A Study of Software Security Approaches for Protection Against Social Media Phishing Attacks

R.Padma Devi*[1], V.Khanaa[1]

[1]Department of Computer Science and Engineering, Bharath institute of higher education and research, Chennai,Tamilnadu, India
drvkannan62@yahoo.com

Abstract. The high growth of internet has changed the way many social and economic activities are carried out and organizations are now able to provide their services worldwide using e-commerce and digital mediums. Nonetheless, this development has also predisposed users to cyber threats especially phishing which tricks people into disclosing sensitive information by masquerading as genuine websites. Examples of such attacks include financial loss, manipulation of data, damaged reputation and less trust in online services. This paper provides a detailed overview of phishing activities, their causes, effects, prevention methods, and the present threat. It further emphasizes the need to have strong cybersecurity laboratories to examine the emerging attacks and enhance defense mechanisms. Furthermore, demonstrate the importance of high-tech research settings in the detection, prevention, and comprehension of threats in the form of phishing and malware.

Keywords: Phishing, Cybersecurity, Cyber Threats, AntiPhishing Techniques, Social media security, Malware Detection, Digital Forensics

1. Introduction

In the digital era, the internet has become an essential element of everyday life that has been used in all manners of interaction, including communication, social networking, internet business, and internet banking. People regularly post personal data, post pictures, announce their current positions, and make financial transactions on the Internet, and in many cases, they are not fully aware of the security consequences. Such prevalence of the online platforms has provided an opportunity to cybercriminals to take advantage of unsuspecting users, and cyberattacks have increased dramatically. One of the most widespread and harmful threats is phishing among them. Phishing is a form of cybercrime where offenders display themselves as a trusted person or an organization with good status using electronic means to lure the victims to divulge sensitive details. Such credentials can be bank account numbers, passwords, credit cards or any other personal data. Using social engineering strategy and psychological exploitation, phishers can influence people to make the wrong choice, clicking on the malicious links, accessing the fraudulent websites, or downloading the harmful files. Phishing has over the times become numerous including email phishing, spear phishing, smishing, vishing and whaling, all making use of various channels of communication yet with the similar motive of extracting confidential data. Ever since phishing appeared at the middle of the 1990s, it has become more sophisticated, and

S. P. Vijayaragavan et al. (eds.), *Proceedings of the Global Conference on Sustainable Energy Systems, Smart Electronics and Intelligent Computing (GCSESEIC 2025)*, Advances in Engineering Research 297,
https://doi.org/10.2991/978-94-6239-654-8_51

cybercriminals are constantly improving their methods. The emergence of generative AI over the last few years has tremendously reshaped the phishing environment, allowing scamming individuals to develop very convincing and customized ones with the bare minimum effort. [1][2]

This democratization of sophisticated attack tools has reduced the threshold to entry into the world of inexperienced cybercriminals, and resulted in a boom in high scale, highly target-oriented phishing attacks. This leads to more and more challenges in protecting their systems and data by organisations. In a bid to counter these fears, different cybersecurity research organizations, such as ThreatLabz team of Zscaler, have come up with detailed reports that can assist organizations to make sense of the prevailing phishing trends. The 2024 ThreatLabz Phishing Report, which was conducted on the analysis of more than 2 billion phishing transactions, is a great source of information regarding active attack campaigns, new approaches, impersonated brands, and targeted industries. The results underline the necessity of constant attention, sophisticated threat identification, and Zero Trust security architectures to prevent the contemporary phishing attacks. The current paper examines the increasing menace of phishing, its development, the way in which this is executed, and the effects that phishing has on both individuals and organizations. It also mentions prevention measures and the use of cybersecurity laboratories in obtaining, examining, and eliminating phishing and malware attacks. The research also addresses how having a fully equipped cyber lab can bolster the security awareness, improve the incident response, and conduct research on the new cyber threats.[3][4]

2. Development Of Phishing Attacks

Phishing as a cybercrime has radically changed since its creation and developed into an advanced, AI-oriented cybercrime scheme instead of primitive deception plots. Though the COVID-19 pandemic increased this development because of the mass transition to remote work, phishing is not a new concept but has existed decades before and keeps evolving with new technological improvements. The historical development of phishing offers a clue to why this type of cyber threat is one of the most long-term and harmful in the present day. [5]

