Proceedings of the 1st International Conference on Statistical Sciences and Data Analytics

SYSTEMATIC LITERATURE REVIEW ON MOBILE PHISHING TECHNIQUES: DETECTION, OPEN ISSUES AND FUTURE DIRECTION

Abubakar Ibraheem Labbo*[1], John Kolo Alhassan[1] and Ahmad Suleiman[1]

[1] Department of Cyber Security Science, Federal University of Technology, Minna Nigeria

***Corresponding Author Email: jkalhassan@futminna.edu.ng**

ABSTRACT

In an increasingly digital world, phishing attacks have become a significant threat to personal and organizational security, particularly through mobile devices. This study aims to explore the evolving tactics employed by cybercriminals in mobile phishing attacks, focusing on understanding the methods used to exploit user trust and the implications for cybersecurity awareness. A systematic review of recent literature (2017-2024) was conducted, analyzing various mobile phishing techniques, including SMS phishing (smishing), voice phishing (vishing), and social media phishing. The review utilized databases such as ACM Digital Library, IEEE Explore, and Google Scholar to gather peer-reviewed articles and industry reports. The findings reveal that mobile phishing tactics have diversified significantly, with attackers increasingly leveraging social engineering techniques to manipulate victims. The study highlights the unique vulnerabilities associated with mobile devices, such as smaller screens and the prevalence of app-based communication, which make users more susceptible to deceptive practices. Notably, the rise of mobile device phishing and the use of fake profiles on social media platforms have become prevalent methods for data theft. The research also emphasizes the effectiveness of these tactics in compromising user information and the challenges in detecting such attacks on mobile platforms. The research underscores the urgent need for enhanced cybersecurity awareness and education among mobile device users to mitigate the risks associated with mobile phishing attacks. Organizations must implement robust security measures and training programs specifically tailored to mobile environments to empower individuals to recognize and respond to phishing threats effectively.

Keywords: Phishing, Cybersecurity, Social Engineering, User Awareness, Data Theft.

1. INTRODUCTION

The term "phishing" was first coined in 1996, during a period when numerous fraudulent users registered on America Online (AOL) using fake credit card details. AOL approved these accounts without proper verification, allowing attackers to exploit the system's resources. When it came time to pay for services, AOL discovered that many of these credit cards were invalid and that the accounts were fraudulent. As a result, these accounts were terminated. In response, AOL began authentically verifying credit card information. This prompted attackers to seek alternative methods for gaining access to AOL accounts. Instead of creating fake accounts, they shifted their tactics to stealing passwords from legitimate AOL users by contacting them through emails or messages that appeared to be from trusted sources (Goel & Jain, 2018).

Phishing is a technique employed by cybercriminals to gain access to sensitive and restricted information from end users through a combination of social engineering and technological methods. It has been identified as the primary tactic utilized by attackers to compromise the privacy of internet users (Basit et al., 2021). Most individuals who fall victim to phishing attacks lack awareness of these threats. The prevalence of phishing attacks targeting mobile devices, IoT devices, and personal computers is increasing rapidly (Naaz, 2021). Despite various security measures implemented to mitigate this issue, attackers continually develop innovative strategies to exploit sensitive information and identities using advanced technologies (Ghazi-Tehrani & Pontell, 2021).

The most common phishing method involves sending fraudulent emails to potential victims. These emails often originate from accounts mimicking those of legitimate government agencies, digital banks, electronic payment platforms, and e-commerce sites such as Flipkart. These deceptive websites extract sensitive data from users through various tactics (Basit et al., 2021). For instance, they may send links for account updates, verification emails, or enticing messages claiming that the user has won a prize, such as "Congratulations! You've won 400,000 thousand Naira Only! Click the link below to claim your reward." These approaches rely heavily on social engineering techniques to manipulate internet users into providing their information (McAlaney & Hills, 2020). Attackers often create the illusion that these emails are sent from legitimate organizations. Additionally, phishing can occur via fraudulent phone calls. In such cases, the caller may impersonate a representative from a bank and request sensitive information, such as bank account details, credit card numbers, ATM PIN codes, one-time passwords (OTPs), usernames, and passwords (Biswal & Pani, 2021).

Mobile devices have evolved to function similarly to personal computers due to advancements in technology and computing capabilities. They are now integral to everyday interactions and transactions, leading to heightened security concerns for users. As global adoption of mobile devices rises, so do the associated security threats. Phishing attackers are continuously seeking new methods to compromise these devices (Owen, 2024) . As users increasingly rely on mobile devices, their vulnerability to information technology threats also escalates. Consequently, it is essential to comprehend the avoidance motivations and behaviours of users (Faklaris, 2024).

Mobile device phishing is a deceptive tactic used by cybercriminals to manipulate users of smartphones and tablets into disclosing sensitive information or executing harmful actions. These phishing attacks often involve the impersonation of legitimate entities, such as banks, social media platforms, or online retailers, with the intent to deceive users and obtain unauthorized access to their personal or financial data (Owen, 2024). In mobile device phishing, attackers leverage various communication channels frequently used on mobile devices, including text messages (SMS phishing or smishing), voice calls (vishing), emails, quick response code (QR code attack or quishing) social media applications, instant messaging platforms, and mobile apps. They commonly employ social engineering tactics, such as crafting urgent scenarios, presenting enticing rewards, or invoking fear and intimidation, to manipulate users into disclosing their confidential information, scanning a QR code or installing malicious software (Ghazi-Tehrani & Pontell, 2021).

The primary objective of mobile device phishing attacks is to obtain sensitive information, including usernames, passwords, credit card details, social security numbers, and other personal and financial data. This information can be exploited for identity theft, financial fraud, or unauthorized access to sensitive accounts. Additionally, phishing attacks may result in the installation of malware on the victim's device,

enabling attackers to gain remote control or unauthorized access to the device and its data (Goel & Jain, 2018).

It's important to recognize that mobile device phishing attacks can be highly sophisticated, utilizing techniques such as URL spoofing, creating counterfeit mobile app interfaces, and exploiting vulnerabilities in mobile operating systems or applications. As mobile devices increasingly store and manage sensitive personal and financial information, understanding and mitigating the risks associated with mobile phishing is essential for protecting user privacy and security (Kulkarni et al., 2024).

Mobile device users are at least three times more susceptible to phishing attacks. This increased vulnerability can be attributed to several factors, including the small screen size, the absence of clear identity indicators, challenges associated with user input, the frequent switching between applications, and the specific habits and preferences of mobile device users (Arshad et al., 2021).

By exploiting the hardware limitations of mobile devices and the careless behaviour of users, attackers can easily execute phishing attacks on smartphones. A significant knowledge gap exists among users regarding phishing threats and prevention strategies. According to a study, 44% of users are unaware of the security solutions available for mobile devices (Sylvester, 2022).

The security of mobile devices is influenced by various factors, including existing security threats and the specific security requirements of users. Currently, there is no reliable method to verify whether credentials are being sent to a legitimate server or a malicious one. If the operating system (OS) of a mobile device is compromised, malicious applications can access sensitive information, such as the device's camera, SMS messages, contacts, and location data, thereby compromising user privacy (Weichbroth & Łysik, 2020).

Furthermore, phishing attacks have a detrimental impact on the economy due to the financial losses incurred by both businesses and individuals. Numerous solutions have been proposed for the detection and prevention of phishing attacks; however, the threat remains pervasive. Various methods, such as blacklisting, URL-based detection, static detection, and heuristic techniques, are employed to identify phishing attempts. Some users utilize anti-phishing software available in the market, which primarily relies on blacklists to detect malicious and phishing applications installed on devices. However, blacklists are ineffective against zero-day phishing attacks (Gupta et al., 2017). A significant number of phishing websites emerge and disappear daily. According to the Anti-Phishing Working Group (APWG), the average lifespan of a phishing site is approximately 4.5 to 5 days, with some sites remaining active for only a few hours (Ijaz et al., 2021).

