server, if one of the entity has been compromised then it is vulnerable to Man in the Middle Attack [8].

### *D. visual similarity technique*

By developing a highly similar website to the original one, users could easily fall into the trap of phishers. This is achieved through visual appearance manipulation, where the phishing website mimics the authentic site using techniques such as copying the HTML code of the genuine website. Additionally, attackers may employ scripts or images to cover the address or URL bar in the browser, further misleading users into believing they are interacting with a legitimate website. These tactics make it easy for users to be ensnared by attackers. To address this issue and enhance detection and prevention, a technique called visual similarity has been introduced which have several advantages [9]. These techniques are able to identify the maliciously embedded objects such as images, Flash, ActiveX, and Java Applets that attackers often use to evade traditional phishing detection techniques. These techniques utilize a signature that captures common features across the entire website rather than just a single webpage. Consequently, a single signature can effectively detect various targeted web pages within a website or even different versions of the same website. Furthermore, visual similarity-based techniques provide a dual layer of phishing URL filters. However, there are also some disadvantages associated with visual similarity-based detection. One limitation is the reliance on blacklists, which require constant updating and may not always capture new or evolving phishing websites. Additionally, the performance of these techniques can be influenced by internet speed and the complexity of web pages. Overall, visual similarity-based detection methods offer advantages in combating phishing attacks, but they also have inherent limitations that need to be considered for effective implementation [10].

### *E. Fuzzy Logic*

The phishing detection that implements fuzzy logic obtained the prominent results in the literature [11]. In [11], the phishing detection was approached in two levels. In the first level, various machine learning algorithms were trained with the selected features and in the second level, Fuzzy logic algorithms were employed. From the result analysis, it is observed that, FURIA algorithm with only five features obtained the best accuracy as 99.98%. However, the Fuzzy information-based frameworks require extensive testing with various equipment to ensure the effectiveness. Additionally, establishing accurate fuzzy guidelines and acquiring the necessary expertise can present significant challenges [11,12].

### *F. Machine Learning*

The working flow diagram of machine learning based detection is depicted in Fig. 3. The heuristic-based method is a

TABLE I
LIST OF ANTI-PHISHING TOOLBARS

| Toolbar | Browser Extensions | Description | Disadvantages |
|---|---|---|---|
| Netcraft | Mozilla Firefox | Displays the information about date of site registration, page rank, country in which site was hosted, and name of the organization hosts that site | If netcraft server goes down the legitimacy of the website under doubtful |
| Spoofstick | Mozilla Firefox, Microsoft Internet Explorer | Displays the website's real domain name to get rid of URL obfuscation | Time consuming |
| Spoofguard | Microsoft Internet Explorer | The degree of spoofing is decided by performing certain checks on Domain Name, URL,Email, Password, Link, and Image | Spoofguard warnings are mainly based on level of alarm indicators that depends on attribute weight set by the user. Hence the user knowledge is required |
| Trustbar | Mozilla Firefox | Analyses the website with respect to logos and certificate authority | fails if fake SSL Certificate is used |
| iTrustpage | Mozilla Firefox | Decision is based on external information Such as Google'S search index, PageRank | False negatives can be increased |
| eBay Account Guard | Internet Explorer | Warns user in terms of three color of signals | May increase false positives If genuine website left unverified |
| Phishtank site checker | Mozilla Firefox | Add on service provided by phish tank which offers community based phishing protection | Bandwidth usage |
| Trustwatch | Internet Explorer | Indicates by three color signal green, yellow, red | Not suitable for zero day phishing attack |
| Gralic Wrap | Microsoft Internet Explorer | verifies every website visited by the user against the known fraudulent websites | May slow down the performance of the System |

