Pages :109-122

A Comprehensive Study of Phishing and Defense Strategies

Nair Sruthi Sreekumar

Department of Information Technology and Computer Science

Somaiya Vidyavihar University Mumbai,

Maharashtra, India

Email: sruthi.nair@somaiya.edu

Abstract

As internet usage continues to grow, individuals increasingly disclose private data online. Consequently, the vast quantity of personal data and financial transactions becomes susceptible to cyber-criminal activities. Phishing exemplifies a notably effective cybercrime that allows perpetrators to mislead individuals and obtain critical information. Since its inception in 1990, phishing has transformed into a more advanced attack modality. At present, phishing ranks among the most prevalent forms of fraudulent behaviour on the Internet. Phishing incidents can result in significant repercussions for victims, including the loss of sensitive data, identity theft, and breaches of corporate and governmental confidentiality. This article seeks to assess phishing attacks by delineating the contemporary landscape of phishing and analyzing existing methodologies employed in such attacks. Research has categorized phishing incidents based on essential phishing frameworks and countermeasures, neglecting the significance of the comprehensive phishing lifecycle. This article introduces a novel, intricate framework of phishing attack encompassing different stages of attacks, classifications of attackers, security flaws, threats, intended victims, mediums of attack, and techniques employed. Additionally, the recommended framework will enhance viewer's comprehension of the phishing attack life cycle, thereby fostering greater awareness of these threats and the strategies utilized; it also contributes to the formulation of a comprehensive anti-phishing strategy. In addition, safety protocols are examined, and innovative strategies are proposed.

Keyword: phishing anatomy, defenses against phishing, phishing targets, Ai phishing attack, phishing attacks, phishing examples.

◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇◇

Received	: 10 October 2024
Revised	: 16 November 2024
Accepted	: 05 December 2024

1. INTRODUCTION

With the considerable expansion of internet utilization, individuals are progressively disclosing their personal data in online globally. Consequently, a vast quantity of personal information and financial transactions are rendered susceptible to cybercriminal activities. One such cyber-attack is called as Phishing. Phishing involves sending malicious messages designed to trick victims into disclosing their sensitive information or to distribute malwares such as ransom ware, into a victim's infrastructure. Phishing employs techniques of impersonation and various forms of deception to create the illusion that the communication originates from a trusted individual, thereby convincing you that the actions you undertake will yield some form of benefit. All of the highly publicized phishing scam cases, 'The John Podesta Case' proves that regardless of a user's background and technical knowledge, how anyone can fall victim and the consequences can be huge.

Studies show a steady increase in phishing activities as well as the related cost. India experienced over 79 million phishing attacks, ranking it the third most targeted country. In the initial quarter of the year 2024, it was observed that approximately 37.6 percent of global phishing assaults were directed towards social media platforms. The subsequent category, comprising web-based software services and webmail, accounted for nearly 21 percent of the documented phishing incidents. Users in Vietnam were the most phished in 2023.

During the review, Peru ranked second, with nearly 17% of the population affected. Taiwan followed closely behind, with an attack rate of 15.59 percent (Schafer, 2024). The rise in phishing attacks is primarily due to insufficient awareness of hackers' methods. This paper focuses to analyze phishing attacks trends, identifying and assessing the latest phishing techniques used by cybercriminals. This research will also discuss the changing nature of attack methods, new patterns, as well as different phishing techniques such as spear phishing, whaling, and smishing etc. This article also seeks to assess effective prevention strategies against phishing through the evaluation of diverse methodologies and technologies.

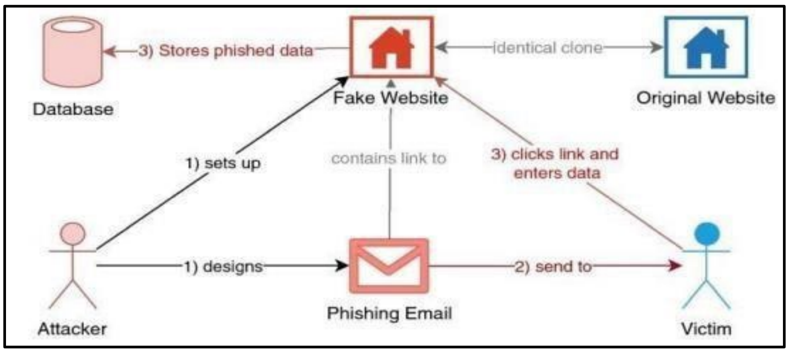

Figure 1. Example-of-an-email-based- phishing-attack (Fortinet, n.d.)

