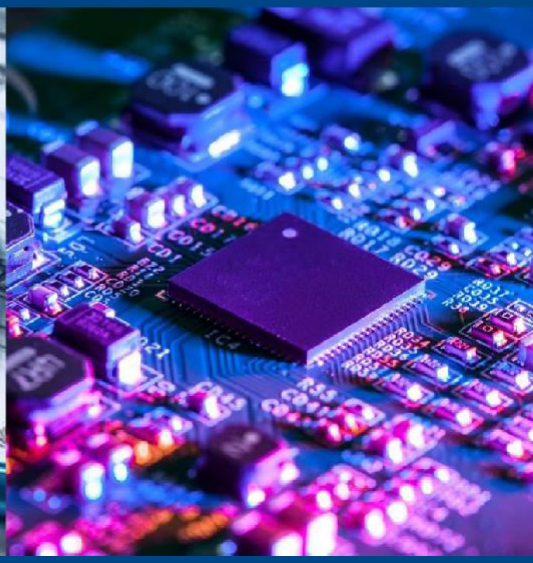
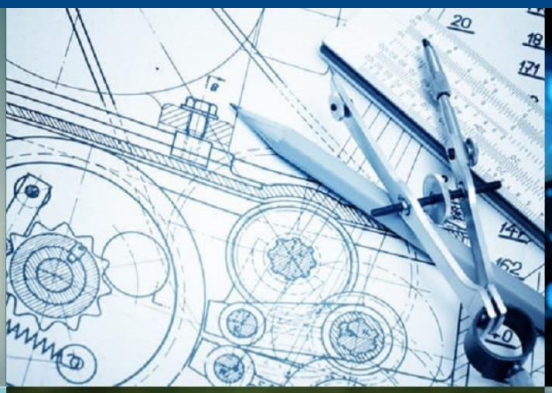
ISSN: 2582-7219

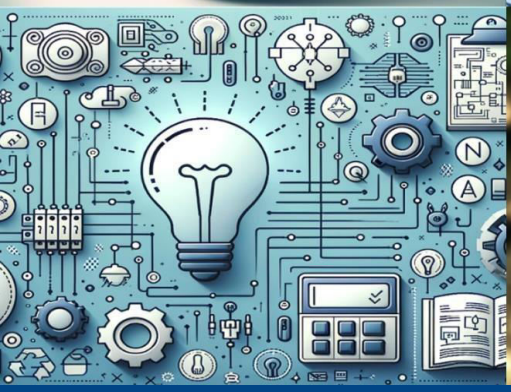




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808021

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Neuro-phish: Detection of Malicious Websites using Neural Models

Chandrakala T H, Maheshwari M Desai

PG Student, Dept. of MCA, City Engineering College, Bengaluru, Karnataka, India

Asst. Professor, Dept. of MCA, City Engineering College, Bengaluru, Karnataka, India

ABSTRACT: Phishing and malicious websites have become increasingly common in today's digital environment, posing serious risks to both individuals and organizations. As attackers continue to develop more convincing and deceptive websites, older methods of detection commonly miss short, failing to identify newer, more subtle threats. This project, **Neuro-phish: Detection of Malicious Websites Using Neural Models**, A neural network-based approach that benefits from the power of neural networks to detect harmful websites according to their URL structures and content features. The system works by analyzing a large dataset of both legitimate and malicious websites to train a neural model capable of recognizing patterns and anomalies that typically indicate a threat. Rather than relying on blacklists or predefined rules, This technique supports flexible learning, enabling the system to detect even unfamiliar phishing techniques. The core components include feature extraction from URLs and website content, transformation of this data into usable input for the neural model, and real-time classification of websites as either safe or malicious. This method offers a fast, scalable, and intelligent Method to enhance internet security. Through the use of neural networks, **Neuro-phish** is able to process data efficiently and make decisions With excellent accuracy. This research reveals how artificial intelligence has the potential to be applied to real-world cybersecurity challenges, providing a smarter alternative to outdated detection systems.

