# Identification of Phishing Attacks using Machine Learning Algorithm

*Dinesh* P.M[1*], *Mukesh* M[1], *Navaneethan* B[2], *Sabeenian* R.S[1], Paramasivam M.E[1], and *Manjunathan* A[3]

[1]Department of Electronics and Communication Engineering, Sona College of Technology, Salem, India
[2]Spring Five, Bangalore, India
[3]Department of Electronics and Communication Engineering, K.Ramakrishnan College of Technology, Trichy-621112, Tamil Nadu, India

**Abstract**. Phishing is a particular type of cybercrime that allows criminals to trick people and steal crucial data. The phishing assault has developed into a more complex attack vector since the first instance was published in 1990. Phishing is currently one of the most prevalent types of online fraud behavior. Phishing is done using a number of methods, such as through emails, phone calls, instant chats, adverts, pop-up windows on websites, and DNS poisoning. Phishing attacks can cause their victims to suffer significant losses, including the loss of confidential information, identity theft, businesses, and state secrets. By examining current phishing practises and assessing the state of phishing, this article seeks to assess these attacks. This article offers a fresh, in-depth model of phishing that takes into account attack stages, different types of attackers, threats, targets, attack media, and attacking strategies. Here, we categorise websites as real or phishing websites using machine learning techniques including Random Forest, XGBoost, and Logistic Regression. Additionally, the proposed anatomy will aid readers in comprehending the lifespan of a phishing attack, raising awareness of these attacks and the strategies employed as well as aiding in the creation of a comprehensive anti-phishing system.

## 1 Introduction

Due to the significant increase in internet usage, individuals are increasingly sharing their personal information online. This has led to a rise in incidents where fraudsters gain unauthorized access to personal data and engage in financial fraud. Phishing is a technique used by malicious actors to deceive users by impersonating reputable websites and tricking them into revealing sensitive information like passwords, account details, and credit card numbers. While various anti-phishing tools and methods exist to detect and prevent such attacks in emails and websites, phishers continuously develop new and hybrid methods to evade these defenses. According to research conducted by the Anti-Phishing Working

* Corresponding author: pmdineshece@live.com

Group, there were 1,220,523 distinct phishing scams reported from January to March 2018, with an increasing number of attacks reported daily. Researchers are constantly working on improving existing models to enhance their accuracy and effectiveness. This article presents a comprehensive model of phishing that considers various aspects, including different stages of attacks, types of attackers, threats, targets, attack media, and strategies. The model utilizes a dataset of phishing URLs collected from an open-source service, and employs machine learning techniques such as Random Forest, XGBoost, and Logistic Regression to classify given URLs as either legitimate (0) or phishing (1) websites.

All of these models were developed using the dataset, and the test dataset was used to assess the models.

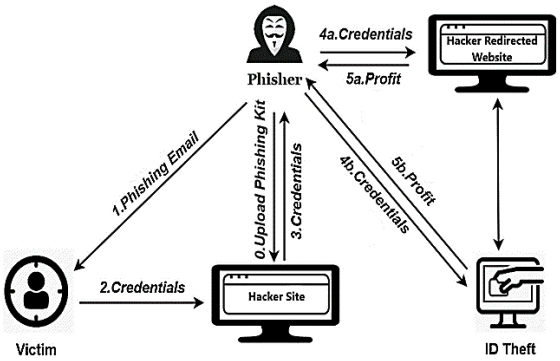


**Fig. 1.** Typical phishing attack

## 2 Literature survey

In their study, Sami Smadi et.al [3] have proposed a novel approach for identifying digital phishing emails using a dynamic expanding neural network that incorporates reinforcement learning. While there are advanced methods available for detecting phishing attacks, there are still limitations in online detection systems that can lead to gaps in web-based transactions. To address this, the researchers have developed a unique framework that combines a neural network with reinforcement learning to identify phishing attacks in online applications. By utilizing reinforcement learning, the proposed model continuously improves over time and adapts to new phishing behaviors that may emerge. To overcome the challenge of limited data in the database, the model dynamically expands the offline database while operating in the online mode. The researchers have also introduced a new algorithm to analyze and detect new phishing tactics in the expanded database. Extensive testing using well-known databases has demonstrated the effectiveness of the proposed method, achieving high levels of accuracy, True Positive Rate (TPR), and True Negative Rate (TNR) at 98.63%, 99.07%, and 98.19%, respectively. The model also exhibits low False Positive Rate (FPR) and False Negative Rate (FNR) with values of 1.81% and 0.93% respectively. In comparison to other methods tested on the same database, the proposed model outperforms existing approaches, showcasing its superiority in phishing detection.

