Journal of
Cyber Security

Tech Science Press

DOI: 10.32604/jcs.2023.043359

ARTICLE

Detecting Phishing Using a Multi-Layered Social Engineering Framework

Kofi Sarpong Adu-Manu* **and Richard Kwasi Ahiable**

Department of Computer Science, University of Ghana, Legon-Accra, +233, Ghana

*Corresponding Author: Kofi Sarpong Adu-Manu. Email: ksadu-manu@ug.edu.gh

Received: 30 June 2023 Accepted: 15 September 2023 Published: 19 October 2023

ABSTRACT

As businesses develop and expand with a significant volume of data, data protection and privacy become increasingly important. Research has shown a tremendous increase in phishing activities during and after COVID-19. This research aimed to improve the existing approaches to detecting phishing activities on the internet. We designed a multi-layered phish detection algorithm to detect and prevent phishing applications on the internet using URLs. In the algorithm, we considered technical dimensions of phishing attack prevention and mitigation on the internet. In our approach, we merge, Phishtank, Blacklist, Blocklist, and Whitelist to form our framework. A web application system and browser extension were developed to implement the algorithm. The multi-layer phish detector evaluated ten thousand URLs gathered randomly from the internet (five thousand phishing and five thousand legitimate URLs). The system was estimated to detect levels of accuracy, true-positive and false-positive values. The system level accuracy was recorded to be 98.16%. Approximately 49.6% of the websites were detected as illegitimate, whilst 49.8% were seen as legitimate.

KEYWORDS

Phishing; social engineering; multi-layer framework; data protection; privacy

1 Introduction

As businesses develop and expand with a significant volume of data, data protection and privacy become increasingly important. Research has shown a tremendous increase in phishing activities during and after COVID-19; therefore, this research needs to be conducted. Over the years, the number of phishing sites has grown massively from 138,328 (as of the fourth quarter of 2018) to 1,097,811 (as of the second quarter of 2022). Perpetrators have developed new methods of utilizing social networks and mobile devices to gather data on their victims and analyze and use the data on phishing-associated victims [1,2,3]. Phishing is mentioned severally in the scientific literature, often heard in the media domain, and widely mentioned among organizations, banks and law enforcement agencies due to the harmful effects the act brings upon such organizations and individuals [4]. Phishing is classified as a scalable act of deception whereby an attacker, under the mask of another person, tries to obtain helpful information from a user within an information system [3,5]. According to research, phishing is the most pervasive among the leading social engineering techniques aimed at hacking information from users [6]. Typically, phishing attack approaches are predominant on Android and iOS systems through social media [7,8].

A phishing attack aims to manipulate the weakest part of a user of an information system to reveal valuable information or access a restricted area. Most phishing attacks occur online through websites and web applications [9]. Fig. 1 depicts an attacker using a phishing technique to reveal valuable information from a potential victim through the internet. For these reasons, it is critical to distinguish between genuine and phishing websites to develop measures to limit security hazards to both individuals and organizations.

Figure 1: The act of phishing

These threats begin when a single breach of concealment is accompanied by a slew of intimidations, resulting in unlawful financial transactions and organizational losses. Therefore, a multi-layered phish detector system was designed to evaluate the algorithm. Phishing activities on the internet have caused individuals and organizations financial loss, identity theft, loss of intellectual property, disruption of business activities and many more. Meanwhile, phishing detection techniques have a low detection rate and a high proportion of false alarms, mainly when new phishing strategies are used (site). Furthermore, the most often used technologies, Blacklist-based detection and PhishTank are ineffective at responding to newly discovered phishing attempts. Moreover, because of the ease with which new domains can be registered, no comprehensive Blacklist can ensure that its database will always be up to date [8]. Research has shown how massive the general phishing activities on the internet have increased since the outbreak of COVID-19 [9,10]. According to APWG, phishing activities on the internet have increased almost exponentially each year since the beginning of COVID-19 (2019), represented in Figs. 2 and 3.

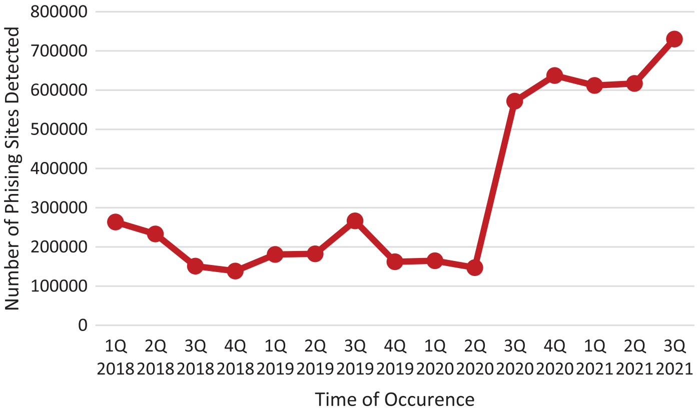


Figure 2: Phishing trends from 2018 to the third quarter of 2021

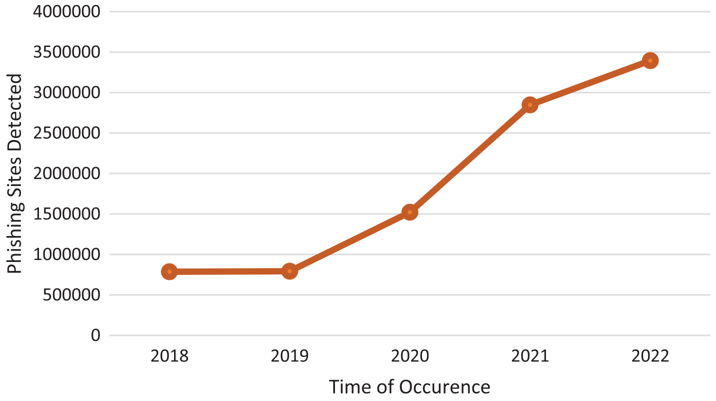


Figure 3: Phishing trends from 2018 to the second quarter of 2022

The number of new phishing emails intruders create each year has also increased (2019–2020) but has dropped in recent years, as shown in Figs. 4 and 5. The attackers do not border creating new emails but use existing emails for a successful phishing attack. The attacks are mainly focused on SaaS and Email.