common method of the phishing detection technique. In this technique, the majority of these features are derived from a variety of sources like URLs and the HTML Document Object Model (DOM) of the given webpage. In [13], the Decision Tree (DT) algorithm was used to classify the phishing websites. This is one of the machine learning algorithm techniques in which decisions can be built based on the conditions of the features. It has a lot of advantages compared to other algorithms such as normalization of data is not necessary for the decision tree algorithm. However, the minor alterations in the data can lead to significant changes in the decision tree's structure, resulting in instability. Also, it may take longer time to train the models. Likewise, the Random Forest (RF) algorithm used to detect phishing attacks [14]. Random forests are an ensemble of decision trees, where the outcomes of individual trees are combined to produce a final result. These models possess the remarkable capability to control overfitting while minimizing the impact of bias on error. One approach to reducing variance in random forests is by training on diverse samples of the data. However, the ensemble nature of the algorithm which comprising multiple decision trees hinders interpretability and makes to ascertain the individual significance of each variable. Another technique that is used to detect phishing attacks by machine learning technique is the Support Vector Machine (SVM) technique [15]. The algorithm demonstrated the strong performance in detecting the phishing websites when limited information is available.

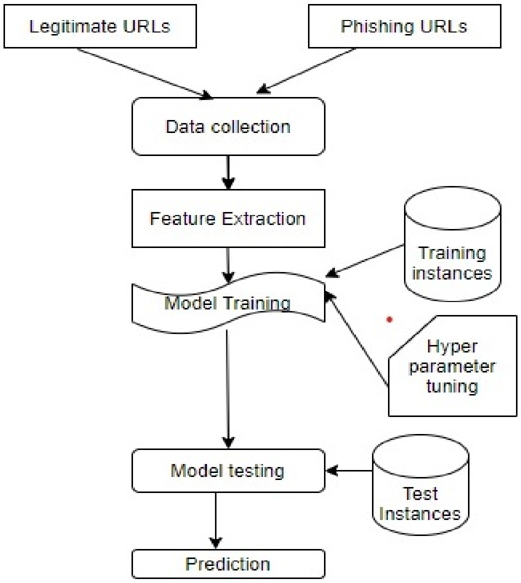


Fig. 5. Machine learning based detection

TABLE II
LIST OF PHISHING DETECTION TECHNIQUES

| Technique | Advantages | Disadvantages |
|---|---|---|
| Blacklist based Approaches [6] | • Demand minimum resources on the host machine<br>• Effectiveness in scenarios where minimal FP rates are desired | • Lead to an increased number of queries when servers are heavily loaded<br>• Mitigation of zero-hour phishing attacks |
| White-list based Approaches [7] | • Logic systems are simple and justifiable<br>• To control access | • Manage vulnerabilities in the design process<br>• Strong as no exact information sources are required |
| Two factor authentication [8] | Two level of security | Possibility of Man-in-the Middle attack |
| Visual similarity techniques[9-10] | • Can find out such embedded objects<br>• Two layers of phishing URL filters | • The requirement of blacklists<br>• Depending on internet speed, web |
| Fuzzy techniques [11-12] | • The rationale is not always exact | Setting accurate, fuzzy guidelines and, enrollment capacities can be a tough task |
| Machine Learning techniques[13-15] | To mitigate zero-hour attacks | • Having a higher FP rate<br>• higher computational cost |
| Decision Tree Algorithm [13] | • Not require normalization of data<br>• Requires less effort for data preparation<br>• Very intuitive and easy to explain to technical teams | • Involves higher time to train the model<br>• relatively expensive<br>• A small change in the data can cause a large change<br>• Not suitable for regression tasks and predicting continuous values |
| Random Forest Algorithm [14] | • It reduces overfitting<br>• Flexible to both classification and regression problems<br>• Works well with both categorical and continuous values | • Requires much computational power<br>• requires much time for training |
| Support Vector Machine (SVM) [15] | • Offers a convenient kernel solution function, enabling it to effectively address complex problem domains<br>• Shows favorable scaling properties when confronted with high-dimensional data, making it suitable for analyzing and processing datasets with many features. | • Selecting the most suitable kernel solution function can pose a challenge due to its complexity<br>• Interpretability and understanding of the model may be hindered by subjective factors and variable weights, leading to difficulties in interpretation |
| Neural network [16-19] | • Reduce overfitting<br>• Stable convergence property | • It is weak due to duplicate points |

