International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 10 | Oct - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

A Comprehensive Review of Phishing in Cybersecurity: Risks, Impacts, and Defence Strategies

Aditya Chowdhury[*1], **Ashwani Dwivedi**[*2], **Shweta Sinha**[*3]

[*1] Scholar, Computer Science, National P.G. College, Lucknow, Uttar Pradesh, India,
chowdhuryaditya004@gmail.com

[*2] Scholar, Computer Science, National P.G. College, Lucknow, Uttar Pradesh, India,
bhanuking0786@gmail.com

[*3] Assistant Professor, Computer Science, National P.G. College, Lucknow, Uttar Pradesh, India,
sinha.shweta020776@gmail.com

Abstract

Phishing is probably one among the many serious challenges in the realm of cybersecurity today, it both exploits a very clear dimension of technological vulnerability and exploits human psychology. The review consolidates research on phishing-from simple email scams to very sophisticated attacks using machine learning and artificial intelligence and discusses their key techniques along with the psychological roots of trust exploitation, cognitive overload, and emotional manipulation for the users. Moreover, the paper identifies the critical impacts both to people and organizations: monetary damage, identity theft, and reputational damage. A review of the defences currently in use ranges from user education and training to the very advanced technological solutions, including AI-driven phishing detection. The identified gaps in literature include the necessity of studies on the long-term effects on the thought of people and a much stronger integration of human-centred and technological defences. The paper also discusses future research directions by motivating and proposing more adaptive and resilient defence mechanisms to combat this continuously evolving nature of phishing attacks in the world.

Keywords: Phishing, Cybersecurity, Social Engineering, Cybercrime, Information Security, Psychological Manipulation

I. INTRODUCTION

These sophisticated types of cybercrime have become rampant, threatening individuals and organizations security breach. It is basically a form of fraud whereby an individual is manipulated into divulging sensitive information or performing an action that would breach security. Growing reliance on digital communication makes phishing a huge threat; therefore, concern about phishing is always up in the cybersecurity domain. It will gather information and analysis regarding phishing together for a comprehensive understanding of the risks, impacts, and strategies related to its mitigation. This paper synthesizes research from an existing body to determine gaps in knowledge and outline future research directions to deal with the phishing attacks.

Most of the time, phishing attacks are routed in spam or pop-ups and are sometimes difficult to identify at all. Once the attacker captures your personal information, he can use all types of it for instance, identify theft, and placing the good credit into bad ones by manipulating with the data. Since phishing is one of the most insidious types of identity theft, let us try to get acquainted with different types of phishing attacks, and also find out what preventive measures exist [1]. In essence, phishing attacks involve deceitful efforts to obtain sensitive information, like usernames, passwords, and credit card details, while pretending to be a reliable and trustworthy source [2].

II. METHODOLOGY

The review systematically and structurally collects relevant literature on phishing and cybersecurity for an analysis. The process of tricking the recipient to take the attacker's desired action is considered the *de facto* definition of phishing attacks in general [3]. On the whole, most of the research incorporated in the review focuses on capturing the widest possible insights from contemporary influential research literature to provide balanced coverage of theoretical perspectives and practical findings. It is possible to systematically identify user's behaviour by monitoring their online activities, using online tests, and providing them relevant trainings based on the detected weaknesses [4]. The prime objective of the discussion is to reveal the various phishing approaches, data sets utilized in the relevant studies, the algorithms used in the area, and the highest accuracy achieved by the implemented algorithms [5].

III. LITERATURE REVIEW

3.1 Evolution of Phishing:

- Phishing has dramatically changed since its origin in the 1990s. At first, it was always the case that the early phishing attempts were attackers who would send mass emails entice victims to give out sensitive information by pretending to be a legitimate organization, such as a bank or service provider. These early phishing attacks were crude even by the most indifferent measurements, they often relied on poorly constructed e-mails, but they managed to be successful because of the relatively low level of awareness of internet users in such matters during that time. The phisher sends out the messages to thousands of users and usually only a small percentage of recipients may fall into the trap but this can result in high profits for the sender [6]. Primarily, attackers used fear-based messaging claiming that one's account has been compromised and requesting them to validate the identity through sensitivities.

- Spear phishing and whaling were some of the significant milestones in the history of phishing attacks. It is targeted like generic phishing compared to casting a wide net. phishing is not merely a technique to steal information from an individual victim. Phishing attacks may also be used to disable systems via malicious URLs or infected email attachments or even as a means to gain prolonged access to devices, systems, and/or databases to carry out sophisticated reconnaissance and exfiltration campaigns (Verizon 2015) [7]. Sometimes, attackers would spend much time researching their victims, especially gathering private information from social networks, professional networks like LinkedIn, and other sources publicly available to write emails that would have a greater chance of deceiving the receiver.