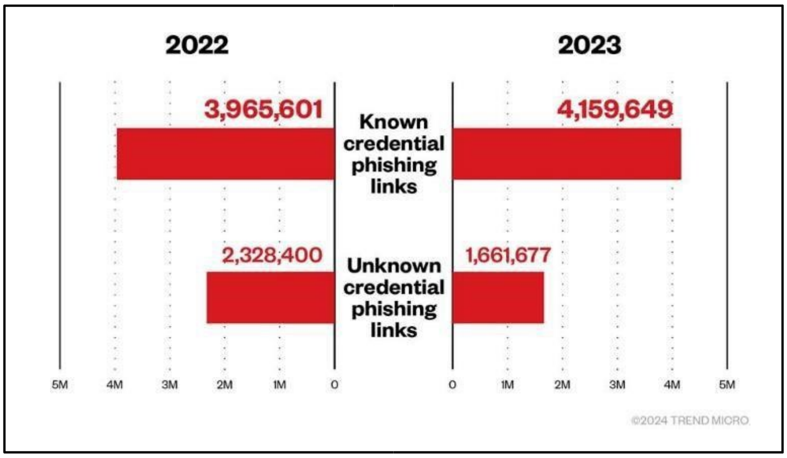

Figure 2. Statistics of credential Phishing Links (Statista, 2024)

2. LITERATURE REVIEW

Phishing is a tactic used to get private information about a target by sending out fraudulent emails and links. It's among the riskiest cyberattacks that may happen to individuals, businesses, or other electronic equipment. It might be challenging to tell the difference between phishing and legitimate emails. There exist several techniques to evade this assault. Regularly updating anti-phishing tools and platforms on a regular basis may be quite effective. The research paper "Analysis of phishing attacks and countermeasures." by Issac, Biju, Raymond Chiong, and Seibu Mary Jacob presents information about phishing, its mechanism, the different kinds it can take, and potential countermeasures.

PHISHING ATTACKS TYPES

Phishing has grown beyond just stealing login details and information. An attacker's approach to setting up a campaign hinges on the phishing type. Here are some types of phishing:

Email phishing: Phishing emails is one of the leading type of phishing types, and hackers have used it since the 1990s. As shown in Figure 1, the scammers creates an email that includes a link to any fake website which is sent to any email addresses that they can get their hands on. The message tells the victim that someone has broken into his/her account and need to act fast by interacting with a link they provide. The sensitive information entered by the victim is stored in their databases to exploit for malicious purposes. One can often spot these attacks because the email's wording has spelling mistakes and/or grammar slip-ups. (Khalifa & Khalifa, 2023) (Statista, 2024).

Some emails can be tough to spot as phishing scams when the writing is more polished. To figure out if the source is real, you can look at the email's origin and check the link, they want you to click on for any odd wording. These steps can give you hints about whether it's legit or not (Schafer, 2024).

Spear phishing: Cybercriminals send these emails to certain individuals in a company those with high-level access. The goal is to fool them into sharing sensitive info transferring money to the bad guys, or downloading harmful software (Statista, 2024).

Link manipulation: Emails have links to fake websites that look like real company sites. These links take people to servers run by hackers. There, victims are tricked into logging in to fake pages. This sends their login details straight to the bad guys (Statista, 2024).

Whaling (CEO fraud): These types of emails are sent to important staff members of a company to fool them to think that the CEO or another executive have asked them to move money. CEO email scam is a type of phishing, but the attacker pretends to be the CEO of the targeted company instead of mimicking a well-known website (Khalifa & Khalifa, 2023) (Statista, 2024).

