Phishing and Spoofing Websites: Detection and Countermeasures

Wee Liem Lai [1], Vik Tor Goh [1+], Timothy Tzen Vun Yap [2], and Hu Ng [2]

[1] Faculty of Engineering, Multimedia University, 63100 Cyberjaya, Malaysia

[2] Faculty of Computing and Informatics, Multimedia University, 63100 Cyberjaya, Malaysia

Abstract. This project aimed to develop a multi-layered URL-based malicious website detection system to combat cyberattacks, particularly phishing and spoofing attacks. The system employed several defense mechanisms, including whitelist filtering, API requests to domain blacklist providers, and string comparison algorithms. To evaluate the system's performance, a testing phase was conducted on a dataset containing malicious and legitimate websites. The results showed a high true positive rate of 0.94 and an overall accuracy of 0.93, indicating the system's ability to accurately classify legitimate and malicious websites. The system showed promising results in accurately classifying websites and raising user awareness to prevent phishing and spoofing attacks.

Keywords: phishing attacks, domain name spoofing, user alert system, multi-layer malicious website detection model

1. Introduction

In today's interconnected digital world, phishing and spoofing attacks have become a significant threat, exploiting vulnerabilities in communication channels and posing risks to individuals and organizations. The increasing reliance on digital technologies and the surge in online activities, especially during the COVID-19 pandemic, have provided opportunities for cybercriminals to launch malicious activities. The lack of user education and awareness further contributes to the success of these attacks. To address this growing threat, a multi-layer malicious website detection system is designed and developed, incorporating various defense mechanisms to accurately identify and categorize websites as legitimate or malicious.

The main problem lies on the ignorance and lack of awareness among users regarding phishing and spoofing attacks, leading to their susceptibility to deception by malicious attackers. Users often struggle to differentiate between real and fraudulent websites due to the increasing sophistication of these attacks. Hence, this project aims to enhance user awareness and develop an effective tool for identifying and mitigating phishing and spoofing attacks. The objectives include understanding social engineering attack techniques, evaluating detection and prevention mechanisms, proposing a domain-based legitimacy algorithm, and designing a system to prevent users from accessing fraudulent websites.

[+] Corresponding author.
Tel.: +603-8312 5380; *E-mail address*: vtgoh@mmu.edu.my

2. Literature Review

2.1. Phishing Attacks

Cyber threats pose significant risks in today's interconnected digital world as communication and transactions take place predominantly over the Internet. Among all types of cyberattacks, phishing and spoofing have gained prominence due to their ability to deceive people. Phishing attacks involves malicious actors attempt to trick individuals into disclosing private information or performing specific actions by posing as trusted entities ("Phishing", 2023). The word "phishing" is derived from the analogy of fishing, where attackers cast a wide net to lure unsuspecting victims into their fraudulent schemes, similar to how a fisherman would use bait to catch fish (Singh et al., 2021).

Phishing attempts often take place through a variety of communication methods such as email, webpages, phone calls, advertisements or text messages (University of Massachusetts Amherst, n.d.). Attackers often impersonate reputable companies, government organizations or popular online services to gain trust from victims. The objective of phishing attacks is to obtain valuable information for financial gain, identity theft or unauthorized access to accounts and systems (Kathrine et al., 2019).

Phishing and spoofing are illegal and unethical in most jurisdictions as they aim to steal private information for identity theft (CyberTalk, 2022). The consequences of a successful attack are disastrous, including compromised financial and personal information, unauthorized access to critical systems, and networks breaches. Attackers are continuously adapting and utilizing more complex methods, posing significant challenges for individuals, businesses, and cybersecurity experts. Common types of phishing attacks include spear phishing, whaling, pharming, bulk phishing, vishing, and smishing. Few signs to indicate phishing email or websites (Chebac, 2023):

- The content of emails or websites contains noticeable grammatical or spelling errors, which may suggest a lack of professionalism to details.
- The text of the hyperlink and the actual URL do not match, which will redirect users to a completely different page.
- The domain of the website closely resembles a legitimate one but has slight differences, such as misspellings or added characters.
- The domain of the website does not match the name of the company or organization that the cybercriminals are attempting to impersonate.