1990s: The Beginning of Phishing Phishing was first reported in the year 1996 and was used to refer to scams of an early nature aimed at attacking Americans online (AOL). In the age, hackers posed as AOL administrators to defraud users into giving away their user names and passwords. The stolen credentials were used by hacker groups like the so-called Warez community to access the internet free of charge, get false credit card numbers, and supply fraudulent accounts. The success of these initial attacks was partly due to the fact that internet security awareness was very minimal and the internet users had little knowledge of internet deception. Though crude by contemporary definition, these strategies formed the basis of the massive and systematic phishing campaigns that have plagued companies to date. [6]
2000s-2010s: Years of Rapid Growth and Sophistries. The methods of phishing developed considerably in the 2000s when attackers started targeting more than just a simple login. At the beginning of the decade, phishing frauds had not attracted

awareness, and therefore, most users were easy prey to criminals who represented a reputable financial institution. Internet hackers started targeting online payment systems including PayPal and E-gold by sending fake security warnings or account balance update emails with a view to
embezzle financial information.[7]

In 2008, the advent of cryptocurrencies further transformed the nature of cybercrime by offering a means of payment that is anonymous and cannot be traced. This eased the cooperation between cybercriminals and helped them to make money through criminal acts without disclosing who they are. Ransomware attacks, which were mainly carried out in a form of phishing emails, also started increasing in the 2010s. Examples of the latter are CryptoLocker in 2013 and the worldwide disruptive ransomware, WannaCry and Petya. These attacks incurred huge financial costs not only due to payment of ransom but also downtime, compliance fines as well as payment to recover systems. Phishing was also used to manipulate politics and politics became a weapon during this time, as seen in the 2016 phishing campaign against John Podesta, the chairman of the Hillary Clinton presidential campaign.[8]

Modern Age: Intelligent, AI-assisted, and Extremely Personalized Phishing**.** Phishing has become more refined in the recent years as cybercriminals are using the benefits offered by technologies to enhance their success levels. Facebook, Instagram, and LinkedIn are social media sites that allow attackers to access large quantities of personal data that they could use to craft highly persuasive spear-phishing messages that specifically address each individual victim. Such attacks are based on trust, familiarity and personalization and it is much more difficult to get noticed. The attack surface was only increased by the transition to remote work in the COVID-19 pandemic. Most organizations had weak security measures outside the office setting and people working at home were more prone set aback by fake emails. As INTERPOL suggests, the number of phishing attempts has increased by an incredible 589 percent in March 2020 as compared to the prior month, which explains how cybercriminals were taking advantage of the uncertainty and panic around the world. The war against security experts and cyber attackers is growing today. With the emergence of generative AI tools, untrained hackers have obtained the ability to produce a refined, high-quality phishing content, and the defender is busy innovating more sophisticated detection solutions. Since phishing attacks evolve alongside the new technologies and human habits, companies should be careful and implement multi-layered approaches to cybersecurity to prevent the constantly developing
threat.[9][10]

3. Classification

Phishing attacks can be of multiple types and each is aimed at controlling the users and using their trust. Although there are dozens of different phishing versions, ten different ones are referred to as the most important as they are the most frequent, have the greatest impact, and are the most
advanced.[11][12][13]

- **Spear Phishing**
  Spear phishing is aimed at a particular person or worker in the company. The attackers perform background research to understand the role of the victim, his/her contacts and duties and create very personal messages. Due to the earnestness of the email, the victim is more likely to share confidential details or open malicious links equation (1). The spear phishing is among the most effective types of phishing due to familiarity and trust exploitation.
  $$R = NTX \cdot PD \quad (1)$$

- **Email Phishing**
  The most common phishing is email phishing. Hackers use forged emails which resemble established organizations, banks or service providers. The content of these emails is usually threats or urgent information which pushes the recipient to press a harmful link or even fill in sensitive details. Although the problem has become more visible, email phishing has been one of the predominant data breaches and credential theft causes.
  $$S = D \cdot AP + U \quad (2)$$

- **Smishing (SMS Phishing)**
  Smishing involves the use of text messages or SMS, rather than email. Attackers use tricky messages which are supposed to be sent by one of the reputed organizations like a bank, courier or even government. Criminals usually tempt victims by clicking on an unscrupulous link or providing personal information. Smishing is an important security issue with a growing popularity of mobile banking and authentication on the basis of applications.