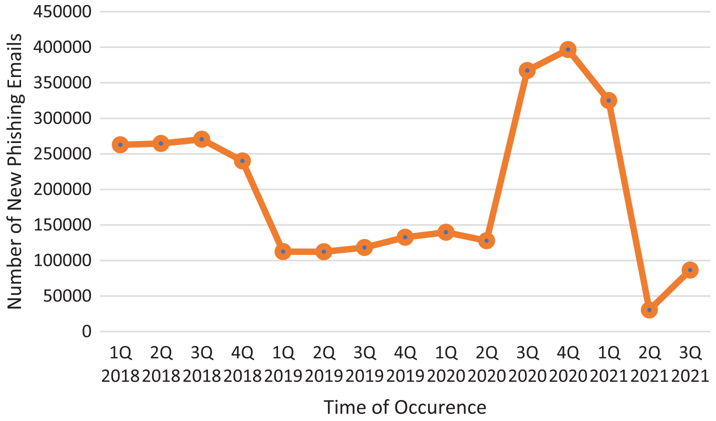


Figure 4: Number of new phishing emails created from 2018 to the third quarter of 2021

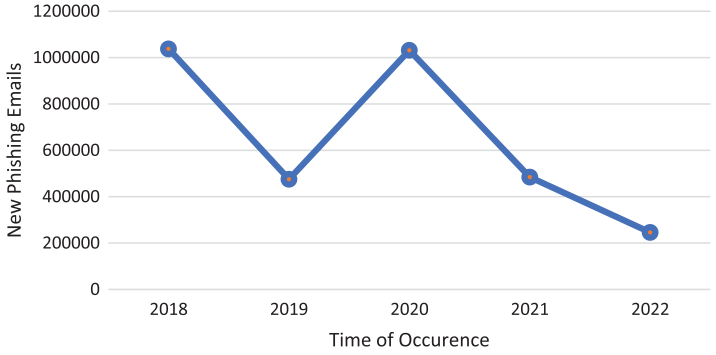


Figure 5: New phishing emails created from 2018 to the second quarter of 2022

Our contributions for merging Blacklist, Blocklist, and PhishTank to detect phishing involve the development of a more complete and adequate approach to detecting and stopping phishing attacks. By combining these strategies, we propose a framework to provide a more robust and accurate means of recognizing and restricting access to dangerous websites or content that may be exploited to deliver phishing attacks. Blacklists and Blocklists are databases that contain known unsafe URLs or IP addresses and can be used to prevent access to potentially harmful websites or material. Phishtank is a collaborative repository for phishing data and information on the Internet. By combining these strategies, our proposed framework can detect phishing websites and emails more effectively, lowering the risk of a successful phishing attack.

2 Related Works

Several research works have been done to increase the effectiveness and quality of phishing detection approaches to stop phishing activities on the internet. Still, none was able to zero down the ineffectiveness. Table 1 describes recent works, categorized according to their underlying techniques of phishing detection on the internet, their accuracy, and limitations. The most popular methodologies in detecting and preventing phishing attacks techniques have been categorized into social, technical and socio-technical [10,11].

Table 1: Categorization of related works

Underlying technique	Proposed solution	Limitations	References
Machine learning	Using computer vision/Artificial intelligence (Machine Learning: Artificial neural network, Deep Learning, Natural Language Processing, Convolutional Neural Network, Random Forest)	According to the literature, this approach is the most trending approach in technically detecting phishing activities. This is because it is versatile and relies on a classification algorithm. Even though this approach is versatile, it is still not a 100% solution for attack mitigation simply because the attack is human-centred, not machine-centred—the levels of accuracy range from 92.0 to 99.68. The algorithms can only mimic the behavioural pattern of humans up to a certain level. Furthermore, the algorithms often classify the suspicious websites and replicate them when the new suspected website is to be authenticated. Due to the evolving nature of phishing attacks, the previous knowledge learned by the approach is ineffective.	[1,4,12–18]

(Continued)

Table 1 (continued)

Underlying technique	Proposed solution	Limitations	References
Blacklist/Whitelist/ Blocklist/Phishtank	Data repository for reported phishing cases	These domains are noted for producing information about reported phishing cases with an accuracy of 94.8%. The problem is that the data produced by these domains are scattered. For example, one domain can record a website as a phishing website, and the other might not have any information. This will make the user find detection very difficult. The suspected website is not reported to the domain when the user reports the issue. When a new suspected website is submitted for verification, the return time for feedback is heart-breaking.	[8,19–24]
Web structure/content	Matching the content on web pages to others	Web content and the similarity approach work well with phishing attacks that impersonate other pages. However, the method might not detect phishing attacks that use their web content and structure it up to standard. The approach might also detect genuine domains with similar structure and content to other genuine websites as illegitimate.	[1,3,25–27]
URL similarity	Comparing the URL of suspicious web pages to legitimate ones	URL similarity approach works well with phishing attacks that impersonate other web addresses by imitating their uniform resource name. The method does not detect phishing attacks using unique, consistent resource names. The approach is also likely to report similar but legitimate websites as phishing websites.	[25,28]

(Continued)

Table 1 (continued)

Underlying technique	Proposed solution	Limitations	References
Web access log.	Matching the URL of web pages to the access log the server provides	This approach is practical to users on the same server where the access log has been generated. The process will record newly registered domains as phishing domains for the first time. For the approach to be practical, the data must be a web access log collected from all web servers. Also, the method can continue to detect illegitimate websites as legitimate if the domain is recorded in the access log.	[15,25,29–31]
Multi-layer	Authors combined two or more system interventions with user intervention	This approach seems to be the perfect approach to phish detection. It combines technical and user interventions. When combined, the problem is which strategies will be the best solution. Even though only a few works were done using this approach, the combination does not produce a more effective solution. However, it is foreseen that improving this approach will eliminate phishing attacks.	[14,24,32–34]
Hybrid	Authors combined two or more approaches	The approach combines two or more machine learning algorithms and a phishing mitigation approach to make the classification more effective in detecting phishing. However, the method does not involve solutions that protect the human (user interventions).	[15,18,32,35]

2.1 Social Approach to Phishing

The social approach is considered a human-centred intervention. Phishing detection and prevention solutions designed with this concept focus on protection mechanisms against user manipulations rather than direct system manipulations. The social approach makes available to the user ways to protect themselves and the consequences if users fail to protect themselves [9,10,36–38]. The social approach focuses on the following to ensure users are protected from phishing scams:

- Educate and train users during and after recruitment on cybersecurity traits and vulnerabilities.

- Ensure technical procedures are implemented to restrict users from actions that make them vulnerable to social engineering attacks.
- Ensure the existence of solid network protection with a *Blacklist* of suspected websites and a *Whitelist* of all website's users can access.
- Ensure frequent cyber security audits and updates of software and information. This action will uproot most loopholes intruders might have in the system.

Despite the rigorousness and effectiveness of the social technique, intruders still find their way into manipulating the users due to the evolving nature of phishing attacks and the state of mind of the user at the time of the attack [11]. In work done by Wash, 2020 to find expected solutions to phishing attack detection, the author discovered that even with education and training, users can still fall victim to the attack. Therefore, he advised improving education and training [11]. It was also found out by Jin-Hee and Hasan in their work on personality traits and phishing analysis that although openness and conscientiousness are a eager influence in phishing, agreeableness and neuroticism have a considerably strong influence on perceived trust and risk, as well as decision performance [39]. Furthermore, users may develop a habit of clicking and sharing links on their social media pages, like posts, copying and pasting messages, and uploading and downloading media assets due to the continual updating of information on social networking sites, leading to information overload. This is because users do not cognitively evaluate communications with a security lens. As a result of this behavioural priming, they become more vulnerable to social engineering assaults on social networks [40].

2.2 Technical Approach to Phishing

A handful of work has been done to provide a technical solution to combat phishing attacks [41]. According to the literature, there are currently nine different ways in which mitigation mechanisms are developed to combat these phishing attacks on the internet. These are Web Content Similarity, Web Structure Similarity, Web Access Log, Domain Blacklist, Domain Blocklist, Domain Whitelist, URL Similarity, Phishtank and Machine Learning. Unfortunately, despite their accuracy, some of these recommended mitigation approaches require complicated calculations, robust configurations and skills, making them difficult for users' free use [23,34].