The objective of this paper is to provide a comprehensive overview of mobile phishing attacks by examining various techniques employed by attackers and the corresponding detection methods. Additionally, we highlight several open challenges and issues associated with mobile phishing attacks.

2. REVIEW OF RELATED LITERATURE

Sylvester, (2022) conducted a thorough examination of contemporary phishing tactics, aiming to raise awareness and educate readers about the diverse range of phishing threats. This paper advocates for the adoption of robust anti-phishing solutions to enhance overall cybersecurity resilience.

As highlighted by (Chiew et al., 2018) , there is a trend among researchers to focus on publishing findings related to anti-phishing techniques rather than analyzing the phishing techniques themselves. However, several reviews addressing phishing have emerged in recent years (Nadeem et al., 2023). Phishing is characterized by a lifecycle, meaning that a phishing attack can be delineated into distinct stages (Gupta et al., 2017). These stages are often summarized as follows:

i. **Planning**: This stage involves identifying targets, determining the information sought, and developing or selecting the tools and techniques to be used in the attack. This may include crafting phishing emails containing malicious links and setting up spoofed websites.
ii. **Phishing**: At this stage, the identified targets are engaged using the resources developed in the planning phase.
iii. **Infiltration**: Depending on the attack method employed, this stage varies but fundamentally involves the target's response and the phisher gaining access to the desired personal information.
iv. **Data Collection and Exploitation**: During this phase, the phisher extracts the sought-after information and utilizes it to fulfil the objectives established in the planning stage. This often leads to fraudulent activities where attackers impersonate victims to access their accounts. Another common practice is selling the acquired personal data on the dark web.
v. **Exfiltration**: In the final stage, the phisher or the attacker seeks to erase all traces of their activities, such as deleting fraudulent websites. This phase may also involve analyzing the attack's success and planning for future phishing attempts.

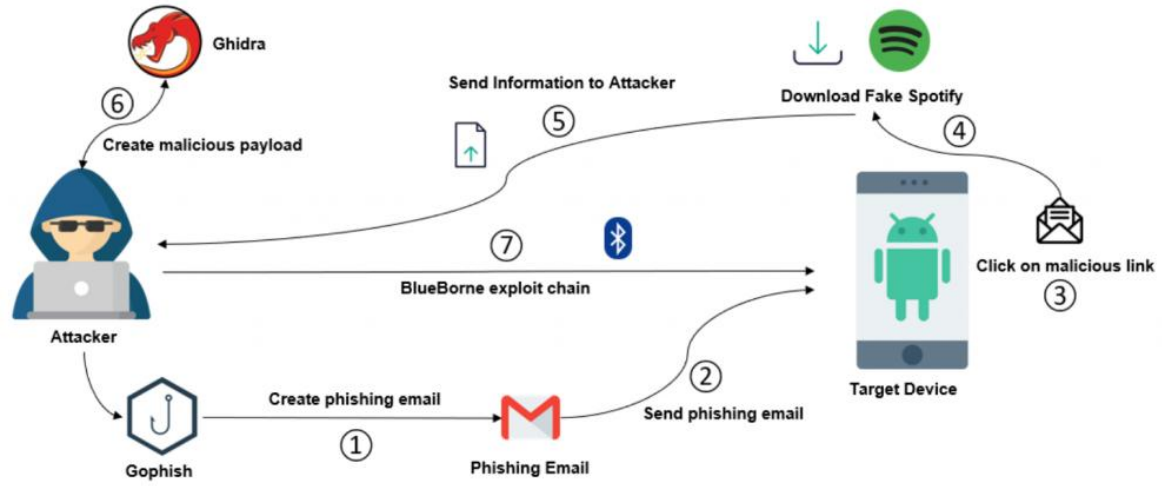

Figure 1: Phishing Attack Lifecycle (Gupta et al., 2017)

Janulevi, (2020) introduced a phishing attack taxonomy focused on email, addressing the limitations of existing phishing taxonomies. They concluded that their proposed taxonomy offers a more comprehensive classification, featuring twice as many categories compared to previous frameworks. Meanwhile, (Aonzo et al., 2018) provided a succinct analysis of the vulnerabilities in Android password managers, identifying these weaknesses as significant contributors to phishing attacks. Their paper highlighted several design flaws in password managers that facilitate these security breaches.

Kunju & Anthony, (2019) conducted a survey to evaluate phishing techniques and detection algorithms. Their findings yielded numerous solutions and approaches for attack detection. However, they indicated that many of the proposed methods lack the effectiveness necessary to adequately address these phishing threats.

Jain & Gupta, (2022) introduced a comprehensive taxonomy encompassing various phishing techniques, their vectors, and corresponding countermeasures. The paper emphasized the environments most frequently targeted by these attacks. This taxonomy aims to guide the development of effective anti-phishing strategies and serves as a valuable resource for developers and practitioners seeking diverse methods and tools to mitigate phishing threats.

(Yet & Attacks, 2019) detailed the initiatives undertaken in the fight against phishing. A dedicated team conducted multiple awareness sessions and workshops for internet users to promote the adoption of anti-phishing techniques and enhance their overall online safety. They concluded that ongoing awareness programs are essential for effectively combating phishing attacks.

Cui, Qian et al. [19] proposed a method for analyzing phishing attacks by counting HTML tags within the Document Object Model (DOM). Utilizing clustering techniques, they identified attack patterns occurring within specific spatial ranges and suggested that these clusters could be aggregated and made publicly accessible. Their findings indicated that this approach could effectively detect a substantial number of new phishing attacks. Table 2.3 presents a summary of literature review. The author(s), year of publication, problem addressed, methodology, result obtained and limitation of some papers reviewed were summarised in the table.

2.1 Classification of mobile phishing attacks

Figure 2 illustrates the classification of mobile phishing attacks. These attacks can be categorized based on several factors, including social engineering tactics, mobile applications, malware, social networking platforms, content injection techniques, and wireless communication methods. Below are some mechanisms employed in executing phishing attacks on mobile devices:

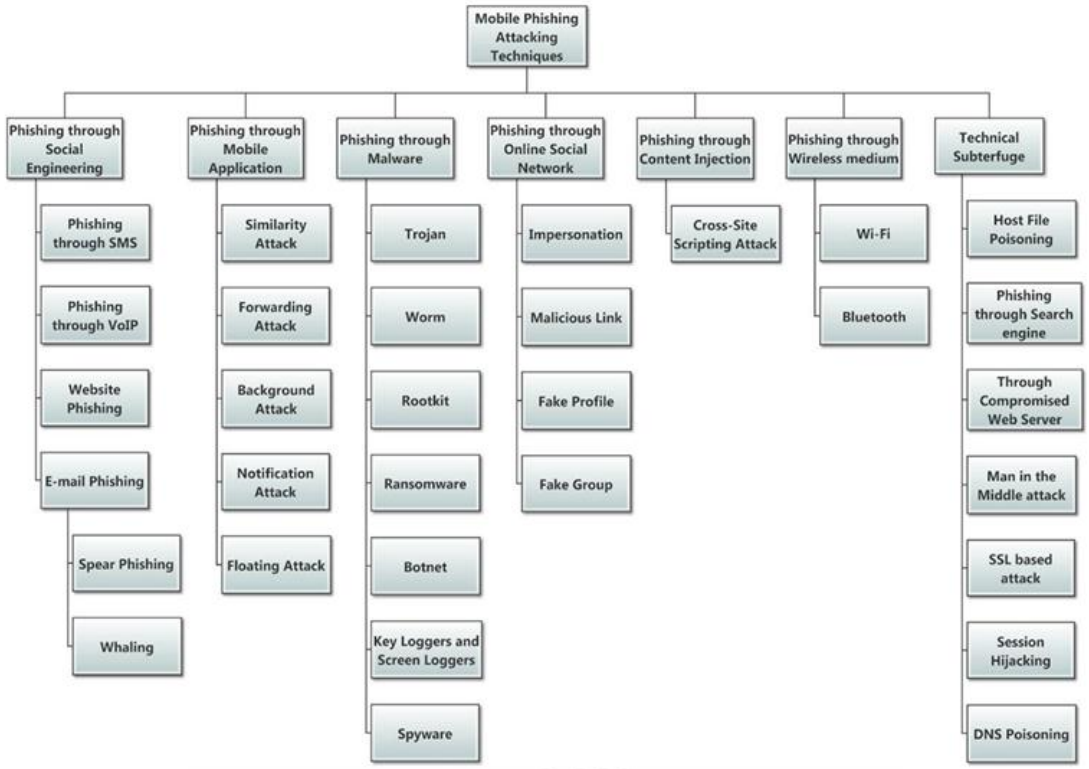

Figure 2: Classification of Phishing Attacks (Goel & Jain, 2018)

2.1.1 Phishing through Social Engineering

Techniques that manipulate users into divulging personal information, often through deceptive messages or scenarios. In this type of attack, technical defences prove to be less effective because the primary target is the user rather than the device itself. Additionally, many individuals tend to overestimate their ability to detect such threats, believing they are too clever to be deceived by phishing attempts (Chetioui et al., 2021). Various social engineering strategies can be employed, including:

i. **Phishing through SMSes**: One of the most prevalent methods for executing phishing attacks on mobile devices is through SMS, commonly known as Smishing. This type of attack aims to steal personal and financial information from users. Smishing messages typically include a text along with a link that, when clicked, either redirects the user to a counterfeit website or initiates the installation of a malicious program (Salahdine & Kaabouch, 2019).
This approach allows malware to infiltrate the device. Smishing relies heavily on social engineering tactics, making it particularly effective in targeting unsuspecting users. Although various methods have been proposed to detect malicious links in SMS messages, these links are frequently altered. Additionally, the use of URL shortening services complicates the identification of harmful URLs, further enhancing the challenge of effective detection (Nadeem et al., 2023)

ii. **Phishing through Voice over Internet Protocol (VoIP):** This technique operates on the same principles as phishing but is executed over the phone, known as vishing. Consider the last spam call you received about a cruise you "won," requiring you to provide personal information to claim your prize, this is a classic example of vishing (Chetioui et al., 2021). Scammers often ask for sensitive details such as your address, date of birth, and financial information.

Alternatively, you might receive an email from your "bank" instructing you to call a number to verify your identity by entering a password after clicking on a link. In this case, you would be contacting the scammer directly.

iii. **Website phishing**: In a website phishing attack, the attacker targets individuals rather than systems. Creating an exact replica of a legitimate website is relatively easy for cybercriminals. They aim to deceive users by setting up phishing sites that mimic well-known platforms such as eBay or PayPal, in order to harvest personal and financial information. A phishing website can either be a legitimate site with malicious content injected or a site owned entirely by the attacker (Tang & Mahmoud, 2021).

To detect phishing webpages, two primary methods are employed: blacklisting and heuristic-based detection. Blacklists contain known suspicious IP addresses and URLs. This approach involves checking a website against this list, which can yield a low false positive rate but fails to protect against zero-day phishing attacks. Heuristic methods, on the other hand, rely on identifying features commonly found in phishing webpages, though not all websites share these characteristics. To circumvent this, attackers may design phishing sites that lack the typical indicators of fraud, making detection more challenging (Alkhalil et al., 2021).

2.1.2 Phishing through Mobile Applications:

The use of malicious or counterfeit applications designed to mimic legitimate ones, tricking users into providing sensitive data. Application-based phishing attacks represent a significant threat to mobile devices. While browsing or downloading apps, users can easily fall victim to these types of attacks. Once a malicious application infiltrates the device, it can collect sensitive information such as login credentials and passwords, which is then transmitted to the attacker. In some cases, attackers may install a backdoor or other malicious software that compromises user privacy (A. K. Jain & Gupta, 2017). Below are various techniques employed in mobile application phishing attacks are discussed:

i. **Similarity Attacks**: In a similarity attack (A. K. Jain & Gupta, 2017), the phishing application, webpage, or login interface closely mimics the legitimate counterpart, using the same name, user interface (UI), and icon. The attacker encourages the user to install the phishing application and enter their login credentials into the fraudulent Login User Interface (LUI) rather than the legitimate one. This deceptive design aims to exploit user trust and trick individuals into providing sensitive information.

ii. **Floating attacks**: The attacker exploits a feature of Android devices that allows an application to overlay actions on top of currently active applications. A phishing application that has been granted **SYSTEM_ALERT_WINDOW** permission can display a transparent input field over the legitimate application's login and password fields (Korkmaz et al., 2020). While the user sees the genuine login interface, the hidden input field remains undetectable. When the user enters their credentials, they are captured by the phishing application, compromising their sensitive information without the user's knowledge.

iii. **Background attacks**: In some cases, the malware or phishing application operates stealthily in the background, utilizing Android's **Activity Manager** to monitor the applications running on the device. When the user launches a legitimate target application, the phishing app activates itself in the foreground, presenting a deceptive phishing screen. This tactic effectively tricks users into entering their credentials, believing they are interacting with the genuine application (Alabdan, 2020).

iv. **Notification Attacks**: In notification attacks, the attacker can display a fraudulent notification that prompts the user to provide personal details. The notification window can be manipulated to closely resemble a legitimate notification, making it difficult for users to distinguish between the two. This deceptive tactic exploits user trust in system notifications, leading them to inadvertently share sensitive information (Hawa Apandi et al., 2020).

2.1.3 Phishing through mobile malware

The term "malware" was first introduced in 1990 by computer scientist and researcher Yisrael Radai. Malware refers to malicious software that gains unauthorized access to a user's device without their consent. Its primary purpose is to steal data, damage the device, or disrupt the user's experience. Malware typically spreads through malicious attachments or links, tricking users into installing harmful applications that provide attackers with unauthorized access (Sylvester, 2022) . Below, are various techniques employed in phishing through mobile malware.

i. **Trojans**: Trojans are a type of malware that allow attackers to gain control over a device through seemingly legitimate mobile applications. These apps appear to offer useful functionality in the foreground while executing malicious actions in the background. Attackers can use Trojans to collect private information or to install additional malicious software, such as bots or worms (A. Jain et al., 2021).

ii. **Worm**: A worm is a type of malicious software that is self-replicating and can spread to uninfected systems autonomously, without any human intervention. Worms propagate by exploiting vulnerabilities in networking protocols. Due to their ability to replicate and spread across networks, they can significantly damage devices, compromise security, and consume considerable bandwidth (A. Jain et al., 2021).

   The introduction of **Cabir** marked a significant milestone, as it allowed malware to be transmitted to mobile devices. The Cabir worm specifically targets Symbian S60 devices and spreads via Bluetooth (A. Jain et al., 2021). Worms often go unnoticed until their replicated instances begin to consume system resources, resulting in slower device performance.

iii. **Mobile Ransomware:** Mobile ransomware is a type of malware that locks a user's device, preventing access to their data by encrypting files on the infected system and only decrypting them once a ransom is paid. It can target both computers and mobile devices, often altering the PIN to demand payment for release, and comes in two main types - crypto ransomware, which encrypts files, and locker ransomware, which locks the device itself, most strains announce their presence to pressure the owner into complying with the ransom demand (A. Jain et al., 2021).

