DS Journal of Cyber Security
Volume 2 Issue 4, 19-28, Oct - Dec 2024
ISSN: 2584-0665/ https://doi.org/10.59232/CYS-V2I4P103

*Original Article*

# Simulating Phishing and Security Step (2FA) and Detecting Fake URLs Using Plugin and Browser Extension Detection

**K. Dhivya[1], S. Anisha[2], V. Dheepa Muthu Jothi[3], S. Kavishree[4], R. Madhangi[5], M.G. Meena Abinaya[6]**

[1,2,3,4,5,6]*Department of Computer Science and Engineering (Cyber Security), Sri Shakthi Institute of Engineering and Technology, Tamilnadu, India.*

[5]madhangiradhakrishnan23cys@srishakthi.ac.in

Received: 04 October 2024; Revised: 10 November 2024; Accepted: 28 November 2024; Published: 21 December 2024

**Abstract -** Phishing attacks remain a universal and evolving threat, targeting both individuals and organizations by misusing trust and social engineering to gain access to confidential information such as usernames, passwords, and financial data. With the increasing cleverness of these attacks, traditional security measures are often insufficient to moderate the risks fully. This paper investigates the deployment of browser-based tools—specifically, plugins and extensions—for the real-time detection of phishing URLs, combined with Two-Factor Authentication (2FA) as an additional security layer. By simulating real-world phishing situations, Explore how browser extensions can enhance security by detecting and alerting users of suspicious URLs before they have interacted. Integrating 2FA adds another layer of protection, ensuring that even if credentials are compromised, unauthorized access is further delayed. The proposed system architecture focuses on combining URL pattern recognition, blacklist verification, and investigative analysis within browser extensions to provide immediate feedback to users about possibly malicious links. These measures are improved by 2FA, which requires a secondary verification step, drastically reducing the success rate of phishing attempts. Experimental results demonstrate a significant reduction in phishing success rates, highlighting the effectiveness of this multi-layered approach. Statistical analysis reveals a marked decrease in successful phishing incidents when both browser-based detection and 2FA are employed together. This study underscores the necessity of adopting proactive, layered security frameworks to address the growing phishing threat. The findings suggest that future enhancements could involve incorporating machine learning algorithms into the detection mechanisms to improve accuracy further and adapt to the rapidly changing strategies used by phishing attackers.

**Keywords -** Phishing attacks, Two-Factor Authentication (2FA), Phishing prevention, Phishing detection, User protection, Malicious links.

## 1. Introduction

Phishing attacks are among the most intentional and harmful forms of cybercrime and involve techniques that trick trusted organizations into revealing sensitive information such as credentials, financial information, and personal information. Advanced security technologies have improved, but phishing remains a major source of data breaches due to sophisticated techniques such as domain spoofing designed to bypass traditional detection systems.

Two-factor authentication (2FA) enhances account security through password requirements and secondary improvements, further improving security; however, phishing attacks can bypass 2FA to deceive users and use it to provide login credentials and authentication codes to fraudulent websites. A multi-layered approach combining 2FA and browser-based phishing detection mechanisms provides a robust solution to these challenges. Plugins and extensions are important in detecting and alerting users to suspicious URLs in real time. Phishing examples are important tools in cybersecurity training to make people aware of the phishing threat and assess how vulnerable they are to being attacked. Simulating a real phishing scenario helps users detect phishing attempts, thus reducing the success of social engineering tactics. Increased awareness improves alertness when dealing with suspicious emails and websites, increasing the overall level of security.

Browser extensions and plugins are necessary to spot fake URLs and phishing sites. These tools analyze URLs in real time, cross-reference phishing databases, and use heuristics to identify suspicious patterns, providing immediate alerts. Challenges continue when phishing techniques are in progress, including random domain generation. There is also an algorithm that generates fraudulent URLs and increases searchability. It is going to be hard. The extension improves browser performance by analyzing URLs in real time, comparing databases of malicious websites, and providing warnings of potential threats. This analysis allows users to avoid dealing with phishing websites, improving online security. Plugins add functionality to applications by analyzing URLs, warning users of suspicious links, blocking access to phishing domains and mitigating risks. The VirusTotal API integration in PHP enables comprehensive threat analysis by aggregating results from multiple antivirus engine scanners. Using PHP, you can create plugins for WordPress that perform real-time analysis of URLs to determine security exposure and block access to insecure sites. The method focuses on identifying suspicious transactions and domains to mitigate phishing threats effectively.