In their research paper, Medvet et.al [5] propose a Visual-Similarity-Based Phishing Detection approach to address the ongoing security issue of phishing, which involves fraudulent attempts to obtain sensitive data from users. Phishing attacks typically deceive victims into providing their confidential information on fake web pages that mimic legitimate ones. The increasing prevalence of phishing attempts necessitates effective countermeasures. The authors present a novel technique that focuses on visually contrasting

phishing pages with genuine pages to determine if they are visually similar. They identify and consider three crucial aspects of websites that contribute to the resemblance of phishing pages to genuine ones. These aspects include the textual content and writing style, embedded images, and the overall visual appearance of the page as rendered by the browser. To validate the effectiveness of their approach, the researchers conducted an experimental investigation using a sample dataset consisting of 41 real-world phishing websites and their corresponding legitimate targets. The experimental results align with the expectations of the researchers in terms of false positives (incorrectly identifying genuine pages as phishing pages) and false negatives (failing to identify phishing pages). Overall, the Visual-Similarity-Based Phishing Detection approach proposed by Medvet et.al demonstrates promise in effectively detecting phishing attempts by considering visual cues and characteristics of web pages, providing an additional layer of defense against this form of online fraud.

Alam et.al [15] propose a Phishing Attacks Detection using Machine Learning Approach to address the increasing cybersecurity risks associated with the digital transformation. With the expanding scope of digitization, cybercriminals have more opportunities to exploit security vulnerabilities. Phishing attacks are commonly employed as initial tactics to deceive users and obtain their private passwords. By manipulating users through phishing, hackers aim to gain unauthorized access to networks and digital assets of organizations. To combat these phishing threats, the researchers propose a machine learning-based model. They utilize machine learning techniques, specifically random forest and decision trees, to detect phishing attacks. The model is trained and evaluated using a valid Kaggle dataset consisting of phishing assaults. Feature selection procedures, such as principal component analysis (PCA), are applied to analyze the dataset's characteristics. The suggested approach demonstrates promising results, with the random forest algorithm achieving a maximum accuracy of 97%. By leveraging machine learning and feature selection techniques, the model shows potential in effectively identifying phishing threats. While behavioral analytics and threat intelligence solutions aid in identifying anomalous traffic patterns, the researchers emphasize the importance of a defense-in-depth strategy to prevent phishing attempts. Overall, the Phishing Attacks Detection using Machine Learning Approach proposed by Alam et.al presents a valuable contribution in the ongoing battle against phishing attacks. By leveraging machine learning algorithms, organizations can enhance their defenses and mitigate the risks associated with phishing attempts.

Buber et.al [9] has proposed an NLP Based Phishing Attack Detection from URLs. Phishing has grown in importance as a danger in the cyberspace in recent years, particularly with the increased usage of messaging and social networks. Users are encouraged to visit a fake website that has been meticulously created to exactly resemble a well-known banking, e-commerce, social networks, etc., website in a traditional phishing attack in order to provide personal information like credit card numbers, passwords, usernames, and even cash. Many attackers typically use emails to forward to the target website as part of their attacks. Even experienced users with little expertise can access these fake websites and divulge their private data. China, Turkey, and Taiwan are the three countries most frequently affected by malware, with rates of 47.09%, 42.88%, and 38.98%, according to a luring threat survey of 45 nations in the fourth quarter of 2016. Phishing attacks are regarded as semantics-based attacks that primarily target the vulnerabilities of computer users, making their detection a difficult task. This study develops a phishing identification method that can identify these types of assaults by utilising machine learning algorithms and spotting perceptual similarities using NLP approaches. The suggested system has undergone a number of testing, and the findings of the experiments revealed that the Random Forest algorithm performs quite well, with a success rate of 97.2%.