- Whaling is the much more advanced form, but it addresses only top persons like company executives, government personnel, or other individuals who have the highest possible access to

confidential information. These individuals have the authorization to access to the company high-value information such as economical secrets, admin password for company management account [8].Whaling attacks are much more dangerous, for the attacker's objective in most cases is either gaining access to critical systems or authorizing major financial transfers.

- The next development of phishing has been multi-channel phishing, which integrates emails, phone calls called vishing, SMS called smishing, and impersonation on social media. As often seen, the attacker resorts to such diverse channels with the purpose of making the request more legitimate. For example, after receiving a phishing email, a call may be made from a spoofed number calling for "confirmation" of details or compelling the victim to act quickly. Intrinsic to the messaging system, SMS messages can provide additional obfuscation, for example, spoofed phone numbers and organization names for the attacker to trick their target into obtaining the victim's response as well as access to fraudulent websites and shortened links [9].

- The one major development in the advancement of phishing technology has been the one involving the uses of machine learning (ML) and artificial intelligence (AI). Now, both are being used by attackers as well as by defenders for the data. To train a machine learning model for a learning-based detection system, the data at hand must-have features that are related to phishing and legitimate website classes [10]. The attackers use AI for the purposes of generating phishing emails that would look like any other authentic communications, thus making them less detectable. Another approach with AI would be continuous, real-time tweaking of phishing messages to evade automated filters on email systems. But that being said, the defenders also employ AI-based tools to detect patterns of phishing attacks on emails, such slight anomalies that might not be noticed by the human user.

- Vishing (voice phishing) is also become more dangerous with AI-enhanced voice cloned technology. This technology lets fraudsters to make out known people's voices, like family, friends or known relatives. Natural language processing provides attackers to have complex, content precise, making the interaction seems more natural and difficult to recognise.

- QR codes are now omnipresent and cybercriminals have noticed to use it for their purpose. A new type of phishing which known as, "quishing," uses these codes to believe the users. After scanning QR codes, the victim is sent to a fake web page that looks genuine, with the purpose of stealing sensitive information of the users [11].

3.2 Psychological Manipulation in Phishing

- Phishing attacks are based on the exploitation of fundamental principles of psychology. For example, power figures are often used in phishing emails to describe the attackers, like a bank executive or government official, even the CEO of the client's organization. Typically, phishing emails create a sense of urgency and instruct the recipient to act quickly to resolve an urgent issue, such as verify account information of account holder while completing some sort of financial transaction.

- Another often exploited principle is fear, used to make the recipient feel panic or sense of urgency. A common threat in phishing emails is that of account suspension or lawsuits unless they comply

with the request immediately. The combination of urgency and fear adequately deters the victim's defences, forcing them to act impulsively.

- **Trust**: This is another prime factor in the psychological manipulation used in phishing. Social proofs that make their way into all this are such that victims end up believing the phishing message comes from some trusted source: perhaps a friend, colleague, or well-known company. People tend to act out in situations that make requests appear to come from someone they know or trust. They capitalize on this by pretending to be addresses or social media harvested information to make the email look personal and trustworthy.

- In emotional manipulation, the phishing attacker capitalizes on greed as an emotion. Normally, these criminals mounted the attack through electronic e-mails promising some form of financial reward, or a free vacation, or some other bonus. Such scams can only work if the victim's desire to appropriate personal gains overcome his or her normal scepticism.

- Curiosity may also be another driving factor. In this case, the victims are least likely to make a critical judgment about the authenticity of the email because their concentration is focused on finding something new or important.

- Another means of advantage that phishing hackers enjoy is cognitive overload. This has been realized when hackers write emails that are complex in nature or will confuse the recipient. This is very effective when it is applied in spear phishing attacks of busy professionals. In this respect, the victim lacks extra time or mental capacity to study the message in detail; therefore, they respond to the request raised by the attacker without knowing the broader implications and impact.

- Technical approaches to phishing detection and prevention such as the comprehensive multi-dimensional model based on a machine learning algorithm have identified personality, cognitive processes, and computer knowledge as the most influencing factors of susceptibility in predicting phishing victims [12].

- **Baiting:** It is a social engineering tactic that also used presently which involves offering something of a value, such as a free gift discount card or a USB drive, in exchange for sensitive information of the users. Sometimes the attacker may leave the USB drive in a public place, such as a coffee shop, restaurants, parks and more in the hopes that someone will pick it up and take it to their home to plug it into their computer or laptops so that they access the system [13].

3.3 Technological Aspects of Phishing

- Phishing tactics change with time, but they only differ in the fact that attackers use new technologies while defenders still depend heavily on email. Phishing attacks have evolved from the traditional email to be complex they use many digital tools and technologies current Phish attack are more sophisticated than before. The most interesting evolutions generally revolved around **AI** and **ML** in conducting or combatting phishing. Three of the more popular approaches to combat phishing attacks include: (1) one-time passwords to be a successful tool for phishing protection, (2) multi-level desktop barriers, and (3) behaviour modification [14].