Content injection: A hacker who can sneak harmful content into a legitimate website has the ability to fool visitors. This trickery leads to users seeing a dangerous pop-up or ending up on a fake site designed to steal their information (Statista, 2024).

Malware: Users who are duped into opening a file or clicking a link risk having malware downloaded to their devices. Common malware threats that steal data and demand payments from targeted victims are called ransom ware, root kits, or key loggers (Statista, 2024).

Vishing: Attackers use Ai softwares to leave a message telling the targeted victims that they must call a number where they can be scammed (Khalifa & Khalifa, 2023) (Statista, 2024). The usage of voice changers to mask an attacker's gender or accent during communication with certain victims allows them to pass for someone else entirely.

"Evil Twin" Wi-Fi: Man-in-the-middle attacks are carried out by the attackers by utilize free Wi-Fi spoofing to deceive users into connecting to a malicious hotspot.

Pharming: The two-phase approach known as "pharming" is used to get account credentials. In the first stage, a targeted victim is infected with malware, which then takes them to a fake website and browser where they are tricked into providing login credentials. Users can potentially be sent to fake domains using DNS poisoning (Schafer, 2024).

Angler phishing: Attackers utilize social networking sites to respond to posting posing as representatives of legitimate companies, fooling users into disclosing login passwords and other data (Schafer, 2024).

Watering hole: An attacker can employ malware to take control of targeted user computers and manipulate users to visit phony websites or send a payload to the local network in order to transfer information (Schafer, 2024).

Smishing: Attackers use SMS messages to get consumers to visit malicious websites on their smartphones. Attackers transmit a malicious link along with a text message offering discounts, incentives, or freebies to a specific victim (Schafer, 2024).

3. RESEARCH OBJECTIVES

The escalating sophistication and impact of phishing scams pose a significant threat to people and businesses worldwide. Despite ongoing efforts to mitigate these risks, phishers continue to adapt their techniques, exploiting vulnerabilities in human behaviour and technology.

Comprehensive Analysis of Phishing Tactics: To undertake a comprehensive examination of modern phishing methodologies, encompassing email phishing, spear phishing, smishing, and vishing, for the purpose of discerning novel trends and patterns.

Identification of Vulnerable Populations: To determine demographic, socioeconomic, and behavioural factors that contribute to individual susceptibility to phishing attacks, enabling targeted prevention strategies.

Evaluation of Phishing Prevention Measures: This entails a systematic analysis of existing defensive measures in place and their sufficiency in combating ethereal terrorism attack endeavour, which include use of technology, education, users and morphological means.

Development of Advanced Prevention and Detection Methods: The aim is to develop, implement and evaluate new and promising strategies in regard to the prevention and detection of phishing, for example, security awareness training combined with behavioural targeting and machine learnings.

Assessment of the Economic and Social Impact: Evaluation of the Interpersonal and the Macroeconomic Impact: It is necessary to measure the costs and the impacts including financial losses, identity theft, brand harm, etc. caused due to phishing attacks so that it will assist appropriate policy formulation and resource allocation.

By focusing on those research objectives, this study helps contribute to the development of more robust and effective means of countering phishing attacks toward both individuals and organizations that involve such risks.

4. RESEARCH FINDING

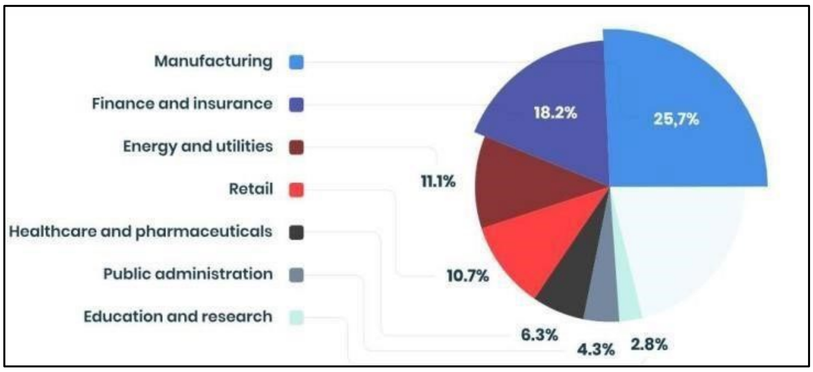

Figure 3. Statistics of Industries affected by Phishing (Pryimenko, 2024)

The adaptability of phishing attacks have targeted diverse sectors. Figure 3 illustrates the different industries affected by phishing, as reported by Pryimenko (2024).