### *G. Deep Learning*

The neural network can be used to detect phishing websites with high accuracy and strong active learning abilities from massive datasets. Reducing overfitting and stable convergence property is the main advantage of using neural network techniques for the detection of a phishing attack. On the other hand, the detection of phishing attacks using neural techniques has its own disadvantage, there are challenges associated with public datasets, including the presence of duplicate points, as well as the inclusion of negative and irrelevant features in the feature vector. These factors can hinder the training process of neural networks, leading to overfitting issues. Consequently, the trained classifier may become ineffective in predicting the phishing websites accurately, compromising its overall strength and performance [16]. The deep learning algorithms such as CNN, LSTM, and DNN are used for the detection of phishing websites in recent researches. In [17], the deep learning models were used to automatically extract optimal feature representations from raw inputs. The deep URL detect (DUD) encodes raw URLs using character-level embedding for representing characters in a numeric format. In DUD, hidden layers in deep learning architectures extract features from the character-level embeddings. These features are then passed through a feed-forward network with a non-linear activation function to estimate the probability of a URL being malicious. The experiment was conducted with 500 epochs and a learning rate of 0.001. The performance of DUD was compared with other state-of-the-art deep learning-based character-level embedding methods. DUD demonstrated comparable performance while being computationally efficient across all test cases. Additionally, deep learning architectures [18-22] based on character-level embedding models outperform n-gram representations due to the embedding's ability to capture the sequence and relationships among all the characters in a URL. In [18], a novel approach to combat phishing attacks that leverages a deep learning trained security measures. The authors suggested that incorporating an intermediate security layer within ISPs serves as a protective barrier between multiple servers and end-users. The effectiveness of the framework lies in its ability to provide protection to a significant number of users against specific phishing attacks through a single blocking point. The detailed analysis of existing works are given Table II.

### H. Future Research Directions

The current anti-phishing approaches examine the characteristics of phishing strategies extensively. However, the complexity and variety of phishing attempts still continues to evolve. Therefore, it can be said that always a rat race exists between the phishers and the researchers. The challenges such as Embedded objects and Image-based phishing, Language dependency, Minimization of response time, Divergent phishing behavior, Compromised web server, Phishing detection on the darknet in detecting phishing attacks may be addressed in the evolving phishing detection. The presented challenges can help researchers to design an anti-phishing method that can withstand future sophisticated phishing tricks.

## III. Conclusion

In this paper, the different techniques used for detecting phishing attacks are analyzed and classified based on the functionalities. The insight into the toolbars used for detecting phishing websites are also given which can help the researchers to simulate the attacks in a real-time scenario and to derive a robust solution based on the experience. The limitations and the challenges involved in the current phishing detection approaches are also discussed which can motivate the researcher to develop a future solution to address these issues. From this extensive survey of phishing attacks, it is understood that phishing continues to be successful because of the evolving nature of attack strategies and the ignorance of warnings provided by the anti-phishing systems. Also, the current solutions proposed for detecting phishing attacks may fail against future attempts of phishing. Hence the researchers must look beyond the current tools and methods to propose adaptive techniques to detect phishing attacks efficiently.

## References

[1] Chiew KL, Yong KS, Tan CL. A survey of phishing attacks: their types, vectors and technical approaches. Expert Systems with Applications, 106:1-20, 2018.

[2] https://docs.apwg.org/reports/apwg_trends_report_q2_2022.pdf accessed June 2023.

[3] https://www.getastra.com/blog/security-audit/phishing-attack-statistics/ accessed June 2023.