- **Vishing (Voice Phishing)**
  In vishing attacks, the hackers send phone calls to their victims in order to lure them into disclosing their personal or financial details. Attackers can pretend to be bank representatives, officials or company officials. Vishing attacks through the use of fear, authority, or urgency will be able to get account credentials, card details, or OTPs. These attacks rose in the pandemic period when remote communication was on the increase.

- **Whaling**
  Whaling is a phishing technique that targets top management like CEOs, CFOs, or directors. Since the top executives access crucial financial resources, an effective whaling attack may result in tremendous losses. Hackers prepare extremely professional convincing messages, which they pretend are official business messages, and in most cases that are full of malware or bogus links to meet.

- **Pharming**
  Pharming changes the user without his or her awareness to a fake site. This is through placing malicious code in the computer of the victim or manipulating the DNS settings. Although users can enter the right URL, they

can end up on a phishing page that will steal logins. Pharming is hazardous since it is not easily detected by the victims.

- **Website Spoofing**
  Website spoofing is the use of an imitated site which is similar to a legitimate site. The attackers imitate the design, the layout, and the branding of the original web page to make users input the usernames, passwords, or even payment information. These counterfeit sites usually sport URLs that are one or two characters different and thus become hard to after all, they are not detected easily by untrained users.

- **Clone Phishing**
  Under clone phishing, they steal a genuine mail sent to the target by someone in the past and replicate it in very close detail. The hacker sends in place of the genuine attachments or links the dangerous ones and redispatches the message in the name of resending or changing the message. Since the victim is well aware of the original message, he or she is likely going to trust the faking counterpart.

- **Watering Hole Attacks**
  Watering hole attacks are used to attack a collection of users by infecting a web site visited by them. By using the hacked site, malware will be automatically installed on the systems of the users. This is a particularly widespread attack methodology used in attacks on government institutions, research groups, or corporate networks. The strength of the strategy is that it reflects on the behavior of the mass users instead of on individuals.

- **Man in the Middle (MiTM) Phishing.**
  MiTM attacks are based on hacker being in a secret interception between two parties like a user and a web site. Attackers intercept the data that is in transit and their targets include the login credentials, financial statements, or cookies of the session. MiTM attacks are typically used on unsecured WiFi networks and may also result in a total takeover of an account.

4. How It Works

The main feature of the phishing attacks is the utilization of human nature to generate a feeling of urgency, fear, or curiosity and control users to act fast. Attackers can send threatening messages or warnings about account suspension or suspicious access to intimidate victims to a point of responding without checking the authenticity. Even the modern phishing methods have become more adaptable to overcome the security measures by adopting techniques such as spear phishing where messages are targeted to specific people and whaling where the high profile executives of the companies are targeted. Moreover, attackers can perform clone phishing, which is the copy of a legitimate email with some minor modifications with malicious links. After the victim accesses the fraud information, the attacker accesses the sensitive

information or system without authorization, which may result in identity theft, loss of money or even a data breach on a large scale. With the increasing sophistication of phishing attacks, companies should focus on cybersecurity awareness programs, multi-factor authentication, and email filter solutions to decrease the amount of successful attacks.[14][15]

4.1 How To Recognize

Besides these standard indicators, phishing emails in the contemporary world can also be much more advanced in their methods of deceit, which complicates the issue of identification. Attackers frequently employ the writing style of the parties or organizations that are trusted to look genuine. Although certain phishing emails have glaring mistakes, others are well developed and targeted to the receiver, thus the scrutiny is all the more essential. When a user receives an email, it is important to look at the full email address of the sender since most attackers may manipulate one character or domain to look like a legitimate one. Unforeseen attachments, particularly the compressed files or documents that require the use of Macros are good indicators of ill motive. The second red flag is that the text in the email does not correspond to hyperlinks; when passing a cursor over a link, a suspicious Internet Protocol can be observed. The emails that demand actions that are against the regular course of action like transfer of urgent funds, password resets without request, or sharing of confidential information should as well create red flags. A good method of preventing the victimization of phishing is by validating the authenticity of the communication with another trusted channel[16][17]