2.1.4 Phishing through online social networks

Social networking sites have become integral to both professional and personal communication, with millions of users worldwide interacting and sharing ideas. However, this vast user base presents a new landscape for attackers, who exploit users' trust for their own gain (Kuss & Griffiths, 2017). Various methods that attackers use to deceive users on social networking sites include:

i. **Impersonation:** Impersonation is a common tactic on social networking sites, where users often follow famous personalities and join interest-based groups. However, there is typically no

verification process to confirm the authenticity of virtual profiles (Bidgoli & Grossklags, 2017). Attackers exploit this vulnerability by pretending to be well-known figures, posting malicious links related to sales or offers. When users click these links, they may be prompted to provide personal details or inadvertently download malware (Trapp, 2020). This strategy leverages users' trust and desire for connection, making it a particularly effective method for cybercriminals.

ii. **Fake Profiles**: Attackers often create fake profiles and send friend requests to users, posing as old friends or acquaintances. Once the user accepts the request, the attacker gains access to private information shared within the user's network of friends, family, and colleagues. To gather even more personal data, the attacker may then message the user directly, requesting additional information such as phone numbers or email addresses (Karantias et al., 2020). This tactic exploits the trust inherent in social connections, making it easier for attackers to gather sensitive information.

iii. **Fake communities**: Attacker may create a fake group with the name of well-known organisation and add some members to the group who are already the part of that organisation but are also with the attacker to carry out the scam (Wani, 2017). They send group request to other members of the organisation who after seeing that their colleagues are also the members of the group, join the group. Attacker then obtains the secret information from their discussions and use it for his personal gain.

2.1.5 Phishing through Content Injection:

In phishing through content injection, an attacker modifies parts of the content on a legitimate website to deceive users, directing them away from the authentic webpage where they are prompted to provide personal information. For example, an attacker might inject malicious code designed to record user information and send it to the attacker's server (Singh & Imphal, 2018).

i. **Cross-Site Scripting (XSS):** A common method of content injection is Cross-Site Scripting (XSS), an application-layer web attack that targets vulnerable scripts embedded in webpages executed on the client side. Attackers use JavaScript to deliver malicious content to users, altering the client-side scripts of the web application so that they execute according to the attacker’s intentions. XSS attacks can have severe consequences, including the compromise of user accounts, unauthorized modification of webpage content, and exposure of credentials or session cookies (Torres & Flores, 2019).

2.1.6 Phishing through Wireless Medium

i. **Wi-Fi:** Wi-Fi has become an essential part of modern life, but it also serves as a hotspot for attackers. Users often do not authenticate the access points they connect to, making it easy for an attacker to set up a fraudulent access point with a Service Set Identifier (SSID) that resembles a legitimate one. This allows the attacker to intercept communication between the user's mobile device and the Wi-Fi hotspot (Ijaz et al., 2021). The architecture of public hotspots is inherently vulnerable, as it typically lacks encryption to protect the data being transferred. When users connect to such hotspots for the first time, the connection is often insecure, enabling attackers to hijack sessions and control traffic.

ii. **Bluetooth:** Bluetooth technology allows data sharing over short-range wireless links, but it also has vulnerabilities that attackers can exploit. Devices equipped with Bluetooth may have flaws that permit unauthorized connections without user consent. When two mobile devices are within range, an attacker’s device can send malicious data to the victim's device by

establishing a Bluetooth connection using default passwords (Lonzetta et al., 2018). Once the attacker gains access via Bluetooth, they can access the victim's contacts, messages, and files, posing a significant security risk.

2.2 Classification of mobile phishing defence and detection mechanisms

Various strategies exist for detecting and defending against phishing attacks on mobile devices. These approaches encompass a range of techniques aimed at identifying and mitigating the risks associated with phishing.

Table 2.1 presents anti-phishing solutions of smishing and spam SMSes detection techniques tailored to specific types of mobile phishing attacks, offering insights into their functionality and application. Additionally, analysis of different mobile phishing defense techniques is summarized in Table 2.2, highlighting their effectiveness, implementation challenges, and use cases. These tables provide a comprehensive overview of the current landscape of mobile phishing defenses, assisting users and organizations in selecting appropriate strategies to enhance their security posture against phishing threats.

2.3 Detection of smishing and spam SMSes

Smishing, or SMS phishing, involves fraudulent text messages that include a URL, which, when clicked, can trigger malicious actions. Cybercriminals leverage social engineering tactics to entice victims, making it easy for unsuspecting users to become targets of these scams. To identify smishing and spam messages, a range of classifiers using effective feature sets have been developed. Below, we discuss various approaches to smishing detection.

2.3.1 S-Detector:

Woong et al., (2017) introduced a security model called "S-Detector" designed to detect and block smishing messages. This model employs a Naïve Bayesian Classifier to differentiate between smishing and normal text messages by analyzing frequently used words in smishing texts. The S-Detector comprises four components: SMS Monitor, SMS Determinant, SMS Analyzer, and Database.

The S-Detector follows these steps to identify smishing messages:

1. SMS Monitoring: When a text message is received, the SMS Monitor logs the message details and timestamps.
2. Blacklist Check: It checks if the sender's telephone number is listed in a blacklist database.
3. URL Detection: The model determines whether the text message contains a URL. If it does, the URL is accessed.
4. APK File Check: It checks if an APK file is downloaded upon accessing the URL. If an APK is downloaded, the message is classified as smishing and blocked; otherwise, the message content is analyzed further.
5. Pre-processing and Analysis: The text message is pre-processed to isolate strings, and morpheme units are extracted. Each word is then assigned a weight value using the Naïve Bayes algorithm.

6. Classification: If the weight exceeds a specified threshold, the message is labelled as smishing and blocked. If not, it is classified as a normal text message.

2.3.2 SMSAssassin

Yadav et al., (2012) developed "SMSAssassin", a mobile application for filtering spam messages based on Bayesian learning. To enhance accuracy, it combines Support Vector Machine (SVM) techniques with Bayesian learning. Since spam SMS often feature frequently changing patterns and keywords, the application employs crowd-sourcing to maintain an updated list of these patterns.

During the training phase, the application calculates the frequency of each word in both spam and legitimate (ham) messages to determine its classification. After training, the probability of an SMS being spam is computed; if it exceeds a certain threshold, the message is flagged as spam. To monitor spam keywords, SMSAssassin utilizes a GlobalSpamKeywords list on the server and a SpamKeywordsFreq list on users' mobile devices. Additionally, the app maintains a UserPreferencesList, allowing users to specify their own ham and spam keywords based on personal preferences. Users of the SMSAssassin app can also share reported spam lists with others. The authors collected a total of 4,318 SMS messages through crowd-sourcing, achieving 97% classification accuracy for ham messages and 72.5% for spam messages.

2.3.3 Dendritic Cell Algorithm (DCA) based approach

Alhasan, (2016) introduced a technique for filtering multimodal textual messages, such as emails and short messages. Drawing inspiration from the human immune system and utilizing hybrid machine learning methodologies, they proposed an innovative approach to information fusion. Their method involves analyzing various features extracted from incoming messages using machine learning algorithms. To enhance mobile spam filtering, they developed a framework based on DCA (Distributed Cluster Analysis) that integrates outputs from multiple machines learning algorithms, effectively improving the accuracy and efficiency of spam detection.

2.3.4 Spam detection using text content

Kaddoura et al., (2022) proposed a content-based approach for spam detection that focuses on semantic groups of words rather than individual words. Their method utilizes two categories of features: Linguistic Inquiry and Word Count (LIWC) and SMS Specific (SMSS) features. By leveraging these semantic features, the researchers were able to reduce the overall feature set, which enhanced the efficiency of the spam detection system. The process consists of two main phases: feature extraction and classification, with a machine learning algorithm employed for the classification task. The accuracy of their system ranges from 92% to 98%, demonstrating its effectiveness in identifying spam.

