

## Understanding Phishing: Creating Effective Strategies For Detection Using Phishscan

B. Geeta Sri<sup>1</sup>, M. Durga Sohan<sup>2</sup>, N. Shanmukha Rao<sup>3</sup>, N. Sri Charishma<sup>4</sup>, Y. Akshaya Deepika<sup>5</sup>

<sup>1,2,3,4,5</sup> Department of CSE, NSRIT, Vishakhapatnam, India

Corresponding Author: [22nu1a0584@nsrit.edu.in](mailto:22nu1a0584@nsrit.edu.in)

### Abstract

In essence, phishing constitutes the major threat to cybersecurity that implies exploitation of human faults and social engineering methods to get unauthorized access to sensitive information. The article entitled "Understanding Phishing: Creating Effective Strategies for Detection Using Barracuda Sentinel" explains an entire way of handling phishing using machine learning, heuristic techniques, and education of users. Machine learning models such as natural language processing and anomaly detection analyze the communication patterns to identify phishing threats, whereas heuristic models are generally designed to detect irregularities like suspicious spelling, emotional man, domain anomalies, etc. In addition, user education becomes a significant component with simulations on phishing scenarios about what such attacks feel like through the media source of emails while educating people for actual recognizing phishing attempts. It is an important feature from which the paper takes stock where the main psychological plays which the cybercriminal understanding like urgency, trust, and false security, manipulate victims. These are the views that put out in conclusion that advanced technologies when combined with user education lead to a great reduction in the success of the phishing attack. The study then prefers the use of a multilayered approach improving technological defenses and then improving the user's resilience to better guard against the threats of phishing.

### Keywords:

Phishing, cybersecurity, social engineering, machine learning, natural language processing, anomaly detection, heuristic techniques, user education, phishing simulations,

### 1. Introduction:

Human error has, for ages now, so recognized as the weakest link in security measures for computer and information systems, to the extent that studies can point to the fact that 95% of all breaches in security are the result of individual's errors. This vulnerability has increased cases of phishing attacks, which now exploit online scams and other misleading ways to draw victims. With the evolution of phishing techniques becoming more sophisticated, tackling threats as such poses a big challenge in the domain of cyber security. The paper titled "The Art of Recognition: Developing Effective Strategies for Phishing Identification" elaborates a broad-spectrum approach for combating these attacks. According to the paper, there is a need for a multifaceted

defense model to tackle these attacks. Central to this defense was training of users and understanding of social engineering tactics, thereby putting individuals at the heart of prevention against phishing. Thus, by educating consumers and empowering them with needed tools and awareness, a stronger defense against phishing and other cyber threats could be achieved while bolstering even further the human aspect of cybersecurity.

### **Literature Review**

Phishing still remains as one of the most constant threats which take advantage of human factor and such weaknesses in technology. As has already been pointed in the literature, there are many concepts and strategies for mitigating the threat of phishing.

The blockchain technology, which is already in use for several services, can aid to make phishing more secure. Other technologies like sophisticated AI algorithms can enhance the performance of machine learning veering it closer to super intelligent models. General learners like ensemble learning models can provide better solutions and gain greater popularity in their use. Another use of AI or other technologies is through the use of behavioural biometrics which enlarges the scope for handling phishing threat. With the aid of the aforementioned technologies, it will allow for the wider and greater use of phishing deterrent systems, which are much needed as the phishing threat is constantly evolving.

A review of Machine Learning in Phishing Detection Research has focused on how machine learning classification techniques can be used to detect phishing messages from the content, message header and sender actions. NLP and other graphical models like RNN and CNN have also been used in the identification of anomalous communication behaviour and trigger suspicious actions. For example, RNNs can be used for patterns recognition captured for the classification of emails by the phishing indicators, such as containing urgent requests or different domains (Alsewari & Shamsuddin, 2020).

Heuristic models alongside the machine learning strategies work through rule such as irregularity of the domain name or address or language induced by urgency, and many others. These models serve as a first-order safeguard to screen out potentially malicious messages from reaching the target users (Toolan & Carthy, 2009).

Realizing the importance of human factors causations in enabling phishing works, academicians have called for awareness creation. Training efforts target familiarizing users with the different types of phishing techniques for example, a fake sender or link. There is awareness that learning that places certain users in front of a simulated phishing attack has been useful in reminding users best security practices (Hadnagy, 2018).