4.2 Trending Report

Phishing has been on a steady increase up to 2025, with multiple reports worldwide reporting a significant increase in the number and the level of attacks(Fig 1, Fig 2). Available statistics of various cybersecurity organizations show that phishing attacks surpassed one million per quarter in 2025 and the number of unique and malicious domains tailored to phishing has significantly increased. Online payment systems, financial institutions, and cryptocurrency users are also on the list of primary targets, as the number of mobile banking malware and crypto-related phishing has increased significantly. There is also an increasing use of AI by attackers to create the most persuasive and polymorphic phishing emails, as well as exploiting compromised accounts to get around the security filters. Social engineering has gone beyond email to voice phishing which has dramatically grown, and Phishing-as-aService platforms enable even low-skilled attackers to launch large campaigns. The onslaught of social media as a source of information acquisition coupled with vulnerability to remoteworking has also contributed to the rise in success rates of phishing, allowing phishing to emerge as one of the most undeterred and rapidly developing cyber threat in 2025.

.

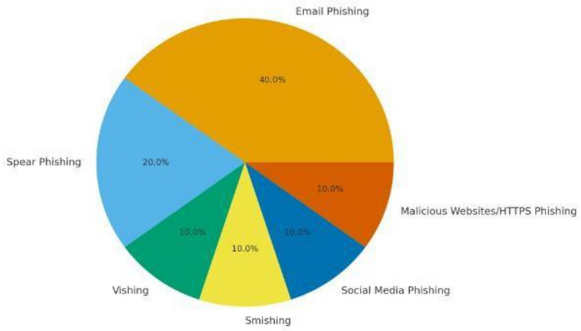

Fig 1. Phishing type report

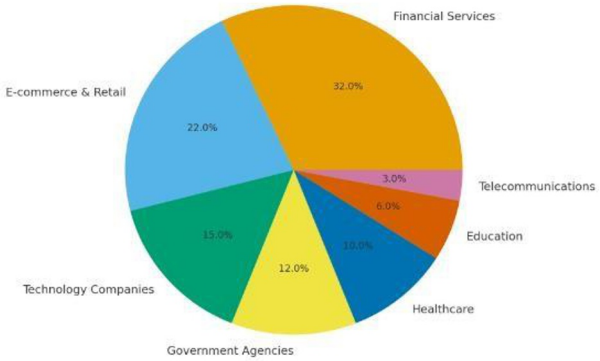

Fig. 2. Sector wise phishing report

4.3 Fraud by Mobile

Fraud by phone is among the most proliferating sub-categories of phishing because it is now easy to contact the victim directly on their personal devices. One of these tricks includes vishing, or voice phishing in the form of making phone calls, which is one of the most popular tricks with scammers masquerading as reputable organisations, customer services, or banks to elicit confidential data. Correspondingly, smishing, or SMS-based phishing, is the sending of text messages that include harmful links or counterfeit notifications, urging the receiver to go to the fraudulent websites that aims to steal credentials and/or banking information and/or personal data. The most common method that has been seen in recent years is the hybrid phishing, which is a combination of email and telephone-based social engineering. In this method, a deceptive email is sent by the attackers first, usually the email is a deception as a receipt of an unknown purchase or renewing of a subscription. The email usually contains a desperate order

requesting the receiver to call a customer-support number in order to challenge the charge. When the victim calls, the attacker then talks to him convincingly to obtain personal information like bank account numbers, credit cards, or personal identification. The scammer can also in other instances manipulate the victim to send money, buy gift cards or give them remote access to their device. Since the start of 2021, experts have observed a steep rise in activities of vishing and smishing. It is associated with this boom because scammers are no longer likely to phish through email because email providers now follow sophisticated spam-filtering and authentication measures that restrict the effectiveness of scammers. Conversely, phone calls can circumvent such protection and get to the victim without much or no filtering whatsoever. Caller ID spoofing also assists the attacker to conceal his identity and seem to be real. Also, voice-based communication provides scammers with greater chances to exploit emotions and establish a temporary trust, create urgency or pressure, and get people to act immediately without checking. This is a very powerful phishing technique because of the combination of the low level of filtering and the high level of psychological influence of phishing attacks on users in phones, which are the favorite tool of contemporary cybercriminals.[18][19]