Basit et.al [28] conduct a comprehensive analysis of AI-enabled phishing attack identification strategies. Phishing attacks have become a prominent threat that affects web users, organizations, and internet service providers. These attacks involve the use of spoof emails or fake websites to trick victims into providing personal data, such as login credentials and credit card numbers. Phishing websites often serve as a launching point for various online scams and social engineering attacks. The researchers focus on examining different Artificial Intelligence (AI) methodologies employed in the identification of phishing attacks. They analyze approaches such as Machine Learning, Deep Learning, Hybrid Learning, and situation-based methods to gain a comprehensive understanding of these attacks. The study also includes a comparison of various research studies that have utilized AI techniques for phishing attack detection, assessing the advantages and disadvantages of each approach. Furthermore, the article provides a thorough overview of the current challenges associated with phishing attacks and proposes recommendations for future research in this field. By exploring the strengths and limitations of AI methodologies for identifying phishing attacks, the study contributes to the advancement of effective countermeasures against these threats. Overall, Basit et.al's research offers valuable insights into the state of AI-enabled phishing attack identification strategies. By understanding the current landscape and exploring potential research directions, this study contributes to the ongoing efforts in combating phishing attacks and enhancing cybersecurity measures.

## 3 Types of phishing

Phishing attacks manifest in diverse forms and are designed to deceive users. Furthermore, numerous methods and approaches have been developed to identify and mitigate these attacks. Classification is a technique commonly employed to detect phishing on websites. Below are examples of typical phishing attack types and the classification techniques utilized to combat them [15].

### 3.1 Algorithm-based phishing

America Online (AOL) detected the first phishing attempt, that was built with an algorithm. The hacker used an algorithm to correlate America Online credit card numbers of various accounts.

### 3.2 Delusive phishing

The fraudster utilises a variety of techniques to trick website visitors. Users receive emails from Fishers asking them to confirm their account verification. They ask users to click on links and buttons. Behind the links on a website, fraudsters collect and store the personal data of users.

### 3.3 HTTP phishing

HTTP phishing is an additional variant of phishing scams that utilizes hidden links. These hidden links direct users to the attackers' website, where they can gather and retain the users' data upon clicking.

### 3.4 Hosts file poisoning

Fraudsters target individuals by impersonating reputable websites in an attempt to deceive them or misrepresent the organization. This practice is commonly known as data spoofing. Attackers utilize this tactic to trick users into providing their data, which is then collected from their server.

### 3.5 Data-Injection phishing

Clone phishing is a type of phishing attack that involves the creation of nearly identical replicas of legitimate emails. In this attack, the attacker gains access to either the sender's or recipient's email account and uses it to compose an email that closely resembles the original message. The malicious email is then sent to the intended target, usually with a link or attachment. The fraudster typically requests that the recipient provide updated information or resend the original document. This deceptive tactic aims to trick the recipient into believing that the email is legitimate and taking the desired action, such as disclosing sensitive information or clicking on a malicious link.

### 3.6 Clone phishing

Clone phishing is a type of phishing attack where the attacker compromises the email account of either the sender or the recipient. In this attack, the malicious actor creates an email that closely resembles a legitimate email and sends it to the intended victim along with a link or attachment. The fraudulent email appears to be a duplicate or an updated version of the original email, tricking the recipient into believing it is legitimate. The attacker typically manipulates the content of the email to request sensitive information or prompt the recipient to take a specific action, such as sending the original document in an updated form. This technique aims to exploit the familiarity and trust associated with the original email, increasing the likelihood of the victim falling for the scam. It is important for users to remain cautious and verify the authenticity of emails, especially when they request sensitive information or unusual actions..

### 3.7 Whaling

The higher executives of the company are the intended target of this kind of phishing. The email was sent to executives and contains content about significant issues. The email's content may include customer complaints.

### 3.8 Spear phishing

Spear phishing is a type of email fraud that specifically targets individuals or organizations with personalized and highly tailored attacks. In spear phishing, the attacker sends emails to the intended victims with the goal of tricking them into taking a specific action or revealing sensitive information.

Unlike generic phishing emails that are sent to a large number of recipients, spear phishing emails are carefully crafted to appear legitimate and trustworthy. The attacker often conducts extensive research to gather information about the target, such as their name, position, company, email address, and other details. This information is then used to make the email seem authentic and increase the chances of the victim falling for the scam.