2.2.1 Machine Learning (ML)

According to the literature, the ML approach is the most common of all techniques proposed for detecting phishing activities on the internet through system intervention because of its versatile nature and the classification algorithm it utilizes. Moruf and Khin used a convolutional neural network and long short-term memory machine learning algorithms to build a classification scheme to detect phishing activities on the internet. The results showed that the model achieved an accuracy of 93% and an average detection time of 25 s [16]. Adebowale and Hossain also used the same set of algorithms and got an accuracy rate of 93.28% [14]. Even though this approach is versatile, it is still not a 100% solution for phishing attack prevention simply because phishing attack techniques are human-centred ways of intruding systems, individuals, and organizations, not machine-centred. Machine learning algorithms can only mimic the behavioural patterns of humans up to a certain level. For example, the user can be affected by personality traits (Greed, Fear, Curiosity and Mesmerise, Sympathy and Empathy, and Excitement), but the algorithm will not [12,39]. Most often, the algorithms classify the suspicious websites and replicate the classification pattern when the new suspected website is to be authenticated. Due to the evolving nature of phishing attacks, the previous knowledge learned by the approach is ineffective.

2.2.2 Blacklist/Whitelist/Blocklist/Phishtank

These domains are designed to produce information about reported phishing cases. Phishtank gives scan results after a rigorous examination by experts in the Phishtank community and on confirmed reported phishing cases. Blacklists, Whitelist and Blocklist also provide results on confirmed detected and reported phishing cases. The problem with these phishing detector domains is that the information produced by these domains is scattered on different web servers [8]. One domain can record a suspected website as a phishing website, and the other might not have any information about it. The scatted nature of information from this domain makes using these systems complicated for users in preventing and detecting phishing activities on the internet [25]. On the other hand, the return time for feedback when a new suspected website is submitted for verification is heart-breaking [8,19–23].

2.2.3 Web Structure/Content Similarity

The web content and structure similarity approach works well with phishing attacks that impersonate other web pages [42]. This approach is best for detecting websites constructed with the same phishing tool [25]. The approach might not detect phishing attacks that use their fraudulent web content and structure the content on the webpage up to standard. The approach might also see domains that are genuine but have similarities in their structure and content with other genuine websites as illegitimate [1,3,25,26,43]. Tanaka et al. used the web structure similarity methodology of phishing detection and prevention in detecting new websites on the internet [25]. In their search, they discovered that phishing websites designed by the same phishing tool have the same web structure, so they compared the web structure of suspected phishing websites to determine illegitimacy. This method can detect phishing websites that have not been Blacklisted or registered in PhishTank or Blacklist [25]. Another way to use this phishing-detecting methodology is to test and check the HTML codes to authenticate the visual similarities. This approach was evaluated by testing with 5500 suspected web pages collected from compromised websites. The system has proven to detect 99% of the dataset [44].

2.2.4 ULR Similarity

The URL similarity approach works well with phishing attacks impersonating other web addresses by imitating their uniform resource name. This detection can also detect phishing websites not yet reported to any domain (Phishtank, Blocklist, Blacklist, Whitelist) [42]. The limitation of this approach is that the system does not detect phishing websites that use their own unique uniform resource names. However, the approach is also likely to report legitimate websites with URLs similar to phishing ones [25,28,45].

2.2.5 Web Access Log

This approach is practical for users on the same server where the access log is generated. The system will record newly registered domains as phishing domains for the first time. For the approach to be effective, the data must be a web access log collected from all web servers. Also, the system can continue to detect illegitimate websites as legitimate if the domain should be once recorded in the access log [15,25,29–31].

2.2.6 Hybrid

This approach to phishing detection combines machine learning algorithms and two or more phishing mitigation approaches. This makes the classification more robust and increases the accuracy of detecting phishing activities. However, the approach does not involve solutions that protect the human (user interventions) from the attack since the attack is directed at the user, not the system [15,18,32,35]. Unfortunately, all the software and advice the writers and developers provide are not effective enough to stop phishing attacks; they only control their effects and minimize the attack's success [11]. Moruf Akin used a convolutional neural network and long short-term memory to create an intelligent phishing detection algorithm to detect phishing websites using their URL. The algorithm attains an accuracy of 93.28% at an average detection time of 25 s.

2.3 Socio-Technical

This form of solution to phishing attack prevention and detection is meant to be multi-layer; that is, it incorporates user interventions (Social) and system interventions (Technical). By visual inspection, the approach seems to be the perfect approach to phish detection. It protects users from phishing attacks through social means (for example, educating and training the user) and technical standards (using software and other technologies). Even though only a few works were done using this approach, the combination seems not to produce a more effective solution due to human nature and the evolving nature of the attack. However, it is foreseen that improving the approach will eliminate phishing attacks in general [14,24,32–34].

3 Methodology

In this research work, we explore the existing approaches and techniques employed to detect phishing activities on the internet. According to the literature, nine (9) different methods are currently proposed to detect phishing activities [24,46]. These include Domain Blacklist, Uniform Resource Locator (URL) Similarity, Web Structure Similarity, Web Access Logs, Domain Block List, PhishTank, Machine Learning, and Screenshot Similarity. If only one of the mentioned approaches were to be perfect, there would not be a cause for this research. These techniques have limitations because phishing activities constantly evolve, requiring a study to be conducted. Therefore, the study will focus on a combination of four existing approaches to detecting phishing activities on the internet in this research work. The researchers have combined the existing approaches so that the other varieties will encounter imperfection in one direction. The researcher will have combined Domain Blacklist, Domain Blocklist, PhishTank and Domain Whitelist as stipulated in the multi-layer phishing detector architecture in Fig. 6.

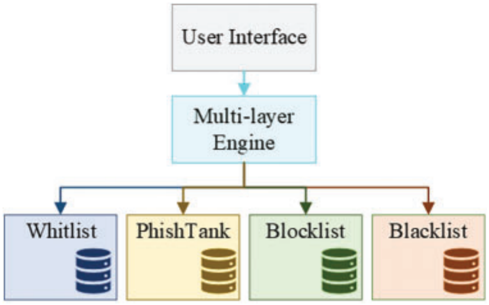


Figure 6: Phish detector architecture diagram

After the design of the multi-layer approach and its algorithm, the researchers will test the effectiveness and efficiency of the new techniques using unified modelling language. The proposed system will be developed using rapid application development tools, for example, the agile method. The researcher will investigate the system's requirements, the hardware and software requirements and the level of computer literacy a user needs to gain while operating the system. The solution proposed would be integrated into browsers and implemented in a web application. The web application because the researcher assumes that web applications can be accessed using the desktop, mobile phone, and most PDAs (Personal Digital Assistants), making the application accessible through these platforms as well. Also, it will make the system accessible everywhere and anytime since it will be in the cloud. Users do not have to go through any stress in case of a system upgrade.