- With AI, not only can the attacker compose and send a phishing mail but also these systems incorporate results from previous campaigns to find what works best i.e. at any point in time attackers have option of improving their ways to grab attention or interest of receiver. Well, generative AI can bypass this as it will have the tendency to send identical or very similar emails over and over again from external sources. Generative AI tools can create different email messages that read as if they were written by a person, although they were generated by a machine and can, therefore, be sent to a large number of people with minimal effort on the side of the attacker [15].

- Flow through AI and ML, these has also increased the phishing detection systems. Modern email filters already ship with machine learning (ML) algorithms that analyze huge data sets in order to detect patterns related to phishing attempts. These systems can be designed in a variety of ways to warn alerts on the email subject line, sender address, presence of malicious links within the provided content and now tone & semantics too. In that sense, AI-based phishing detection systems quite literally are a giant leap forward in the never-ending fight against destructive and damaging attacks. By leveraging machine learning, natural language processing, and deep learning technologies, these systems offer enhanced capabilities for identifying and mitigating phishing threats with greater accuracy and efficiency compared to traditional methods [16].

- However, the effort invested in this area is undermined as on average attackers still manage to bypass detection every 26 hours. A principal example of such a practice is pharming, when the victim ends up redirected to another site hostile that seems identical in design. Phishing, the traditional one… and now we also have pharming menace that would victimize the DNS to redirect your traffic from a real page to some kind of emulation site created by an attacker. These are very difficult to detect, because the URL listed in your browser looks legitimate (although redirected through a fake site).

- Phishing hackers are using **HTTPS encryption** more and more often, which makes their sites look legitimate. In the good old days, HTTPS in the address bar of your browser told you that site was a safe place to be. Some of the attackers have used this technique by getting SSL certificates for phishing sites which makes looks like legitimate. It is possible to embed scripts into a webpage for stealing the cookies stored in a browser. In such cases the proposed mechanism would fail to detect phishing webpages [17].

- One is another phishing technology, which too adds up to mobile. Increasingly access to internet is expanded; you find more number of people using mobiles, tablets for accessing the web. In response, attackers eventually pivoted to use mobile devices by way of **smishing** and **vishing**. Mobile phishing differs-primer comparison to the technologies which are already studied — in terms that screen dimensions might be small, and user interface is a lot easier; hence it gets more difficult for a person lucky enough to understand that he continues being targeted of your farming tries by attackers.

- A Man-in-the-Middle (MITM) attack is a type of phishing where the attacker intercepts communications between two parties, such as a user and a legitimate website, aiming to extract sensitive information from both sides. Rather than the data being transmitted directly to its targeted recipient, it is first captured by the attacker, who can then exploit this information. During a MITM attack, the attacker reroutes the user to a malicious server through methods like Address Resolution

Protocol (ARP) poisoning, DNS spoofing, Trojan-based keyloggers, or URL obfuscation. The attacker may record and misuse the intercepted data at a later time [18].

3.4 The Role of Social Engineering

- **Phishing** is often described as an online form of **pretexting**, where the attacker creates a false scenario (pretext) to convince the victim to provide information or perform an action. Social engineering relies on exploiting human psychology rather than technical vulnerabilities, making it one of the most difficult forms of attack to defend against.

- Whereas the success of the phishing attack can be dramatically improved if an attacker comes up with a convincing pretext, typically made out of all information about a victim taken from his social networks or professional resources. This data certainly enables the shift for attackers to design very personalized phishing emails- and most likely more successful than generic ones.

- **Authority bias**: we have the authority bias which is yet another massive fail in social engineering techniques that happens more often than not. Phishing attacks often impersonate people who are more senior, such as CEOs or government officials, to leave the impression of authority and rush a target into agreement. This kind of attack in particular works best with spear phishing attacks such as ones targeting corporate employees, where an email can claim to be from the CEO asking you to approve a financial transaction or reveal confidential details.

- A social engineering attack using the phishing tool is **reciprocity**, in which attackers provide a valuable item to victims so that they collaborate. This means offering free downloads, sale on purchases or certain exclusive content in exchange for login particulars of users and some sensitive information.

- Psychological Phishing (Driven by the **need of consistency**): Phishing emails for example, phishing is an attacking method where its hooks in their payloads, when a naive player takes the bait of clicking in a link or downloading some attachment they are hooked and could end up shooting each one further shot. This is mainly a principle of consistency that you could generally find who the attacker proceeds from asking simple, benign requests to some level deeper demands or goals such as clicking on your link prompting an email verifying account and then it led gradually for requesting sensitive stuff like login credentials, or worse case securing money.