Manufacturing: The data shows that this industry is affected the most at 25.7%. The data suggests that the Made-in-China certification organization is the most frequently impersonated entity within the manufacturing sector, despite its role as a certifying body for manufacturers and suppliers (Imber, 2024).

Primarily, the sector is dependent on specialized machinery, intricate production processes, and proprietary technologies that pose significant challenges in comprehension and may not present substantial value or ease of monetization for cybercriminals, particularly in contrast to industries such as finance (Pryimenko, 2024).

Furthermore, manufacturing firms generally possess limited direct access to high-value personal or financial records, including debit/credit card number and personal identification number that are frequently sought after by cyber criminals. This diminishes the potential incentives for phishing attacks targeting these organizations. Additionally, the lack of extensive Personally Identifiable Information (PII) databases within the manufacturing domain serves as a disincentive for cybercriminals, who typically favour sectors that yield larger quantities of personal data for exploitation (Pryimenko, 2024).

Finance: Since a significant proportion of scammers are primarily motivated by financial gain, it is not particularly surprising that financial institutions rank as the foremost targets of phishing schemes. It is estimated that approximately 96% of cyber intrusions directed at insurance or financial entities are driven by monetary objectives.

Credentials for financial service platforms are especially in demand by cyber criminals, as the financial information procured can be exploited in various manners or traded; thus, numerous targeted fraudulent schemes concentrate on these credentials.

Furthermore, they may aim to infiltrate the organizations' email or communication systems to leverage the reputable identity of the firm, thereby persuading clients to transfer funds into the fraudster's bank account (Pryimenko, 2024).

Phishing schemes that deceive employees into clicking hyperlinks that lead to malware downloads are also prevalent; this malware can potentially allow fraudsters to monitor users entering passwords or even facilitate unauthorized access to the device itself (Pryimenko, 2024).

There has been a serious increase in cyber-attacks against financial sector that specifically target mobile devices, with the intent of installing trojanized applications (Pryimenko, 2024).

Energy and Utilities: Out of all the industries polled, this one was most affected by lost worker productivity; of those surveyed, over half (52%) cited this as a result of the attack, compared to just 38% overall. The fact that 48% of workers had more than half of their staff working remotely or in the field—where they would be unable to work during downtime is probably why productivity dropped (Pryimenko, 2024).

The companies that were the victims of spear phishing experienced effects that were, albeit seldom, as noticeable in other industries. 64% of respondents reported that malware or viruses had infected computers or other devices, compared to 55% of respondents overall; 62% reported that sensitive or confidential data had been taken, compared to 49% of respondents overall. According to 45% of respondents, reputational harm appears to have been a significant impact on this industry once more. When compared to the 37% total for the entire industry, this is higher than any other industry. Out of the 47% who claimed having virus and malware filters installed, just 37% said they had them in place (Pryimenko, 2024).

Retail: The retail industry's lax security standards are the main contributor to data breaches. Retailers either don't worry about security at all or primarily rely on outside organizations to provide security services.

Even though the majority of attacks only reveal names and other basic personal information, things can quickly get worse if the victim uses bad password hygiene. In 2013, hackers breached Target's security, revealing the personal data of 70 million customers as well as 41 million payment cards (Alkhalil, Hewage, Nawaf, and Khan. 2021*)*.

Retailer JD Sports experienced a cyber-attack in 2023 where hackers gained access to customer data, including full name, delivery and address credit, contact number, and email, as well as the company's sales database from 2018 to 2020 (Imber, 2024).