Our strategy of combining PhishTank, Blacklist, Blocklist, and Whitelists to construct a phishing detection system may assist in preventing zero-day attacks. Zero-day attacks target vulnerabilities in software or procedures that the vendor or user is unaware of and for which no patch is available. Traditional signature-based security methods make detecting and preventing these attacks difficult. Cybercriminals frequently utilize phishing as an attack vector to deploy zero-day exploits. Our approach potentially increases the detection of phishing websites and emails by combining PhishTank, blacklist, Blocklist, and whitelists, reducing the risk of a successful zero-day attack. Our framework provides a more comprehensive and successful strategy for identifying and stopping phishing attempts by integrating the techniques. This helps reduce the likelihood of a successful zero-day attack by blocking access to malicious websites or content that may deliver zero-day exploits. Our approach targeted more than one domain for detection, making URL authentication more robust and efficient than just one domain (PhishTank). Our approach relieves users of the stress of looking for other domains when one domain fails. Our approach authenticates the URLs with all the selected techniques before the user receives feedback. The approach works independently of any web browser security features. As evaluated, the approach works well on Google Chrome, Mozilla Firefox, Maxthon, Opera, Microsoft Edge, and Internet Explorer.

4 Multi-Layer Approach: Algorithm and Design

In this section, a detailed description of the proposed solution is discussed. The multi-layer approach considers the strengths and weaknesses of existing phish-detecting algorithms (Blockilst, Blacklist, Phishtank and Whitelist) from different perspectives. These mentioned selected strategies have the capability of collecting data on phishing activities on the internet. These data are stored in their respective databases and accessible to users on the internet. The disadvantage of these selected approaches is that they do not have a unified database. This makes it difficult for users to get a valid and best solution to determining whether a website or an email is phishing or not phishing. For example, if a suspected phishing website is registered in the domain blocklist for being a phishing website and a user who knows nothing about the Blocklist went authenticates the link in the domain Blacklist where the link is not yet reported as a phishing website for the platform to register. This action will then mislead the user into believing that the suspected website is authentic. This problem applies to Domain Blacklist, PhishTank, and Domain Whitelist platforms as well. It is for this reason that in this work, a combination of the four approaches in conjunction has been designed in a multi-layer framework to curb phishing activities. This will make URL authentication easy and more effective for the users. Also, users will not have to move from approach to approach; there will be efficient utilization of time surfing the internet and authenticating every domain before a page load or reload.

The proposed algorithm designed to implement the multi-layer architecture is presented in Algorithm 1 (Multi-layer Phish Detection). Fig. 7 represents the sequence of activities of the multi-layer architecture passes through to detect phishing URLs. The algorithm accepts the URL of a suspected website from the user and presents "Phishing" or "No Phishing" to the user as a response after passing through a series of activities. The algorithm designed for implementing the web application is described in Algorithm 1.

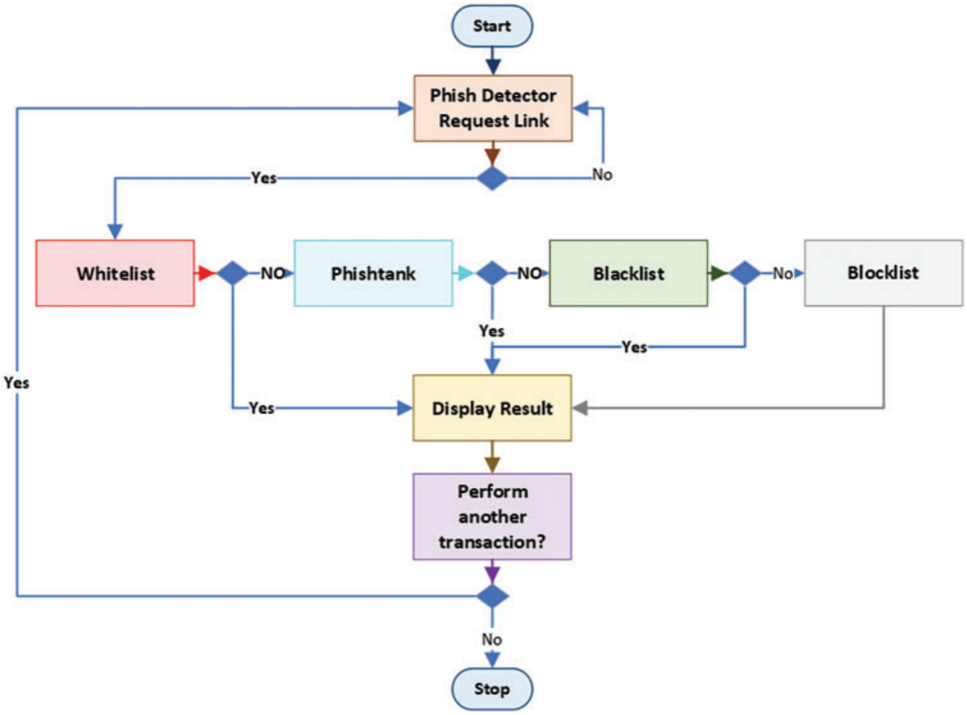


Figure 7: Multi-layer phishing detection framework design

Algorithm 1

```
Step 1 Fetch the URL from the text field
Step 2 Authenticate URL in databases
Step 3 if ($URL_{sus}$ ! == $URL_{whitelist}$) && then $URL_{unknown}$
Step 4 if ($URL_{sus}$ == $URL_{whitelist}$) && then $URL_{legitimate}$
Step 5 if ($URL_{sus}$ ! == $URL_{phishtank}$) && then $URL_{unknown}$
Step 6 if ($URL_{sus}$ == $URL_{phishtank}$) then $URL_{illegitimate}$
Step 7 if ($URL_{sus}$ ! == $URL_{blocklist}$) then $URL_{unknnown}$
Step 8 if ($URL_{sus}$ == $URL_{blocklist}$) then $URL_{illegitimate}$
Step 9 if ($URL_{sus}$ ! == $URL_{Blacklist}$) then $URL_{unknown}$
Step 10 if ($URL_{sus}$ == $URL_{Blacklist}$) then $URL_{illegitimate}$
Step 11 else "$URL_{sus}$ is Legitimate"
Step 12 end if
```

In Algorithm 2, we implemented an automatic browser extension to provide users with immediate feedback immediately after they open a legitimate or illegitimate website with relevant information about the site.