2.2. Spoofing Attacks

Spoofing attacks are closely related with phishing and play an important role in cyberattacks. Phishing aims to steal information, while spoofing is a technique used to enhance phishing attacks by posing as trusted sources to exploit the users' trust. Various types of spoofing attacks are shown as below (Kaspersky, n.d.):

- Email Spoofing - Cybercriminal imitates trusted email address by using similar characters that to deceive users into revealing sensitive information or clicking on malicious link.
- Internet Protocol (IP) Spoofing - Manipulating the source IP address in network communications to impersonate a reliable source or bypass security measures, concealing their identity or location.
- Domain Name System (DNS) Spoofing - Manipulating DNS records to associate a legitimate domain name with a malicious IP address, tricking users into thinking they are visiting trustworthy sites.
- Link Manipulation – Altering website links in phishing attacks to mislead individuals. By modifying the destination of a link, attackers redirect users to malicious websites instead of the intended destination.
- Website Spoofing – Creating fake websites that mimic existing ones by copying their appearance,

layout and content. Victims may be directed to these fraudulent websites via phishing emails or manipulated hyperlinks, allowing attackers to steal credentials and personal information.

2.3. Impact of Phishing and Spoofing Attacks

Phishing and spoofing are social engineering attacks that pose significant threats to individuals, businesses government organizations. They expose various vulnerabilities to deceive victims and gain unauthorized access to sensitive information or systems.

The consequences of these attacks can be severe. IBM (n.d.) states that phishing is the most common cause of data breaches, with an average cost of USD 4.91 million. Attackers trick users into revealing credentials, leading to privacy violations and financial losses. Moreover, phishing attempts often aim to collect personal information for identity theft, causing financial losses, credit impairment, and emotional distress. Financial transactions are mostly targeted, providing attackers with opportunities for quick profits and unauthorized transactions that can lead to significant financial difficulties and mental repercussions. The impacts highlight the importance of vigilance, robust security measures and awareness. It is crucial for individuals and organizations to understand these threats and take steps to protect themselves from these attacks.

2.4. Preventive Measures

Preventing phishing and spoofing attacks is important to protect individuals and organizations from the risks associated with social engineering tactics. Robust security measures help protect sensitive information from falling into the hands of unwanted authorities. Implementation of antivirus software, user education, authentication mechanisms, website or email filters, and strong passwords practices can reduce the risk of falling victim to phishing. However, cyber-attacks are always adaptive to bypass existing defences, making it challenging to completely eliminate them.

2.5. Antivirus Software

Antivirus software is widely used by Internet users to secure their computers from various cyber threats, including phishing attacks. It detects and blocks malicious code by scanning files, emails, websites, and other digital content for known patterns and signatures of malware. Modern antivirus software also provides real-time protection, monitoring online activities to identify suspicious conduct. According to Hsu et al. (2012), 81% of computer users protect their devices with antivirus software.

However, the efficiency of antivirus software is limited by several factors, and it is not enough to protect users from these attacks. Attackers are constantly evolving their techniques to evade antivirus detection, and antivirus software may not able to detect new and emerging threats until updated signatures are available. Moreover, antivirus software is particularly focuses on protecting individual workstations or network servers and may not provide comprehensive security measures for other aspects of computer systems, such as network infrastructure, web applications, or human behaviour (Post & Kagan, 1998).

2.6. Website Reputation Services

Website reputation services are commonly used by individuals and organisations to evaluate the trustworthiness and safety of websites. These services rely on various algorithms and data sources to generate reputation scores for websites. Users can enter the URL or domain name into the search engine of these platforms to obtain an accurate and up-to-date reputation score (Webroot by opentext, n.d.). However, it may produce false negatives as they may fail to identify newly compromised websites that are not yet blacklisted. Additionally, these services also required users to manually visit their platforms and perform checks, which is inconvenient and negatively impact user experience.

2.7. Mutual Authentication Scheme

Mutual authentication is crucial for verifying the legitimacy of a website and ensuring the security of user credentials. It verifies the identities of both the customer and the legitimate website in order to prevent malicious actions. However, many websites currently do not provide authentication process to customer before collecting sensitive data, relying only on the password entered by users at the login page. This exposes users to phishing attacks, as fake websites are almost identical to legitimate ones, making it difficult to distinguish between them. To address this, online banking websites usually implement mutual authentication schemes. Several online financial institutions have distributed an enormous amount of security tokens to their customers in order to provide stronger mutual authentication mechanisms. The authentication schemes help customers differentiate between legitimate banking websites and fake ones (Pietro et al., 2005). Hence, implementing mutual authentication schemes is an important step in getting rid from phishing attacks by preventing financial fraud and ensuring the security of online transactions. Fig. 1 and Fig. 2 show some examples of mutual authentication scheme used by popular banking websites from Malaysia:

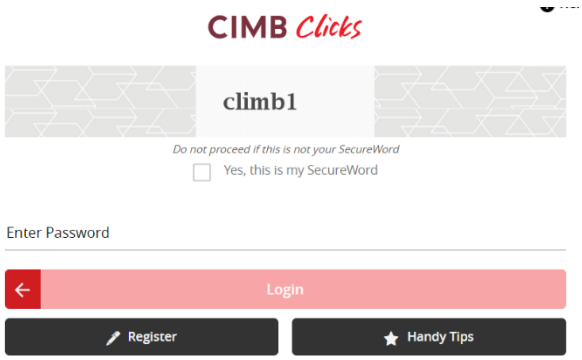

Fig. 1: SecureWord from CIMB Clicks

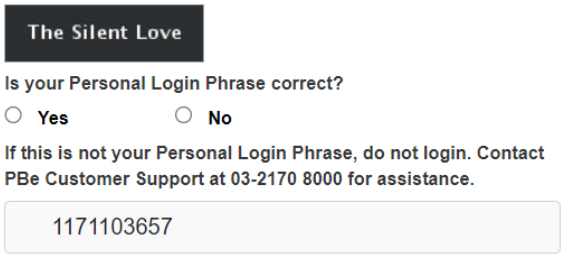

Fig. 2: Personal Login Phrase from PBe

In Malaysia, online banking websites like CIMB Clicks, Maybank2u, and PBe employ mutual authentication to help users to recognize legitimate sites. These schemes involve the use of security phrases, images, and login phrases that users choose during the login process. For example, CIMB Clicks utilizes SecureWord, Maybank2u uses Security Phrase, and PBe incorporates Personal Login Phrase. When users enter their login ID, they are directed to a second page where their chosen security phrase or image is displayed, accompanied by the message "Do not proceed if this is not your security word". This approach theoretically prevents users from sharing their credentials with cybercriminals when they accidentally visit phishing websites.

However, there is always a chance for hackers to trick users through spoofed websites. For instance, cybercriminals may replace the security image with an "under maintenance" message to deceive users. In a study conducted by Lee et al. (2014), it was found that the effectiveness of the security image in preventing phishing attacks was limited. In the experiment, 73% of participants entered their passwords even when the security image or caption were not displayed, indicating that users are often careless and unaware to small differences on websites. This highlights the necessity to develop or modify more effective schemes to better protect customers from becoming victims of cybercrime.

3. System Design and Implementation

3.1. Multi-Layer Phishing Detection Model

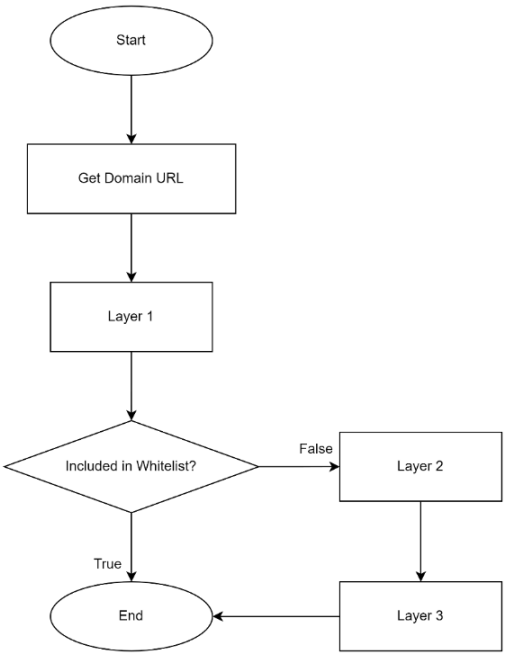

Fig. 3: Flowchart Representation of Website Detection System

Due to their adaptive nature, cyberattacks constantly evolve to bypass existing defenses, making it difficult to completely stop these attacks. Therefore, a Chrome extension with multilayer filter was developed as part of this project. This extension aims to identify and prevent phishing websites by implementing multiple layers of filters and validations. When a new tab is opened or activated, the extension performs multiple validations on the domain of current website to detect malicious activities. By utilizing multiple layers of filters, the system provides robust protection and alerts users when they unknowingly visit malicious websites. Real-time feedback is provided through messages and alarm triggered for detected malicious websites. The system consists of three distinct parts: whitelist check, API-based checks for blacklist and domain age, and domain-whitelist comparison on string similarity. Each layer carries out specific verifications and validations, gradually increasing the accuracy of the results.