Health and Pharmaceuticals: Health care organizations in 2023, saw the largest data breach since 2009. One of the main motivations for hackers to break into reek into health care facilities is to make money. Stolen records are also be used to gain unauthorized access to medical data or obtain prescriptions (Pryimenko, 2024).

The number of phishing assaults on the health care industry is expanding, in spite of organizations giving online security preparing to representatives. Numerous of the fruitful assaults are inferable to the expanding number of workers utilizing their portable gadgets at work, who come up short to decipher their online security preparing to their portable online exercises. With the expanded selection of BYOD approaches within the health care industries, organizations ought to increment their endeavours to secure health care information from phishing (Pryimenko, 2024).

Public Administration: One of the most popular targets for hackers and cyber-attacks is the public administration sector. A common outcome of data theft for financial gain is the loss of government information. A multitude of sensitive and valuable data, including resident personal information, information on classified documents, payment card and banking information, and details on vital infrastructure, are stored in government systems. If an attacker gains access to this information, they can sell it on the dark web, commit identity theft or launch additional attacks (Pryimenko, 2024).

Security events within the government sector are still becoming more frequent. Cyberattacks against governmental and public institutions surged by 40% in the second quarter of 2023 compared to the first, according to BlackBerry's Global Threat Intelligence Report. It makes sense that authorities are working hard to strengthen their cybersecurity and are taking precautions against cyberattacks, particularly those that are sponsored by the government (Alkhalil, Hewage, Nawaf, & Khan, 2021*)*.

Education and Research: Verizon's 2023 Data Breach Investigation Report reveals that system intrusion and human error continue to be the primary reasons for data breaches in the educational sector. Pretexting one of the most popular technique of social engineering, with a 21% increase from 14% in 2022 to 21% in 2023. Through the use of deceptive communications, attackers utilize this tactic to trick their victims (Pryimenko, 2024).

Accountancy information, personally identifiable information, bank routing information, health records, research data, and other information may be exposed by data breaches at educational institutions. In one instance, in March 2023, unauthorized party access resulted in the disclosure of personal data, including the social security numbers of workers and students at Connecticut College (Pryimenko, 2024).

AI in Phishing Attack

An AI phishing campaign uses artificial intelligence to make phishing emails appear more convincing and tailored. An adversary might construct customized ads by using AI algorithms to evaluate a large quantity of data about a target group, including social media profiles, internet activity, and publicly accessible information (D'Andrea & D'Andrea, 2024) *(Afridi S., 2024).*

It's possible for the phishing message to contain recognizable elements like mentions of the user's previous interactions, hobbies, or purchases. The probability of success is increased with this degree of customisation. Additionally, AI is capable of producing convincing duplicates of authentic websites with ease, making it challenging for the receiver to tell the difference between the two. Artificial intelligence phishing is based on a set of principles that provide an infinite array of potentialities (D'Andrea & D'Andrea, 2024).

Artificial intelligence (AI) enables fraudsters to launch increasingly potent phishing attacks against both people and companies. One of the biggest example is *'Deepfake Phishing' (Dixit, Kaur, & Kingra, 2023).*

Deepfake phishing is the practice of tricking someone into disclosing personal information by using Deepfake technology, which uses machine learning and artificial intelligence to produce realistic-looking but fraudulent audio-visual content.

5. Defenses against Phishing Attack

Anti-phishing mechanisms conduct analyses to identify inconsistencies between the perceived sender and the genuine sender, hyperlinks that direct to recognized nefarious websites, and harmful attachments. An effective anti-spam mechanism will obstruct numerous phishing attempts without necessitating an examination of the message for harmful content, merely due to the discrepancy between the perceived sender and the actual sender, or because the legitimate sender disseminates the identical message to multiple recipients simultaneously (Imber, 2024).

Nonetheless, the education of users remains a critical factor even in the presence of a phishing detection system. Cyber criminals perpetually seek innovative methodologies to circumvent filters. For instance, they frequently establish new domains daily and dismantle domains once they have been flagged as fraudulent by security vendors (Pryimenko, 2024).