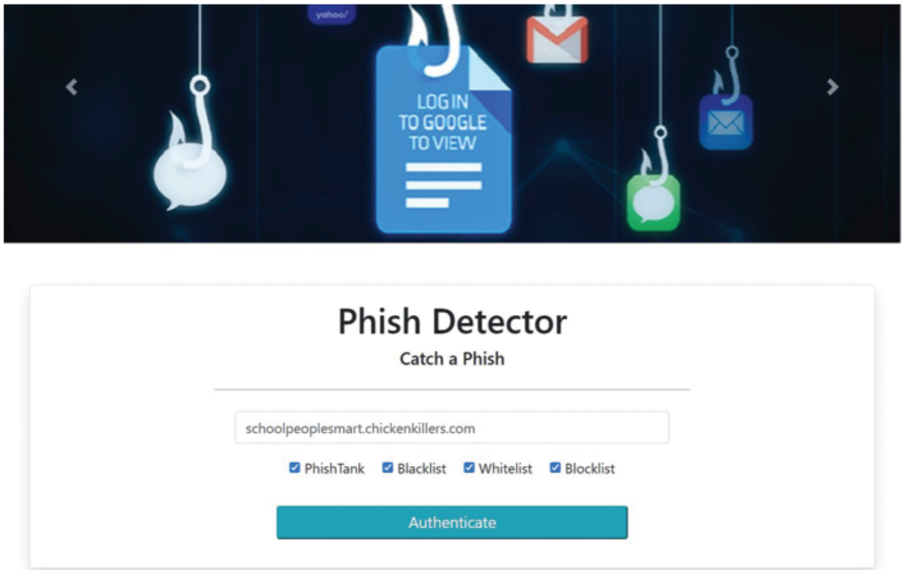
Algorithm 2

```
Step 1    Fetch the URL from the text field
Step 2    Preload page with suspicious ULR
Step 3    Fetch all Anchor tags <a> on the page
Step 4    for each Anchor tags <a> on the page
Step 5        if ($URL_{sus}$ ! == $URL_{whitelist}$ &&) then $URL_{unknown}$
Step 6        if ($URL_{sus}$ ! == $URL_{whitelist}$ &&) then $URL_{unknown}$
Step 7        if ($URL_{sus}$ ! == $URL_{phishtank}$) then $URL_{unknown}$
Step 8        if ($URL_{sus}$ == $URL_{phishtank}$) then $URL_{illegitimate}$
Step 9        if ($URL_{sus}$ ! == $URL_{blocklist}$) then $URL_{unknown}$
Step 10       if ($URL_{sus}$ == $URL_{blocklist}$) then $URL_{illegitimate}$
Step 11       if ($URL_{sus}$ ! == URL Blacklist) then $URL_{unknown}$
Step 12       if ($URL_{sus}$ == URL Blacklist) then $URL_{illegitimate}$
Step 13       else "$URL_{sus}$ is Legitimate"
Step 14       end if
Step 15       end for
Step 17       Stop the page from loading
Step 18       Display an error message or continue to load the site
```

4.1 Design

A multi-layered phishing detecting system is designed from the multi-layered phishing detection algorithm. The system gives options (Phishtank, Whitelist, Blacklist and Blocklist) for the user. It also represents the number of tasks the user is required or allowed to perform with the system. Each layer in the multi-layer phishing detection system is a step to authenticate a suspected phishing website using its URL. First, the user must input the URL of the suspected phishing website and an option to select any of the four provided domains (Phishtank, Whitelist, Blacklist and Blocklist). After our system starts the authentication process by first checking with the domain Whitelist to check if the website is registered with them as an authentic website, the system returns a false value and warnings if the website is not registered with them or an actual value and advises the user to go ahead and trust the website. It moves on the domain blocklist to authenticate if the URL has been registered with them as a phishing website; "*NO*" means the ULR is "*clean*", and the algorithm moves to the following domain for authentication and "*YES*" means the suspected website contains phishing activity or linked with a phishing website. These authentication processes continue until the last domain has been checked and the URL confirmed not to be suspicious with any phishing-related activity before the user is advised to trust the website.

The application package comes with a browser extension. This extension helps detect and authenticate the websites automatically without the user's permission. The extension is made to preload the suspected webpage, collect all its URLs, and authenticate them. The page can open if no phishing activities are detected on the page. Still, if phishing activities are detected on any of the pages the URL contains, the page is denied access, and an error message is sent to the user. The system permits the user to continue if the user trusts the page (after giving the user caution). When tested, the extension is compatible with most common browsers (Google Chrome, Firefox, Maxthon, Microsoft Edge and Opera). Fig. 8 shows the sub-URLs the page to be loaded contains when "schoolpeoplesmart.chickenkillers.com" was entered.



Phish Detector

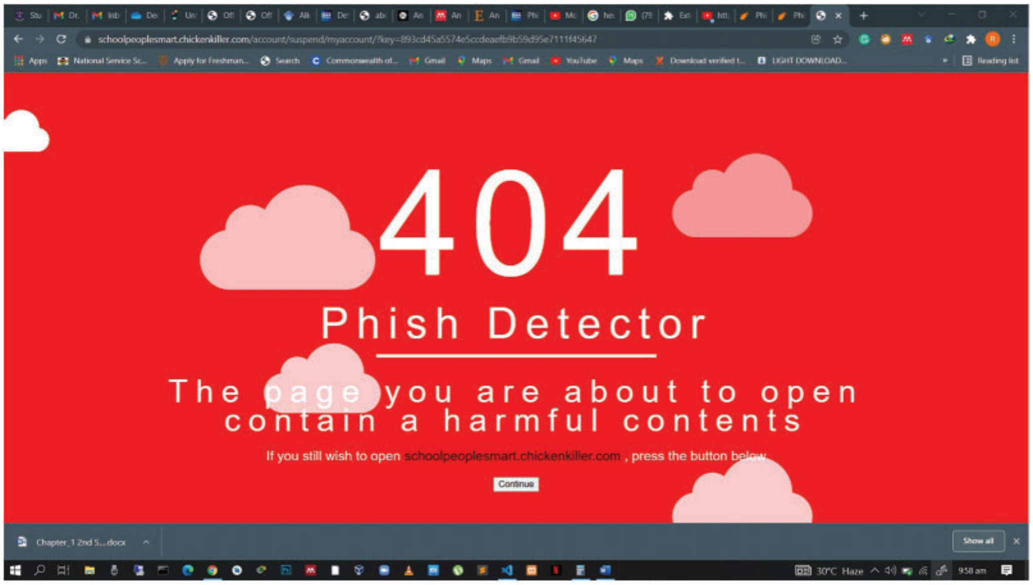
Catch a Phish

schoolpeoplesmart.chickenkillers.com

☑ PhishTank ☑ Blacklist ☑ Whitelist ☑ Blocklist

Figure 8: The multi-layer phishing detector system interface

Fig. 9 shows the error message posted by the extension after authentication. Finally, the user is given a choice to go ahead and open the page even if phishing activities are detected on the page.


schoolpeoplesmart.chickenkiller.com/account/suspend/myaccount/?key=893cd45a5574e5ccdeaefb9b59d95e7111f45647

404

Phish Detector

The page you are about to open contain a harmful contents

If you still wish to open schoolpeoplesmart.chickenkiller.com , press the button below

Figure 9: The web browser extension with an error message

5 Performance Analysis and the Evaluation Matrix

Implementing our algorithm, we tested the accuracy and correctness of each of the layers in our algorithms employed to detect phishing activities online. Aside from testing the accuracy and correctness of individual approaches combined in our algorithm, we measured similar parameters with the multi-layer approach.