## 2. Literature Survey

This study investigates using simulated phishing attacks to increase users' cybersecurity awareness [1]. The authors designed and conducted phishing simulations to test the effectiveness of such exercises in detecting vulnerabilities. Research highlights how simulation can be a useful training tool for organizations. Key findings show a significant improvement in users' ability to detect phishing attempts after training. The study highlights the importance of continuing education in maintaining strong cybersecurity protections.

This paper examines methods and tools for detecting phishing attacks in digital environments. The authors review existing detection methods, including machine learning, heuristic analysis, and URL verification. They emphasize the importance of implementing real-time detection systems to prevent user abuse. The findings suggest that hybrid methods combining multiple methods give the best results. The study also discusses the challenges of adapting detection methods to changing phishing techniques. It concludes with recommendations for improving detection accuracy [2] and reducing false positives.

This review presents a Chrome browser extension [3] designed to detect phishing websites in real-time. The network uses machine learning algorithms and URL analysis to classify websites as safe or malicious. Its purpose is to provide additional security by alerting users to potential threats. The authors describe the methodology used, including feature extraction and model training. Research confirms the effectiveness of the extensions in reducing phishing risks.

This paper introduces a framework for real-time detection and prevention of phishing attacks in online environments. The authors propose a method that combines URL analysis, web content comparison, and heuristic methods to detect phishing sites. Their approach emphasizes seamless operation to ensure a seamless user experience while providing robust security. The test results show the system's effectiveness in detecting phishing attempts with high accuracy. The study also discusses ways to prevent users from interacting with identified

phishing sites. It concludes with recommendations for improving detection techniques [3] to combat the evolving phishing techniques.

This review presents a browser plugin that detects phishing websites using a Random Forest classifier. The plugin [4] analyzes website elements such as URLs, metadata, and page content to determine whether websites are legitimate or malicious. The authors describe in detail the methodology used, including material selection and model optimization for accuracy. The review highlights the plugin's functionality and its compatibility with existing websites. Experimental analysis shows that the plugin achieves high detection rates with few false positives. The paper concludes with recommendations for integrating plugins into a broader cybersecurity framework.

This paper introduces an improved detection system for phishing attacks in online financial transactions [5]. The authors use a hybrid approach that combines machine learning algorithms with real-time interaction monitoring to detect fraudulent activities. The system emphasizes high detection accuracy and flexibility with evolving phishing techniques. Experimental test results show significant improvement in phishing attempts with reduced false positives. The study also discusses the implementation challenges and the system's scalability for different communication systems. It concludes with insights on enhancing security in the digital payments ecosystem.

This paper provides an in-depth analysis of phishing attacks, specifically through their methods, impact and mitigation strategies. The authors will reveal its breadth and evolution by dissecting the phishing techniques of email phishing, spear phishing and deceptive websites, among others [6]. The study also attempts to assess the psychological and technical strategies used in the role of deception. It then looks at existing countermeasures in the form of spam filters, user education, and even detection tools. The authors highlight the need for further research and advanced technologies to combat the emerging phishing threat. The paper concludes with recommendations for raising awareness and improving safety measures.

Phishing attacks: a comprehensive recent review [7] and new physiology. Frontiers in Computer Science. This paper is a comprehensive analysis of phishing attacks in terms of their history, mechanisms, and impact on the world of cybersecurity. In this paper, the authors propose a new "anatomy" of phishing to break down the lifecycle of attacks from planning to execution and beyond. The effectiveness of existing detection and prevention methods is reviewed by identifying gaps in current safety strategies. The authors suggest a multi-pronged security approach and proactive measures to combat emerging threats. The paper concludes with future directions for phishing detection and mitigation research.

This comprehensive analysis examines various phishing attack techniques, including email phishing, spear phishing, and pharming. The authors review existing security measures [8], such as machine learning, browser-based plugins, and user identification systems. The strengths and limitations of these approaches are explored in dealing with phishing threats. The paper also identifies open research challenges, such as optimizing evolving methodologies and reducing false positives. According to the authors, robust solutions to anti-phishing problems necessitate a multidisciplinary approach. The study will help guide researchers seeking improvement in detecting phishing prevention measures.