A simple flowchart representing the overall function of the phishing detection system is shown in Fig. 3. The layers of phishing detection model are:

- Layer 1 – Whitelist Filter: Compares the domain with a predefined whitelist of trusted online banking websites. If the domain is not included in the whitelist, the system will automatically

proceed to the next two layers.

- Layer 2 – Domain Blacklist Filter: Make API requests to APIVoid services to check for blacklist detections and domain age data. A website is considered as malicious when it receives a high blacklist score or is relatively new.
- Layer 3 – String Comparison Filter: Compares the domain with predefined whitelist using the Levenshtein distance algorithm. If the similarity score exceeds a certain threshold, it is considered as a possible typo and suggests the intended URL.

The Chrome extension utilizes event listeners and functions to perform multi-layer phishing detection. When a new tab is opened, an event listener is triggered ad the URL of the current tab is The 'layer1' function is called to check if the domain is included in the whitelist. If it is not on the whitelist, the program proceeds to execute 'layer2' and 'layer3' functions for further validation. In 'layer2', API requests are made to APIVoid to check for domain age and blacklist detections. If the domain is identified as malicious (blacklist score >= 1 or domain age < 30 days), an alert is triggered. In 'layer3', the domain of the activated tab is compared to the whitelist based on string similarity. If the similarity score exceeds a threshold, indicating a possible typo or misspelling, an alarm is triggered.

3.2. Layer 1 – Whitelist Filter

The ‘layer1’ function performs the initial domain validation against a whitelist of 60 popular websites. It uses an if-else statement to checks if the domain is included in the whitelist array. If the domain is found in the whitelist, a message is logged stating that it is a verified website, and the program terminates. If the domain is not found in the whitelist, the function returns 'false', indicating that the domain failed in verification and suggesting that it is not a verified website from the whitelist. This allows the program to proceed to subsequent layers of verification.

Overall, 'layer1' acts as the first layer of defense by ensuring that only reputable and secure platforms listed in the whitelist are granted access. It provides an initial level of protection against potential phishing or fraudulent attempts on these websites. Users have the flexibility to modify the whitelist according to their preferences. The function's flowchart is presented in Figure 4.

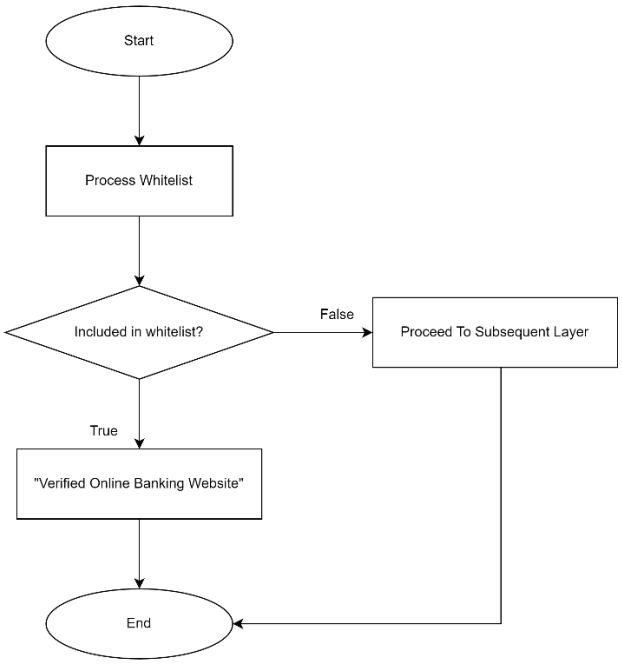

Fig. 4: Flowchart Representation of Layer 1

3.3. Layer 2 – Domain Blacklist Filter

The 'layer2' function is an asynchronous function that takes a domain as input and makes API calls to two endpoints for information about the domain. It determines if the domain is potentially malicious or secure based on the received data. This layer utilizes the APIVoid threat analysis platform to analyze cyber risks. In this layer, two APIs are used: the domain reputation API and the domain age API. The domain reputation API checks if the domain is blacklisted by 45 popular and trusted domain blacklist services, such as ThreatLog, OpenPhish, Spam404, PhishTank, and others (APIVoid, n.d.). This analysis helps identify potentially malicious websites. However, it should be noted that newly created malicious websites may not yet be blacklisted.