The testing and evaluation of the proposed multi-layered phishing detector system were carried out with information/data randomly collected from websites over the internet. A total of ten thousand URLs were collected to verify the effectiveness of the proposed approach. Among the collected URLs are those detected as phishing and the authentic URL. After the experiment, four thousand nine hundred and seventy-nine (4979) URLs were confirmed to be phishing websites. In contrast, four thousand nine hundred and eighty-nine (4989) were detected to be legitimate. Fig. 10 describes the data and test results. Four thousand nine hundred and seventy-nine (4979) representing 49.7% of the total URL tested, and 4989 representing 49.8% of the entire URL tested.

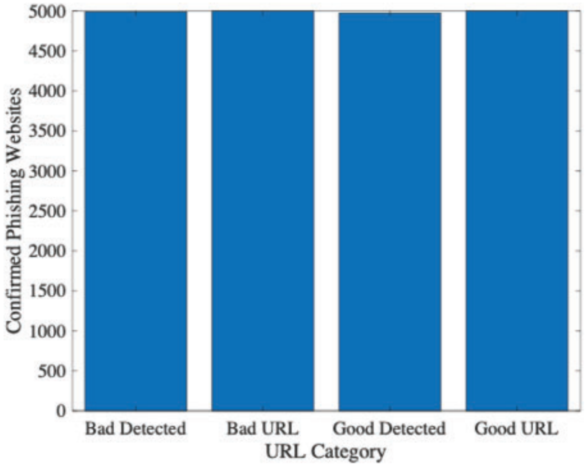


Figure 10: The performance of the approach

The performance of the multi-layered phish detector algorithm depends heavily on the domains the writers selected for the approach. Fig. 11 depicts the result from the test conducted with the same dataset. It may be observed that the Phishtank domain (with 98%) is the most accurate in detecting phishing websites according to the dataset used, followed by the domain Blacklist (with 91%) and by Blocklist (with 81%). Domain Whitelist detected 89% of the legitimate websites it was tested with.

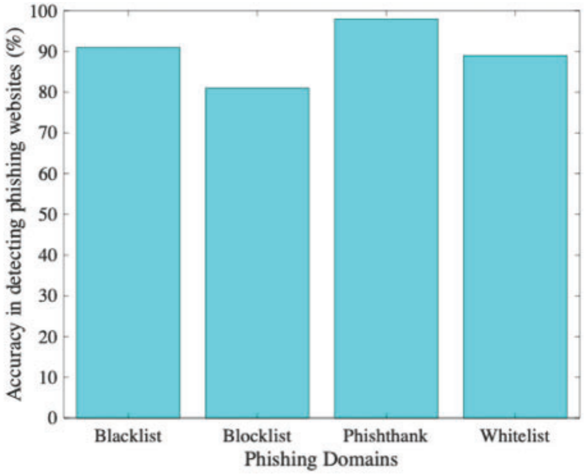


Figure 11: Individual validation of the selected approach

5.1 Intra-Approach Variations Test

The approaches were further tested again, this time by pairing each approach with one another. The pairing was done one is to one. Fig. 12 stipulates the results of the test, and it may be observed that pairing Phishtank with a domain Whitelist yields the best result with 92% of a total of 10,000 URLs tested, followed by Domain Blacklist and Whitelist, which produced 89.7%. The test showed that pairing any approaches with a Whitelist increased the detection rate. This is because the Whitelist can detect and find legitimate websites. For this reason, the legitimate website does not become unknown to the detection technique.

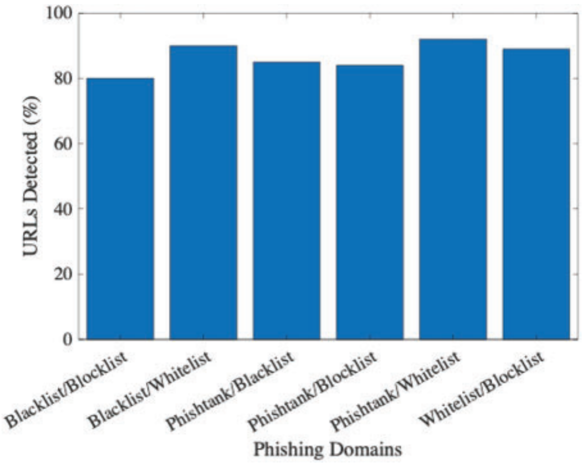


Figure 12: Inter-approach validation

5.2 Performance Evaluation Matrix

The performance of the multi-layer framework system for phishing detection is evaluated as follows: Accuracy, True-positive rate (TPR), False-positive rate (FPR), True-negative rate (TNR), False- negative rate (FNR), Precision, Recall, F-measure, and Matthews Correlation Coefficient (MCC). To best understand the formula, the following are the explanations for its notations: let *Nl* denote the total number of legitimate websites and *Np*, the total number of phishing websites. Let *Nl*→*l* represents the total number of websites classified as legitimate and *Np*→*p* the total number of phishing websites classified as phishing. *Nl*→*p* denotes the total number of legitimate websites classified as phishing, and *Np*→*l* is the total number of phishing sites classified as legitimate. Also, in this section, we will use all the selected approaches as the variables [47–49]. Fig. 13 provides a graphical representation of the methods evaluated.

In Table 2, we provide experimental results and evaluate the system with various data, from a high volume of websites (10,000) to a lower volume (1000), and we recorded different results. It has been observed that the lower the amount of data tested, the higher the accuracy of the approach.

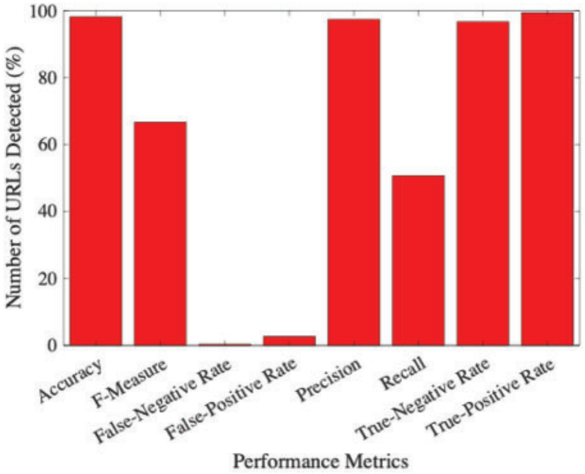


Figure 13: The evaluation matrix

Table 2: Performance evaluation of the number of URLs

Number of URLs	Evaluation parameters							
	Accuracy (%)	True-positive rate (%)	True-negative rate (%)	False-positive rate (%)	False-negative rate (%)	Precision (%)	Recall (%)	F-measure
10000	99.68	99.58	99.78	0.42	0.22	99.77	49.94	66.56
8000	99.75	99.64	99.86	0.36	0.14	99.85	49.94	66.57
6000	99.85	99.80	99.90	0.20	0.1	99.89	99.97	66.61
4000	99.89	99.86	99.92	0.14	0.08	99.87	49.98	66.61
2000	99.94	99.92	99.96	0.08	0.04	99.95	49.98	66.63
1000	99.99	99.98	100	0.02	0	100	49.99	66.65

6 Conclusion

Due to the nature of online activities and the significant number of times users spend online, phishing attacks have become the most rampant fraudulent activity online today. In this paper, the authors aimed to design a phishing detector tool with a multi-layer functionality to detect phishing activities. The four techniques used in creating the multi-layer architecture engine of the system include Blacklist, Whitelist, Blocklist, and Phishtank. The multi-layer framework works for mobile applications and is a browser extension in web browsers for automatic detection. The performance evaluation matrix has proven the efficiency and effectiveness of the multi-layer framework system designed to detect phishing activities.