This paper provides a systemic review of current methods to mitigate phishing attacks. It focuses on the methodologies' effectiveness and their various limitations [9]. The authors classify the mitigation strategies into technical solutions, user training programs, and organizational systems. They provide key findings from this study, indicating how AI and machine learning enhance search accuracy. Optimizing advanced phishing techniques to meet usability-security balance is mentioned as one of the main challenges. The authors make several

recommendations for enhancing the currently applied methodologies and suggest research directions for the future. It is yet another added valuable resource for researchers and practitioners in the field of cybersecurity.

This paper focuses on increasing phishing detection accuracy through feature selection methods. The authors explore various selection methods, such as genetic algorithms and decision trees, to identify the most suitable features for detecting phishing websites [10]. Their goal is to improve the efficiency of feature detection models and perfection by reducing available resources. The study examines the performance of these techniques in terms of detection rate and false positive reduction. The paper concludes with a recommendation to include options in phishing detection systems for more robust cybersecurity solutions.

This paper presents a rule-based method for detecting phishing attacks [11], focusing on detecting malicious websites and fraudulent emails. The authors formulate rules based on common characteristics of phishing sites, such as URL structure, content analysis, and visual cues. Their approach combines these codes to create an effective detection system to detect phishing attempts in real time. The study demonstrates the effectiveness of the rule-based method through experiments and comparisons with other detection methods. The paper highlights the value of using a lightweight and interpretable framework for phishing detection. It concludes by discussing the scalability of rule-based systems and the adaptability of developing phishing techniques.

This paper entails a detailed overview of the phishing attack and discusses evolution and its information security implications. The authors include several forms of recognition strategies that might be used, namely, based on machine learning, inference algorithms, and URL filtering. Prophylaxis measures [12]. The study reviews techniques of this nature, including multifactor systems user authentications together with email filtration tools, to assess their validity in effecting the realization of threats and identify potential issues within this approach. Lastly, the paper has ended on what is needed: an integrated and multi-layered security solution in order to possibly defeat phishing threats.

This paper discusses various types of phishing attacks [13], in particular, email phishing, spear phishing and vishing. The authors review various detection techniques, including machine learning methods, search engine optimization, and web fingerprinting. The case study points out the dynamic way of phishing techniques and obstacles in developing adaptive detection. It also discusses user awareness and security measures to prevent phishing attacks. The paper concludes with future research directions to improve the detection accuracy and reduce false positives.

The paper presents a method of detecting phishing websites through the analysis of URL objects using neural networks [14]. This proposal introduces a deep learning-based approach to classify URLs as either legitimate or phishing through the patterns found in the URL structure. Various architectures of neural networks, such as feed-forward and recurrent neural networks, are used to increase search accuracy. It compares neural performance with traditional machine learning algorithms and emphasizes methodological learning.

## 3. Phishing Detection

The Phishing Simulation Module is responsible for simulating common phishing scenarios that mimic real-world attacks. This module is critical for testing the detection system's effectiveness and training users to recognize phishing attempts.

### *3.1. URL Spoofing*

Creating fake websites that appear legitimate to device users into entering their credentials.

### *3.2. Credential Harvesting*

Mimicking login pages of popular websites to collect user credentials when they enter their information.

### *3.3. Phishing Detection Workflow*

*3.3.1. Create Website*

Creating and cloning a website, which could be a legitimate site or a phishing site.

*3.3.2. Analyze and perform Phishing Attacks*

A phishing attack is simulated by cloning an existing website. This cloned version will mimic the original site to test how users or systems detect it as a phishing attempt.

*3.3.3. Add Security Step (2FA)*

Two-factor authentication (2FA) is added to increase security. This step confirms that even if someone accesses the login page, they need an additional authentication factor, such as a code sent by the Authentication app, SMS, or email, to log in.

*3.3.4. Create Extension and Plugin to Detect Fake URLs*

A browser extension and plugin are used to detect phishing URLs or fake websites. This tool checks if a URL is safe or malicious.

*3.3.5. Fake URL*

If the extension and plugin detect a fake or malicious URL, it triggers an alert, notifying the user that the website they are trying to visit is fraudulent.

*3.3.6. Safe URL*

If the URL is verified as safe, the user is allowed to proceed and access the legitimate website.