[4] Bhardwaj, Akashdeep, Fadi Al-Turjman, Varun Sapra, Manoj Kumar, and Thompson Stephan. ”Privacy-aware detection framework to mitigate new-age phishing attacks.” Computers & Electrical Engineering 96 (2021): 107546.

[5] Sánchez-Paniagua, Manuel, Eduardo Fidalgo, Enrique Alegre, and Rocío Alaiz-Rodríguez. ”Phishing websites detection using a novel multipurpose dataset and web technologies features.” Expert Systems with Applications 207 (2022): 118010.

[6] Burke, Stephen. ”How to prepare for the onslaught of phishing email attacks.” Computer Fraud & Security 2021, no. 5 (2021): 12-14.

[7] Jain, Ankit Kumar, and Brij B. Gupta. ”A novel approach to protect against phishing attacks at client side using auto-updated white-list.” EURASIP Journal on Information Security 2016 (2016): 1-11.

[8] Sun, Y., Zhu, S., Zhao, Y. and Sun, P., 2022, October. A User-Friendly Two-Factor Authentication Method against Real-Time Phishing Attacks. In 2022 IEEE Conference on Communications and Network Security (CNS) (pp. 91-99). IEEE.

[9] Jain, A.K. and Gupta, B.B., 2017. Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks, 2017.

[10] Goel D, Jain AK. Mobile phishing attacks and defence mechanisms: State of art and open research challenges. computers & security. 2018 Mar 1;73:519-44.

[11] Abuzuraiq A, Alkasassbeh M, Almseidin M. Intelligent methods for accurately detecting phishing websites. In2020 11th International Conference on Information and Communication Systems (ICICS) 2020 Apr 7 (pp. 085-090). IEEE.

[12] Aburrous M, Hossain MA, Dahal K, Thabtah F. Intelligent phishing detection system for e-banking using fuzzy data mining. Expert systems with applications. 2010 Dec 1;37(12):7913-21.

[13] Toolan F, Carthy J. Phishing detection using classifier ensembles. In2009 eCrime researchers summit 2009 Sep 20 (pp. 1-9). IEEE.

[14] Subasi A, Molah E, Almkallawi F, Chaudhery TJ. Intelligent phishing website detection using random forest classifier. In2017 International conference on electrical and computing technologies and applications (ICECTA) 2017 Nov 21 (pp. 1-5). IEEE.

[15] Anupam, S. and Kar, A.K., 2021. Phishing website detection using support vector machines and nature-inspired optimization algorithms. Telecommunication Systems, 76(1), pp.17-32.

[16] Wang W, Zhang F, Luo X, Zhang S. PDRCNN: Precise phishing detection with recurrent convolutional neural networks. Security and Communication Networks. 2019 Oct 29;2019:1-5.

[17] Sahoo D, Liu C, Hoi SC. Malicious URL detection using machine learning: A survey. arXiv preprint arXiv:1701.07179. 2017 Jan 25.

[18] Somesha M, Pais AR, Rao RS, Rathour VS. Efficient deep learning techniques for the detection of phishing websites. Sādhanā. 2020 Dec;45:1-8.

[19] Maurya S, Jain A. Deep learning to combat phishing. Journal of Statistics and Management Systems. 2020 Aug 17;23(6):945-57.

[20] Butt, Umer Ahmed, Rashid Amin, Hamza Aldabbas, Senthilkumar Mohan, Bader Alouffi, and Ali Ahmadian. ”Cloud-based email phishing attack using machine and deep learning algorithm.” Complex & Intelligent Systems 9, no. 3 (2023): 3043-3070.

[21] Thakur, Kutub, Md Liakat Ali, Muath A. Obaidat, and Abu Kamruzzaman. ”A Systematic Review on Deep-Learning-Based Phishing Email Detection.” Electronics 12, no. 21 (2023): 4545.

[22] Choudhary T, Mhapankar S, Bhddha R, Kharuk A, Patil R. A Machine Learning Approach for Phishing Attack Detection. Journal of Artificial Intelligence and Technology. 2023 May 10.