A COMPREHENSIVE SURVEY OF PHISHING ATTACKS AND DEFENCES: HUMAN FACTORS, TRAINING AND THE ROLE OF EMOTIONS

Mousa Jari[1, 2]

[1]School of Computing, Newcastle University, Newcastle, UK
[2]College of Applied Computer Science, King Saud University, Riyadh, Saudi Arabia

ABSTRACT

Phishing is a sort of cybercrime as well as a security risk that enables ('phishers') to trick, manipulate, and deceive users into divulging and revealing confidential and sensitive information. Typically, attackers aim to influence and manipulate victims' psyche and emotions. The growing threat of phishing has made it desirable to investigate, and significant research has been undertaken on this matter. This paper explores the human and emotional factors that have been reported in previous studies to be significant in phishing victimization. In addition, we compare what security organizations and researchers have highlighted and emphasised in terms of phishing types and categories as well as training in tackling the problem, in a literature review which takes into account all major credible and published sources.

KEYWORDS

Phishing, emotion, information, victimization, training.

1. INTRODUCTION

Phishing is a kind of social engineering attack that is used to steal an individual's information, including personal identification details, credit card numbers or any other private credentials. This activity occurs when a phisher pretends to be someone who is a trusted individual and persuades a victim to open a certain email or a message. When a victim opens such a communication, his/her information can be hacked/leaked and made available to the email/message sender. McAlanay and Hills defined phishing as a social engineering tool or a threat that causes a risk to cyber security [3]. They further highlighted that phishing emails or messages are based on the assertion of some urgency or threat where an attacker or phisher causes a victim to become blackmailed having been encouraged to respond to the email or message accordingly [3]. According to Shaikh et al., phishing is a serious threat in the cyber world that is causing billions of dollars of losses to internet users through the use of social engineering and technology by gaining access to their financial information [4]. Phishing involves an attacker deceiving victims into divulging their confidential, private and sensitive information by sending them fraudulent emails. These emails are sent to internet users and are designed to look authentic [4]. Consequently, from an analysis of the relevant research based on the common elements which have been identified, one can define phishing as a cyber threat that, due to the deployment of social engineering techniques and technological means, leads to messages and emails being sent to internet users resulting in the retrieval of personal information about victims, hence causing them monetary or other damage through the leaking of information.
In this paper, the aim is to identify human factors, and specifically emotional variables, which lead to a higher probability of phishing victimization. This issue has been the subject of several

studies, and as a result, the approach that has been taken in this work of literature is to provide a comprehensive survey of phishing attacks and defences of the previous studies and research in order to highlight the emotional factors that play a significant role in phishing victimisation. Additionally, the paper will compare how different security organisations define and address phishing, as well as provide advice on how to avoid becoming a victim. This problem has been discussed in various studies, and so the method employed in this paper is to analyse the literature review and secondary research in order to highlight the emotional factors which play a significant role in phishing victimization, as well as comparing how security organizations define and address phishing and provide advice on how to avoid becoming a victim.

2. OVERVIEW OF PHISHING

Phishing is a relatively new concept that was first utilised and deployed in the 1990s, and there has been a growing trend of harm and damage caused by phishing in recent years. Rather than simply the deployment of technical expertise to attempt to successfully compromise system security, phishing can also be defined as a semantic attack that uses social engineering tactics to persuade internet users to disclose their private and confidential information such as login credentials, social security numbers, and bank account details. Phishers most commonly use an e-mail which includes an embedded hyperlink with a message either sharing some threat, such as a warning message about account closure or reporting positive news, for example hinting at an unclaimed reward, to attract a potential victim. When a person clicks on the malicious link, it leads to a web-based form that mimics those of valid and authentic websites asking a user to enter login credentials. Once added, such information is then used to compromise network security and thus sensitive information reaches the phisher. Once phishers have obtained sensitive information from victims, they can sell it, set up bank accounts for the victim, or even steal their money. These phishing efforts are believed to be cybercriminals' "vector of choice.".

The Anti-Phishing Workgroup has discovered up to 40,000 phishing websites per month, targeting almost about 500 unique brands; however, the US Department of Defense and the Pentagon have reported more than 10 million phishing attacks daily, which is obviously an enormous number [4][6]. However, Harrison also highlighted the fact that the success rate of phishing attacks is never 100% and often varies between 30-60% [4][6]. This paper aims to explore what makes these attempts successful, focusing on the human emotional factors that may lead users to share confidential information with someone unknown to them. Also, it focuses on the other important elements in phishing victimization.

2.1. Types of Phishing: What We Know from Studies and Security Organizations

Researchers and professionals in the security industry have compiled a list of the numerous forms of phishing that are used to target users of the internet. According to the findings of a study published under the title "Fifteen years of phishing: will technology help us?" Furnell et al., highlighted the four most prominent forms of phishing attacks which are spear phishing, clone phishing, whaling, and bulk phishing [3][5]. In spear-phishing, specific individuals or companies are targeted using a tailored message. In this type of attack, the attacker is more likely to have some background knowledge about the victim, based on which the message that is created becomes more convincing and successful in deceiving and fooling the receiver. As a result, users increase their risk of being targeted and of having their personal and confidential information compromised. Meanwhile, clone-phishing attackers make use of a valid email that contains a URL or attachment and retain the content of the actual message. However, the embedded link or attachment is replaced with a malicious file so that the original sender is spoofed due, for example, to a claim that the email message is an update of an earlier version. In contrast, whaling

is considered to be a particularly threatening type of phishing where CEOs or other senior or high-value individuals in an organization are targeted. Here, the medium used in communicating the message is still the email, but in addition, similar threats are also sent through 'vishing' (voice phishing) and 'smishing' (SMS phishing) which are terms used to specify threats via voice telephony and text messaging. The final category of bulk phishing occurs when there is no specific target or any tailored message. The approach employed instead is to send bulk emails to as many users as possible, and the success of this kind of scam depends on such large-scale mailing where a sufficiently large number of recipients mistakenly believe that the email is relevant to them [3][5].