System of Multi-Layered Protection It is therefore clear that having a mixture of technical and

social measures form the best defence against phishing. For example, tools like zveloDB combine URL categorisation with threat intelligence to identify these activities, but Organisations are told to go for multi-factor authentication (MFA), threat intelligence sharing protocols etc, (Symantec, 2021).

This is because the nature of these phishing schemes is changing from time to time, and therefore the detection methods have to be changed as well. New researches have focussed on psychological angles of the attack, what the attackers are trying to achieve, indicating the fact that just performing a pseudo psychological analysis of the attack is not sufficient, but the fact as to what the attacker wants to achieve and wants to avoid must be understood in this context one can mention urgency, trust, etc. Kahneman 2011.

## 2. Methodology

### 2.1. Leveraging Machine Learning for Phishing Detection

Phishing, using domain names and email as a medium, impose a great danger to many individuals. Many heavy-handed techniques are regularly employed to commit this fraud. Machine learning technologies, more recently those on RNNs and NLPs, are proclaimed as the means for detecting phishing messages by indicating whatever might seem urgent or typographical mistakes in communications. As an example, a small bank created scripts that utilized NLP in order to identify common phishing phrases, such as the somewhat generic pronouncement, "Please act immediately to verify your account," which filtered these messages out before they reached end user inboxes. These machine learning systems can efficiently spyware emails through subtle issues like poor word choices, graphical design mistakes, and linguistic inconsistency, thereby improving defenses against dynamic phishing dangers and cybercriminal tactics.



**Fig -1: Consequences of Phishing-Attacks**

One of the identities that seemed to have been targeted by the offending party, seems to have tried to resolve the issue with the concerned party outside; given that the phishing email under concern was in a little more than a spoofed bank account statement, even the most obvious mistyping of some dictionary words, let alone graphic design and essential linguistics, should have been quite enough.

## 2.2. Email Classification Using Deep Learning Techniques

Up next is classification of emails that are entirely based on the learned patterns and features from advanced deep learning algorithms like RNN and CNN. Since these models are trained to learn on patterns, they can effectively classify the trusted emails into the suspicious ones that seem to be following phishing standards- typical of all phishing attempts.

CNN, for instance, can easily narrow down from analyzing email header metadata wherein it can

catch discrepancies such as unusual domain names or typographical variations that are common markers of phishing.

For example, an email that originates legitimately from PayPal, but presents as example support@paypal-secure.com instead of the legitimate support@paypal.com, is actually regarded as a phishing attempt. This type of domain discrepancy can be detected via pattern recognition methods by this CNN model, thus flagging it for the system as potentially malware harmful. The results of such systems in using these deep learning models help them accurately demarcate benign communications from messages having deceptive or malicious intents.