To address this, the domain age API is utilized to determine the age of the domain. Users can retrieve the registration date and its age in days. This information is helpful in identifying suspicious domains that were recently registered. Sytnik and Bubnov (2021) indicates that 71.4% of phishing websites stop displaying phishing activity after 30 days. Although some of them may continue their operations by converting to an IP address, the web server will no longer respond. Therefore, a threshold of 30 days is used in this project to consider a domain as potentially suspicious. The statistics on the number of active days for phishing websites are depicted in Fig. 5, illustrating the relevance of the chosen domain age threshold.

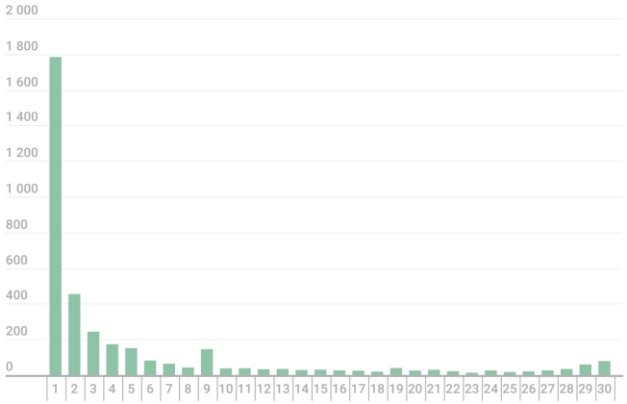

Fig. 5: Number of Active Days of a Phishing Website

The function extracts the 'score' variable from the first API response, representing the number of blacklist detections, while the 'age' variable is also assigned the domain's age in days. Next, the function checks if the 'score' is greater than or equal to 1 (indicating number of detections in blacklists) or if the 'age' is less than 30 days, which would classify the website as potentially dangerous. If either condition is met, the function logs "Malicious Website" to the console and triggers the 'onAlarmMalicious' function to initiate an alarm. Otherwise, the function logs "Safe" to the console if neither condition is met.

In summary, the 'layer2' function verifies the safety of a domain by querying the APIVoid service to examine the domain's blacklist status and age. Based on the retrieved information, it provides a simple mechanism to determine whether a website is potentially safe or harmful.

3.4. Layer 3 – String Comparison Filter

The 'layer3' function utilizes the Levenshtein Distance algorithm to compare the provided domain with a whitelist of domains and determine the similarity between them. The Levenshtein Distance, also known as the edit distance, is a metric that measures the minimum number of changes required to transform one string

into another (insertions, deletions, or substitutions). This layer stops users from mistakenly entering an erroneous domain name from the whitelist, which could lead them to unintended websites. For example, www.g00gle.com instead of www.google.com. Even though www.g00gle.com does not exist, there are still chances to unintentionally access a potential fake website with a domain name that closely resembles the real website. It serves as an additional measure to prevent users from visiting such websites.

The algorithm constructs a matrix, where the rows represent the characters from one string and the columns represent the characters from another string. The Levenshtein distance between two strings, a and b can be calculated using the formula *lev(a,b)* (Grashchenko, 2022):

$$\mathrm{lev}_{a,b}(i,j) = \begin{cases} \max(i,j) & \text{if } \min(i,j) = 0, \\ \min \begin{cases} \mathrm{lev}_{a,b}(i-1,j) + 1 \\ \mathrm{lev}_{a,b}(i,j-1) + 1 \\ \mathrm{lev}_{a,b}(i-1,j-1) + 1_{(a_i \neq b_j)} \end{cases} & \text{otherwise.} \end{cases} \quad (1)$$

The 'layer3' function compares the given domain with a whitelist of domain names using the Levenshtein Distance algorithm. It initializes an empty matrix and fills it in based on the algorithm's calculations. Then, the function iterates over the whitelist array and calculates the similarity between each element in the whitelist and the specified domain using the edit distance. The similarity is obtained by subtracting the normalized Levenshtein distance from 1. A higher similarity value indicates a closer match. If the similarity falls within a certain threshold, indicating a potential danger or suspicious domain, the function logs a warning message while triggering the alarm.

In summary, the 'layer3' function identifies potentially suspicious domains based on the detections from blacklist providers. It also provides an additional layer of protection against mistyped or misspelled domains that could lead to fraudulent websites. The function's flowchart is presented in Fig. 6.