The email may contain personalized content, such as references to specific projects, colleagues, or recent events, to create a sense of familiarity and establish credibility. The

attacker may also use social engineering techniques to manipulate the recipient's emotions or create a sense of urgency, further increasing the likelihood of a response.
Spear phishing attacks can be highly sophisticated and difficult to detect, as they exploit the trust and familiarity between the sender and the recipient. It is crucial for individuals and organizations to exercise caution when receiving emails, especially those that request sensitive information or prompt unusual actions. Verifying the legitimacy of the sender and being mindful of any suspicious signs can help mitigate the risks associated with spear phishing attacks.

## 4 Existing system

The currently used techniques hardly ever involve brand-new internet users. Once they recognize a phishing website, it either becomes inaccessible or the user is warned that there is a chance the website is not legitimate. Several anti-phishing strategies include The well-known authentication tool Gemini is used to safeguard users against phishing. Today, other anti-phishing measures are available to stop users from visiting fraudulent websites by offering a robust, secure authentication process. Some well-known websites include a security indicator on their pages to let visitors know that they are not visiting a phony website. Users can recognize the site as legitimate by looking for the URL indicator. In other instances, consumers refrain from typing passwords when there are no such security signs present.

## 5 Proposed system

Even though there are many ways to identify phishing today, it has grown to be exceedingly challenging to identify false emails and messages in the contemporary environment. Whitelisting, heuristics, blacklisting, and machine learning are some of the tools available today for identifying phishing emails. This chapter suggests a machine learning strategy to recognize phishing emails and prevent users from disclosing their pin, user ID, or passwords. In this research, we presented a variety of machine-learning methods to detect phishing attempts of any form. Given that the input URL might either be considered phishing (1) or legal(0), we employed the data set that falls within the classification problem. In this project, the following supervised machine learning models (classification) are taken into consideration to training the dataset:

### 5.1 Random forest

Supervised machine learning methods such as random forest has been widely utilized in classification and regression problems. To increase the predictive accuracy of that dataset, it builds decision trees on numerous samples and utilises their maximum vote for classification and mean in the case of regression.

### 5.2 XGBoost:

It is a supervised learning process that incorporates the predictions of number of weaker, general models to try to properly predict a outcome variable. It uses the Gradient Boosting framework to implement machine learning algorithms. It offers a parallel tree boosting to quickly and accurately address a variety of data science challenges.

### 5.3 Support vector machines:

An systematic analysis to supervised machine learning known as SVM is applied to regression or classification problems. Your information are processed by using procedure called as the kernel functions, and the optimal output margin is determined based on these modifications. All of these models were developed using the dataset, and the test dataset was used to assess the models. Phishing Website Detection Models & Training.ipynbOpen in colab contains detailed information on the models and their training.

## 6 Results and discussions

The aim of this project is to use the dataset produced to predict phishing websites to build machine learning algorithms and deep neural networks. In order to create a dataset from which the necessary URL- and website content-based attributes may be extracted, both phishing and innocuous URLs of internet sites are collected. Each model's performance level is assessed and contrasted. First, we gathered the set of phishing URLs from PhishTank, an open-source service. This site offers a collection of phishing URLs that are updated hourly in a variety of formats, including csv, json, etc. To develop the ML algorithms, 5000 random phishing URLs are collected from this dataset. The open source datasets are used to obtain the reliable URLs. This dataset contains a collection of URLs that aren't malicious, spammy, phishing, or defacement. The benign url dataset is taken into consideration for this study out of all of these types. To develop the ML algorithms, 5000 random genuine URLs are obtained from this dataset. Therefore mentioned datasets are placed in the "DataFiles" folder, and the information about these features is placed in the "Colab". The elements are taken directly from the various phishing websites. The data is separated into 8000 training samples and 2000 testing samples before beginning the ML model training. This is an obvious supervised machine learning challenge based on the dataset. Classification and regression are the two main subtypes of supervised machine learning issues. This data collection has a classification system because the input URL might be either legal or phishing (1). (0). In this project, the following supervised machine learning models(classification) are taken into consideration to train the dataset:

1) Forest Random

2) Support Vector Machines and

3) XGBoost

All of these models were developed using the dataset, and the test dataset was used to assess the models. Phishing Website Detection Models & Training.ipynbOpen in Colab contains detailed information about the models and their training.