- **Scarcity** is another tactic used in phishing, where attackers create a sense of urgency by suggesting that the victim will miss out on an opportunity if they do not act quickly. This might involve claiming that the victim's account will be suspended unless they verify their information immediately or offering a limited-time discount on a product or service. Also, it plays one the victims fear of loss which is used to make them act almost impulsively without considering if what they are being asked for has any legitimacy.

- Phishing as well used **liking** and **similarity** the suggestion is that attacker develops messages to foster a connection with the victim. By mimicking the tone, language, or interests of the victim, attackers can make their phishing emails feel more personal and relatable. For example, a phishing

email might reference a shared hobby or interest that the attacker discovered through the victim's social media profiles.

- Therefore, by means of social engineering, an organization can collapse or lose its privacy and important information. It is a technique and an art that attackers try to manipulate or lure users and institutions [19].

3.5 Impact of Phishing on Organizations and Individuals

- There are a variety of ways that an organization is affected by phishing, including direct monetary loss, operational costs, and brand damage. Each of these metrics is equally important when considering the amount of money that should be invested into counteracting phishing attacks [20].

- It significantly impacts on individual, organizations and industries in general. The consequences of phishing are not just limited to the temporal financial loss symptoms but also long-term effects like identity theft, brand damage and business disruption. Phishing attacks also result in financial losses to the company which can include loss of company money, loss of important items and security costs from corporate phishing attacks, as these phishing attacks often lead to the theft of financial information, such as credit card numbers and banking passwords [21].

- **Economical Damage**: Phishing is one of the very most dangerous kinds regarding cybercrime. Firstly, the businesses are at risk of experiencing substantial financial losses due to a phishing attack that ultimately results in company funds and intellectual property (as well as other sensitive assets) getting stolen. **Business Email Compromise (BEC)** is a particularly costly form of phishing attacks and involves fraudsters utilizing spoof emails in order to deceive employees into approving fraudulent wire transfers.

- **Identity Theft and Privacy Problems**: Identity theft is not a new type of crime. It has been used for centuries to impersonate someone and thereby obtaining a way of committing a crime anonymously [23]. There has been an endless list of cases of identity theft, a category under which crime is not new. Phishing is the main protocol for identity theft and a large number of cases are headed by phishing every year. Identity theft victims can spend years and even decades cleaning up their personal and financial records: this includes repairing wrecked credit scores or closing bogus accounts fraudulently opened in a victim's name. The other aspect is that identity theft can have severe psychological effects on the victims. Identity theft causes victims suffered pain, stress and violation.

- **Stealing of Private Data**: Hackers can easily steal private information which is residing on a computer with the help of phishing. Personal health data, financial records and IP are examples of the type of sensitive information that can exist. Many industries such as healthcare, finance, and government are highly victim to phishing attacks since they maintain lots of confidential data about people. Typical techniques involve the exploitation of flaws in the software of web-based forums, photo galleries, shopping cart systems, and blogs. The security 'holes' that are taken advantage of are usually widely known, with corrective patches available, but the website owner has failed to bother to apply them [24].

- **Long Term Impact of Reputation**: The reputational hit that a phishing attack makes, is irreversible and it may affect in long term end also. It is very difficult when a company now has been the entity tagged as involved in a data breach to garner successor of its customer, stakeholders or business partners again. Reputational damage has also a down side effects that could compound further financial loss for companies, by losing market shares and under greater scrutiny but most importantly they would be less or have no capacity to rebuild their reputation.

- **Data breach:** Data breaches happen when unauthorized individuals gain access to sensitive information, typically due to phishing attacks, Insufficient security measures, or clan threats. Such breaches can occur considerable financial damage on organizations, arising from expenses related to investigations, legal liabilities, and the loss of customer trust. For individuals, these incidents heighten the likelihood of identity theft, cause emotional distress, and compromise privacy, as sensitive personal data may be exposed. To effectively tackle these threats, organizations should implement strong encryption, provide cybersecurity awareness training among the employees, and regularly update their systems to enhance security measures [25].

- **Operational Disruption**: Organizations too can also experience a short-term operational impact from the phishing attack, direct to its services and structure. This results in a great deal of operational downtime and diminished efficiencies. The cost to repair the phishing damage can be huge - recovery of data, incident response, and upgrades in cybersecurity.