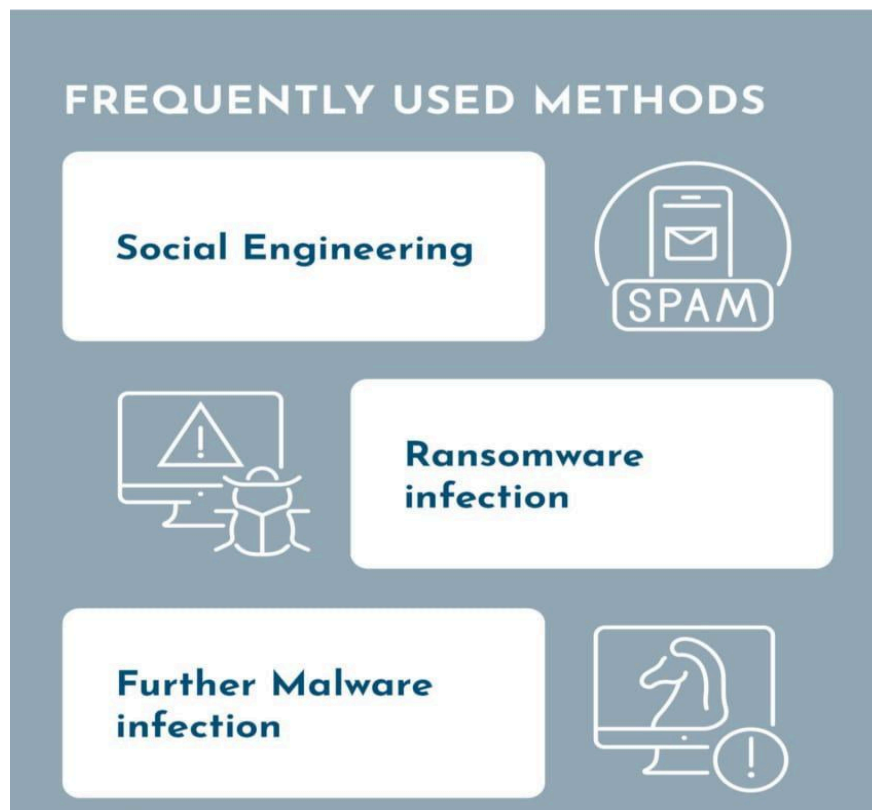


Fig-2: Frequently used methods

### 2.3. Rule-Based Heuristic Approaches to Identify Phishing Attempts

Heuristic analysis further utilizes the usual detection mechanisms with rule-based strategies that function in conjunction to determine the phishing attempts through some behaviour or linguistic indicators. These heuristic rules can flag phishing attempts. For example, they can indicate "urgency-in-dominated language" or "suspicious domain names." An email can be flagged, for example, when the deviations from the expected domain are found, say, "bankname.co" rather than the official "bankname.com."

This is why the message may even have server typical phrases of phishing attack like: "Your account is at risk of suspension," thus showing the threat behind it. A good example of using heuristic analysis might detect phrases with too much urgency or alarm, such as "Act Now!" and is accompanied by a suspicious link. Such a system, therefore, categorizes the messages under high risk to warn users to be suspicious of phishing. Typical cases of such messages are those fake ones that allow for e-commerce order confirmation but which ask users to "confirm" payment information.

Heuristic logic would analyse these messages for their intensity of urgency and classify them as potentially dangerous. Thus, the rules would detect a phrase such as "Confirm your purchase NOW to avoid charges!" with an unusual sender address. In this setting, the heuristic layer stands guard and intercepts the message before delivery to the recipient user. As a proactive defence method, it sends notices to individuals who would otherwise have been recipients of the attempted phishing attack. This way, false transactions are avoided, as well as damage to the institutions. It will also make the overall security posture better, as it will identify and block high-risk communications from sending phishing attacks successfully against these potential vulnerabilities.

#### **2.4. Empowering Users: The Role of Training in Phishing Prevention**

End-user training will go a long way into reducing the phishing threats from end users. The specialized training and awareness workshops should increase end users' capacities to detect and counteract phishing attempts. For example, training employees to identify suspicious emails, especially unsolicited links or attachments, may be a possibility. During training, users are shown how to "hover" the mouse cursor over the hyperlinks to verify the URL destination before actually clicking. So much as they would be relatively unaware to phishing, such simple prevention measure prevents them from being victimized by malicious phishing tactics. In one example, a government agency organized a workshop on identification of phishing threats among its employees. They were trained to recognize common indicators that may hint of false email, such as typographical errors, surprise variations in domain names, or odd extensions. Some practical trainings include scrutinizing email headers and proving link authentications by checking their real targets before interacting with them. Apart from this program, warnings were given to the employees about unsolicited emails purportedly from internal IT departments regarding password resets. In fact, such emails were unnecessary responses but will not open any link in them. Therefore, by making them more aware, user training will contribute toward a safer environment for organization networks against phishing through strengthening the cybersecurity outlook of the organization.

#### **2.5. Enhancing Cybersecurity Awareness Through Phishing Simulations**

Phishing simulations are the potent ways to check and strengthen the end-users' potential of effectively identifying and responding to phishing risks. These phishing simulation campaigns act as training modalities. That is repeatedly exposing users to fake threats to develop the muscle