2.3.5 MDLText Approach in Cybersecurity

As the volume of data on smartphones continues to grow, there is an increasing need for effective text classification techniques. (Page & Moher, 2017) introduced "MDLText," a lightweight and scalable multinomial text classifier rooted in the Minimum Description Length (MDL) principle. This approach is designed to be efficient, fast, and robust, addressing the challenges of rapid learning while minimizing the risk of overfitting. Thanks to its incremental learning capabilities, MDLText is well-suited for both

online and dynamic environments. Notably, it maintains a low computational cost even when processing large datasets, making it an ideal solution for modern cybersecurity applications.

Table 1: Summary of Smishing and Spam SMSes Detection Techniques

Author	Techniques	Tailored for	Advantages
(Lonzetta et al., 2018)	Machine Learning	Mobile Webpages	90% classification accuracy, 89% true positive rate, 8% false positive rate.
(Wu et al., 2016)	Optical character recognition	Mobile webpage, application, and persistent account.	Web-Fish achieves 100% verification rate.
(Cata et al., 2013)	Mobile QR code	Webpage authentication scheme	Data is encrypted so credentials are safe even if attacker obtain them; user can check if server is phishing or not .
(Hashmi et al., 2019)	Blacklist and data mining approach	Mobile Webpages	Ensure zero-hour protection; Protect android devices from phishing attack.
(Alhasan, 2016)	Dendritic cell algorithm	Emails and SMS	The dendritic cell algorithm improves recall and precision of spam and non-spam messages; accuracy approx. 100%.

Table 2: Summary of Mobile Phishing Defense Techniques

Author	Techniques	Tailored for	Advantages
(Alhasan, 2016)	Naive Bayes classifier	SMS	Approach is able to detect and block smishing messages with high accuracy rate.
(Silva et al., 2016)	Minimum description length principle	SMS	Able to process high dimensional data at fast speed; Low computational cost.
(Almeida et al., 2017)	Text processing with lexicographic and semantic dictionaries	SMS	For the Wilcoxon Signed-Ranks Test, the null hypothesis is rejected with α=0.05 with a confidence level of 95%.
(Canbay, 2017)	J48 classification and K-Means clustering algorithm	Mobile Application	Approach can detect malign and benign applications with 98.6% accuracy.
(Goel & Jain, 2018)	augments user's credentials with hardware and software information	Mobile Application	Prevent phishing attacks through secure, hardware isolated environment for password input and transmission.

Table 3: Summary of Literature Review

S/No	Author(s) /Year	Problem Addressed	Methodology	Result obtained	Limitation
1	(Choudhary et al., 2023)	Develop a model that will detect phishing attacks by analyzing patterns using ML	Analyzing structure and contents and comparing with known phishing website databases using machine learning (ML) algorithms	The method outperformed in terms of accuracy precision, recall F1-score and ROC value on the datasets used. Validation of ML algorithms outperformed other state-of-the-art methods yielding high results in terms of accuracy.	The model developed can only analyze pattern to detect phishing attack.
2	(Omari, 2023)	websites that impersonate legitimate entities to deceive users into disclosing sensitive information, highlighting the need for robust detection methods	Gradient Boosting Classifiers (GBCs)	performance across various metrics, showing exceptional resilience against adversarial tactics in phishing attacks, marking a significant advancement in online security.	potential biases in the dataset, the need for continuous model updates, and reliance on specific features that may not capture all phishing aspects.
3	(Orunsolu et al., 2022)	The need for an effective anti-phishing solution that leverages existing feature datasets.	Support Vector Machine and Naïve Bayes	Results indicate a remarkable performance with 0.04% False Positive and 99.96% accuracy for both SVM and Naïve Bayes predictive models.	The model may not account for evolving phishing techniques and requires continuous updates to maintain effectiveness.

S/No	Author(s) /Year	Problem Addressed	Methodology	Result obtained	Limitation
4	(Said et al., 2024)	phishing website detector based on improving the	Convolutional Neural Networks (CNN) with	The reported results show that using the self-attention mechanism has	computation complexity

		convolutional neural network (CNN) with a self-attention mechanism	Self-Attention mechanism	improved the detection accuracy and made the CNN model more efficient for detecting phishing websites	
5	(Aldakheel et al., 2023)	Introduce a novel method for detecting phishing sites with high accuracy	Convolution Neural Network (CNN)-based model for precise classification that effectively distinguishes legitimate websites from phishing websites	The research confirms the classification of phishing attacks by 1D-CNN and its preventative measures and consequences, with each algorithm having an accuracy of up to 98.77%	The research only adopted Convolution Neural Network (CNN)
6	(Taseer & Mahmood, 2019)	websites Phishing attack detection using Genetic Algorithms	Genetic Algorithm (GA) was used to extract significant features for detecting the phishing websites	The feature obtained using GA outperformed in accuracy than the original feature set	The research only addresses website phishing attacks

Table 4: Anti-phishing solution for various Phishing techniques

Mobile Phishing Techniques	Anti-Phishing Solution
Smishing	Dynamic models and framework Blacklist
Vishing	User training Blacklist
Phishing websites	Password management tools Trusted path ensured browser Client server authentication Browser extension Pattern matching Blacklist
Phishing and spam emails	Anti-spam filters Client server authentication User training
Phishing applications	Personalized security indicators permission-based analysis
Malware	Anti-malicious programs

3. METHODOLOGY

The systematic literature review is a protocol-based research methodology. The systematic literature review conducted in this research aim to provide comprehensive insights into mobile phishing detection: techniques, trend and future direction.
Table 5 depicts the data search string and comprehensive overview of the research methodology is illustrated in Figure 2, which presents a flowchart outlining the process.

Table 5: Data Search Strings

List	Source
Electronic Database	ACM digital Library (ACM Digital Library) IEEE Explore(https://ieeexplore.ieee.org/) Springer Link (link.springer.com). Google Scholar (scholar.google.com). ResearchGate (researchdate.net)
Searched item Search applied on Search words	Conference, journal and books Do not miss articles that are relevant to our study, doesn't matter if those articles do not include search keywords Mobile phishing detection" AND "Techniques" AND "Trends," "Machine learning approaches" OR "Artificial intelligence methods" OR "Data mining techniques," and "Mobile phishing threats" AND "Cybersecurity strategies" AND "Future directions
Language	English
Publication period	2017 -2024

3.1 Article selection method

In the article selection method, we apply the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) exclusion criteria and the filtering process of the relevant and representative articles in the research. Table 6 presents the summary for Selection criteria of the retrieved literature.

Table 6: Selection criteria for the retrieved literature

Selection criteria	Scientific Database		Grey Literature
Inclusion criteria	Only peer- reviewed scientific research papers (including article in English language)		Industry reports, policy brief (written in English language)
	With time-frame restriction 2017-2024		With time frame restriction 2017-2024
Exclusion	Before import to the bibliography manager	Non-English written papers published in conference, proceedings, papers with missing abstract.	Generic paper relevant to mobile phishing without addressing, types and techniques for detection.
	During abstract screening	Papers belonging to other discipline than area of interest.	
	During full text reading	Papers describing mobile phishing without addressing, types and techniques for detection.	

Table 7 below represents a systematic mapping study of article database selections. This category of selection indicates number of articles downloaded per database used.