This incessant evolution complicates the efforts of security vendors to maintain their signature files in a current state. Some general precautions that can be taken against phishing at a user level are as follows:

Anti-Phishing Software: Numerous firewalls, which are also referred to as Unified Threat Management (UTM) systems, undertake the scrutiny of incoming electronic mail to identify potential security threats. An essential procedure in utilizing a firewall as a measure against phishing attacks is to verify that its anti-phishing capabilities are activated and to ensure that it is regularly updated, thereby encompassing newly emerged phishing threats immediately upon detection by the security vendor (Pryimenko, 2024) (Alkhalil, Hewage, Nawaf, & Khan, I. 2021*)*.

Spam Filter: Whether it is hosted internally by Linux Send email or Exchange from Microsoft, or it is hosted by a third party like Google, for example, your email system can use spam filters to identify a variety from dangerous email types. This covers unwanted commercial emails, malware in emails, and phishes. (Pryimenko, 2024).

Antivirus Solution: Install an antivirus solution, set up signature updates, and keep track on the antivirus status on all equipment. It's essential to have good antivirus software. It will prevent many forms of harmful material in addition to phishes (Pryimenko, 2024).

Two-Factor Authentication: Two-factor verification, commonly labelled 2FA, establishes an added safeguard in the user login mechanism. Instead of merely necessitating username and CMT password, 2FA dispatches a text message or another supplementary factor to which the user must accurately respond prior to being granted access. In instances where a malicious actor possesses both a user's login username and their password, they remain unable to gain entry to a website due to their inability to correctly provide the requisite second factor (Pryimenko, 2024) (Isaac, Chiong, & Jacob, 2014) *(*Abbas, A. 2024)..

Password Management: Rather than needing to type a password each time a website is accessed, a password manager safely houses the credentials in a protected database. Upon navigating to the login interface of a specific website, the password manager automatically populates the username and password fields (Abbas, A. 2024). Given that the password manager maintains the authentication details for each website independently, a website whose URL is similar to that of the legitimate site, yet not an exact replica, will lack any stored login credentials. This serves as an additional indicator to the user that an anomaly may be present (Pryimenko, 2024).

Educating Employees on Phishing Attack:

Teaching the employees about phishing email and how it looks like, how to identify fakes and what to do when they get one (Phishing attack, n.d.).Instructing employees to come forward in the event, where they believe they've received one (Phishing attack, n.d.).

Ensure that your staff members are regularly informed on successful phishing attempts that have occurred within your industry (Phishing attack, n.d.).

Run a simulated phishing assault. Make a third-party email account and periodically send emails to see if you can identify anyone clicking on links that they shouldn't be (Phishing attack, n.d.).

Make sure to include high management. They must be as prepared as the rest of your organization because spear and clone phishes frequently target them explicitly (Phishing attack, n.d.).

Get the checklist of items to check printed out, and ask your staff to post it in a visible location at their workstations (Phishing attack, n.d.)

Artificial Intelligence:

Recognizing Patterns: AI is great at noticing details. It looks at things like the sender's email address or the tone of a message. If something feels "off," like a slightly different email domain or an unusual subject line, AI can catch it—things most of us might overlook.

Watching User Habits: AI learns how we usually communicate—who we email, how we write, and what we talk about. If an email suddenly asks for your password or money, and it doesn't fit your usual style, AI raises a red flag.

Staying Up to Date: Cybercriminals are always coming up with new tricks. AI connects to global security networks to learn about the latest scams and quickly adapts to spot them *(Afridi, S. 2024).*

Taking Immediate Action: If AI detects a suspicious email, it can block it or send you a warning right away. This quick response protects your data and saves your IT team a lot of time and effort *(Afridi, S. 2024).*

Team Player: AI works best when combined with other security measures, like firewalls and employee training. Together, they create a strong defense to keep phishing scams out.