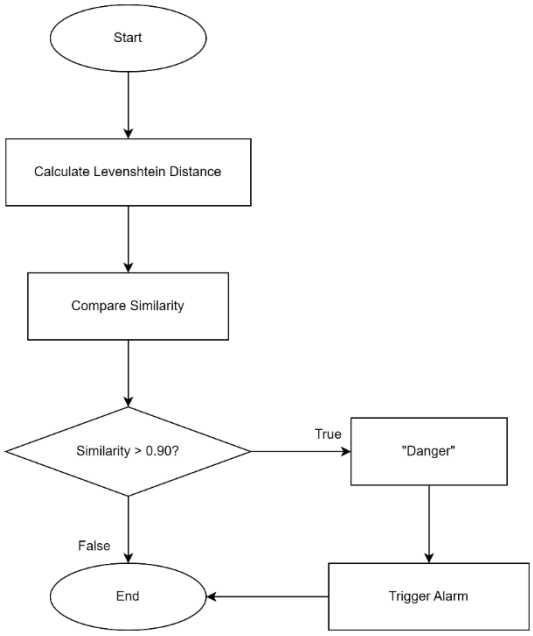

Fig. 6: Flowchart Representation of Layer 3

4. System Evaluation

4.1. Scenarios

The system involves multiple layers to evaluate the legitimacy and similarity of domains, resulting in different outcomes for various domain names. Table 1 provides a summary of the scenarios and their respective situations, illustrating the diversity of results obtained from the experiment.

Table 1: Possible outcomes on different types of domain names

Scenario	Domain	Outcome
1	www.cimbclicks.com.my	Layer 1: true (included in whitelist) - console log 'Verified Online Banking Website'
2	www.good.com	Layer 1: false (not included in whitelist) Layer 2: true (score = 0 | age > 30) Layer 3: true (similarity < 0.9) - console log 'Safe'
3	www.bad.com	Layer 1: false (not included in whitelist) Layer 2: false (score > 0 | age < 30) Layer 3: true (similarity < 0.9) - console log 'Malicious Website' - onAlarm 'Malicious Website: + URL'
4	www.c1mbclicks.com.my	Layer 1: false (not included in whitelist) Layer 2: true (score = 0 | age > 30) Layer 3: false (similarity > 0.9) - console log 'Danger! Similarity Exceed 0.9!' - onAlarm 'Are you searching for: + name'

There are four possible scenarios that can occur when the phishing detection model is applied to various URLs. These scenarios include:

- Verified Website: If the URL is on the whitelist, the model recognizes it as a verified website and logs the message "Verified Website" on its console, the process is then terminated.
- Safe Website: www.good.com represented the case of a trusted website that is not on the whitelist. If the website meets specific criteria, such as having a score equals to 1 and an age greater than 30 days, it is classified as "Safe".
- Blacklisted Website: The second layer of filtering determines that www.bad.com (analog for blacklisted websites) has a high score larger than 0 or the domain age is less than 30 days. Hence, it is classified as a malicious website. The user is warned with an alarm.
- Typo or Misspelled URL: In the case of a URL like www.c1mbclicks.com.my, which is not on the whitelist, the second layer determines it to be safe based on a low score. However, the third layer found the similarity between the URL and the whitelist exceeds the threshold, indicating a high level of similarity. This suggests that the user may have made a typographical error. An alert is triggered, providing a suggestion for the correct URL or an alternative search option.

4.2. Experimental Result

An empirical evaluation was conducted to determine the appropriate threshold value for the string comparison filter. The evaluation focused on websites from the whitelist that had multiple subdomains by comparing them with their alternative domains. For example, websites like www.google.com have more than 50 different subdomains, including news.google.com, meet.google.com, and maps.google.com.

Similarly, similar websites such as www.nba.com and www.nfl.com were also chosen for testing. By comparing the domain names that appeared to be almost identical to those on the whitelist, the results that are calculated using Equation 1 are recorded in Table 2 to determine the optimum threshold value.