Phishing has been characterised in a variety of various ways by different security groups; nonetheless, the forms listed overlap with the four basic categories described above. Reports published by the US Federal Trade Commission, the Surveillance Self Defense and Get Safe Online groups, and Phishing.org specify 14 major types of phishing, including spear phishing, session hijacking, email spam, content injection, web-based delivery, phishing through a search engine, link manipulation, vishing, smishing, key logging, malware, trojans, ransomware, and malvertising [5–10]. The common element in all phishing categorizations provided by security organizations and Furnell et al.'s research is the fact that attackers use email, voicemail, or SMS to accomplish phishing [5]. Similarly, victims in all types vary from ordinary internet users to specific companies and businesses or high-profile persons. In addition, the concepts exploited in all the phishing types overlap with the categories recognized by the security organizations, except for web-based delivery, phishing through a search engine and key logging. In web-based delivery phishing, which is also called 'man-in-the-middle' phishing, the attacker is positioned between the customer and the original website. Using his phishing system or network, the phisher identifies the confidential information of the victim during the completion of a deal between the user and the legitimate website. In the case of search engine-based phishing, the user is captured by being (re-)directed to websites purportedly offering low-priced products or services. When the user tries to purchase a product by adding his credit card details, the data are collected by the phisher. Moreover, key logging phishers identify keyboard strikes and mouse clicks performed by a user, and from this information, they manage to retrieve passwords and other confidential data [3][5].

2.2. Training and Awareness

It is not simple for users to practise online safety and avoid all of the dangers that continue to exist in their environments. Phishing is a special type of scam that exploits vulnerabilities in human psychology to gain the attention of potential victims and then uses a variety of deceptive strategies to commit the fraudulent behaviours that were previously described. Therefore, questions arise regarding how people can be trained to stay safe from phishing. The purpose of this section is to compare publications from various researchers and security organisations that address this issue in order to draw conclusions and comparisons about how to protect users against the rising threat of phishing.

Jensen et al. considered aspects of training that can help to mitigate the impact of phishing attacks, focusing on the use of 'mindfulness' techniques [9][11]. The authors specified that simple decision-making or mental shortcut methods to avoid phishing are no longer effective, since not only are they short-term strategies but also phishers are now very familiar with such models. So, the researchers wanted to create an innovative approach to training that can teach internet users to develop new mental models and strategies for the allocation of attention when examining online messages. Rather than a rule-based approach which repeats multiple rules and cues, the training was designed as an exercise to enhance the degree to which users attend to and understand the approach being used in the received message; in other words, to promote

'mindfulness' in evaluating the message. The concept of mindfulness here concerns paying receptive attention to one's experience and surroundings so as to improve the ability to understand one's environment along with an enhanced self-regulation capacity and stronger behavioural control. Their training module consisted of graphics in addition to text promoting mindfulness and helped provide a better understanding of how to avoid phishing attacks since the graphical representation of concepts is thought to enhance the capacity to acquire information leading to better performance in complicated tasks [9][11]. The study aimed to provide participants with a blend of mindfulness training techniques and a rule-based approach so that they could respond to phishing attacks more effectively. To test the effectiveness of the training, a dummy phishing attack was launched in which the participants were directed towards a fictitious website where they were asked to enter their university account login credentials. The results indicated that the graphic and text-based training formats were equally successful in decreasing participants' probability of responding to phishing messages in such a way as to become victims. However, the approach using mindfulness significantly reduced the likelihood of participants responding to the phishing messages, and hence was found to be useful against phishing [11].

Wash and Cooper have also explored and discussed the training models that can work best against phishing scams [12]. The researchers indicate that raising awareness among users through facts-and-advice training or storytelling models works better in combating phishing but using professional security experts or peers to deliver such training is required and necessary in order to maximise its effectiveness. The methodology of the study involved sending 2000 participants phishing emails to gather data necessary to assess the effectiveness of the activity. The lessons that could be learned included to "type in URLs; don't click on them" and "look for HTTPS", that "misspellings can signal fake emails" and "phishing is your problem; don't rely on others to protect you". In total, 17 lessons were compiled from the results of the activities performed. When adopting the fact-telling strategy, it was discovered that not all of the lessons were helpful in protecting against phishing attempts; nonetheless, it was determined that each one was substantial enough to be presented to the participants when using this approach. Meanwhile, the comparison with a story-based strategy led to the surprising outcome that the facts-and-advice approach resulted in fewer clicks leading to scams when an expert was used for the training, whereas the storytelling approach also resulted in lower click rates but only when peers were used rather than experts [12]. From the above-mentioned studies, it can be concluded that multiple factors may lead a user to become caught by a phishing attack, and that appropriate training and education are needed in order to be safer.