4.4 Most Targeted Sector Phishing Report

Phishing operations were also on the rise in 2025, as the attackers increasingly moved to the industry that had fewer security barriers and greater user interaction. The most targeted industry was still social media sites, which make an estimated 35 38 percent of all attacks on phishing due to their huge number of users and the ease of hacking an account with no strong authentication measures. The level of fraud targeting SAAS and webmail services also escalated to nearly 15-17 percent as account owners offering services which offer access to other related services became the most valuable targets by the attackers in terms of their secondary uses. In the meantime, phishing targeted traditional financial institutions dropped even more, to approximately 89 percent, with the downward trend that started in 2023 as the majority of financial institutions have taken up multifactor authentication and new anomaly-detection systems, making banks less vulnerable to email-based phishing.[20][21]

The online payment platforms like PayPal, Venmo, and Stripe have taken up an approximation of 6-7 percent of the attacks, as fraudsters find it more convenient to use phonebased fraud-related activities such as vishing and smishing to better target payment users(Fig 3). Hand in hand with phishing, which became one of the most rapidly increasing types of frauds in 2025, hybrid phishing (a hybrid of email lures and social engineering via phone) also spurred up. Scammers used forged order receipts, immediate dispute notices and spoofed support calls to coerce victims into providing financial information or authentication codes. The ability of mobile calls and SMS messages to be minimally filtered as compared to email gave phone-initiated phishing a better payoff to scammers. Consequently, 2025 was the beginning of a distinct movement towards voice-based and SMS-based fraud that was real-time and therefore emphasizing the tougher cross-channel authentication and user awareness efforts.

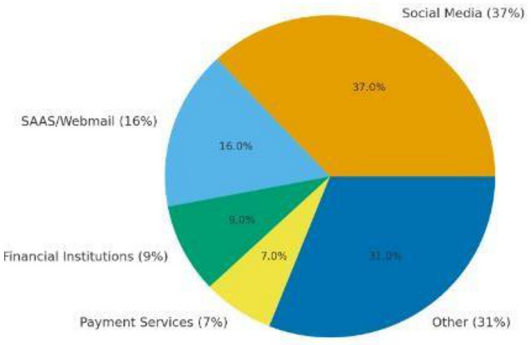

Fig 3. Most targeted sector phishing report

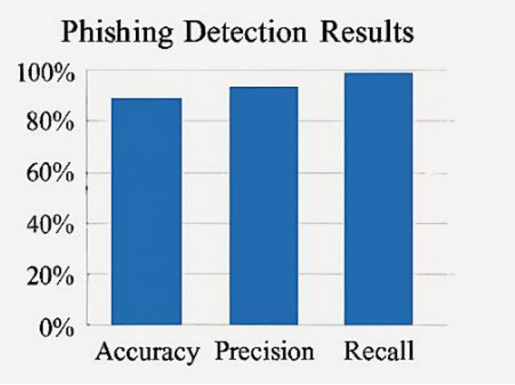

Fig. 4. Social media phishing

Table 1. Categories of social media phishing attacks

Prevention Method	Approach	Effectiveness
AI-Based Detection	Machine learning models analyze posts, links, and user behavior	High (80–90%)
Multi-Factor Authentication	Requires additional verification beyond passwords	High (85–95%)
User Awareness Training	Educates users to recognize phishing attempts	Moderate (60–75%)
Firewalls & Filters	Blocks suspicious traffic and malicious URLs	Moderate (65–80%)
Cybersecurity Labs	Research and testing of emerging phishing techniques	High (90%+)