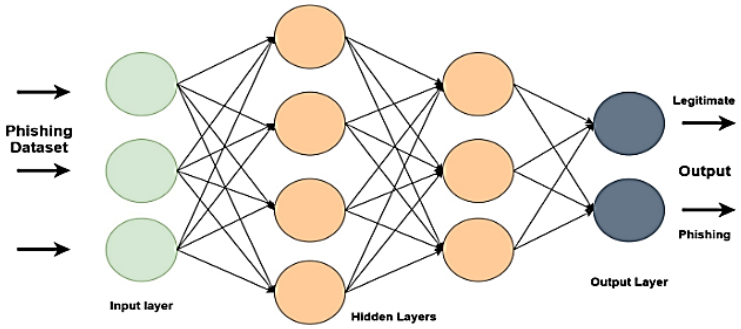


**Fig.2**. Machine Learning model for Phishing attack detection.

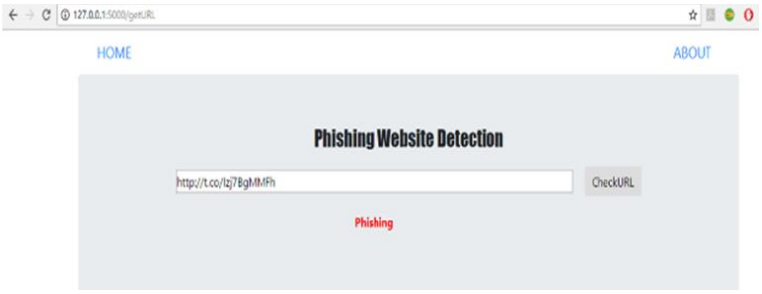


**Fig. 3**. Detection of Phishing websites


**Fig. 4.** Detection of Legitimate website

## 7 Conclusion

Attacks using phishing are still one of the biggest dangers facing people and businesses today. Parallel to the expansion of social media, phishing on social media has become more prevalent. In this project, we used different supervised machine-learning techniques to detect phishing attacks. We collected a dataset of phishing URLs from an phishTank and classified the datasets. As a result, the classification model depicts the websites as legitimate or phishing. Fig. 3 shows the URL is a phishing one and Fig 4 shows the website is a legitimate one. The XGBoost Classifier has the highest model performance of 94.2% based on the findings from the above mode. This project may be further improved to include the development of browser extensions or a GUI that analyses a URL to determine whether it is real or phishing. Developing effective anti-phishing tactics that shield users

from the attack is a crucial first step in minimizing these attacks, even if ongoing security awareness training is the key to avoiding phishing attempts and lessening their impact.