When it comes to the advantages of receiving this type of education, Chaudhary's research came to the following conclusions and suggestions, which are among the most important: [13]:

I. Providing any new knowledge in order to be up to date is important, but security education should also result in eliminating misconceptions relating to security.
II. The security education that should be part of a curriculum needs to be up-to-date, and it should cover both new technologies, and information about sophisticated phishing threats and attacks.
III. Security education should teach people about both technology and non-technological forms of attack and danger.
IV. The design of curricula for security education should be based on the input of relevant stakeholders, including teachers, learners, and IT and security professionals, since their experience, skills and knowledge can help in covering a wide range of security-related topics.

V. The adoption of a more interactive way of teaching and learning methods can be quite helpful in making both security learning and teaching more interesting and potentially effective [13].

In parallel with academic researchers, many security organizations have also put a lot of emphasis on user security against phishing attacks, because its severity can vary from password retrieval to stealing money, ultimately causing considerable damage. Among the most prominent security organizations is the National Cyber Security Centre (NCSC), which is a UK-based organization that provides support to critical organizations, including many in the public sector and industry as well as the general public.

In response to the rapid increases in cyber threat levels, the NCSC provides efficient incident responses to mitigate harm and facilitate recovery, and compiles information on the lessons learned that can be useful in the future. Apart from providing solutions to potential phishing threats, NSCS is also concerned with educating people to develop self-reliance against phishing attacks. For this purpose, a major contribution of the Centre is the design of practical resources for school students who take an interest in cyber security studies. The projects on which NCSC is working to provide cyber security education include the CyberFirst courses, schools, colleges, bursaries and apprenticeships and associated resources, and the CyberSprinters programme [14].

In a similar vein, Get Safe Online publishes informative articles on its website that raise users' awareness of phishing and other forms of online fraud. The organisation also shares phishing-related tips and tricks with users in an effort to increase users' awareness of phishing attacks. Advice is offered on a variety of topics, including but not limited to how to make effective use of email, how to recognise fraudulent emails, how to differentiate between genuine websites and emails and phishing websites, and what steps to take in the event that a person has lost money as a result of an online scam. [10].

The Surveillance Self-Defense organization is also based on providing general public protection from phishing attacks. Its literature specifies the intensity of malware and its role in introducing phishing threats. The implementation of malware by phishers is usually based on stealing passwords, where the malware is installed when a user opens or clicks on a malicious link, downloads an unknown file, visits a compromised website, downloads automatic content, or even when USBs are shared while plugging into suspicious ports. However, despite the multiple ways through which malware can be used for phishing [9], users can be educated to avoid being a phishing victim by implementing five important measures:

1. Updating systems and using licensed software.
2. Backing up data.
3. Pausing before clicking, and thus to be more vigilant and to avoid clicking immediately.
4. Using full-disk encryption along with a strong password.
5. Using better anti-virus techniques.

From the discussion above and in the light of the relevant research, it can be concluded that the frequency and intensity of online scam, phishing, and fraud activity are increasing with the passage of time, and so, in order to be safe, security education and training are necessary and perhaps should be mandatory.

2.3. Failure to Train People and the Ineffective Methods

Sonowal has discussed some drawbacks of the training methods used by organizations. One of these drawbacks is that It is not possible to teach only through lectures how to detect and avoid

phishing attacks in real-time. In order to be effective, they will need a laboratory, several simulation tools, and other resources [34]. Also, individuals often have the impression that they are highly knowledgeable and capable of spotting phishing scams, but when they let their guard down, they are more likely to become victims of these scams. No matter what phishing training techniques are utilised, if they are inconsistent, both the trainers and the individuals will struggle. Training must be done on a frequent basis to keep the material fresh in the minds of the users [34]. Another point Sonowal discussed is that sometimes there are inadequate training program resources; some phishing experts know a lot about the subject, but they can't convince people for a number of different reasons. One reason for this is that there aren't enough resources [34].

Kweon et al highlighted some of the elements and factors for unsuccessful, difficult and infective training programs in organisations [1]. Because of the limited security budgets, many companies have trouble making decisions about how to set up the best security training programmes. Also, education time is one of the important factors that affect training and awareness successes. Moreover, the likelihood of security breaches decreased in direct proportion to the amount of time put in by members of the company toward information security training and education [1].

2.4. Human Factors in Phishing Victimization and the Role of Emotion

Chaudhary has emphasized the role of emotion in his research [13], explaining that the manipulation of emotion is generally found to be a prime target of phishers. Ignorance, a desire to be liked, gullibility, and wanting to be helpful to others are among the aspects associated with emotionality which are commonly targeted by scammers or phishers, who rely on the exploitation of vulnerability and weakness. People are found to be more inclined towards sharing their information with others when strong emotions have been triggered, and human behaviour when triggered this way is more likely to be driven by subconscious processes. The problem here is that the functionality of the subconscious mind is not based on logical or analytical behaviour, a fact which is exploited by phishers in pursuing their aims [13]. However, although emotions are very important and can be used against a victim as a weakness, they can also act in the victim’s favour as a strength too. If the emotions which are exploited by phishers instead remain under the control of the user, this may help to combat phishing, which implies that emotions should also have a significant role in training and awareness-raising.