Table 7: Systematic Mapping Study of Article Database Selections

S/N	Journal Databases	Number of Articles
1.	ACM Library	3
2.	Elsevier	7
3.	Google Scholar	9
4.	IEEE Xplore	12
5.	Research Gate	8
6.	Science Direct	5
	TOTAL	44

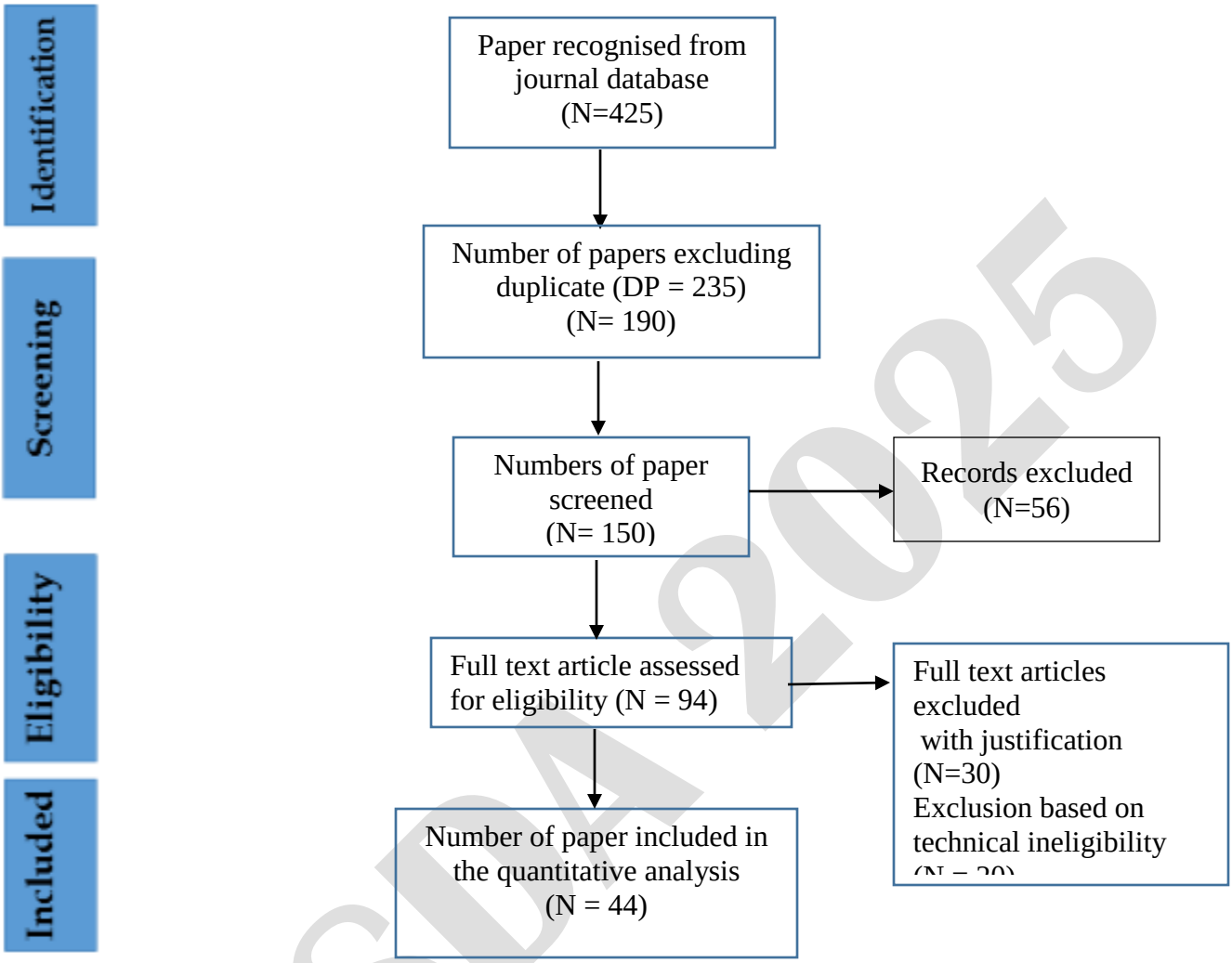

Figure 3: PRISMA SLR Block Diagram

4. RESULTS AND DISCUSSION

From total of 44 articles discussed in SLR, 6 mobile phishing techniques have been identified which are presented in Table 4.1.

Table 8: List of Identified Phishing Techniques

S/No	Identified phishing techniques	Frequency (N=44)	Percentage%
1	Smishing	22	50
2	Vishing	20	45
3	Phishing websites	11	25
4	Phishing and spam emails	22	50
5	Phishing applications	18	41
6	Malware	31	70

Figure 4 below illustrates the journal articles from diverse online databases, serving as a comprehensive literature base to support a thorough review of the discussed subject.

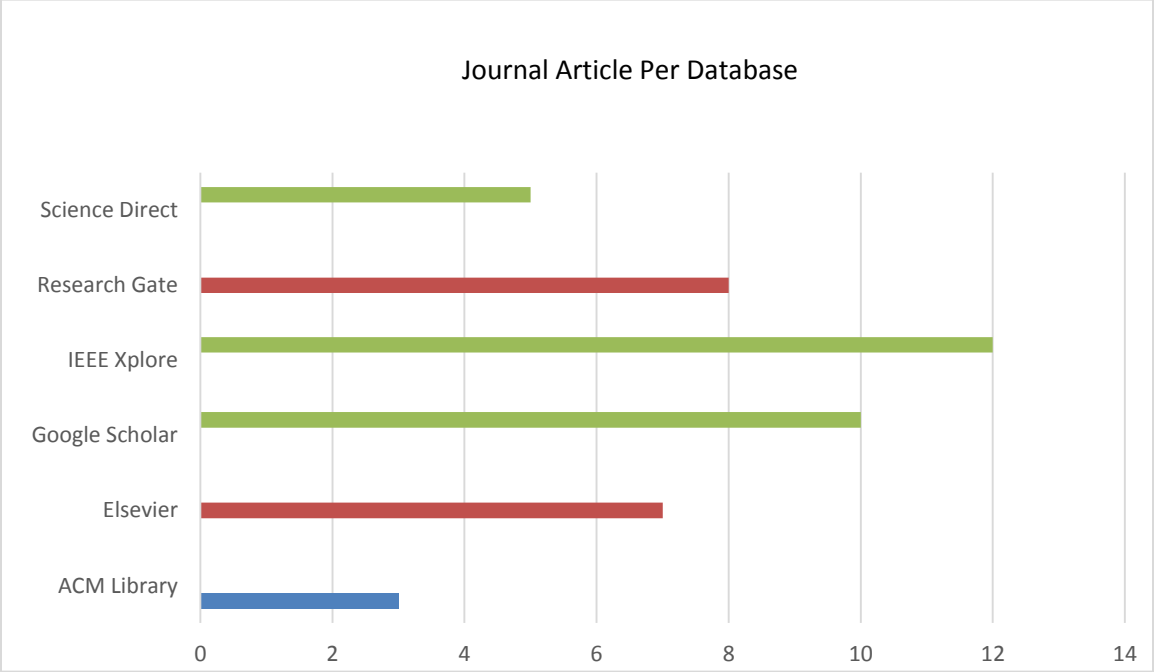

Figure 4: Total Journal articles distribution per database

From total of 44 articles discussed in SLR, 6 anti-mobile phishing techniques have been identified which are presented in Table 9.

Table 9: List of Identified Anti-Phishing Techniques

S/No	Identified Anti phishing techniques	Frequency (N=44)	Percentage%
1	Content Filtering	4	9
2	OCR method in mobile	3	7
3	Visual cryptography and code generation technique.	11	25
4	Multi Factor Authentication	10	23
5	Machine Learning Approach	12	28
6	Black listing	8	19

Figure 5 depicts the distribution of articles across different years, providing a comprehensive literature base to support the review of the subject under discussion.