The system's accuracy, as evaluated per the data set used, was 98.16%. This is because the system did not identify some of the websites recorded in the data set as to whether they are phishing sites or legitimate websites. The true-positive rate was 99.42%, illustrating the system's effectiveness in detecting phishing websites. The false-positive rate was 2.64%, meaning the multi-layer framework system could detect illegitimate websites that are phishing users. An actual negative rate of 96.7% was also recorded. This means that the system could not only identify phishing websites but also legitimate websites. Based on the outcomes presented in this paper, many possible future research directions should consider integrating machine learning algorithm(s) with human or user interventions to increase the detection mechanism. Finally, it will be an exciting experience to combine all the approaches found in the literature with human or user interventions to detect phishing activities on the internet.

Acknowledgement: We acknowledge contributions from colleagues who took the time to go through the manuscript.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: The authors contributed to completing the manuscript. Richard Ahiable wrote the draft, developed the integrated system, and worked on the performance evaluation. Kofi Sarpong Adu-Manu reviewed the manuscript, conducted the system testing with relevant phishing activities and drew the figures: the results and discussions.

Availability of Data and Materials: Data available within the article or its supplementary materials. The authors confirm that the data supporting the findings of this study are available within the article.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Nagaraj, B. Bhattacharjee, A. Sridhar and G. S. Sharvani, "Detection of phishing websites using a novel twofold ensemble model," *Journal of System and Information Technology*, vol. 20, no. 3, pp. 321–357, 2018. https://doi.org/10.1108/JSIT-09-2017-0074

[2] S. Aonzo, A. Merlo and G. Tavella, "Phishing attacks on modern android," in *Proc. of the 2018 ACM SIGSAC Conf. on Computer and Communications Security (CCS '18)*, Association for Computing Machinery, New York, NY, USA, pp. 1788–1801, 2018. https://doi.org/10.1145/3243734.3243778

[3] E. E. H. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Science Journal*, vol. 3, no. 1, pp. 1–10, 2014. https://doi.org/10.1186/s40163-014-0009-y

[4] A. A. Alsufyani, "Social engineering attack detection using machine learning: Text phishing attack," *Indian Journal of Computer Science and Engineering*, vol. 12, no. 3, pp. 743–751, 2021. https://doi.org/10.21817/indjcse/2021/v12i3/211203298

[5] C. Iuga, J. R. C. Nurse and A. Erola, "Baiting the hook: Factors impacting susceptibility to phishing attacks," *Human-Centric Computing and Information Science*, 2016. https://doi.org/10.1186/s13673-016-0065-2

[6] P. Y. Leonov, A. V. Vorobyev and A. A. Ezhova, "The main social engineering techniques aimed at hacking information systems," in *Ural Symp. on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, Yekaterinburg, Russia, pp. 471–473, 2021.

[7] H. Samrat, "Library as an instrument for social engineering: The Bangladesh experience," *International Scholars Journal*, vol. 2, no. 2, pp. 181–185, 2016.

[8] S. Bell and P. Komisarczuk, "An analysis of phishing blacklists: Google safe browsing, OpenPhish, and PhishTank," in *Proc. of the Australasian Computer Science Week Multiconf. (ACSW'20)*, Association for Computing Machinery, New York, USA, pp. 1–11, 2020. https://doi.org/10.1145/3373017.3373020

[9] S. Venkatesha, K. R. Reddy and B. R. Chandavarkar, “Social engineering attacks during the COVID-19 pandemic,” *SN Computer Science*, vol. 2, no. 2, pp. 1–9, 2021. https://doi.org/10.1007/s42979-020-00443-1

[10] M. Hijji and G. Alam, “A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: Challenges and prospective solutions,” *IEEE Access*, vol. 9, pp. 7152–7169, 2021. https://doi.org/10.1109/ACCESS.2020.3048839

[11] R. Wash, “How experts detect phishing scam emails,” in *Proc. of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW2, pp. 1–28, 2020. https://doi.org/10.1145/3415231

[12] M. Rajab, “Visualisation model based on phishing features,” *Journal of Information & Knowledge Management*, vol. 18, no. 1, pp. 1–17, 2019. https://doi.org/10.1142/S0219649219500102

[13] O. K. Sahingoz, E. Buber, O. Demir and B. Diri, “Machine learning based phishing detection from URLs,” *Expert Systems with Applications*, vol. 117, no. 4, pp. 345–357, 2019. https://doi.org/10.1016/j.eswa.2018.09.029

[14] M. A. Adebowale, K. T. Lwin and M. A. Hossain, “Intelligent phishing detection scheme using deep learning algorithms,” *Journal of Enterprise Information Management*, 2020. https://doi.org/10.1108/JEIM-01-2020-0036

[15] A. Zamir, H. U. Khan, T. Iqbal, N. Yousaf, F. Aslam *et al.,* “Phishing web site detection using diverse machine learning algorithms,” *The Electronic Library*, vol. 38, no. 1, pp. 65–80, 2020. https://doi.org/10.1108/EL-05-2019-0118

[16] J. Soyemi and M. Hammed, “An enhanced authentication scheme for preventing phishing attacks on Whatsapp accounts,” in *Proc. of the 2nd Int. Conf., The Federal Polytechnic*, Ilaro, Nigeria, pp. 102–108, 2020.

[17] A. Kumar, J. Ninmoy, D. Arvind and K. Jain, “APuML: An efficient approach to detect mobile phishing webpages using machine learning,” *Wireless Personal Communications*, vol. 125, no. 4, pp. 3227–3248, 2022. https://doi.org/10.1007/s11277-022-09707-w

[18] X. D. Hoang and T. H. Nguyen, “Detecting common web attacks based on supervised machine learning using web logs,” *Journal of Theoretical and Applied Information Technology*, vol. 99, no. 6, pp. 1339–1350, 2021.

[19] R. M. Mohammad, F. Thabtah and L. Mccluskey, “Tutorial and critical analysis of phishing websites methods,” *Computer Science Review*, vol. 17, no. 12, pp. 1–24, 2015. https://doi.org/10.1016/j.cosrev.2015.04.001

[20] I. Qabajeh, F. Thabtah and F. Chiclana, “A recent review of conventional vs. automated cybersecurity anti-phishing techniques,” *Computer Science Review*, vol. 29, no. 3, pp. 44–55, 2018. https://doi.org/10.1016/j.cosrev.2018.05.003

[21] M. H. Alkawaz, S. J. Steven and A. I. Hajamydeen, “Detecting phishing website using machine learning,” in *16th IEEE Int. Colloquium on Signal Processing & Its Applications (CSPA)*, Langkawi, Malaysia, pp. 111–114, 2020. https://doi.org/10.1109/CSPA48992.2020

[22] B. B. G. Aakanksha, T. Ankit, K. Jain and D. P. Agrawal, “Fighting against phishing attacks: State of the art and future challenges,” *Neural Computer Applications*, 2016. https://doi.org/10.1007/s00521-016-2275-y