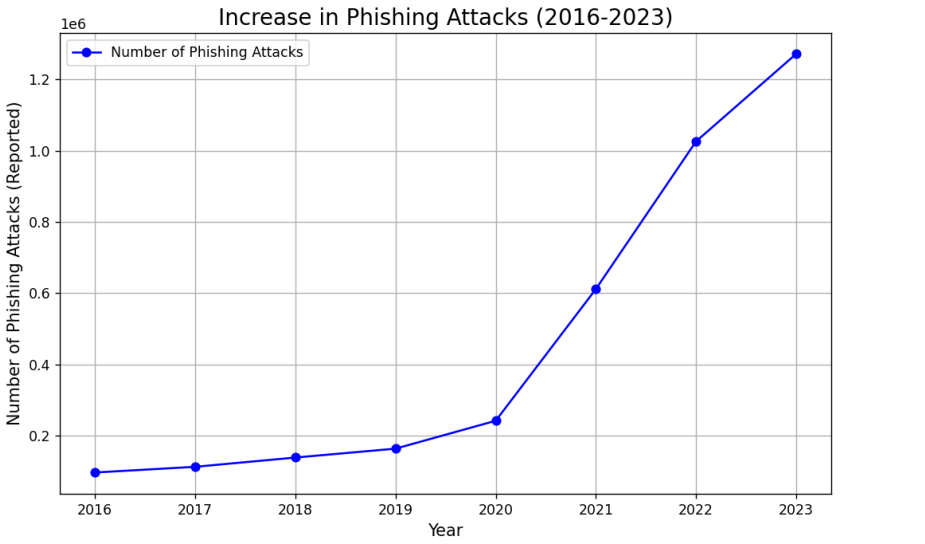

Figure 1: Increase in Reported Phishing Attacks (2016-2023)

IV. Defence Mechanisms and Prevention Strategies

Fighting phishing is something that needs a holistic approach, using a mix of technological solutions along with education and policy decisions.

- **Education and Training**: Without question the most critical pieces to a successful anti-phishing program. The literature specifies that the techniques behind carrying out attacks are ever-changing; consequently, security awareness should be a form of continuous education.

- **Technology**- Anyone interested in experimenting with phishing has to use technology of some kind. Modern email filtering solutions, dedicated anti-phishing technology and detection tools based on artificial intelligence sense threats before they land in the inbox. Machine learning algorithms are able to effectively detect phishing emails, that traditional filters fail to recognize any anomaly or pattern violation (SecureWorks 2020).

- **Multi-Factor Authentication (MFA)**: MFA is another critical security provision that provides a significant lift to account protection as the user has to pass through multiple verification steps. This matters so as to keep the secret data secure from direct invasion and remarkably cuts down on situations for those passwords that could be endangered using a directory of unfamiliar actions. MFA used the conventional build comprising of 3 items - that which a person knows (such as a password/PIN), that which they have such - either phone or smart card, and something special relating into this customer just like biometric information including fingerprints.

  The importance of MFA has grown as cyber threats continue to evolve. Research suggests that organizations that implement MFA see a noticeable decrease in successful phishing attacks and account takeovers, making it a valuable tool in today's digital landscape. By adopting this multi-layered security approach, companies not only protect their information but also build trust with their customers, demonstrating a commitment to cybersecurity [26].

- **Policies and Legal Frameworks**: This is very crucial to have at a place, mostly you would find this in action combating phishing. With a view to enhance cyber-security and also for safeguard the integrity of people or organizations, governments and regulatory authorities have implemented various laws & regulations so that phishing exploits are lessened. According to the literature, compliance with these practices is essential not only for preventing phishing attacks but also will reduce financial losses and reputational damage in case of a breach.

- **Phishing simulation**: Companies now provide training via phishing simulations to strengthen the security of an organization from such attacks The idea here is to trick the employees in a controlled way by sending them fake phishing emails that simulate how valid phishing attempts usually occur. By conducting phishing simulations, the companies can identify where employees are least aware and also, they would be able to test how fit their current training initiatives. Though it allows some learnings when employees miss out to an integrated simulated attack by being given the chance to correct those specific mistakes with certain training that could help develop better judgment and response towards real phishing attacks. Studies show that organizations that regularly implement phishing simulations experience a marked reduction in successful phishing incidents, ultimately strengthening their overall cybersecurity framework [27].

- **Incident Response and Recovery Plans**: The last line of defence that is provided by which the potential impact can remain minimal, well an event response plan. A good incident response plan as described in the literature is sure to reduce downtime and operational disruption due to a successful phishing attack. Good recovery planning means an org can be back to normal sooner afterwards, with less ultimate damage.

V. Challenges and Gaps in the Literature

Despite the advances in phishing research, there remains significant challenges (as exacerbated by industry and traditional controls) and precious little white space. You might get the feeling that some things will end up a bit too cryptic, and I would argue by nature of phishing being dynamic around both human factors as well as on new technological frontiers still may be hard to tell apart maybe not eradicate at this time. In this section, we describe some of the most prominent literature gaps and difficulties that stand in the way of progress.

- **Psychological Trauma for Victims in the Long Run**: Existing studies have focused mainly on short-term consequences of phishing attacks (e.g., financial loss or data leak), but few attempted to investigate long-term psychological damages that affect victims. A significant proportion of phishing victims experience violation, guilt and embarrassment as a result but far less is known about more repeatable impacts; i.e. any long-term impact from such attacks (e.g., post-traumatic stress or chronic anxiety).