6. CONCLUSION AND FUTURE WORK

We have examined many phishing attack features theoretically in this paper. In the corporate world of today, we have offered some of the defences that are required to thwart some of the most prevalent attacks, which we have briefly outlined. Furthermore, in order to forecast the expanding issue of phishing spam, we have chosen a few recent data findings. In our opinion, since the advent of e-commerce, businesses have been subjected to a variety of new cyber security concerns. New technical opportunities that arise in fraud also entail business strategies that change to stay up with the development of new technology. Thus, our article put up an anti-phishing approach with the expectation that a greater awareness of phishing and online crime in general will help prevent many identity theft occurrences.

The frequency of phishing and malware assaults continues to provide a daunting issue year after year. However, given the recent notable technological advances, the approaches and plans that hackers use to carry out these assaults are always changing. To safeguard against phishing attacks that exploit cloud infrastructure, organizations should implement a comprehensive, multi-layered cyber security strategy:

Organizations should utilize CSPM solutions to oversee and enforce security best practices within their cloud environments. These tools are designed to identify misconfigurations, unauthorized access, and unusual activities, thereby assisting organizations in maintaining a robust cloud security posture (Isaac, Chiong, & Jacob, 2014).

Security Measure	Description
User Awareness Training	Educating employee on recognizing phishing attempts and suspicious communications.
Email Security Gateways	Deploy gateways that detect and block phishing emails using machine learning and threat intelligence.
Endpoint Protection	Implementing solutions with cloud based threat detection to protect against malicious activity on end point
Phishing Simulation	Conduct a simulated phishing exercises to test and improve employee response to phishing attempts.
Security Updates	Updating softwares and systems time to time to prevent vulnerabilities that can be exploited by phishing attacks.

REFERENCES

Isaac, B., Chiong, R., & Jacob, S. (2014). Comprehensive analysis of phishing attacks and mitigation strategies. ArXiv. Retrieved from https://doi.org/10.48550/arxiv.1410.4672

Khalifa, P. I., & Khalifa, I. M. S. (2023). Insights into phishing attacks and their implications. IASMS Research Studies. Available at https://www.academia.edu/106372716/Study_on_Phishing_Attacks?auto=download

Phishing Attacks Overview. (n.d.). The Security Company. Accessible at https://thesecuritycompany.com

Cybersecurity and Infrastructure Security Agency (CISA). (2024, October 1). Homepage. Retrieved from https://www.cisa.gov/

Pryimenko, L. (2024, July 31). Industries most vulnerable to phishing attacks: Insights and analysis. Ekran System Blog. Available at https://www.ekransystem.com/en/blog/5-industries-most-risk-of-databreaches

Imber, D. (2024, June 26). Current trends in phishing: Updated statistics and findings. AAG IT Support Blog. Retrieved from https://aag-it.com/the-latest-phishing-statistics/

Fortinet. (n.d.). A guide to 19 types of phishing attacks with examples. Retrieved from https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks

Statista. (2024, September 13). Global phishing distribution in 2023 by region. Retrieved from https://www.statista.com/statistics/266362/phishing-attacks-country/

Schafer, N. (2024, August 28). The rise of AI in phishing: Risks and strategies to counteract. Mailgun Blog. Available at https://www.mailgun.com/blog/email/aiphishing/#chapter-3

D'Andrea, A., & D'Andrea, A. (2024, September 13). Enhancing phishing attacks with AI: Challenges and countermeasures. Keeper Security Blog. Retrieved from https://www.keepersecurity.com/blog/2024/09/13/how-ai-is-making-phishing-attacksmore-dangerous/

Dixit, A., Kaur, N., & Kingra, S. (2023). Advancements in audio deepfake detection: Opportunities and challenges. Expert Systems, 40(8). DOI: https://doi.org/10.1111/exsy.13322

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). An extensive study of phishing attacks and a new structural analysis. Frontiers in Computer Science, 3, Article 563060. DOI: https://doi.org/10.3389/fcomp.2021.563060

Abbas, A. (2024). Innovative mechanisms for phishing defense: A focus on effective strategies and evaluations. DOI: https://doi.org/10.13140/RG.2.2.18505.97128

Afridi, S. (2024). A transformative perspective on phishing defense mechanisms and their evaluation. DOI: https://doi.org/10.13140/RG.2.2.36331.76322