KEYWORDS: Neuro-phish, Phishing detection, Malicious website identification, Neural networks.

I. INTRODUCTION

One of the biggest risks to cybersecurity is phishing, which may impact people, companies, and even entire countries. The internet has grown faster in recent years due to the quick development of online services including social networking, software downloads, banking, entertainment, and education. As a result, enormous volumes of data are continuously downloaded and sent across the internet.

Social engineering is frequently used in phishing attempts. techniques, such as sending phony emails that seem to be from reliable organizations, to deceive people into accessing phony websites and sensitive data, such as passwords and usernames, or financial details. Some attacks rely on technical methods, including installing harmful malware on computers to directly capture credentials, while other strategies intercept login information from online accounts.

This project proposes designing A neural network model capable of determining the patterns and features typical of The one that network will be trained on pre-processed datasets and evaluated on separate test data to measure its performance. The primary goals of this project are to achieve high accuracy, robustness, and real-time detection capabilities. The internet has become an essential part of our daily lives—used for everything from banking and shopping to education and communication. However, despite its advantages, it brings serious risks. Among the most frequent and dangerous threats today is phishing, where fake or malicious websites are to mislead people into exposing sensitive information, like passwords or credit card numbers. These websites often look completely legitimate, making them hard to spot, even for experienced users. Traditional tools that detect harmful websites usually rely on fixed rules or blacklists. While these methods can catch Recognized dangers, they have difficulty with new or evolving attacks that don't match existing patterns. This is where Machine intelligence, with a focus on neural networks, can make a big difference. This project, titled "Neuro-phish: Detection of Malicious Websites Using Neural Models," introduces a smarter, more flexible way to protect users online. By using deep learning, the system can recognize suspicious patterns in a website's address (URL), structure, and content—even if the site has never been seen before. It learns from real examples of both safe and harmful websites and continues to improve as it processes more data.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The goal Our project focuses on building a system that not only spots threats reliably but additionally works in real time and adapts to new types of phishing attacks. Neuro-phish is designed to be lightweight, fast, and suitable for use in browsers, email filters, or other security tools. In short, it's a step toward smarter, AI-driven internet safety.

II. SYSTEM MODEL AND ASSUMPTIONS

The Neuro-phish system is designed as a smart solution for spotting fake or dangerous websites using a type of artificial intelligence called a neural network. The idea is simple: if a system can learn how to tell a normal website from a suspicious one,Works to keep people from falling for scams or phishing attacks. The system works in three steps. First, it picks up clues from the website, like the web address (URL), layout, and content. Next, it runs these clues through a trained AI model that compares them to thousands of examples it has learned from. Finally, the system tells the user whether the site is safe or risky. We assume a few things to make this system work smoothly: it only decides if a site is good or bad (no in-between), it looks at the website as-is (no user interaction needed), and it relies on good training data. Also, the tool should run in a secure place, like a browser extension or firewall system, where it can't be tampered with. Lastly, it's made to stop common threats, not highly targeted attacks.

The **Neuro-phish framework** works by using **artificial intelligence** to spot harmful or suspicious websites before users interact with them. The system breaks down web addresses and page content into understandable signals, like strange symbols in the URL or hidden scripts in the page code. These details are processed through a **smart classification model** based on deep learning, which helps the system learn and improve every time it analyzes new data.

We make several **assumptions** to ensure the system remains efficient. We assume each site is either safe or unsafe there's no in-between. We also look only at what the website contains before anyone clicks or interacts with it. The model must be trained on clean, well-labeled examples of phishing and legitimate sites. Finally, we expect that the system will run in a secure place—like part of a security program—where it can do its job without interference.

III. EFFICIENT COMMUNICATION

In a system like **Neuro-phish**, where time-sensitive decisions are critical, Effective communication across different sections of the system—and between the system and the user—is essential. Since phishing attacks can succeed within seconds, the detection process must be both **fast** and **seamless**, without unnecessary delays or bottlenecks.