  Rather more work needed in terms of the psychological consequences for individuals who are affected after being phished and further investigation is calls regarding their personal lives (if any) or earning judiciary livelihood from identity theft / financial loss due to phishing. And this knowledge can be useful in developing support systems and tools may work more for effective designs, as well a better prevention, awareness campaigns.

- **Competing Lens of Effectiveness Behavioural Interventions**: Although education and training programs are often seen as the panacea to prevent phishing, literature has consistently delivered mixed findings about their overall effectiveness.

  The basic training programs, however, are often templated with a one size fits all mentality that may not factor in individual susceptibility to phishing. Common aspects like cognitive biases, cultural differences or different levels of digital literacy affect the way people respond to phishing.

  Longitudinal studies on long-term retention of anti-phishing knowledge are another gap. Although research has demonstrated that you can teach people to spot phishing attacks following just one training session, very little is known about how long such abilities last or how often a person needs "refresher" sessions in order to remain effective. This clearly points towards a need for additional empirical studies that examine the long-term sustainability of educational interventions.

- **Phishing techniques have evolved with unprecedented speed in the past decade**: a dynamic environment which presents great difficulties to both researchers and practitioners. Sophisticated phishing emails and websites may deploy machine learning, artificial intelligence to further improve the veracity of both email and text.

While attacks thus have changed, and particularly become increasingly well-equipped with more sophisticated technology than captured in the literature. Almost all of the prior research work focuses on classic phishing attacks, e.g., email-based phishing. Indeed, various new forms of phishing (i.e. social media phishing, vishing and smishing etc) have been well documented. Yet has not been addressed properly yet. Different attack vectors are attacking that means different forms of detection and prevention strategies on the other end which is still to see light. Thus, a majority of the defence mechanisms approaches that we discussed in literature are likely not enough to combat new phishing threats.

The second one includes phishing attacks with new technologies in line like deepfakes and Augmented Reality. Across temporal, these methods have to be upgraded time-by-time. As such, greater research is needed to detect the evolutionary attack strategy in advance so that defences can be ready.

- **Limited Considering integration of Technical and human-centric solutions**: Phishing research mainly focused on the purely technical solution or purely user-centric, it never focussed later one though which led to not gives more comprehensive defence assessment. Although there are means to hinder before-phases of spoofing attacks—block the attempts, afterwards measures cannot guarantee zero phishing success with high false alarm rates. Mostly social engineering techniques are used by attackers to exploit human psychology vulnerabilities to get around the defence mechanisms.
  Much of the literature treats phishing as either a social phenomenon or adds some technical granularity to its elucidation self-sufficiently. Whilst this is true on the face of it, phishing in reality takes different forms and addressing it requires an integrated approach. To use one example, all the effort poured into applying machine learning algorithms for phishing detection could be combined with lessons on how phishing messages cause reactions in a victim based of psychology (emotions). Training programs and other human-centred defence strategies such as real-time, forward-looking guidance could be better served by actionable recall through this type of feedback or simulated phish.

  The space could be filled up by the interdisciplinary research between technocratic approach and social perspective. Today, holistic ways to fight phishers must incorporate education about human behaviour as well tech-based defences from persuasive technologists.

- **The research on the matter of phishing**: still predominantly hinges upon references to vulnerabilities within particular groups, and more specifically among elderly people, minors themselves or individuals with low digital literacy. They are not experienced and do a lot of trial and error; hence they always fall for phishing attempts. For example, elder adults cannot recognize whether an email or message is a scam because they not very bounded to the norms of digital communication. Children also do not have the high level of critical thinking which helps to differentiate safe from malicious content, thus it is an open field for attackers.

  Recognizing this gap in research is essential, as it can lead to more effective educational initiatives tailored to the needs of these groups. By exploring how various age ranges and levels of digital proficiency react to phishing tactics, we can better design awareness campaigns and protective measures that truly resonate with and support these vulnerable populations [28].

- **Incomplete Reporting and Data Availability**: A primary problem to tackle within phishing research is the difficult in which reporting incidents manifest as well as lack of open, accessible data. This does not mean that a phishing attack on their systems is disclosed to the public, since this can damage reputation and open organizations up for legal liability. The data gaps also mean no identifiable funds (measurable mile points) are on site to determine the scale and nature of phishing.

  Data is usually not only fragmented but also uncharted, the third-best category. As a result, while some reports might represent successful phishing attacks only, others will show attempted/blocked attacks. The lack of commonality in the nature of reporting in phishing incidents hinders comparison between findings among studies, due to no clear standards for defining defence mechanisms.

  Researchers, industry and government agencies should work hand in hand to come up with standardized reporting protocols on phishing incidents. The release of disclosed data on phishing attacks could generate a wealth of extremely useful information about the progress seen in threat landscape research and international practice, even if anonymous.