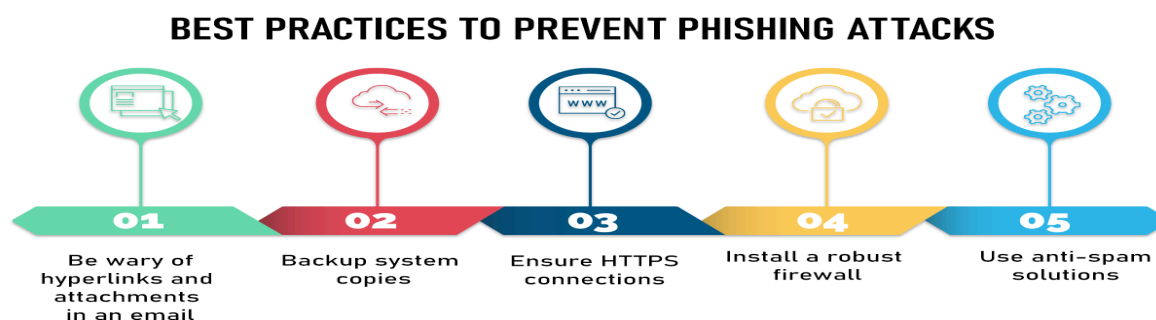
memory of recognizing malicious emails. That could take the form of fake phishing emails appearing to come from "IT support" requesting employees to reset their passwords. This allows the system to see how many employees would succumb to such a fake attack situation.

As an instance, phishing simulations involved sending a batch of emails with a subject line like "Urgent: Verify Your Payroll Details," followed by the monitoring of responses to catch those employees who act by clicking the links or doing actions suggesting their vulnerability to phishing. It assesses user behavior while identifying those who need additional training in cybersecurity, whose intent is to make them less vulnerable to real-world attempts of phishing.

One type of a phishing simulation campaign might include subject lines such as "You've won an Amazon gift card!" or "Urgent payroll update," created to invoke a reaction in the users and have them engage with the email. So, the email goes on to provide semi-official-looking messages to "legitimize" the communication while subtly request some confidential information to "enhance services." The technique is not too dissimilar to the way in which actual phishing methods are applied, making it hard for users to differentiate between real messages and scam messages.

## **2.6. Continuous Improvement of Phishing Detection Through Data Analysis**

Based on aggregated and analyzed information about historical phishing attempts, simulation results, and user feedback, the refinement and optimization of models for the detection of phishing behaviors and the general understanding of such attacks continue being carried out. Key metrics such as the true positive rate of testing for false positives and click-through rates aggregate such models that can be modified to differentiate between phishing and legitimate emails. For example, a multinational reflects on historical data such as click-through rates and phishing detection results in order to assess its training program for employees. Analysts identify new trends such as HR-themed phishing tactics that exploit a sense of urgency, allowing them to customize training content to respond to specific threats while also modifying their detection algorithms to flag similar future emails. This provides both the acute accuracy of phishing-detection technologies and a lowering of the risk of specific departments, such as Human Resources, being targeted by phishing attacks, thus improving cybersecurity posture for the entire organization.



**Fig -3: Best Practices to prevent Phishing Attacks**

### 3. Abbreviations

**AI** - Artificial Intelligence

**NLP** - Natural Language Processing

**URL** - Uniform Resource Locator

**MFA** - Multifactor Authentication

**SOC** - Security Operations Center

### 4. Summary of Algorithms and Formulas:

**Email Filtering and Security Gateways:** Implementation of heuristic and machine-learning advanced email filtering solutions that can analyse incoming email messages will render many of the phishing attempts useless before they even reach the user's inbox.

**Multi-Factor Authentication (MFA):** The use of MFA creates another hurdle into phishers' attempts to get into users' accounts when they obtain user credentials using some phishing techniques.

**Threat Intelligence Sharing:** Working with a cybersecurity organization to get a known threat intelligence feed on phishing tactics will provide useful detection and response strategies.

**Behavioural Analysis:** Monitoring user behaviours for unusual activities such as logging into accounts from unfamiliar locations or devices to flag possible phishing attacks in real-time.

**Link Scanning Tools:** Use of tools to scan URLs for known evil sites or to assess the safety parameters of links will help avoid compromising users to phishing websites.

**Email Header Analysis:** The verification of the email headers for discrepancies, whether in the sender's declared IP address or routing information, can help in spotting spoofed emails.