Chaudhary has discussed a very interesting type of phishing and social engineering attack in his research. This is called farming, where a phisher develops a relationship with a victim and continues to obtain relevant information over a certain period of time [15][13]. This activity is usually conducted in four phases. The first phase is information gathering, which involves the collection of the necessary data so that a relationship with a potential victim can be built. The second phase is based on developing the relationship, such as by coordinating with the victim and building a trust-based connection. In the third phase, exploitation starts where the victim is manipulated and deceived to obtain critical desired information, and the final phase is the execution of an attack using the information provided, to the detriment of the victim but beneficial to the attacker.

Emotion may exert a significant influence on many human cognitive processes such as attention, perception, memory, learning, reasoning and questioning, and problem-solving. If a person can manage to understand his emotions and learns how to control them, he can understand his surroundings better, communicate more efficiently, and even appreciate the worth of any relationship [16]. In relation to phishing, it can therefore be proposed that, if internet users are provided with training and awareness based on emotional control, then they will be less likely to be successfully targeted by phishers.

To mitigate the malevolent exploitation of emotions, Jaeger and Eckhardt have highlighted the significance of emotions in awareness-raising and training [15]. They believe that human emotions are learned, and when they are taken under appropriate control the impact of phishing attacks may be overcome. The researchers analyzed the relationships among the constructs of protection-motivation theory (PMT) Nomology [22] that involve fear and the motivation for protection and in actual security-related behaviour, indicating that perceived threat perceived coping efficacy in response to threat encourages a person's motivation towards self-protection in combatting the threat. So, when an individual encounters a phishing attack and faces its likely consequences; then, after being threatened, he starts to believe that he can respond to the situation using learnt behaviours and emotions which can ensure protection against such threats in the future [15]. In addition, not only does this help in terms of training, but it also helps in terms of raising awareness among peers. Such learning can also lead to technical solutions, such as users protecting themselves from phishing by implementing technical countermeasures including deciding not to click on any unknown or potentially malicious link, not downloading an .exe file, and deleting any dubious email or sending it to the junk folder.

Sonowal held the belief that phishing used people's emotions to trick them, and users are more susceptible to being exploited by social engineering and phishing than through technological means [34]. It is feasible to correct technological problems by adding more security measures, but it is considerably more challenging to fix problems that are caused by human error and emotions. Mostly due to the fact that humans are mentally governed by powerful emotions such as fear, greed, and curiosity [34]. A significant number of phishing attacks motivate their victims to act on the basis of their emotions and feelings.

If one asks what makes phishing successful or what causes victims to become entrapped in phishing, the answer is simple: the victim himself. More specifically, it can be said that phishers target the victim's emotions which they manipulate to achieve their aims [16]. The above sections have indicated that emotions have a major role in phishing attempts, and the focus of the remaining discussion is to answer the research question of the study: what the human factors are, and specifically the emotional variables, which lead to phishing victimization.

In considering the nature of emotions and other psychological variables, Chaudhary cited various aspects of the human psyche which play a major role in phishing victimization [13] and specified several psychological states and factors that are mainly targeted by phishers which may lead a user to comply with the instructions given as part of the phishing attempt [13]. These include:

i) Reciprocation: where potential victims are more likely to comply with malicious instructions when they have a feeling of gratitude towards the phisher and feel that they are granting a favour to one in need.
ii) Consistency and commitment: since individuals like to be seen as trustworthy by fulfilling promises. If this trait is targeted by the phisher, to make one feel that he has made a promise, then it is possible that the person may comply with the phisher's instructions and demands.
iii) Social proof: People are more prone to fall victim to deception if they are presented with evidence that is convincing, such as being persuaded that one is not alone in doing something and that everyone else is doing the same thing. This makes it more probable that a victim would fall into the criminal's trap.
iv) Liking: because individuals are more likely to cooperate with someone they like, phishers and attackers frequently take use of the sentiment of liking someone as a tactic. This is because people are more likely to trust someone they like. Phishers have a better chance of succeeding if they are able to fool their victims into believing they are someone they know and like.

v) Authority: people generally comply with authority since being a responsible individual usually means complying with an authorized person. So, if a phisher manages to appear authoritative, he can use the victim's tendency to comply with the demands of an authority to manipulate him.
vi) Scarcity: if a phisher manages to convince his target that something he wants is in short supply and will not be available afterwards, then it is more likely that the victim may comply with the phisher's instructions.

In addition to the above-mentioned psychological states and emotions described by Chaudhary, Vishwanath et al. considered the dimensions of the email and social media behaviour of individuals which result in getting trapped by phishing attempts [17]. They emphasised the fact that social media users, and especially those who regularly check Facebook notifications, are more likely to be targets of social media phishing. However, social media are quite distinct in providing relational information which can help in the detection of deception. Social media-based phishing attacks are multi-staged in the sense that the user receives a friend-request followed by messages. This is in contrast to email-based phishing which is single-staged, where a phisher uses a persuasive subject line that either causes a feeling of fear in cases of a threat, or a sense of happiness following a piece of fake news such as concerning winning a lottery or an amount of money. Vishwanath et al. concluded that users with low levels of emotional stability are more likely to start worrying and lose their emotional control based on the subject of the email. This kind of behaviour can create impulsive email habits. For example, in response to the sound of a single email notification, a user may react by checking and immediately opening an email to answer it, which may lead to reactively clicking on malicious phishing links [17]. Responding to emails with feelings of being nervous, curious, happy or under threat has also been explored by other researchers because this area of research has shown considerable promise.