- **Underrepresentation of Phishing in Different Cultural and Organizational Contexts**: Most phishing research is focused on Western countries such as the United States and Europe while less is known about approaches to, implications of applying them elsewhere. This also implies that culture determines the function of crafting and receiving messages: attackers generally adjust their techniques based on what they believe about cultural norms. Nevertheless, the literature does not answer these differences sufficiently so there is a gap to investigate how phishing works in other contexts.

  The organizational context, too, affects the way phishing is approached and man-aged; however little research dedicated to identify responses for different kinds of industry or organization there is. For instance, both healthcare and finance are priceless pieces of gold for phishing due to nature the data exchanged have on each area yet there is less research evidence about defence strategies in individual sectors. We should undertake one or more subsequent studies that account for the influence of organisational culture, industry requirements and internationalisation on phishing attacks as well defence mechanisms.

VI. Future Directions

These threats will already have moved on, and if this work were to be built upon for future use — defence mechanisms would need to consider how adaptable they are in quickly changing phishing threat landscape. Based on these vast data sets, we might one day see technologies that can identify phishing attempts with far more accuracy by detecting the intricate patterns beyond traditional defence mechanisms. Plagued with new phishing tricks, these tools are learning constantly through AI and help you identify quicker as it happens.

Then of course I had to think about how little we really know about the psychological impact phishing has on its victims. Phishing attacks not only lead to loss of money or data but also have chronic psychosomatic and psychological implications in-terms-of stress, anxiety and a constant fear for their next attack. Further research

should investigate the impacts of these types of attacks on not just what can be considered more immediate or short-term consequences but also longer-term implications. This in turn will inform more victim-centred recovery programs and psychological support services. Phishing attack cause to the disclosure of information by which the attacker gets access to the victim's account. Year by year, the increase in the number of phishing attacks is evident thus; we have to devise ways to curb this [29].

We also need to check more deeply the effectiveness of education and training programmes. Although most organizations use awareness campaigns as a way of reducing vulnerability to phishing, it is unclear if such programs would be effective in the long-term. Longitudinal studies have yet to demonstrate how much anti-phishing knowledge people remember over time and that persistent training is necessary for maintaining vigilance. It is topical that research should also focus on how to tailor the training based on differences in digital literacy, psychological traits and demographic factors. Blockchain will be more significant way of protection in next defence strategies, data encrypted and less chance for phishing. Since the structure in blockchain is decentralized, with which it becomes difficult for spoiling identities or modifying data by an attacker; therefore, research can be done on looking at how to embed blockchain within already existing cybersecurity frameworks that will eventually help us as a reinforced digital space (as someone might say regarding security when identifying verifications and communicating securely).

Also, the day-to-day need for international cooperation in phishing is also evident. Phishing constitutes a worldwide problem that typically escapes beyond the frontiers of any single nation, making almost always unfeasible for individual countries to wage war against this kind of offenses in their own way. One implication of our results would be learning from large-scale responses to phishing like the campaigns identified in this research with respect to an eventual international framework for sharing threat intelligence and setting cybersecurity standards, which should serve as a future avenue for research. Collaboration among nations, private entities and international security specialists around the world would provide more collective defence against phishing campaigns.

VII. Conclusion

Phishing, without a shadow of questions is one the most complicated and worth it matters in cybersecurity as phishers often grow to be upgraded. At the same time, despite more and more sophisticated attackers utilizing cutting edge technology as well as exploiting human nature with greater ease from year to year, it seems that threats are not going anywhere soon. These attacks are a threat to both individual and corporate security, as well as national infrastructure, with phishing stories covering several types. Hence, we are trying to reflect the key results of these studies shows how it is important for us to comprehend the psychological and technical parts behind phishing attacks.

Innovation plays a major role with defence strategies such as the advanced mail filters to multi-factor authentication that has progressed tremendously along with solid training programmes taken into consideration. However, much is left to do when considering long-term psychological effects on victims, sustainability in educational interventions and just how fast-changing phishing techniques are with the entrance of new technologies like AI and social media. In order to better explain the evolutionary origin of such defence mechanisms, these gaps must be filled. Additionally, further development of these ideas coupled with greater collaboration between researchers and corporate executives as well as policy makers will help the cybersecurity community create even more sophisticated defences to be better prepared for emerging phishing threats.