### 5. Preventions and Solutions:

#### 5.1. Applicative Solutions: Tools and Techniques to Detect Phishing Emails

The detection of phishing emails requires a multi-pronged approach using technical tools in combination with user awareness strategies. Primary methods include a wide array of email



authentication such as sender policy framework (SPF), domain keys identified mail (DKIM), and domain-based message authentication, reporting, and conformance (DMARC)-these help in ascertaining the genuineness of the email sender and foiling email spoofing. Email filtering and security solutions such as antivirus solutions and email security gateways (such as Proof point, Mimecast, Barracuda) scan incoming emails for residual malware signatures and phishing indicators. User behaviour analytics (UBA) tools scrutinize user activity to ascertain anomalies indicative of compromised accounts. Phishing simulation platforms (such as KnowBe4 and PhishMe) provide training to employees in recognizing and responding to phishing attempts, raising awareness. Manual inspection techniques-such as inspecting email headers, hovering over links to check URLs, and the detection of common phishing indicators like poor grammar and urgent requests-are critical. Moreover, automated incident responses and reporting processes go a long way in encouraging users to report dubious emails, thus helping organizations in monitoring and responding to phishing threats. Combined, these tools and techniques will help to strengthen the defences of organizations against phishing attacks, thus safeguarding both their data and users.

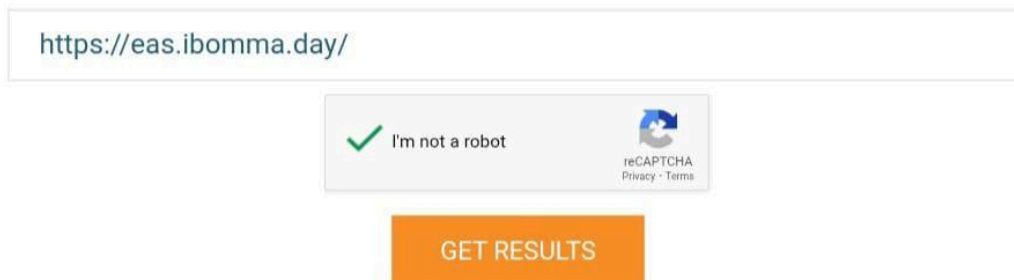
## **5.2 The best tool in detecting phishing attacks is zveloDB**

The zveloDB is actually a complete service and database by zvelo for the improvement of web security through enriched categorization and classification information of websites. Its applications include identification and blocking of phishing, mushrooming online threats, and other similar activities. The roots of this database crawl threat intelligence and put it up with machine learning and human analysis to maintain and prove very much accuracy against threats either classified under URLs or content. Benefits of zveloDB: The greatest point of the zveloDB is complete URL Classification, classifying millions of URLs as per the aforementioned presence of phishing, malware, or any other malicious activity. Thus, it allows organizations to detect potential threats and act upon them immediately.

zveloDB real-time threat detection lets organizations stay ahead of emerging phishing threats and act promptly. It provides high accuracy with a new algorithm and human verification which lessens false positive cases and builds confidence on the data given.

## Check A URL with zveloLIVE

zveloLIVE allows you to check a URL for its category and safety status. Found a Miscategorization? [Report It!](#)

The screenshot shows the zveloLIVE web interface. At the top, there is a text input field containing the URL 'https://eas.ibomma.day/'. Below the input field is a reCAPTCHA verification box with a green checkmark and the text 'I'm not a robot'. To the right of the reCAPTCHA box is a small icon for reCAPTCHA with the text 'reCAPTCHA Privacy - Terms'. Below the reCAPTCHA box is a large orange button with the text 'GET RESULTS' in white capital letters.

**Fig -4: Check a URL with zveloLIVE**

### 5.3. How to Verify and Identify Phishing Using zveloDB

**URL Lookup:** zveloDB can help an organization conduct real-time lookups concerning URL suspected as malicious since it allows querying the database to check whether a URL falls under phishing or has another potential threat.

**Security Tool Integration:** With zveloDB incorporated into existing security solutions Web filter, email gateways, or SIEMs, organizations can automatically block access to known phishing websites and notify users of other possible threads.

**Threat Intelligence Feeds:** zveloDB can be a supplier of threat intelligence feeds for use by organizations to update their security systems with the latest phishing threat data to ensure they stay before newly identified phishing sites.

**Monitoring and Reporting:** Organization monitoring web traffic, as well as emails for suspicious URL, will also generate reports for phishing attempts by using zveloDB classification data that would help in identifying patterns and improving security.

**User Awareness Training:** Using data from zveloDB, organizations can educate their users about the kinds of phishing threats they could come across, making their users aware of recognizing such threats and preventing being victims of phishing attacks.