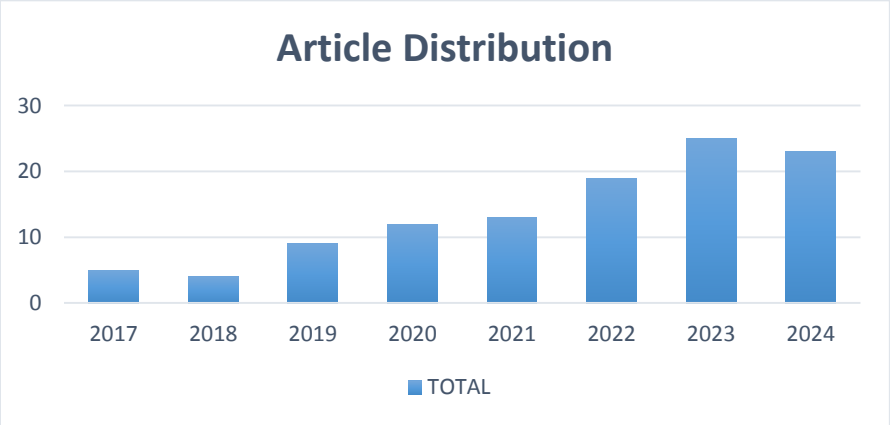

Figure 5: Total Journal articles distribution per year

5.1 CONTRIBUTION TO KNOWLEDGE

This article contributes to the existing body of knowledge on cybersecurity by identifying existing mobile phishing attacks, a rapidly evolving threat in the digital landscape. It highlights the unique vulnerabilities associated with mobile devices and the sophisticated tactics employed by cybercriminals to exploit these weaknesses. By systematically reviewing recent literature, the study identifies key trends in mobile phishing techniques, such as SMS phishing, voice phishing, and social media manipulation, thereby offering valuable insights into the mechanisms of these attacks.

Furthermore, the research emphasizes the critical role of social engineering in mobile phishing, illustrating how attackers leverage psychological manipulation to deceive users. This understanding is essential for developing effective countermeasures and enhancing user awareness. The findings advocate for targeted educational initiatives and robust security protocols tailored to mobile environments, thereby informing both practitioners and policymakers about the necessary steps to mitigate the risks associated with mobile phishing.

Ultimately, this article serves as a foundational resource for future research in the field of mobile cybersecurity, encouraging further exploration into innovative detection methods and preventive strategies to combat the growing threat of mobile phishing.

5.2 Open issues

As cybercriminals continuously evolve their tactics to exploit vulnerabilities in mobile devices, a significant open issue in the realm of mobile phishing research is the challenge of adaptive phishing techniques. These techniques often leverage sophisticated social engineering strategies that can deceive even the most vigilant users. The dynamic nature of these attacks necessitates ongoing research to develop detection and prevention mechanisms that can keep pace with the rapid evolution of phishing methods.

Current detection systems, including traditional blacklisting and heuristic approaches, frequently fall short in identifying new and innovative phishing schemes, particularly those that mimic legitimate services or utilize advanced technologies such as artificial intelligence. This gap in detection capabilities poses a critical risk to users, as they may unknowingly engage with malicious content that appears trustworthy.

5.3 Direction for future work

To address the above stated issue, future research must focus on creating adaptive detection frameworks that utilize machine learning and behavioural analysis to identify phishing attempts in real-time. Additionally, there is a need for comprehensive studies that explore the psychological factors influencing user susceptibility to these adaptive techniques, enabling the development of targeted educational initiatives that empower users to recognize and respond to evolving threats.

5.4 Conclusions

This study conducts a systematic literature review (SLR) focused on various types of mobile phishing, corresponding anti-phishing techniques and detection. The aim is to enhance understanding among readers, mobile device user and the internet users, and security managers regarding these issues. The study examines and surveys both phishing and anti-phishing techniques. The findings indicate that the most commonly employed phishing methods include spear phishing, email-based attacks, and phone phishing, while machine learning techniques, particularly deep learning, are identified as the most effective anti-phishing strategies. Ultimately, this study seeks to provide a comprehensive understanding of current and prevalent phishing, anti-phishing techniques and detection techniques.

REFERENCE

Alabdan, R. (2020). *Phishing Attacks Survey : Types , Vectors , and Technical Approaches*. https://doi.org/10.3390/fi12100168

Aldakheel, E. A., Zakariah, M., Gashgari, G. A., Almarshad, F. A., & Alzahrani, A. I. A. (2023). A Deep Learning-Based Innovative Technique for Phishing Detection in Modern Security with Uniform Resource Locators. *Sensors*, *23*(9). https://doi.org/10.3390/s23094403

Alhasan, A. A. (2016). Spam filtering framework for multimodal mobile communication based on

dendritic cell algorithm. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2016.02.018

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(March), 1–23. https://doi.org/10.3389/fcomp.2021.563060

Almeida, T. A., Silva, T. P., & Santos, I. (2017). *Text Normalization and Semantic Indexing to Enhance Instant Messaging and SMS Spam Filtering*. https://doi.org/10.1016/j.knosys.2016.05.001

Aonzo, S., Merlo, A., & Tavella, G. (2018). *Phishing Attacks on Modern Android*. https://doi.org/10.1145/3243734.3243778

Arshad, A., Rehman, A. U., Javaid, S., Ali, T. M., Sheikh, J. A., & Azeem, M. (2021). *A Systematic Literature Review on Phishing and Anti-Phishing Techniques*. 163–168. http://arxiv.org/abs/2104.01255

Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems*, *76*(1), 139–154. https://doi.org/10.1007/s11235-020-00733-2

Bidgoli, M., & Grossklags, J. (2017). "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. *ECrime Researchers Summit, ECrime*, 57–69. https://doi.org/10.1109/ECRIME.2017.7945055

Biswal, C. S., & Pani, S. K. (2021). Cyber-Crime Prevention Methodology. *Intelligent Data Analytics for Terror Threat Prediction: Architectures, Methodologies, Techniques and Applications*, *December*, 291–312. https://doi.org/10.1002/9781119711629.ch14

Canbay, Y. (2017). *Detection of Mobile Applications Leaking Sensitive Data*. https://doi.org/10.1109/ISDFS.2017.7916515

Cata, T., Patel, P. S., & Sakaguchi, T. (2013). *QR Code : A New Opportunity for Effective Mobile Marketing*. *2013*. https://doi.org/10.5171/2013.

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2021). Overview of Social Engineering Attacks on Social Networks. *Procedia Computer Science*, *198*(2021), 656–661. https://doi.org/10.1016/j.procs.2021.12.302

Chiew, K. L., Sheng, K., Yong, C., & Tan, C. L. (2018). PT. *Expert Systems With Applications*. https://doi.org/10.1016/j.eswa.2018.03.050

Choudhary, T., Mhapankar, S., Bhddha, R., Kharuk, A., & Patil, R. (2023). *A Machine Learning Approach for Phishing Attack Detection*. 108–113. https://doi.org/10.37965/jait.2023.0197

Faklaris, C. (2024). *Mitigating Smishing: Challenges and Future Work*. *3*, 1–5. https://doi.org/10.48550/arXiv.2401.14520

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing Evolves: Analyzing the Enduring Cybercrime. *Victims and Offenders*, *16*(3), 316–342. https://doi.org/10.1080/15564886.2020.1829224

Goel, D., & Jain, A. K. (2018). Mobile phishing attacks and defence mechanisms: State of art and open research challenges. *Computers and Security*, *73*, 519–544. https://doi.org/10.1016/j.cose.2017.12.006

Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629–3654. https://doi.org/10.1007/s00521-016-2275-y

Hashmi, S. S., Ikram, M., & Smith, S. (2019). *On Optimization of Ad-blocking Lists for Mobile Devices*. *October 2020*. https://doi.org/10.1145/3360774.3360830