### *3.4. Work Overflow*

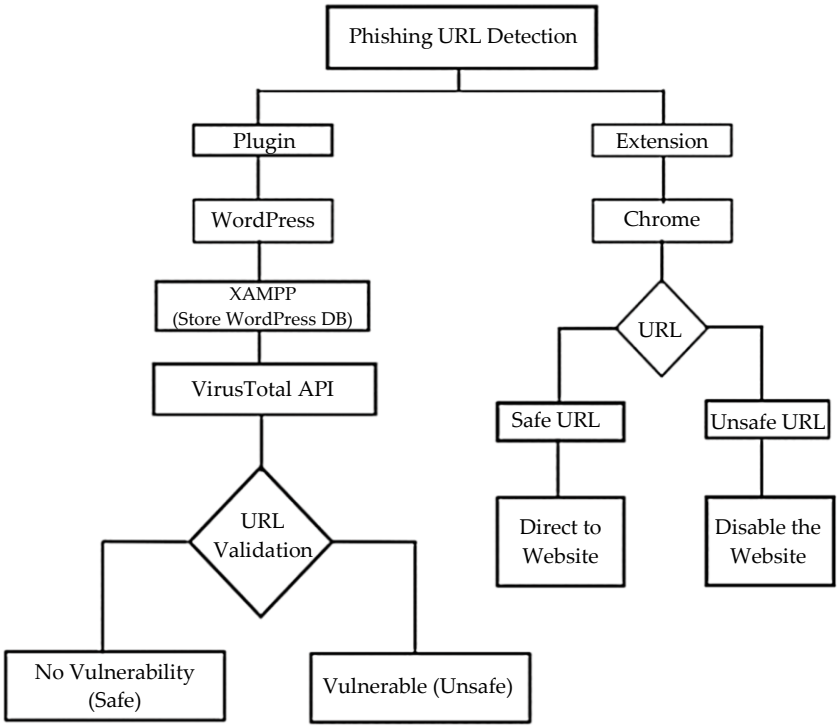


**Fig. 1 Work flow diagram**

## 4. Architecture Diagram

- Phishing Attack Practice: A special tool copies fake websites and phishing tricks to test system strength and prepare for real-life phishing problems.
- Extra Security with 2FA: Two-Factor Authentication (2FA) adds an extra step to log in safely, ensuring access is granted only to authorized individuals.
- Spotting Fake Links: A browser extension add-on or plugin searches for fake website links, sending warnings when a malicious link is detected to enhance user safety.