Categorization Results for <https://eas.ibomma.day/>

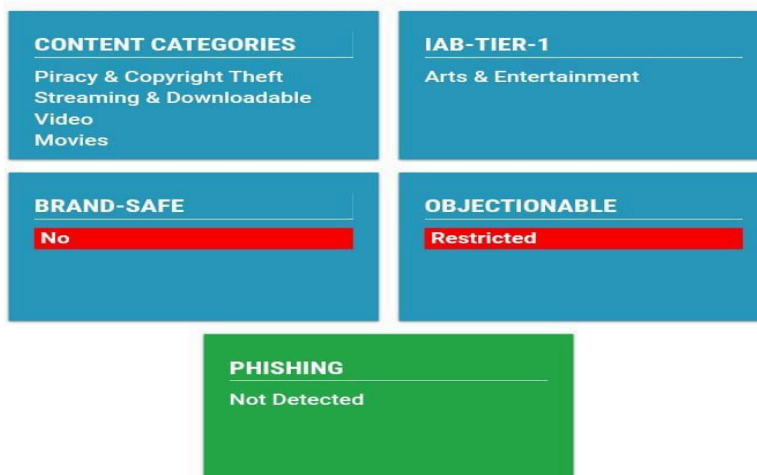


Fig -5: Checking and showing the results of zveloDB

## 6. Conclusion

This study recommends that a synchronized, internal, multi-pronged strategy need to be developed from the ground up to deal efficiently with phishing, which involves processes of machine learning and heuristics and enhanced training for the users. Such technologies as NLP or RNN could enhance phishing probing via the study of linguistic structure or email composition. Heuristics provide another practical layer of protection, as they can spot some signs of an attack like an odd domain name or urgency. Users would find it relatively credible to recognize and respond to suspicious messages if they were exposed to they would be real, structured training together with simulated attacks.

This multi-prong approach not only adds to the organization's security level but also addresses technological issues as well as social engineering concerns. Furthermore, accommodating tactically the ever-changing strategies of the enemy, this study proposes that provision of technological facilities and training for end-users confer efficient protection towards reduction in the phishing occurrences and development of a greatly enhanced cybersecurity milieu.

## 7. Acknowledgement:

We express our wholehearted thanks to all those individuals who have, in one way or the other, contributed to this research. We also owe special gratitude to the experts in cyber security and researchers who somehow could spare invaluable time to share information, data, and expertise

in formulating measures for phishing identification. Special thanks also to AI and machine learning engineers who further strengthened the technical foundation of this study with insights within NLP, RNN, and anomaly detection.

Thanks also go to organizations that volunteered to the phishing simulations; their feedback and participation helped us to improve the methodology. All study participants are acknowledged and appreciated for their contribution as their inputs and comments have contributed enormously to the practical approaches to fighting phishing. Without all contributors' commitment, expertise, and hard work, this work could not be achieved, and such topics as improvements in cybersecurity measures would not exist..

### References:

1. Alsewari, A., & Shamsuddin, S. M. (2020). "Phishing Attacks: A Systematic Review of the Detection Techniques." *Journal of Information Security*, 11(2), 89-104. DOI: 10.4236/jis.2020.112007.
2. Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley. This book explores the psychology behind social engineering tactics, including phishing.
3. Jansen, W., & Takemura, T. (2019). "Phishing Defense: A Comprehensive Review." *IEEE Access*, 7, 58042-58064. DOI: 10.1109/ACCESS.2019.2911043.
4. Kahneman, D. (2011). *Thinking, Fast and Slow*. Farrar, Straus and Giroux. This book discusses cognitive biases and decision-making processes, relevant for understanding how individuals fall for phishing schemes.
5. O'Brien, J. (2020). "Understanding Phishing: A Review of Current Literature." *Cybersecurity and Privacy*, 1(1), 15-27. DOI: 10.3390/cybersecurity1010002.
6. Symantec. (2021). "Internet Security Threat Report." Symantec Corporation. Retrieved from <https://www.broadcom.com/company/newsroom/press-releases?filtr=1571>.
7. *The Phishing Guide Understanding & Preventing Phishing Attacks* By: Gunter Ollmann, Director of Security Strategy, IBM Internet Security Systems, 2007.
8. *Phishing: Cutting the Identity Theft Line* Published by Wiley Publishing, Inc. 10475 Crosspoint Boulevard Indianapolis, IN 46256 [www.wiley.com](http://www.wiley.com), 2005, Rachael Lininger and Russell Dean Vines.
9. Anti-Phishing Working Group (APWG), "Phishing activity trends report—first quarter 2013." <http://antiphishing.org/reports/apwgtrendsreportq12013.pdf>, accessed September 2014.
10. Aloul F (2010) The need for effective information security awareness. *Int J Intell Comput Res* 1(3):176–183.
11. eCrime Trends Report: Fourth Quarter (2013) <http://Internetidentity.com/resource-tags/quarterly-ecrime-reports/>. Accessed Sept 2014 .
12. Anti-Phishing Working Group (APWG) (2016) Phishing activity trends report—first-third quarter 2015. <http://antiphishing.org/reports/apwgtrendsreportq12013.pdf>. Accessed Feb 2016.
13. Husna H, Phithakkitnukoon S, Palla S, Dantu R (2008) Behavior analysis of spam botnets. In: *Communication systems software and middleware and workshops, 2008. COMSWARE 2008. 3rd International Conference, Bangalore, India, 2008*, pp 246–253.