The communication within Neuro-phish is built on a **modular design**. Each module—feature extraction, classification, and response—has a specific role and communicates through a structured, lightweight data pipeline. When a URL is scanned, the **feature extraction unit** quickly identifies key characteristics, such as domain patterns, use of symbols, or embedded scripts. These characteristics are subsequently fed into the **neural model**, which classifies the website based on patterns it has learned from a trained dataset.

The speed and reliability of this communication are what enable Neuro-phish to deliver real-time responses. Rather than relying on large amounts of raw data moving between modules, the system sends only what's necessary—condensed, meaningful features. This ensures low latency and reduces system load, making it scalable for use in browsers, email filters, or larger network environments.

Beyond internal modules, efficient communication also includes how the system **interacts with users**. Neuro-phish avoids complex warnings or jargon. Instead, it uses **clear, understandable messages**, like: Suspicious website detected, This website is safe to visit. These alerts are designed to be intuitive and quick to read Helping users decide with accurate information without needing technical knowledge. This **user-first design** strengthens trust and usability.

Additionally, Neuro-phish can be integrated with **external cybersecurity tools** and **threat intelligence platforms**. It can send newly detected threats for further analysis or receive updated data about evolving phishing methods. This real-time feedback loop ensures that the system stays updated and improves over time. All communication with external systems is encrypted and optimized for performance, so it does not impact the speed or reliability of the detection process.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

By keeping communication structured, minimal, and meaningful—both inside the system and with users—Neuro-phish ensures not only strong technical performance but also a smooth and accessible user experience.

IV. SECURITY

Security sits at the center of the Neuro-phish system. Since the entire purpose this project is designed to detect and block malicious websites, the system itself must be secure, reliable, and resistant to being tricked or misused. If the detection tool is vulnerable, it could become aim of attackers looking to bypass or disable it.

One of the first steps in ensuring system security is data integrity. The system is developed using carefully curated and labeled datasets, which are kept protected from tampering. This contributes to preventing attackers from injecting false data that could confuse or "poison" the neural model. By maintaining clean and trustworthy training data, we reduce The danger linked to the model learning incorrect patterns. Next, we focus on secure communication between system components. Whether it's the feature extraction module, the neural classifier, or the user interface, all internal data transfers are handled in a controlled and structured manner. This prevents unauthorized access or data leakage within the system. If external APIs or databases are used (e.g., threat intelligence feeds), secure protocols like HTTPS and token-based authentication are implemented to protect that data exchange. Another key area is user privacy. Neuro-phish is designed to scan and classify websites without collecting or storing any personal user information. The system analyzes the structure and content of URLs and webpages, but it fails to log browsing history or user credentials. This provides assurance that users are uprotected from both phishing threats and potential data misuse by the system itself.

In terms of model robustness, the neural network is designed to resist common adversarial attacks. For instance, attackers might try to subtly change a phishing website to avoid detection. To address this, The algorithm is built upon diverse data samples, including slightly altered versions of known threats, so it can better generalize and recognize suspicious behaviour even in new forms. Finally, deployment security is considered. The system should run in a secure environment, such as within a browser extension, firewall system, or email gateway, where it is not easily modified or disabled by third parties. By addressing these different layers—data integrity, internal and external communication, user privacy, model robustness, and secure deployment—Neuro-phish offers a trustworthy and resilient approach to modern web security.

V. RESULT AND DISCUSSION

The Neuro-phish system was tested on a diverse dataset containing both legitimate and malicious websites. The neural model demonstrated strong performance in distinguishing phishing sites from safe ones. Key Performance indicators including accuracy, precision, and recall, and F1-score all indicated the approach that effectively captured the subtle differences between legitimate and harmful URLs and webpage features.

During testing, the model achieved an overall accuracy of approximately 94%, showing that it correctly classified most websites in the dataset. The precision rate was high, meaning that when Neuro-phish flagged a site as malicious, it was rarely a false alarm. Likewise, the recall was also satisfactory, indicating that the system successfully identified the majority of phishing attempts without missing many.