Hawa Apandi, S., Sallim, J., & Mohd Sidek, R. (2020). Types of anti-phishing solutions for phishing attack. *IOP Conference Series: Materials Science and Engineering*, *769*(1). https://doi.org/10.1088/1757-899X/769/1/012072

Ijaz, M., Mustafa, E., Hamdani, K. J., & Päivärinta, T. (2021). *Effectiveness of Online Anti-Phishing Delivery methods in raising Awareness among Internet Users*.

www.ltu.se

Jain, A. K., & Gupta, B. B. (2017). Phishing detection: Analysis of visual similarity based approaches. *Security and Communication Networks*, *2017*(i). https://doi.org/10.1155/2017/5421046

Jain, A. K., & Gupta, B. B. (2022). A survey of phishing attack techniques, defence mechanisms and open research challenges. *Enterprise Information Systems*, *16*(4), 527–565. https://doi.org/10.1080/17517575.2021.1896786

Jain, A., Zhou, Z., & Guin, U. (2021). Survey of recent developments for hardware Trojan detection. *Proceedings - IEEE International Symposium on Circuits and Systems*, *2021-May*. https://doi.org/10.1109/ISCAS51556.2021.9401143

Janulevi˘, J. (2020). *applied sciences E-mail-Based Phishing Attack Taxonomy*. 1–15. https://doi.org/10.3390/app10072363

Kaddoura, S., Chandrasekaran, G., Popescu, D. E., & Duraisamy, J. H. (2022). *A systematic literature review on spam content detection and classi fi cation*. https://doi.org/10.7717/peerj-cs.830

Karantias, K., Kiayias, A., & Zindros, D. (2020). *Financial Cryptography and Data Security 2013*. https://dx.doi.org/10.1007/978-3-642-39884-1

Korkmaz, M., Sahingoz, O. K., & Diri, B. (2020). Feature Selections for the Classification of Webpages to Detect Phishing Attacks: A Survey. *HORA 2020 - 2nd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, *June*. https://doi.org/10.1109/HORA49412.2020.9152934

Kulkarni, A., Balachandran, V., & Das, T. (2024). Phishing Webpage Detection: Unveiling the Threat Landscape and Investigating Detection Techniques. *IEEE Communications Surveys and Tutorials*, *Ml*. https://doi.org/10.1109/COMST.2024.3441752

Kunju, M. V, & Anthony, H. C. (2019). Evaluation of Phishing Techniques Based on Machine Learning. *2019 International Conference on Intelligent Computing and Control Systems (ICCS)*, *Iciccs*, 963–968. https://doi.org/10.1109/ICCS45141.2019.9065639

Kuss, D. J., & Griffiths, M. D. (2017). Social networking sites and addiction: Ten lessons learned. *International Journal of Environmental Research and Public Health*, *14*(3). https://doi.org/10.3390/ijerph14030311

Lonzetta, A. M., Cope, P., Campbell, J., & Mohd, B. J. (2018). *Security Vulnerabilities in Bluetooth Technology as Used in IoT*. 1–26. https://doi.org/10.3390/jsan7030028

McAlaney, J., & Hills, P. J. (2020). Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking. *Frontiers in Psychology*, *11*(July), 1–13. https://doi.org/10.3389/fpsyg.2020.01756

Naaz, S. (2021). Detection of phishing in internet of things using machine learning approach. *International Journal of Digital Crime and Forensics*, *13*(2), 1–15. https://doi.org/10.4018/IJDCF.2021030101

Nadeem, M., Zahra, S. W., & Abbasi, M. N. (2023). *Phishing Attack , Its Detections and Prevention Techniques*. *October*. https://doi.org/10.37591/IJWSN

Omari, K. (2023). Phishing Detection using Gradient Boosting Classifier. *Procedia Computer Science*, *230*(2023), 120–127. https://doi.org/10.1016/j.procs.2023.12.067

Orunsolu, A. A., Sodiya, A. S., & Akinwale, A. T. (2022). A predictive model for phishing detection. *Journal of King Saud University - Computer and Information Sciences*, *34*(2), 232–247. https://doi.org/10.1016/j.jksuci.2019.12.005

Owen, J. (2024). *Exploring Mobile Device Phishing : User Behavior and Awareness in the Face of Unique Challenges Exploring mobile device phishing : User behavior and awareness in the face of unique challenges*. https://easychair.org/publications/preprint/kxcf/open

Page, M. J., & Moher, D. (2017). *Evaluations of the uptake and impact of the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) Statement and extensions : a scoping review*. 1–14. https://doi.org/10.1186/ss13643-017-0663-8

Said, Y., Alsheikhy, A. A., Lahza, H., & Shawly, T. (2024). Detecting phishing websites through improving convolutional neural networks with Self-Attention mechanism. *Ain Shams Engineering Journal*, *15*(4), 102643. https://doi.org/10.1016/j.asej.2024.102643

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). https://doi.org/10.3390/FI11040089

Silva, R. M., Almeida, T. A., & Yamakami, A. (2016). *MDLText : An Efficient and Lightweight Text Classifier MDLText : An Efficient and Lightweight Text Classifier*. *November*. https://doi.org/10.1016/j.knosys.2016.11.018

Singh, L. J., & Imphal, N. (2018). *A Survey on Phishing and Anti-Phishing Techniques*. *6*(2), 62–68. https://www.ijcstjournal.org/volume-6/issue-2/IJCST-V6I2P13.pdf

Sylvester, F. L. (2022). Mobile Device Users' Susceptibility to Phishing Attacks. *International Journal of Computer Science and Information Technology*, *14*(1), 1–18. https://doi.org/10.5121/ijcsit.2022.14101

Tang, L., & Mahmoud, Q. H. (2021). A Survey of Machine Learning-Based Solutions for Phishing Website Detection. *Machine Learning and Knowledge Extraction*, *3*(3), 672–694. https://doi.org/10.3390/make3030034

Taseer, M., & Mahmood, S. (2019). *Optimization of URL-Based Phishing Websites Detection through Genetic Algorithms*. *53*(4), 333–341. https://doi.org/10.3103/S0146411619040102

Torres, J., & Flores, P. (2019). *Cross-Site Scripting (XSS) Attacks And Mitigation : A Survey*. *November*. https://doi.org/10.1016/j.comnet.2019.106960

Trapp, J. (2020). Predatory publishing, hijacking of legitimate journals and impersonation of researchers via special issue announcements: a warning for editors and authors about a new scam. *Physical and Engineering Sciences in Medicine*, *43*(1), 9–10. https://doi.org/10.1007/s13246-019-00835-5

Wani, M. A. (2017). *A sneak into the Devil ' s Colony- Fake Profiles in Online Social Networks*. http://dx.doi.org/10.48550/arXiv.1803.08810

Weichbroth, P., & Łysik, Ł. (2020). Mobile Security: Threats and Best Practices. *Mobile Information Systems*, *2020*. https://doi.org/10.1155/2020/8828078

Woong, J., Seo, J., Moon, Y., Singh, S., & Hyuk, J. (2017). S-Detector : an enhanced security model for detecting Smishing attack for mobile computing. *Telecommunication Systems*. https://doi.org/10.1007/s11235-016-0269-9

Wu, L., Du, X., & Wu, J. (2016). Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms. *IEEE Transactions on Vehicular Technology*, *65*(8), 6678–6691. https://doi.org/10.1109/TVT.2015.2472993

Yadav, K., Malhotra, A., Kumaraguru, P., Khurana, R., & Singh, D. K. (2012). *Take Control Over your SMSes : A Real-World Evaluation of a Mobile-based Spam SMS Filtering System*. https://repository.iiitd.edu.in/jspui/handle/123456789/38

Yet, S., & Attacks, E. (2019). *Phishing and Fraud*. https://www.f5.com/labs/articles/threat-intelligence/2019-phishing-and-fraud-report