Abroshan et al. recently conducted a noteworthy research study regarding human behaviour and emotions which influence the success of phishing attacks' [18]. They highlighted previous studies which have found that emotional behaviour can significantly affect responses to phishing emails, and proceeded to develop a holistic method including the use of psychological and phishing mitigation to identify highly susceptible users in organizations who are at the risk of clicking on phishing emails. Their proposed solution is comprised of three modules involving behaviour measurement, risk scoring and mitigation, and the system can be delivered online. It is also a flexible solution which can be expanded by adding more human factors root-causes; for example, "more behavioural and emotional factors that might impact falling into a phishing scam" (p. 349). This study significantly highlights the importance of human behaviour and emotions in relation to security behaviour such as the propensity to get caught up in a phishing scam. For example, the emotions of users such as fear and anxiety, especially in certain situations like the Covid-19 pandemic, can play a pivotal role in making phishing attacks successful. This is because the user's awareness and knowledge of security can be overshadowed due to the emotion of fear [18]. In reacting, users might click on a suspicious phishing link without thinking, supposing that the information is required due to Covid-19 health impacts.

2.5. User Knowledge, Education, and Understanding

Dealing with phishing attempts can be controlled through the use of software; nevertheless, the greatest prevention can only be provided through the user's improved knowledge, education and understanding. Arachchilage and Love emphasized that anti-phishing education and knowledge need to be considered to combat phishing [19], and they investigated the extent to which procedural knowledge or conceptual knowledge has a positive effect on users' self-efficacy to be safe from phishing attacks. Using a theoretical model based on Technology Threat Avoidance Theory, data was collected from 161 computer users who were provided with a questionnaire to

get their feedback. It was found that both procedural and conceptual knowledge positively impacted the users' self-efficacy, ultimately resulting in the enhancement of their phishing threat avoidance behaviour. A later study by He and Zhang supported the claim that users' knowledge, education and understanding play a significant role in repulsing phishing attacks, and the authors concluded that "Training programs and educational materials need to relate cyber awareness to employees' personal life, family, and home, in order to be more engaging and to encourage employees to change their cybersecurity behaviour" [20].

Subsequent research regarding knowledge capabilities was conducted by Wash et al., who surveyed 297 participants with matching demographic characteristics in the US, allowing them to share their experiences of phishing emails [21]. This study provides evidence that humans may perceive and experience phishing emails in a very idiosyncratic manner, using different capabilities and knowledge in contrast to technical filters. For example, their past knowledge may assist them in detecting and becoming suspicious of phishing attacks, such as their familiarity with previously received emails as well as their expectations regarding incoming emails. It can be assumed that this knowledge is contextual and every individual would have a unique set of relevant experiences, which will be utilised to detect missing and unexpected informational units in emails. Because technical solutions seldom spot these types of phishing attacks, such knowledge-based information residing only in the human mind is critical in spotting phishing attacks, whereas technical expert-based filters lack this information processing capability. For example, humans can use their knowledge to conduct an investigation or delay the response to an email and request further information from the sender [21]. This shows that the user's knowledge is critically important in combatting phishing attacks.

Even though it is acknowledged that people or users who are not native speakers are more susceptible to phishing attempts [23], the vast majority of studies that have been published have neglected to take language-based phishing susceptibility into account. However, Hasegawa et al. conducted a noteworthy online survey of 302 Japanese, 276 South Koreans and 284 German participants representing a total of 862 non-native English speakers. Participants who did not have a strong knowledge of the English language or who did not feel comfortable communicating in the language had a significant predisposition, according to the findings of the analysis of the data, to ignore any and all emails sent in the English language [23]. Furthermore, qualitative analysis revealed five key factors that aroused the concern of participants in identifying phishing emails in English. These include difficulties in identifying errors in the language, unfamiliarity with the written English in phishing content, difficulty in understanding English content, and decreased attention. These findings suggest that it would be necessary to develop different strategies to tackle the susceptibility to phishing emails among non-native speakers, as well as to consider the importance of language barriers when formulating interventions to assist non-native speakers to combat phishing attacks.

2.6. Demographics Factors

In addition to the emotional factors discussed by Chaudhary and others, various demographic variables are believed to be significant in phishing victimization. However, other demographic characteristics have been found to have an impact on resilience against phishing. For example, Gopavaram et al. found that phishing resilience and age have a negative relationship, so that older users are more likely to become confused about the legitimacy of genuine and phishing websites. However, no significant relationship was identified between phishing resilience and gender [24], whereas Sheng et al. [25] found that age and gender are key demographic factors that can indicate the levels of susceptibility to phishing. Their analysis indicated that women click on malicious links provided in phishing emails more often than men, and hence are more likely to provide phishers with confidential information. Such differences in gender-based behaviour might be

based on the role of technical education since males often have more technical knowledge than females. Age was also found to have a significant relationship with phishing susceptibility, and participants between the ages of 18-25 years were more likely to fall into phishing traps. But this factor was also linked with levels of education since participants in the age group concerned were found to have received a relatively lower level of education, limited training material, fewer years spent using the Internet, and low capacity in risk management [25]. So, in relating demographics to phishing, Arachchilage and Love's conclusion that improved education can reduce phishing victimization was supported.