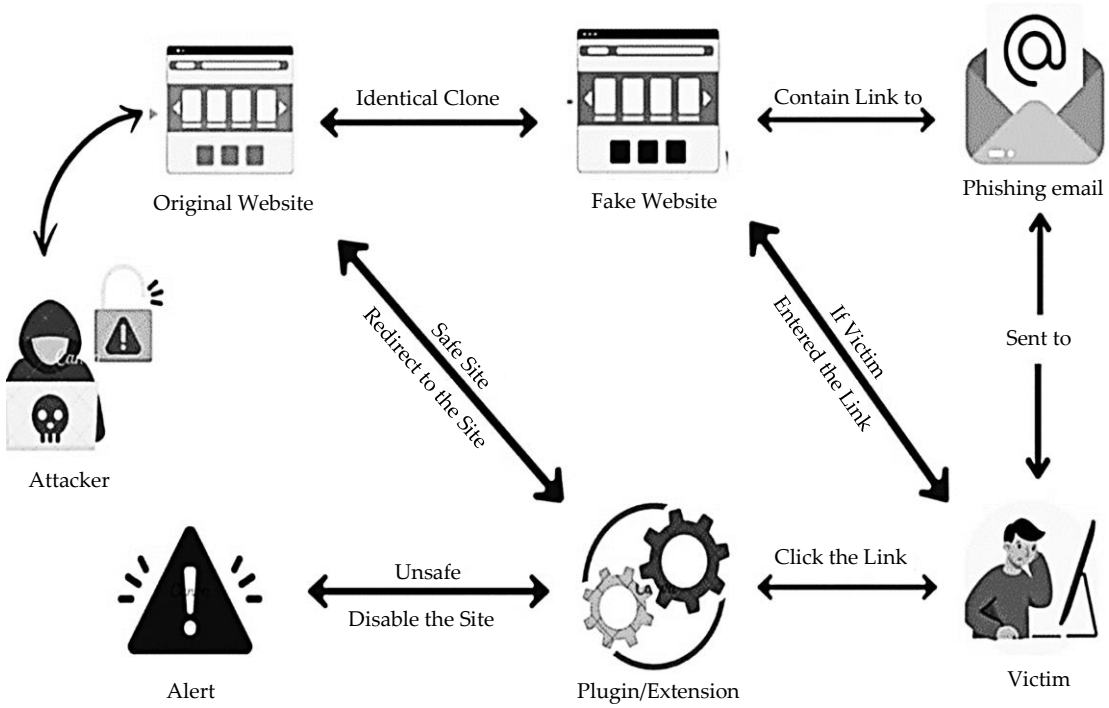


**Fig. 2 Architecture diagram**

## 5. Results and Discussions

Successfully demonstrated a system to detect and mitigate phishing attacks using pre-existing tools and techniques. Began by simulating phishing attacks by creating and testing cloned websites Figure 3, mimicking real-world phishing scenarios. Additionally, the Configuring security step Figure 7 analyses the security feature for the authentication.

Both the plugin and Chrome extension are used to detect the safety of the URL. In Figure 4, Chrome extension with javascript and JSON code is used to detect, it works when the URL is safe it redirects to the page. If it is unsafe, it will block the website. It does not allow it to enter it. The website is vulnerable to the Chrome extension; the website is validated and the website is blocked and shows the alert.

In Figure 5, a vulnerable website is tested in WordPress by activating the plugin using the server-side scripting language PHP and by using the VirusTotal API, the antivirus scanning and URL domain blocklisting services engine detects the safety of the URL, it shows the link is not safe. In Figure 6 the website is not vulnerable, showing the condition as safe.