Table 2: Similarity between sample domain sets

Whitelist Domain	Similar Domain	Similarity
www.google.com	one.google.com	0.786
www.google.com	news.google.com	0.8
www.google.com	docs.google.com	0.733
www.ebay.com	www.ebay.de	0.75
www.ebay.com	www.ebay.com.au	0.8
www.facebook.com	m.facebook.com	0.8125
shopee.com.my	ads.shopee.com.my	0.765
www.yahoo.com	news.yahoo.com	0.786
www.nba.com	www.nfl.com	0.818
www.espn.com	www.epsa.com	0.75

Based on the results, an optimum threshold for the string comparison filter should be set at 0.818 or higher. Therefore, a threshold of 0.85 is chosen for the filter in Layer 3. The threshold value denotes the minimum level of similarity required for a website to be considered similar to an entry in the whitelist. By setting the threshold at 0.85, it ensures that only websites with high degree of resemblance to the domain names in whitelist will trigger the alarm.

A comprehensive study was conducted to evaluate the performance of the proposed model using a diverse set of URLs in different scenarios. The goal was to assess the effectiveness and feasibility of the model in real-world phishing prevention efforts. A list of 30 unique actual websites was generated using Chat GPT to ensure an unbiased selection of samples for testing the system. These websites must be randomly distributed across all four scenarios. The results of the evaluation were carefully recorded to assess the accuracy and effectiveness of each layer within the model for detecting phishing websites.

- True Positive (TP): Refers to the cases where the system accurately identifies malicious websites, which align perfectly with the function of the system.
- True Negative (TN): Describes situations in which the system identifies positive events which represented the success of model in accurately identifying a legitimate website.
- False Positive (FP): Describes instances where the model incorrectly identifies positive events as negative. It indicated that the model misidentified a legitimate website as malicious.
- False Negative (FN): Refers to situations where the model mistakenly identifies negative events as positive. It indicated that the model fails to detect malicious website and incorrectly classifies them as legitimate.

Table 3: Test results for random set of domains

Domain	Scenario	Result	Domain	Scenario	Result
www.microsoft.com	2	TN	www.maybank3u.com.my	4	TP
www.speshbabies.com	3	TP	www.citycredito.com	3	T

www.alimama.com	4	TP	www.ethereumchest.net	3	TP
www.hashmap.tw	3	TP	www.linkedin.com	1	TN
www.freepik8888.com	4	FP	www.twitt3r.com	4	TP
www.instagram.com	1	TN	www.ikea.com	2	TN
zoom.us	1	TN	www.quora.com	1	TN
todayjournal.net	1	TN	greedyfines.org	3	TP
www.oracle.com	2	TN	www.rnudah.my	2	FN
www.malaysiaairlines.cow	4	TP	woow.spotify.com	4	TP
www.netflix.com	1	TN	metamaskofficial.xyz	3	TP
davivienda.shop	3	TP	shopee.com.my	1	TN

Table 3 displays a list of samples along with their corresponding scenarios and the results obtained from the phishing detection system. It reveals that the rates for each scenario are evenly distributed among the 30 samples, as there are no significant variations observed in the line graph. As for the classifications, there were 16 true positives (TP), indicating that 12 websites were correctly identified as malicious by Layers 2 and 3. This demonstrates the system's ability to accurately recognize malicious websites. Additionally, there were 12 true negatives (TN), indicating that the system correctly identified 12 websites as safe. However, it should be noted that there was one false positive (FP) and one false negative (FN) in the results.

The system's performance is evaluated based on its accuracy in identifying different domain names across various scenarios. From the obtained results, the system achieved a true positive rate (TPR) of 0.94. This indicates that 94% of the actual negative cases in the dataset were correctly classified as malicious by the system. A high TPR demonstrates the system's effectiveness in detecting malicious websites. Furthermore, the overall accuracy of the system is calculated to be 0.93. This suggests that the system is accurately categorizing websites with a high level of accuracy across all scenarios.

5. Conclusion

In conclusion, the phishing detection system developed in this project demonstrated its effectiveness in mitigating the risks associated with cyber-attacks and social engineering tactics. By incorporating multiple layers of filtering and employing techniques such as domain similarity and string comparison, the system achieved a high level of accuracy in identifying malicious websites. The evaluation results showed a true positive rate of 0.94 and an overall accuracy of 0.93, indicating the system's ability to successfully detect and distinguish between legitimate and malicious websites.

However, certain challenges were encountered in identifying specific websites, which highlighted the need for continuous improvements. Factors such as the threshold value used in the string comparison filter and unexpected outcomes during API requests impacted the system's performance. Therefore, future research could explore additional features and patterns, such as webpage content analysis, HTML attribute examination, or visual element detection, to enhance the accuracy and effectiveness of the system. Additionally, the development of real-time analysis techniques that dynamically monitor and assess website behaviour can enable the system to adapt to emerging threats and detect new variations of malicious websites.