Figure 4 depicts the multi-layered software security strategies for protecting users from social media phishing attacks. Social media platforms are at the very center of the

picture as they are the main setting for phishing activities through fake profiles, malicious links, and deceptive messages. Around these platforms are various protective layers: firewalls that prevent unauthorized access; AI, powered detectors that spot unusual patterns; users being trained and made aware through educational programs that they can recognize and thus avoid phishing materials; and, finally, secure authentication mechanisms such as multi, factor authentication which helps in preventing unauthorized access to accounts Table. 1. The main flow between those elements highlights that relying on one single method is not enough for efficient protection rather a mixture of both technical safeguards and human vigilance is required. The layered security approach demonstrated here has facilitated the incorporation of leading, edge research, cybersecurity labs, and user training to form sturdy shields against ever, changing phishing attacks.

5. Phishing Prevention Both at the Individual And Organization Levels

Awareness, high-level technology, and effective security measures are all needed to prevent phishing. Although phishing activities cannot be fully eradicated the individuals and the organizations can greatly mitigate their weaknesses
through the use of a layered defence technique.[22][23][24]

- **Multifactor Authentication (MFA) should be enabled:**
  One of the best methods of reducing the effectiveness of phishing attacks is through the implementation of a two-factor or multifactor authentication. MFA will help to prevent unauthorized access even in case a user provides attackers with their credentials via phishing because they will have to provide extra factors of verification. This additional security is such that, unless the passwords are compromised, they cannot be used to log into accounts.

- **Apply Intense Cybersecurity Software:** The companies are advised to implement reliable cybersecurity software that offers real-time detection of threats, URL blocking, malware protection, and behavioral monitoring. The sophisticated security applications assist in detecting phishing, preventing malware links, and preventing the use of deceptive sites. Such systems are important in protecting vital company information.

- **Awareness and Training of the Employees:**
  Major cause of successful phishing attacks is still a human error. The frequent training sessions will provide the employees with knowledge about safe data-handling rules, detect potential spam mail, and recognize the potential red flags that could be false links, a sense of urgency, and uncharacteristic attachments. One of the biggest ways of curbing exposure to social engineering attacks is to teach employees to question their requests first.

- **Email Vigilance and Safety.** Users should be careful when handling emails. People ought to ensure that they confirm that they have checked:

- Mistakes in spelling, weird grammar.
- Dubious or spelled out sender addresses.
- Solicitation of personal data without giving warning.
- Pressure tactics or the urgency of the subject.
- Attachments or links which are not known. A basic and yet efficient way to stay out of misleading redirects is hovering on links to preview the URL.

- **Switch to IPv6 Email Infrastructure.** Switching to the IPv6 based email systems is advantageous in the sense that it facilitates security through increased encryption abilities, decreased chances of IP spoofing and better authentication systems. The modern architecture of IPv6 offers a secure communication environment than IPv4 wherein attackers have less ease in utilizing weaknesses of networks at the network level.

- **Integrate Technology and Human Awareness**. Although user training cannot be neglected, human judgment should not be used as the sole source of information within the organization. Some intelligent email security systems such as Tessian offer machine-learning-driven email protection by examining email relationships, finding anomalies, and impersonation attempts. At this level, AI-driven systems can be used to block minor socialengineering attacks that are not blocked by conventional filters.

- **Apply Major Technical Controls**.
  - **Email Scanning & Filtering:** Email filtering services in the modern world scan and filter links, attachments and spoofed domains in the email messages prior to them arriving in the inbox. The cloud email security provides an additional scanning of external threats in real time.
  - "**Report Phishing**" **Mechanism:** Adding a special phishing-reporting button will enable the employees to identify suspicious emails within seconds. An incident response workflow that is clearly defined guarantees a fast investigation and mitigation process. Encrypted Traffic is inspected to identify the sender, the recipient, and the encrypted message between them.
  - **Encrypted Traffic Inspection:** The Encrypted Traffic is checked to determine the sender, recipient, and the encrypted message between the sender and the receiver. Since more than 85 percent of attacks have turned to the use of encrypted channels, organizations need to scan encrypted and unencrypted traffic. AI tools and phishing-as-aservice websites have increased encrypted phishing attacks majorly. Antivirus and Endpoint Protection are features that detect and remove viruses and malware with high accuracy on your computer.
  - **Antivirus and Endpoint Protection:** This is a feature that identifies and eliminates viruses and malware on your computer with great precision. The download of malware can be avoided by installing and updating antivirus programs every now and then because the malware is activated by phishing links or attachments.
  - **Advanced Threat Protection** Sandboxing tools that are powered by AI are used to examine files on isolated systems to determine new malware types.