Lin et al discussed and explored the effects of user demographics and Email content [35]. The study looked at how spear-phishing (targeted phishing) is influenced by the age of users and the content of the emails, such as "weapons of influence" to lure victims to fall for an attack and "life domains" which is the targetable component of a person's life that can be the subject of a targeted email [35]. They concluded that the biggest percentage of victims who fell for the fake phishing emails was made up of elderly women (43%), and older users compared to young users reported lower susceptibility awareness [35]. They, also, discussed previous studies which showed that older people were not more likely to fall for phishing than young people, and discussed an empirical study by Halevi et al. [36] which investigated the demographic characteristics of users with high susceptibility to phishing and found that females compared to males were more susceptible to phishing scams [35,36].

2.7. Online Habits and Behaviour, Responding Impulsively to Emails, and the Role of Mental Models

In research where the scope and purpose are to understand the phishing attacks and victims' reasons for opening malicious links, an investigation of the mental models used and online behaviour exhibited is very significant. A simple explanation of a mental model is an individual's own thought processes in relation to how a particular phenomenon works in a real-life scenario. Mental models are based on an individual's learning, experience, skills and knowledge which improve the thought process concerned, hence resulting in some specific behaviour or outcome. So, no single mental model can work against phishing, but several mental models can serve the purpose, and Jaeger and Eckhard have described that schemata and mental models are key elements used to achieve high levels of awareness [15]. Critical cues that are needed to activate both of those mechanisms should be based not only on the characteristics of emails but should also be linked to security warning alerts. Meanwhile, mental models specifically relating to phishing could be more complex, since they may vary depending on the type of phishing attacks concerned. An individual's mental model is shaped by past experience where phishing plays a major role in obtaining situational information relating to security awareness. It was concluded that experienced users signify their level of awareness by using the security-related information cues available, which shows that the experience helps in developing schemata and remembering the critical cues, ultimately leading to pattern matching and improved thought processes in working against phishing [15]. A study by Sibrian et al. conceptualized the thought processes and human behaviour involved using a model of the social decision-making process divided into two systems [26]. The first was defined as the source of emotional reactions based on experience, which works quite rapidly and almost impulsively with very little voluntary control, whereas the second system is based on reasoning, focus, and choice. The operations linked to this second system require attention and can be disrupted when it is reallocated or disturbed. Since it is more logical and rational, whereas the emotional system is more impulsive, phishers exploit it so that the other system either does not react or takes too much time to respond. This is how phishers exploit the human mental model, due to which an individual may feel fear, happiness, curiosity or even urgency to respond to the phishing message quickly, which affects the overall user's

behaviour while responding to a phishing attack and leads to getting entrapped in a phishing attack [26].

2.8. Expert versus Non-expert Thought and the Ability to Detect and Avoid Falling Victim to Phishing

Experts and non-experts respond differently to phishing attempts, based mostly on their abilities, skills, knowledge, and experience. Nthala and Wash explain that non-experts follow four sense-making processes according to which they determine if the email they receive is in actuality, a phishing message [27]. In the first stage, they identify, without going into detail, whether or not the email is relevant to them. In the second stage, the goal is to understand why they received the email. Here, non-experts try to understand the email in more depth. In the third stage, they start to take positive action using a sense-making process to fulfil the request made in the email. In the last stage, either the email is closed, deleted, or even moved to re-reading. The core element of this stage is the sense of marking the task as completed by closing the email [27].

As opposed to non-expert behaviour, Wash highlighted that, to identify a phishing email, experts follow a three-stage process [28]. In the first stage, experts tend to consider why such an email has been received and how it is relevant to them and identify any discrepancies. In stage two, they may entertain suspicions about the email by analysing its features such as the presence of a link requiring a click. Here, they manage to identify that the email is based on a phishing message. In the third step after this thought process using their mental model, experts deal with the phishing email either by reporting or deleting it [28].

Expert users utilise a range of indicators to avoid falling victim to phishing scams, and these indicators may be included in the headers or body of phishing emails or the content of bogus websites [37]. In addition, browser-based security indicators and anti-phishing programmes can give hints. Experts advocate deactivating JavaScript in email programmes and carefully examining the URLs behind email hyperlinks or putting any hyperlinks directly into a web browser as opposed to clicking on them [37].

2.9. Communication channels to perform phishing attacks

There are several communication channels that attackers used to perform phishing attacks such as VOIP, SMS, IM, Wi-phishing, and multiplayer games are also utilized as communication channels to perform phishing attacks [29-31]. Alabdan [29] and Krombholz et al. [30] have discussed different technical approaches and types of communication channels that attackers use to perform phishing attacks. These include the following:

i. E-mail is the most popular communication channel used for performing phishing attacks [30]. Organizations and users prefer email to communicate with their customers or with each other. Emails which allow users to keep a record of any correspondence are used to communicate and quickly transmit information to many people, or only one person [33]. According to a recent research report from IRONSCALES written in 2021 by Ian Thomas, over 80% of respondents have experienced an increase in email phishing attacks since the COVID-19 pandemic in 2020 [32]. Also, according to knowbe4.com, the top phishing email subject in 2021 in Europe and the Middle East was “Your document is complete – Save Copy”.
ii. Instant messaging applications are gaining popularity among social engineers as tools for phishing and reverse social engineering attacks. They can also be used easily for identity theft to exploit a trustworthy relationship. Subsequently, instant messaging is generally combined with other social media such as WhatsApp, Facebook, and Telegram [29,30].