By leveraging techniques like network traffic analysis and behavioural monitoring, the system can provide a more comprehensive understanding of website activities and detect any changes that may indicate malicious intent. This dynamic approach would improve the system's ability to detect sophisticated phishing

attempts and overcome traditional detection methods. Continued research and development in these areas will contribute to the ongoing efforts in preventing phishing and spoofing attacks and safeguarding users' online security.

6. Acknowledgements

The researchers sincerely appreciate and express gratitude for financial support from the Ministry of Higher Education, Malaysia, under the Fundamental Research Grant Scheme with grant number FRGS/1/2022/ICT07/MMU/03/1.

7. References

Alghamdi, H. (2017). Can phishing education enable users to recognize phishing attacks? Masters dissertation, Technological University Dublin. https://doi.org/10.21427/D7DK8T

Chebac, A. (2023, March 2). *What is clone phishing? Definition, examples, and prevention measures*. Heimdal Security Blog. [Online]. Available: https://heimdalsecurity.com/blog/what-is-clone-phishing/. [Accessed: 29-May-2023]

Cost of a data breach 2022. (n.d.). *IBM*. [Online]. Available: https://www.ibm.com/reports/data-breach. [Accessed: 4-June-2023]

Grashchenko, S. (2022). Levenshtein distance computation. *Baeldung on Computer Science*. [Online]. Available: https://www.baeldung.com/cs/levenshtein-distance-computation. [Accessed: 28-May-2023]

Hsu, F. -H., Wu, M. -H., Tso, C. -K., Hsu, C, -H, & Chen, C. -W. (2012). Antivirus software shield against antivirus terminators. *IEEE Transactions on Information Forensics and Security*, *7*(5), 1439–1447. https://doi.org/10.1109/TIFS.2012.2206028

Is phishing illegal? (2022, March 3). *CyberTalk*. [Online]. Available: https://www.cybertalk.org/is-phishing-illegal/. [Accessed: 27-May-2023]

Kathrine, G. J. W., Praise, P. M., Rose, A. A., & Kalaivani, E. C. (2019). Variants of phishing attacks and their detection techniques. In *3rd International Conference on Trends in Electronics and Informatics (ICOEI 2019)*, 255–259. https://doi.org/10.1109/icoei.2019.8862697

Lee, J., Bauer, L., & Mazurek, M. L. (2014). The effectiveness of security images in internet banking. *IEEE Internet Computing*, *19*(1), 54–62. https://doi.org/10.1109/MIC.2014.108

Phishing. (2023, June 22). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Phishing&oldid=1161426423

Phishing: Fraudulent emails, text messages, phone calls & social media. (n.d.). *University of Massachusetts Amherst*. [Online]. Available: https://www.umass.edu/it/security/phishing-fraudulent-emails-text-messages-phone-calls. [Accessed: 26-May-2023]

Pietro, R. D., Me, G., & Strangio, M. A. (2005). A two-factor mobile authentication scheme for secure financial transactions. In *International Conference on Mobile Business (ICMB 2005)*, 28–34. https://doi.org/10.1109/ICMB.2005.12

Post, G. & Kagan, A. (1998). The use and effectiveness of anti-virus software. *Computers & Security*, *17*(7), 589–599. https://doi.org/10.1016/S0167-4048(99)80059-5

Singh, N., Thrushitha, L., & Reddy, J. M. (2021). Detection and Prevention of Phishing Attacks. *ResearchGate*. Available: https://www.researchgate.net/publication/356633067_DETECTION_AND_PREVENTATION_OF_PHISHING_ATTACKS. [Accessed: 26-May-2023]

Sytnik, M. & Bubnov, E. (2021). An analysis of the life cycle of phishing and scam pages. *Securelist English Global Securelistcom*. [Online]. Available: https://securelist.com/phishing-page-life-cycle/105171/. [Accessed: 5-June-2023]

Threat analysis APIs for threat detection & prevention: Apivoid. (n.d.). *APIVoid.com*. [Online]. www.apivoid.com/. [Accessed:25-May-2023]

What is spoofing – Definition and explanation. (n.d.). *Kaspersky*. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/spoofing. [Accessed: 24-May-2023]

What is web reputation? (n.d.). *Webroot by opentext*. [Online]. Available: https://www.webroot.com/us/en/resources/glossary/what-is-web-reputation. [Accessed: 28-May-2023]