The further result of the isolation in browsers is that malicious code cannot run on the devices of users.

- **URL Filtering** Access controls are then enforced by policies to restrict access to dangerous categories of websites, recently registered domains and a list of known malicious URLs so that a user cannot access a harmful site.
- **Regular System Patching** Major software, operating systems and security tools should be kept up to date to minimize vulnerabilities that can be exploited by the attackers. Patching vigorously enhances resilience to cyberattacks.

- **Zero Trust Architecture**:
  Zero trust presumes that no user is safe or device is safe. In organizations, they should institute: •
  Network segmentation
  • Least-privilege access control.
  • Constant surveillance and checks. This restricts the movement of attackers in case an initial phishing attack was successful.

- **The threat intelligence integration:** The integration of threat intelligence feeds into already existing security tools allows to detect phishing URLs, indicators of compromise (IOCs), and attack methodologies (TTPs) proactively. Being aware of the new forms of threats will assist organizations in reacting more efficiently and speedily.

6. Conclusion

Phishing is one of the fast-maturing cybersecurity challenges that affect individuals and organizations alike using human vulnerabilities and technological loopholes. Despite the variety of prevention methods, as our research indicates that to establish an effective multilayer defense, it is necessary to prevent phishing attacks in a proactive, personalized way. Analysis of the phishing factors, trends, and prevention strategies identified some of the weaknesses in the existing anti-phishing tools, especially in their failure to automatically train users and adapt to user behavior and continuously optimization of settings. These loopholes underscore the necessity of sophisticated and intelligent solutions that can keep pace with new phishing methods that are being developed, with community-based functionality, including shared templates, threat intelligence, and shared training initiatives. In addition, our discussion is focused on the significance of creating specific cybersecurity laboratories and cooperative spaces to enhance the detection abilities and create new methods of responding to new phishing strategies. Programs such as the Los Angeles Cyber Lab illustrate how well organized and professional settings can contribute to the state of threat consciousness and solution development. Through the combination of the latest technical tools, mechanisms to build user awareness, and means of cooperation in defense, the companies can decrease the likelihood of phishing to a considerable extent and create a more resilient cyber ecosystem. The study eventually helps to fill the gap between the

current anti-phishing solutions and the requirements to fulfill in the long term to provide cybersecurity and protection to users.