iii. Voice, i.e., speaking and the use of language is one of the most successful ways for humans to communicate and connect [29]. Consequently, voice is another frequent method used by attackers to make their victims deliver sensitive information. This attack, voice phishing, is known as Vishing. The attacker would use phone calls pretending to be from the government, a reputable company or organisation, or even a family member who needs help to obtain sensitive information [34]

iv. SMS, or Short Message Service, is a kind of global communication utilised by billions of individuals [33]. SMS is considered more effective than email by many persons and firms because of the speed and ease of response [34]. Due to the advantages of SMS, some attackers are transitioning to SMS phishing, which is known as smishing and sending fraudulent text messages to expand the phishing scams [34]. According to Alabdan, there are two methods or ways for this technique [29]. The first way includes sending an SMS while posing as a reputed source or authority, and the second way is sending a victim a text message with malware or including a link to a website containing malware [29].

Other communication channels to perform phishing attacks are EFAX, social media and networks phishing, websites, Wi-Fi phishing etc [29, 34].

3. CONCLUSIONS

Phishing is one of the most widespread issues that lead to users disclosing private information like passwords or credit card details, which can even result in the theft of money. In this paper, we compared the approaches that security firms and researchers have taken to address the issue of phishing in terms of the various types and classifications of phishing attacks, as well as training and awareness campaigns. Also, we discussed the different communication channels that attackers use to do phishing attacks. This paper has also mentioned the role of demographic factors that impact phishing susceptibility. Additionally, numerous emotional factors are targeted by phishers; however, with the assistance of training and anti-phishing education, we believe that emotions can be regulated and controlled, and self-control can be established that can lead to the failure of phishing attempts.

REFERENCES

[1] Kweon, E., Lee, H., Chai, S. et al. The Utility of Information Security Training and Education on Cybersecurity Incidents: An empirical evidence. Inf Syst Front 23, 361–373 (2021). https://doi.org/10.1007/s10796-019-09977-z.

[2] R. G. Brody and F. St Petersburg Valerie Kimball, "Phishing, pharming and identity theft," *Academy of Accounting and Financial Studies Journal*, vol. 11, no. 3, 2007.

[3] J. McAlaney and P. J. Hills, "Understanding phishing email processing and perceived trustworthiness through eye tracking," *Frontiers in Psychology*, vol. 11, p. 1756, Jul. 2020, doi: 10.3389/FPSYG.2020.01756/BIBTEX.

[4] A. N. Shaikh, A. M. Shabut, and M. A. Hossain, "A literature review on phishing crime, prevention and investigation of gaps," *SKIMA 2016 - 2016 10th International Conference on Software, Knowledge, Information Management and Applications*, pp. 9–15, May 2017, doi: 10.1109/SKIMA.2016.7916190.

[5] S. Furnell, K. Millet, and M. Papadaki, "Fifteen years of phishing: can technology save us?". Journal of Computer Fraud and Security, vol. 2019, no.7, pp.11–16, Nov. 2021, doi:10.1016/S1361-3723(19)30074-0.

[6] B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails: how attention and elaboration protect against phishing," *Online Information Review*, vol. 40, no. 2, pp. 265–281, Apr. 2016, doi: 10.1108/OIR-04-2015-0106/FULL/PDF.