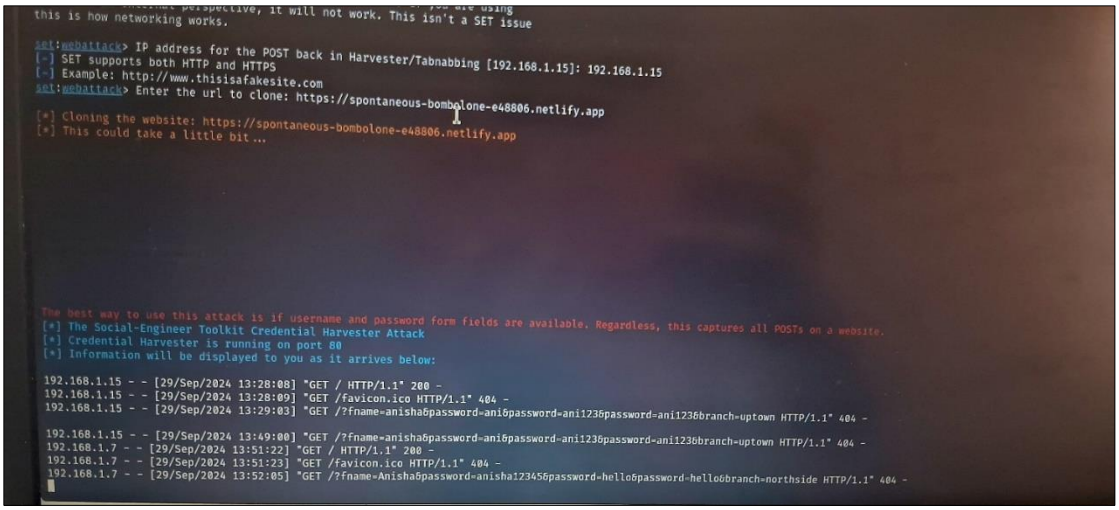


**Fig. 3 Phishing attack**

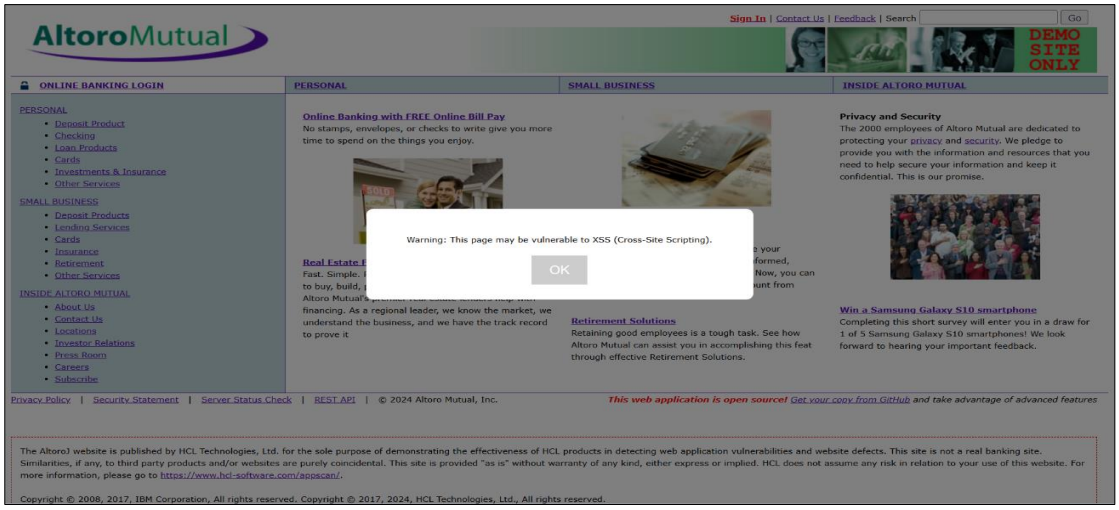


**Fig. 4 Disabled the phishing site (by using extension)**

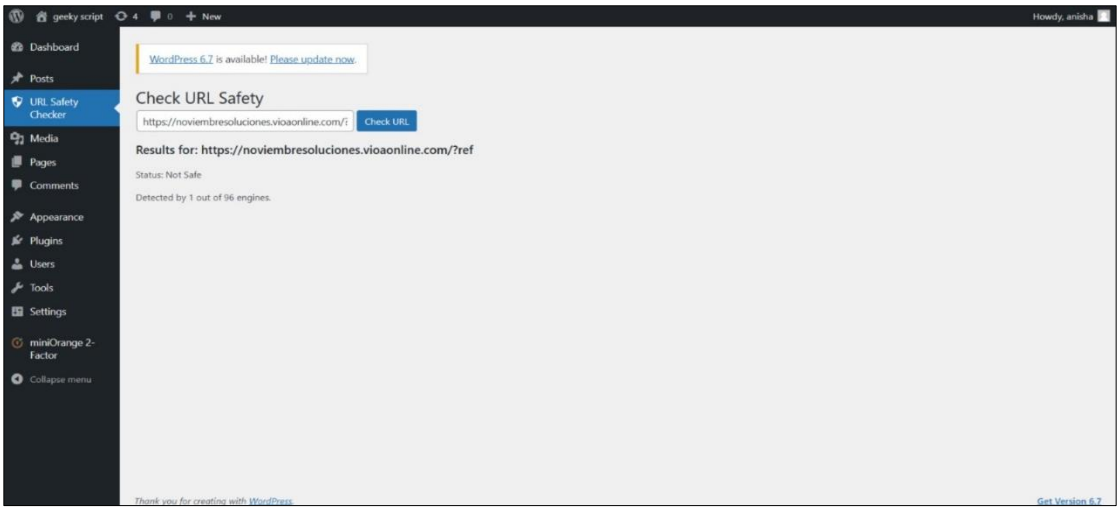


**Fig. 5 URL is unsafe (by using plugin)**

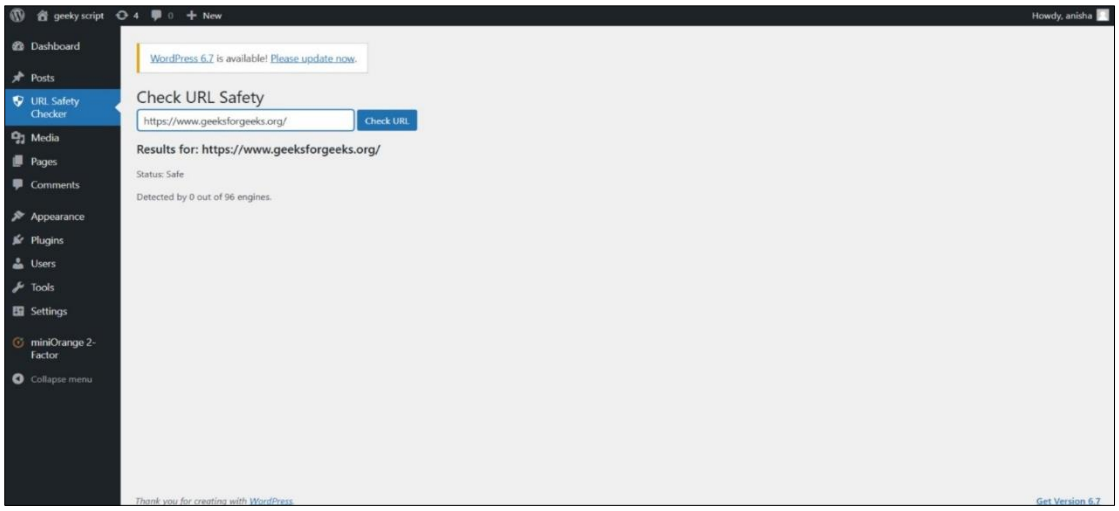


**Fig. 6 URL safe**

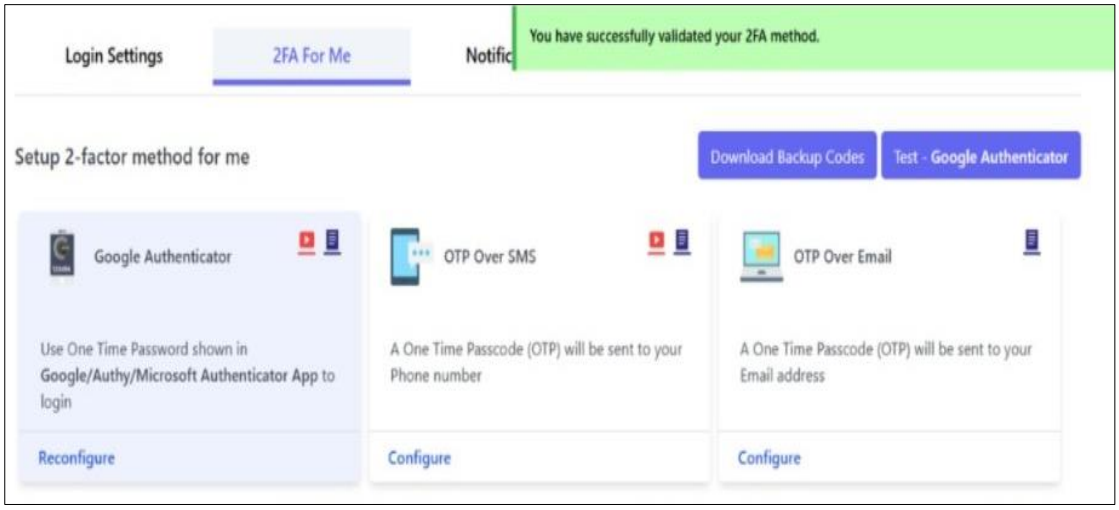


**Fig. 7 Validated 2FA method**

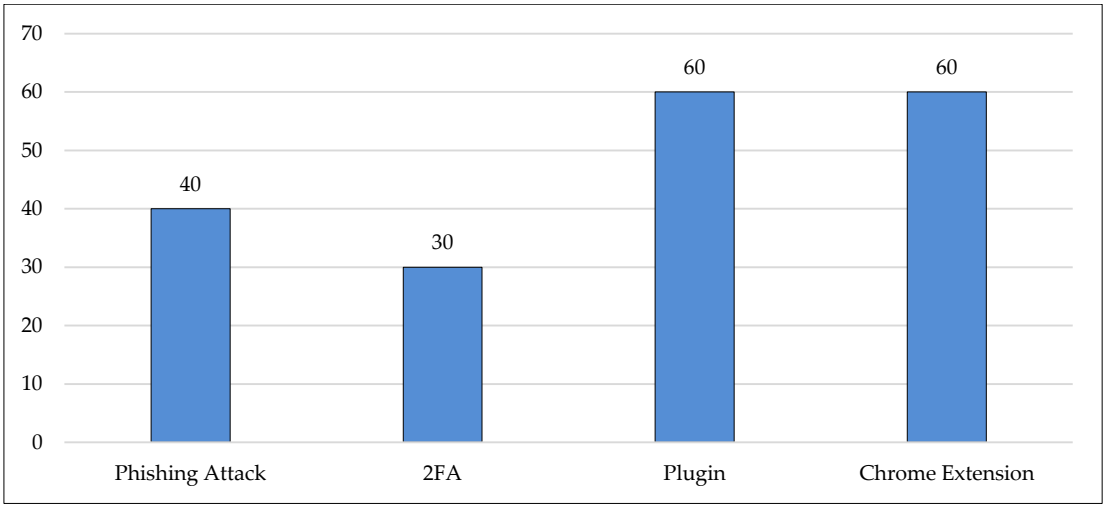


**Fig. 8 Phishing protection (security measures of phishing protection is shown in the graph)**

## 6. Conclusion and Future Enhancement

The extension detection was tested using a browser extension specifically designed to disable access to certain websites. The extension monitors and controls access to predefined websites based on their safety status. Future plans involve expanding functionality to identify phishing links and other fake URLs, enhancing protection against online threats. The extension enables the determination of URL safety by checking against a set of rules and criteria. Using the plugin and extension, the system automatically classifies URLs as safe or unsafe, providing an additional layer of security for web users.