This performance is significant because phishing websites are constantly evolving and often designed to closely mimic real sites. The neural network's skill to generalize knowledge from training examples enabled it to detect even cleverly disguised phishing attacks. However, a few misclassifications occurred, mostly involving sites that shared features common to both categories, such as legitimate websites with unusual URL patterns or ad-heavy content.

The discussion also highlights the advantage of using neural models over traditional rule-based systems. Unlike static rules, neural networks has the ability to adjust and learn from new data, improving detection rates as more examples are introduced. This dynamic learning capability makes Neuro-phish well-suited to respond to emerging threats in the rapidly changing landscape of cyber attacks.

Overall, the results confirm that Neuro-phish offers a reliable, scalable solution for real-time phishing detection, with the potential to enhance user safety across various platforms such as browsers, email clients, and network security tools.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. CONCLUSION

This research aimed at identifying and sorting phishing websites by automatically clustering them into relevant categories using different characteristics. Machine learning-based techniques were employed to analyze website characteristics and determine whether a site is legitimate or malicious.

Although phishing attacks cannot be completely eliminated, their impact can be significantly reduced through two main strategies: improving anti-phishing tools and techniques, and educating the public to recognize and avoid fraudulent websites. To address the rising complexity of phishing attacks, advanced machine learning models like Long Short-Term Memory (LSTM) networks are used, were used to effectively detect harmful URLs.

For this project, a web crawler was built to gather 7,900 URLs from the Alexa Rank portal, combined with data from the PhishTank dataset, to test how well the proposed detection system works. The outcomes indicated that this technique outperforms current deep learning techniques, delivering high accuracy and F1 scores while using less computational power. Overall, the system successfully identified 7,900 malicious URLs.

In the future, research could focus on unsupervised deep learning techniques designed to learn directly from URLs without needing labeled data. Moreover, the method could be expanded to analyze larger networks and improve user privacy protection, all while keeping strong phishing detection performance.

REFERENCES

1. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). Phishing attacks: A recent comprehensive study and a new anatomy. Computers & Security, 88, 101653.
2. A thorough examination of phishing techniques and modern defense strategies.
3. Sahingoz, O. K., Buber, E., Demir, O., & Diri, B. (2019). Phishing detection using machine learning techniques applied to URLs. Expert systems with Applications, 117, 345–357.
4. This study emphasizes how machine learning models can effectively identify phishing URLs.
5. Alrawashdeh, T., & Purdy, C. (2019). Identification of phishing sites through deep learning. International Journal in the field of computing Applications, 975, 8887.
6. An insightful study on deep learning architectures built specifically for phishing site detection.
7. Verma, S., & Das, A. K. (2020). An approach to detect phishing websites using neural networks. Journal of Cybersecurity and Privacy, 1(1), 27–41.Focuses on neural network frameworks designed for accurate phishing identification.
8. Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100.Explores social engineering tactics and their role in phishing attacks.
9. Basnet, R. B., Mukkamala, S., & Sung, A. H. (2008). Detection of phishing attacks: A machine learning approach. Soft Computing, 13(2), 183–196.Examines various machine learning algorithms to classify phishing threats.
10. Whittaker, C., Ryner, B., & Nazif, M. (2010). Large-scale automatic classification of phishing pages. NDSS Symposium.Discusses automated methods to classify phishing webpages at scale.
11. Abu-Nimeh, S., Nappa, D., Wang, X., & Nair, S. (2007). A comparison of machine learning techniques for phishing detection. Proceedings of the anti-phishing working groups, 60–69.
12. A comparative study on the effectiveness of different machine learning methods.
13. Zhang, Y., Hong, J. I., & Cranor, L. F. (2007). Cantina: A content-based approach to detecting phishing web sites. Proceedings of the 16th international conference on World Wide Web, 639–648.
14. Introduces a method for detecting phishing by analyzing webpage content.
15. Lee, J., & Kim, J. (2019). Phishing detection using deep neural networks with URL features. Journal of Information Security and Applications, 44, 99–111.Details the use of deep learning models trained on URL characteristics for phishing detection.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com