[7] Get Safe Online, "Spam and scam email: Get Safe Online." https://www.getsafeonline.org/personal/articles/spam-and-scam-email/ (accessed Feb. 17, 2022).
[8] "How to recognize and avoid phishing scams: FTC consumer information." https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (accessed Feb. 17, 2022).
[9] Surveillance Self-Defense, "How to: avoid phishing attacks." https://ssd.eff.org/en/module/how-avoid-phishing-attacks (accessed Feb. 17, 2022).
[10] Phishing.org, "Phishing: what is phishing?" https://www.phishing.org/what-is-phishing (accessed Feb. 17, 2022).
[11] M. L. Jensen, M. Dinger, R. T. Wright, and J. B. Thatcher, "Training to mitigate phishing attacks using mindfulness techniques," *Journal of Management Information Systems*, vol. 34, no. 2, pp. 597–626, Apr. 2017, doi: 10.1080/07421222.2017.1334499/suppl_file/mmis_a_1334499_sm1984.docx.
[12] R. Wash and M. M. Cooper, "Who provides phishing training? Facts, stories, and people like me," *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, doi: 10.1145/3173574.
[13] S. Chaudhary, "The use of usable security and security education to fight phishing attacks," Ph.D. Thesis, Nov. 2016, Accessed: Feb. 17, 2022. [Online]. Available: https://trepo.tuni.fi/handle/10024/100073
[14] National Cyber Security Centre, "Cyber security for schools." https://www.ncsc.gov.uk/section/education-skills/cyber-security-schools (accessed Feb. 17, 2022).
[15] L. Jaeger and A. Eckhardt, "Eyes wide open: the role of situational information security awareness for security-related behaviour," *Information Systems Journal*, vol. 31, no. 3, pp. 429–472, May 2021, doi: 10.1111/ISJ.12317.
[16] A. Vishwanath, T. Herath, R. Chen, J. Wang, and H. R. Rao, "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model," *Decision Support Systems*, vol. 51, no. 3, pp. 576–586, Jun. 2011, doi: 10.1016/J.DSS.2011.03.002.
[17] A. Vishwanath, "Examining the distinct antecedents of e-mail habits and its influence on the outcomes of a phishing attack," *Journal of Computer-Mediated Communication*, vol. 20, no. 5, pp. 570–584, Sep. 2015, doi: 10.1111/JCC4.12126.
[18] H. Abroshan, J. Devos, G. Poels, and E. Laermans, "A phishing mitigation solution using human behaviour and emotions that influence the success of phishing attacks," *UMAP 2021 - Adjunct Publication of the 29th ACM Conference on User Modeling, Adaptation and Personalization*, pp. 345–350, Jun. 2021, doi: 10.1145/3450614.3464472.
[19] N. A. G. Arachchilage and S. Love, "Security awareness of computer users: a phishing threat avoidance perspective," *Computers in Human Behavior*, vol. 38, pp. 304–312, Sep. 2014, doi: 10.1016/J.CHB.2014.05.046.
[20] W. He and Z. Zhang, "Enterprise cybersecurity training and awareness programs: recommendations for success," Journal of Organizational Computing and Electronic Commerce, vol. 29, no. 4, pp. 249–257, Oct. 2019, doi: 10.1080/10919392.2019.1611528.
[21] R. Wash, N. Nthala, and E. Rader, "Knowledge and capabilities that non-expert users bring to phishing detection," *Proceedings of the Seventeenth Symposium on Usable Privacy and Security*, 2021, pp. 377–396. Accessed: Feb. 18, 2022. [Online]. Available: https://www.usenix.org/conference/soups2021/presentation/acar
[22] Witte, Kim (1992), "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," Communication Monographs, 59, 329–49. [Taylor & Francis Online], [Web of Science ®].
[23] A. A. Hasegawa, N. Yamashita, M. Akiyama, and T. Mori, "Why they ignore english emails: the challenges of non-native speakers in identifying phishing emails". *Proceedings of the Seventeenth Symposium on Usable Privacy and Security*, 2021. Accessed: Feb. 18, 2022. [Online]. Available: https://www.usenix.org/conference/soups2021/presentation/acar
[24] Gopavaram, Shakthidhar and Dev, Jayati and Grobler, Marthie and Kim, DongInn and Das, Sanchari and Camp, L. Jean, Cross-National Study on Phishing Resilience (May 7, 2021). In Proceedings of the Workshop on Usable Security and Privacy (USEC), 2021, Available at SSRN: https://ssrn.com/abstract=3859057
[25] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, "Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions," *Proceedings of Conference on Human Factors in Computing Systems*, vol. 1, pp. 373–382, 2010, doi: 10.1145/1753326.1753383.

[26] J. Sibrian, J. Mickens, and J. A. Paulson, “Sensitive data? now that’s a catch! The psychology of phishing,” Bachelor's thesis, Jun. 2020, Accessed: Feb. 17, 2022. [Online]. Available: https://dash.harvard.edu/handle/1/37364686

[27] N. Nthala and R. Wash, “How non-experts try to detect phishing scam emails”, In Workshop on Consumer Protection, Accessed: Feb. 17, 2022. [Online]. Available: https://msucas-paid.sona-systems.com

[28] R. Wash, “How experts detect phishing scam emails,” *Proceedings of the ACM on Human-Computer Interaction*, vol. 4, no. CSCW2, Oct. 2020, doi: 10.1145/3415231.

[29] Alabdan, Rana. "Phishing attacks survey: types, vectors, and technical approaches." Future Internet 12.10 (2020): 168.

[30] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

[31] Jason Hong. 2012. The state of phishing attacks. Commun. ACM 55, 1 (January 2012), 74–81. https://doi.org/10.1145/2063176.2063197

[32] Ian Thomas, “The IRONSCALES State of Cybersecurity Report | Blog | IRONSCALES,” 2021. https://ironscales.com/blog/ironscales-releases-findings-from-state-of-cybersecurity-survey/ (accessed June. 12, 2022).

[33] Karen Church and Rodrigo de Oliveira. 2013. What's up with whatsapp? comparing mobile instant messaging behaviors with traditional SMS. In Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI '13). Association for Computing Machinery, New York, NY, USA, 352–361. https://doi.org/10.1145/2493190.2493225

[34] Gunikhan Sonowal. 2022. Phishing and Communication Channels. Apress Berkeley, CA. DOI:https://doi.org/10.1007/978-1-4842-7744-7

[35] Tian Lin, Daniel E. Capecci, Donovan M. Ellis, Harold A. Rocha, Sandeep Dommaraju, Daniela S. Oliveira, and Natalie C. Ebner. 2019. Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. ACM Trans. Comput.-Hum. Interact. 26, 5, Article 32 (October 2019), 28 pages. https://doi.org/10.1145/3336141

[36] T. Halevi, N. Memon, and O. Nov. 2015. Spear-phishing in the wild: A real-word study of personality, phishing self-efficacy andvulnerability to spear-phishing attacks. Social Science Research Network. DOI:http://dx.doi.org/10.2139/ssrn.2544742

[37] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. 2006. Decision strategies and susceptibility to phishing. In Proceedings of the second symposium on Usable privacy and security (SOUPS '06). Association for Computing Machinery, New York, NY, USA, 79–90. https://doi.org/10.1145/1143120.1143131