To develop software and a web application for the plugin created in the PHP folder, start by analyzing the plugin's functionality and setting up the development environment, including a web server such as Apache or Nginx, a database like MySQL, and a code editor such as Visual Studio Code. Design the front end with HTML, CSS, and JavaScript, integrating interactivity through frameworks like React.js or plain JavaScript. Build the backend with PHP to implement core features like URL analysis, safety checks, and database interactions.

Place the PHP code in a designated folder and create APIs or function interfaces for seamless interaction. Develop features such as a URL safety checker, a reporting system, and an admin dashboard for managing data. Incorporate user authentication for secure access and add real-time updates using AJAX or WebSockets. Test the application thoroughly with tools like PHPUnit and Selenium to ensure reliability. Deploy the application on a hosting platform such as AWS or Heroku, secure it with HTTPS, and maintain it with regular updates. This approach ensures a scalable, efficient, and secure web application.

## References

[1] Surachai Chatchalermpun, and Therdpong Daengsi, "Improving Cybersecurity Awareness Using Phishing Attack Simulation," *IOP Conference Series: Materials Science and Engineering*, vol. 1088, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Muhammet Baykara, and Zahit Ziya Gürel, "Detection of Phishing Attacks," *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, Turkey, pp. 1-5, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Bhavya Shah et al., "Chrome Extension for Detecting Phishing Websites," *International Research Journal of Engineering and Technology*, vol. 7, no. 3, pp. 2958-2962, 2020. [Google Scholar] [Publisher Link]

[4] Adetokunbo MacGregor John-Otumu, Md Mahmudur Rahman, and Christiana Ugochinyere Oko, "An Efficient Phishing Website Detection Plugin Service for Existing Web Browsers Using Random Forest Classifier," *American Journal of Artificial Intelligence*, vol. 5, no. 2, pp. 66-75, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] T.O. Oyegoke, A.O. Amoo, and J. Aigberua, "An Enhanced Phishing Detection System in Online Transactions," *Twist*, vol. 19, no. 3, pp. 656-666, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] Vaishnavi Bhavsar, Aditya Kadlak, and Shabnam Sharma, "Study on Phishing Attacks," *International Journal of Computer Applications*, vol. 182, no. 3, pp. 27-29, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] Zainab Alkhalil et al., "Phishing Attacks: A Recent Comprehensive Study and A New Anatomy," *Frontiers in Computer Science*, vol. 3, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ankit Kumar Jain, and B.B. Gupta, "A Survey of Phishing Attack Techniques, Defence Mechanisms and Open Research Challenges," *Enterprise Information Systems*, vol. 16, no. 4, pp. 527-565, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Bilal Naqvi et al., "Mitigation Strategies against the Phishing Attacks: A Systematic Literature Review," *Computers & Security*, vol. 132, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Anirudha Joshi, and Tanuja R. Pattanshetti, "Phishing Attack Detection Using Feature Selection Techniques," *Proceedings of International Conference on Communication and Information Processing (ICCIP)*, pp. 1-7, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] Ram B. Basnet, Andrew H. Sung, and Quingzhong Liu, "Rule-Based Phishing Attack Detection RB Basnet," *International Conference on Security and Management*, 2011. [Google Scholar]

[12] Muhammad Nadeem et al., "Phishing Attack, its Detections and Prevention Techniques," *International Journal of Wireless Security and Networks*, vol. 1, no. 2, pp. 13-25, 2023. [Google Scholar] [Publisher Link]

[13] G. Jaspher Willsie Kathrine et al., "Variants of Phishing Attacks and their Detection Techniques," *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, pp. 255-259, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ozgur Koray Sahingoz, Saide Işılay Baykal, and Deniz Bulut, "Phishing Detection from URLs by Using Neural Networks," *Computer Science & Information Technology (CS & IT)*, pp. 41-54, 2018. [CrossRef] [Google Scholar] [Publisher Link]