## References

1. A. Zainab, C. Hewage, L. Nawaf, I. Khan, Front. Comput. Sci. **3**, 563060 (2021).S. Chanti, T. Chithralekha. Classification of anti-phishing solutions." SN Comput. Sci **1,** 1-18 (2020)
2. S. Sami, N. Aslam, L. Zhang. Decis. Support Syst. **107**, 88-102 (2018)
3. R. Gowtham, I. Krishnamurthi, K. Sampath Sree Kumar. Decis. Support Syst **61,** 12-22 (2014)
4. M. Eric, E. Kirda, C. Kruegel. *Visual-similarity-based phishing detection,* in Proceedings of the 4th international conference on Security and privacy in communication networks, 1-6. (2008)
5. W. Liu, G. Huang, L. Xiaoyue, Z. Min, X. Deng. *Detection of phishing webpages based on visual similarity*, In Special interest tracks and posters of the 14th international conference on World Wide Web, 1060-1061. 2005.
6. P. Josna, K.A.F. Fathima, S. Gayathri, G.E. Elias, A.A. Menon. *A comparitative study of machine learning models for the detection of Phishing Websites,* in International Conference on Computing, Communication, Security and Intelligent Systems (IC3SIS), 1-7, (2022)
7. S.O. Koray, E. Buber, O. Demir, B. Diri. Expert Syst. Appl. **117,** 345-357 (2019)
8. B. Ebubekir, B. Diri, O.K. Sahingoz. *NLP based phishing attack detection from URLs*, in International Conference on Intelligent Systems Design and Applications, Springer, Cham, 608-618 (2017)
9. C. Ye, W. Han, Y. Le. *Anti-phishing based on automated individual white-list*, in Proceedings of the 4th ACM workshop on Digital identity management, 51-60 (2008)
10. D. Rachna, J.D Tygar. *The battle against phishing: Dynamic security skins,* in Proceedings of the 2005 symposium on Usable privacy and security, 77-88 (2005).
11. S.P. Kumar. *An Emerging Solution for Detection of Phishing Attacks,* in Cybersecurity Threats with New Perspectives. Intech Open, (2021)
12. T.C. Lin, K.L. Chiew, S.N. Sze. *Phishing webpage detection using weighted URL tokens for identity keywords retrieval,* in 9th International Conference on Robotic, Vision, Signal Processing and Power Applications, Springer, Singapore, 133-139 (2017)
13. F. Anthony Y, L. Wenyin, X. Deng. *Detecting phishing web pages with visual similarity assessment based on earth mover's distance (EMD),* IEEE transactions on dependable and secure computing **3**, 4 (2006)
14. A.M. Nazmul, D. Sarma, F.F. Lima, I. Saha, S. Hossain. *Phishing attacks detection using machine learning approach*, in third international conference on smart systems and inventive technology (ICSSIT), 1173-1179. (2020)
15. G. Brij B, A. Tewari, A.K. Jain, D.P. Agrawal. Neural. Comput. Appl. **28**, 12 (2017)
16. R. Zulfikar. *Phishing attacks and countermeasures*. Handbook of information and communication security 433-448 (2010)
17. C.K. Leng, K. Sheng, C. Yong, C.L. Tan. Expert Syst. Appl. **106** (2018)
18. W. Min, R.C. Miller, S.L. Garfinkel. *Do security toolbars actually prevent phishing attacks?* in Proceedings of the SIGCHI conference on Human Factors in computing systems, 601-610 (2006)
19. G. Sujata, N. Provos, M. Chew, A.D. Rubin. *A framework for detection and measurement of phishing attacks,* in Proceedings of the 2007 ACM workshop on Recurring malcode, 1-8 (2007)

20. A. Mohamed, F. Alaca, S. Chiasson. *Why phishing still works: User strategies for combating phishing attacks,* International Journal of Human-Computer Studies **82** (2015)
21. B. Ram, S. Mukkamala, A.H. Sung. *Detection of phishing attacks: A machine learning approach*" in Soft computing applications in industry, Springer, Berlin, Heidelberg, 373-383 (2008)
22. C. Juan, C. Guo. *Online detection and prevention of phishing attacks*, in 2006 First International Conference on Communications and Networking in China, IEEE, 1-7 (2006)
23. M. Jason, CERT Coordination Center. Technical trends in phishing attacks, **1** (2005)
24. C. Jackson, D.R. Simon, D.S. Tan, A. Barth, *An evaluation of extended validation and picture-in-picture phishing attacks,* in International Conference on Financial Cryptography and Data Security, Springer, Berlin, Heidelberg. 281-293 (2007)
25. Chaudhry, J. Ahsenali, S.A. Chaudhry, R.G. Rittenhouse. Int. J. Sec. Appl. **10**, 1 (2016)
26. H. Tzipora, N. Memon, O. Nov. *Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks,* Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks, January 2, (2015).
27. B. Abdul, M. Zafar, X. Liu, A.R. Javed, Z. Jalil, K. Kifayat. Telecommun. Syst.**76**, 1 (2021)
28. P. Pawan, M. Kumar, R.R. Kompella, M. Gupta. *Phishnet: predictive blacklisting to detect phishing attacks*, in 2010 Proceedings IEEE INFOCOM, 1-5. IEEE, (2010)
29. W. Longfei, X. Du, J. Wu. *Effective defense schemes for phishing attacks on mobile computing platforms*, IEEE Trans. Veh. Technol. **65**, 8 (2015).
30. C Bhuvaneshwari, A Manjunathan. *Reimbursement of sensor nodes and path optimization*, Materials Today: Proceedings, **45**, 1547-1551 (2021).