References

1. Dou Z, Khalil I, Khreishah A, Al-Fuqaha A, Guizani M Systematization of knowledge (SoK): a systematic review of software-based web phishing detection. IEEE Commun Surv Tutor 19(4):2797 2819 17. (2017)
2. Gupta BB, Tewari A, Jain AK, Agrawal DP Fighting against phishing attacks: state of the art and future challenges. Neural Computer Appl 28(12):3629–3654(2017).
3. Nadeem M, Arshad A, Riaz S, Zahra SW, Dutta AK, Almotairi S. Preventing the Cloud Networks through Semi-Supervised Clustering from Both Sides Attacks. Appl Sci; 12(15): 7701. 2022.
4. Rashid A, Chaturvedi A. Cloud computing characteristics and services: a brief review. Int J Comput Sci Eng; 7(2): 421–426. 2019
5. Nadeem M, Arshad A, Riaz S, Band SS, Mosavi A. Intercept the Cloud Network from Brute Force and DDoS Attacks via Intrusion Detection and Prevention System. IEEE Access; 9: 152300 152309. 2021.
6. Jangjou M, Sohrabi MK. A comprehensive survey on security challenges in different network layers in cloud computing. Arch Comput Methods Eng; 29(6): 3587–3608. 2022.
7. Alam A. Cloud-Based E-learning: Scaffolding the Environment for Adaptive E-learning Ecosystem Based on Cloud Computing Infrastructure. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021; 2: 1–9. Singapore: Springer Nature Singapore. 2022.
8. Seifert M, Kuehnel S, Sackmann S. Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions. ACM Comput Surv; 55(11): 1–35.2023.
9. Nadeem F. Evaluating and Ranking Cloud IaaS, PaaS and SaaS Models Based on Functional and Non Functional Key Performance Indicators. IEEE Access; 10: 63245–63257. 2022.
10. Parast FK, Sindhav C, Nikam S, Yekta HI, Kent KB, Hakak S. Cloud computing security: A survey of service-based models. Comput Secur. 2022; 114: 102580. Mohammed CM, Zeebaree SR. Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review. Int J Sci Bus; 5(2): 17–30. 2021.
11. Ali M, Jung LT, Sodhro AH, Laghari AA, Belhaouari SB, Gillani Z. A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security. Alex Eng J; 64(2): 749–760. 2023.
12. Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud Security Threats and Solutions: A Survey. Wirel Pers Commun; 128(1): 387–413.2023.

13. Aoudni Y, Donald C, Farouk A, Sahay KB, Babu DV, Tripathi V, Dhabliya D. Cloud security-based attack detection using transductive learning integrated with Hidden Markov Model. Pattern Recognit Lett; 157: 16–26. 2022.

14. Nadeem M, Arshad A, Riaz S, Zahra SW, Dutta AK, Al Moteri M, Almotairi S. An Efficient Technique to Prevent Data Misuse with Matrix Cipher Encryption Algorithms. Comput Mater Contin; 74(2): 4059–4079. 2022.

15. Upadhyay D, Zaman M, Joshi R, Sampalli S. An efficient key management and multi-layered security framework for SCADA systems. IEEE Trans Netw Service Manag; 19(1): 642–660. 2021.

16. Zahra SW, Arshad A, Nadeem M, Riaz S, Dutta AK, Alzaid Z, Almotairi S, et al. Development of Security Rules and Mechanisms to Protect Data from Assaults. Appl Sci; 12(24): 12578. 2022.

17. Al-Shabi MA. A survey on symmetric and asymmetric cryptography algorithms in information security. Int J Sci Res Publ (IJSRP); 9(3): 576– 589.

18. Musa A, Mahmood A. Client-side cryptography based security for cloud computing system. In 2021 Int Conf on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India. 2021; 594–600.2019.

19. Hossain ME. Enhancing the security of caesar cipher algorithm by designing a hybrid cryptography system. Int J Comput Appl; 183(21): 55–57. 2021.

20. Adewole, K. S., Akintola, A. G., Salihu, S. A., Faruk, N., and Jimoh, R. G. Hybrid rule-based model for phishing URLs detection. Lecture Notes Inst. Comput. Sci. Soc. Inf. Telecommun. Eng. 12, 119–135. doi: 10.1007/978-3-030-23943-5_9(2019).

21. Vanitha, V., Joe, S.B., Krishnan, R., Fletcher, A.S.A., Anju, M., Akila, V.: Cognitive Threats Detection Model using Nature Inspired Chimpanzee Optimization for IoT Networks (CCM-COM). In: Atlantis highlights in engineering/Atlantis Highlights in Engineering. pp. 629–637 (2025). https://doi.org/10.2991/978-94-6463-754-0_55.

22. Aljofey, A., Jiang, Q., Rasool, A., Chen, H., Liu,W., Qu, Q., et al. (2022). An effective detection approach for phishing websites using URL and HTML features. Sci. Rep.12:10841. doi: 10.1038/s41598-022-10841-5. (2020).

23. Jain, A. K., and Gupta, B. B. (2017). Phishing detection: analysis of visual similarity based approaches. Secur. Commun. Netw, 1–20. doi: 10.1155/2017/5421046,2017.

24. Anti-Phishing Working Group (APWG) (2024). Phishing Activity Trends Report, 3rd Quarter 2022.