14. Toolan F, Carthy J (2009) Phishing detection using classifier ensembles. In: eCrime researchers summit, IEEE conference Tacoma, WA, USA, 2009, pp 1–9.
15. Toolan F, Carthy J (2010) Feature selection for spam and phishing detection. E-Crime Researchers Summit, Dallas, pp 1–12.
16. [Google Scholar](#)
17. Anti-Phishing Working Group Phishing Archive (2014) [http://anti-phishing.org/phishing\\_archive.htm](http://anti-phishing.org/phishing_archive.htm). Accessed Sept 2014.
18. Dhamija R, Tygar JD (2005) The battle against phishing: dynamic security skins. Proceedings of symposium usable privacy and security.
19. Aburrous M, Hossain MA, Dahal K, Thabtah F (2010) Predicting phishing websites using classification mining techniques with experimental case studies. In: Seventh international conference on information technology. IEEE Conference, Las Vegas, Nevada, USA, 2010, pp 176–181.
20. PhishTank Phishing Archive (2014) <http://www.phishtank.com/phisharchive.php>. Accessed Sept 2014.
21. Phishing Detection with Generative Adversarial Networks Al-Ahmadi, S., Alotaibi, A., & Alsaleh, O. (2022). Phishing detection with generative adversarial networks. *IEEE Access*, 10, 42459–42468.
22. A Survey on the Detection of Phishing Websites Zieni, R., Massari, L., & Calzarossa, M. C. (2023). Phishing or not phishing? A survey on the detection of phishing websites. *IEEE Access*, 11, 18499–18519.
23. Phishing Account Detection Model via Network Embedding for Ethereum Luo, J., Qin, J., Wang, R., & Li, L. (2024). A phishing account detection model via network embedding for ethereum. *IEEE Trans Circ Syst II Express Briefs*, 71(2), 622–626.
24. Enhancing Phishing Detection: A Novel Hybrid Deep Learning Framework for Cybercrime Forensics Alsubaei, F. S., Almazroi, A. A., & Ayub, N. (2024). Enhancing phishing detection: a novel hybrid deep learning framework for cybercrime forensics. *IEEE Access*, 12, 8373–8389.
25. Phishing Email Detection Using Natural Language Processing Techniques Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2022). A systematic literature review on phishing email detection using natural language processing techniques. *IEEE Access*, 10, 65703–65727. <https://ieeexplore.ieee.org/document/9795286>
26. Bhabad, S., Bhalerao, K., Nagare, P., Shinde, D., & Pandit, P. V. (2024). Real-time object detection using ML (image processing). *The Journal of Computational Science and Engineering*, 2(2).
27. Teja, L. D., Gunasekhar, M., Dinesh, S., Kumar, N. P., Mahendra, S., & Devi, C. (2024). Skin disease diagnosis using convolutional neural network. *The Journal of Computational Science and Engineering*, 2(2).
28. Kavya, P., Vineesh, P. S., Sneha, P., Jayanth, S., & Vardhan, M. H. (2024). Stock market price prediction using machine learning. *The Journal of Computational Science and Engineering*, 2(2).
29. Vyshnavi, K., Shaik, S., Kumar, M. S., Praveen, M. S. V., & Potti, S. (2024). Facial recognition based attendance system using OpenCV. *The Journal of Computational Science and Engineering*, 2(3).