References

[1] Vaishnavi Bhavsar, Aditya Kadlak, Shabnam Sharma, "Study on Phishing Attacks", December 2018 International Journal of Computer Applications

[2] Muhammad Nadeem, Syeda Wajiha Zahra, Muhammad Nouman Abbasi, Ali Arshad, Saman Riaz, Waqas Ahmed , "Phishing Attack, Its Detections and Prevention Techniques", International Journal of Wireless Information Networks July-December 2023

[3] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, "Phishing Attacks: A Recent Comprehensive Study and a New Anatomy", Computer Security, a section of the journal Frontiers in Computer Science

[4] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans, "Phishing Attacks Root Causes", Ghent University Academic Bibliography

[5] Asadullah Safi, Satwinder Singh, "A systematic literature review on phishing website detection techniques", Journal of King Saud University – Computer and Information Sciences

[6] Srishti Rawal, Bhuwan Rawal, Aakhila Shaheen, Shubham Malik, "Phishing Detection in E-mails using Machine Learning", International Journal of Applied Information Systems (IJAIS)

[7] A. J. Burns, M. Eric Johnson, Deanna D. Caputo (2019) "Spear Phishing in a Barrel: Insights from a Targeted Phishing Campaign", Journal of Organizational Computing and Electronic Commerce 29(1):24-39.

[8] Anh Huynh Nhat, "Phishing Detection In Email Ministry Of Education And Training", Capstone Project Document, Thesis - May 2019

[9] Muhammad Lutfor Rahman, Daniel Timko, Hamid Wali, and Ajaya Neupane, "Users Really Do Respond To Smishing", In Proceedings of ACM Conference (CODASPY'23). ACM, New York

[10] Abdul Basit, Maham Zafar, Xuan Liu2, Abdul Rehman Javed3, Zunera Jalil3, Kashif Kifayat3, "A Comprehensive Survey of AI-Enabled Phishing Attacks Detection Techniques", Springer Nature 2020

[11] Nina Jagannathan, "The evolution of phishing: How AI is reshaping digital deception in 2024" (2024)

[12] Ping Wang, Peyton Lutchkus, "Psychological tactics of phishing emails", Issues in Information Systems 2023

[13] Khushboo Chahal, "Psychological Manipulation in Social Engineering: Unveiling the Tactics", (2023)

[14] Bryon Miller, Katelin Miller, Xihui Zhang, Mark G. Terwilliger, "Prevention of Phishing Attacks: A Three-Pillared Approach", Issues in Information Systems (2020)

[15] Chibuike Samuel Eze, Lior Shamir, "Analysis and Prevention of AI-Based Phishing Email Attacks", *Electronics* by MDPI (2024)

[16] Obaloluwa Ogundairo, Peter Broklyn, "AI-Driven Phishing Detection Systems", Journal of Cyber Security (2024)

[17] Roopak Surendran, Athira Vijayaraghavan, Tony Thomas Kallivayalil, "On Effectiveness of Source Code and SSL Based Features for Phishing Website Detection", 2019 International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE)

[18] Ollmann, G. (2004). "The Phishing Guide: Understanding and Preventing Phishing Attacks." ,Jakobsson, M., & Myers, S. (2006). “Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft” Wiley-Interscience.

[19] Abeer F. AL-Otaibi, Emad S Alsuwat, “A Study on Social Engineering Attacks: Phishing Attack”, International Journal of Recent Advances in Multidisciplinary Research (2020)

[20] Brad Wardman, “Assessing the Gap: Measure the Impact of Phishing on an Organization”, Annual ADFSL Conference on Digital Forensics, Security and Law 2016 Proceeding

[21] Fauzan Prasetyo Eka Putra, Ubaidi, Achmad Zulfikri, Goffal Arifin, Revi Mario Ilhamsyah, “Analysis of Phishing Attack Trends, Impacts and Prevention Methods: Literature Study”, Brilliance – Research of Artificial Intelligence (2024)

[22] Blessing Nyasvisvo, Joel M. Chigada, “Phishing Attacks: A Security Challenge for University Students Studying Remotely”, The African Journal of Information Systems (2023)

[23] T Steyn, HA Kruger, L Drevin, “Identity Theft – Empirical evidence from a Phishing exercise”, New Approaches for Security, Privacy and Trust in Complex Environments, Proceedings of the IFIP TC-11 22nd International Information Security Conference (SEC 2007)

[24] Tyler Moore, Richard Clayton, “The Impact of Public Information on Phishing Attack and Defence”, Communication & Strategies (2011)

[25] Cheng, J., Chen, M., & Raghavan, S. (2023). “Data Breach Risks in Organizations: Analysis of Causes and Impacts.”

[26] Kirkpatrick, D. (2021). "The Importance of Multi-Factor Authentication." Harvard Business Review

[27] Ransbotham, S., & Mitra, A. (2018). "Exploring the Effects of Phishing Simulations on Employee Responses to Future Phishing Attempts." Journal of Cybersecurity and Privacy

[28] Hadnagy, C., & Fincher, M. (2015). Social Engineering: The Science of Human Hacking. Wiley

[29] Bhakti Ulhas Desai, Gauri Ansurkar, “Research Paper on Spreading Awareness About Phishing Attack Is Effective In Reducing The Attacks?”, International Research Journal of Engineering and Technology (IRJET) (2022)