[23] R. Alabdan, “Phishing attacks survey: Types, vectors, and technical approaches,” *Future Internet*, vol. 12, no. 10, pp. 1–39, 2020. https://doi.org/10.3390/fi12100168

[24] M. Dadkhah, S. Shamshirband and A. W. A. Wahab, “A hybrid approach for phishing web site detection,” *The Electronic Library*, vol. 34, no. 6, 2016. https://doi.org/10.1108/EL-07-2015-0132

[25] S. Tanaka, T. Matsunaka, A. Yamada and A. Kubota, “Phishing site detection using similarity of website structure,” in *IEEE Conf. on Dependable and Secure Computing (DSC)*, Aizuwakamatsu, Fukushima, Japan, 2021. https://doi.org/10.1109/DSC49826.2021.9346256

[26] M. Moghimi and A. Y. Varjani, “New rule-based phishing detection method,” *Expert Systems with Applications*, vol. 53, no. 13, pp. 231–242, 2016. https://doi.org/10.1016/j.eswa.2016.01.028

[27] R. S. Rao and S. T. Ali, “A computer vision technique to detect phishing attacks,” in *Fifth Int. Conf. on Communication Systems and Network Technologies*, Gwalior, India, 2015. https://doi.org/10.1109/CSNT.2015.68

[28] S. Marchal, K. Saari, N. Singh and N. Asokan, "Know your phish: Novel techniques for detecting phishing sites and their targets," in *2016 IEEE 36th Int. Conf. on Distributed Computing Systems (ICDCS)*, Nara, Japan, pp. 323–333, 2016. https://doi.org/10.1109/ICDCS.2016.10

[29] D. Tripathi, B. Nigam and D. R. Edla, "A novel web fraud detection technique using association rule mining," *Association Rule Mining Procedia Computer Science*, vol. 115, no. 2, pp. 274–281, 2017. https://doi.org/10.1016/j.procs.2017.09.135

[30] R. Kumar, K. Garg and V. Kumar, "Extraction of frequent patterns from web logs using web log mining techniques," *International Journal of Computer Applications*, vol. 59, no. 10, pp. 19–25, 2012. https://doi.org/10.5120/9584-4063

[31] W. Hadi, F. Aburub and S. Alhawari, "A new fast associative classification algorithm for detecting phishing websites," *Applied Soft Computing*, vol. 48, no. 1, pp. 729–734, 2016. https://doi.org/10.1016/j.asoc.2016.08.005

[32] T. Peng and I. G. Harris, "Detecting phishing attacks using natural language processing and machine learning," in *IEEE 12th Int. Conf. on Semantic Computing (ICSC)*, Laguna Hills, CA, USA, 2018. https://doi.org/10.1109/ICSC.2018.00056

[33] Y. Fang, C. Zhang, C. Huang, L. Liu and Y. Yang, "Phishing email detection using improved RCNN model with multilevel vectors and attention mechanism," *IEEE Access*, vol. 7, pp. 56329–56340, 2019. https://doi.org/10.1109/ACCESS.2019.2913705

[34] W. Wei, Q. Ke, J. Nowak, M. Korytkowski and M. Wo, "Accurate and fast URL phishing detector: A convolutional neural network approach," *Computer Networks*, vol. 178, pp. 107275, 2020. https://doi.org/10.1016/j.comnet.2020.107275

[35] A. Oden, A. Alarbi, I. Keshta and E. Abdelfattah, "Efficient prediction of phishing websites using multilayer perceptron (MLP)," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 16, pp. 3353–3363, 2020.

[36] N. Y. Conteh and P. J. Schmick, "Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks," *International Journal of Advanced Computer Research*, vol. 6, no. 23, pp. 31–38, 2016.

[37] A. Jamil, K. Asif, Z. Ghulam, M. K. Nazir, S. Mudassar Alam *et al.*, "MPMPA: A mitigation and prevention model for social engineering based phishing attacks on Facebook," in *IEEE Int. Conf. on Big Data (Big Data)*, Seattle, WA, USA, pp. 5040–5048, 2018. https://doi.org/10.1109/BigData.2018.8622505

[38] C. C. Campbell, "Solutions for counteracting human deception in social engineering attacks," *Information Technology & People*, vol. 32, no. 5, pp. 1130–1152, 2019. https://doi.org/10.1108/ITP-12-2017-0422

[39] J. H. Cho, H. Cam and A. Oltramari, "Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis," in *IEEE Int. Multi-Disciplinary Conf. on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, San Diego, CA, pp. 7–13, 2016. https://doi.org/10.1109/COGSIMA.2016.7497779

[40] E. D. Frauenstein and S. V. Flowerday, "Social network phishing: Becoming habituated to clicks and ignorant to threats?" in *Information Security for South Africa (ISSA)*, Johannesburg, South Africa, pp. 98–105, 2016. https://doi.org/10.1109/ISSA.2016.7802935

[41] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Computer & Security*, vol. 73, no. 4, pp. 519–544, 2018. https://doi.org/10.1016/j.cose.2017.12.006

[42] H. Faris and S. Yazid, "Phishing web page detection methods: URL and HTML features detection," in *IEEE Int. Conf. on Internet of Things and Intelligence System (IoTaIS)*, BALI, Indonesia, pp. 167–171, 2021. https://doi.org/10.1109/IoTaIS50849.2021.9359694

[43] R. S. Rao and S. T. Ali, "PhishShield: A desktop application to detect phishing webpages through heuristic approach," *Procedia Computer Science*, vol. 54, no. 4, pp. 147–156, 2015. https://doi.org/10.1016/j.procs.2015.06.017

[44] I. Corona, B. Biggio, M. Contini, L. Piras and F. Roli, "DeltaPhish: Detecting phishing webpages," in *Computer Security-ESORICS 2017: 22nd European Symp. on Research in Computer Security*, Oslo, Norway, vol. 2, pp. 370–388, 2017.

[45] S. Parekh, D. Parikh, S. Kotak and S. Sankhe, "A new method for detection of phishing websites: URL detection," in *Second Int. Conf. on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, India, pp. 949–952, 2018. https://doi.org/10.1109/ICICCT.2018.8473085

[46] W. R. Flores, H. Holm, M. Nohlberg and M. Ekstedt, "Investigating personal determinants of phishing and the effect of national culture," *Information & Computer Security*, vol. 23, no. 2, pp. 178–199, 2015. https://doi.org/10.1108/ICS-05-2014-0029

[47] F. Feng, Q. Zhou, Z. Shen, X. Yang, L. Han *et al.,* "The application of a novel neural network in the detection of phishing websites," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–15, 2018. https://doi.org/10.1007/s12652-018-0786-3

[48] A. K. Jain and B. B. Gupta, "Phishing detection: Analysis of visual similarity based approaches," *Security and Communication Networks*, 2017. https://doi.org/10.1155/2017/5421046

[49] V. Ramanathan and H. Wechsler, "PhishGILLNET-phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training," *EURASIP Journal on Information Security*, vol. 2012, no. 1, pp. 1–22, 2012. https://doi.org/10.1186/1687-417X-2012-1