Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/160402

Exploring the Factors Influencing Employee Awareness of Social Engineering Threats: A Review

Mohammed Fahad Alghenaim[*], *Nur Azaliah Abu Bakar and Fiza Abdul Rahim*

Advanced Informatics Department, Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, 54100 Kuala Lumpur, Malaysia

Received: 1 Mar. 2022, Revised: 26 Apr. 2022, Accepted: 5 May 2022
Published online: 1 Jul. 2022

Abstract: Phishing is a dynamic threat, making it much more dangerous because a lack of awareness among employees makes it much more difficult for the business to detect and respond to Phishing situations. Social engineering is a process that essentially involves human interactions that can be exploited to the point where typical security methods become defective. The most dangerous risk of social engineering is that the criminals understand human nature and may exploit vulnerabilities without the victims realizing it. This study examines relevant research to determine the factors that may influence employee awareness of social engineering threats. Three demographic factors and seven other factors, according to the literature, may influence employee awareness of social engineering threats.

Keywords: Factors; Employee Awareness; Social Engineering; Threats.

1 Introduction

Most conscious cybercriminals have turned to social engineering to boost the efficiency of their operations and, in the end, defeat automated exploits. For the most part, social engineering is a method that does not require any technical items and mainly involves human interactions that can be exploited to an extent where the common security procedures become flawed [1]. The most danger of social engineering is that the perpetrators understand human nature and can exploit vulnerabilities without the victims realizing it while they are fully engaged in the process [2]. Therefore, social engineering tactics are required to make people prone to manipulations and cause information systems (IS) to break down under the influence of external attacks.

The problem for organizations, in most cases, is that human behaviour establishes the indispensable settings for offenders to reconnoitre vulnerabilities and create crucial gaps that can be violated to gain access to sensitive information and end-user credentials. The multitude of social engineering strategies described above often faces a certain degree of protection established by companies that value privacy and data protection the most, but it does not always help the organization prevent itself from becoming a victim of social engineering actions [3]. Therefore, one way to protect intellectual assets possessed by the company is to see how the organization could improve employee awareness concerning social engineering threats. Even the most secure systems might be breached when end-users do not realize their vulnerability.

According to [4] & [5], one of the basic problems with social engineering is that they consider protection measures and security procedures too complicated and unnecessary, which leads them to overlook the primary instruments used by social engineers to breach systems. The willingness to complete their job quicker, without paying attention to potential security issues, leads most organizations to performance decline because social engineers ideally use their knowledge and experience to make the best use of human fears and vulnerabilities [6]. There is an even bigger number of possible attack angles for larger corporations, leaving both the management and lower-tier employees prone to becoming victims of social engineering attacks. Even worse, numerous cases of computer-based offences linked to social engineering allow respective cybercriminals to rely on computer systems largely when conducting their operations, such as fake email scams, phishing, and many more [7].

Phishing attackers' skills have increased significantly throughout the last decade, creating more room for high-profile cases where millions (or tens of millions) of passwords had been leaked. Interestingly, tech giants such as Google, Dropbox, Facebook, or LinkedIn have also been involved in identity theft cases, meaning that IT moguls are just as prone to social engineering issues as their smaller counterparts due to the presence of the human factor [8]. The dynamics of Phishing threats make it harder for

[*]Corresponding author e-mail: aalghenaim@graduate.utm.my

organizations to respond, as many companies merely overlook the benefits of establishing respective training operations and preventing future cases of data breaches and identity thefts [9]. According to Edwards et al. (2017), with time, more organizations started paying more attention to the advent of physical protection measures, making it considerably harder for phishing to breach systems and gain access to forbidden data [10].

In line with the current evidence, phishing is a billion-dollar business that leads to crucial annual losses that, in most cases, cannot be restored [11]. As it has already been pointed out, phishing is a dynamic threat, making it even more dangerous because the lack of awareness among employees makes it much harder for the organization to face Phishing cases and respond accordingly. The researchers in [12] and [13] claim that many employees merely fail to address their organizations' security policies and perform their functions without proper attention to procedures avert the business coping cases of identity or data theft. Another essential idea is that management units do not exert enough effort to define proper security rules and postpone these activities until the company is attacked [14]. The key reason why many organizations enforce stricter rules for employees is not to protect the infrastructure but to limit the number of potential lawsuits that could arise in a breach. Three (3) demographic variables (age, gender, and education) and seven (7) other factors (internet usage, cybersecurity knowledge, cybersecurity-protective practices, responsible departments' support, strategy training plans, employee accountability, and employee satisfaction) might affect employee awareness regarding social engineering threats. Hence, this paper aims to review the demographic variables and other factors to understand better why the public sector is at risk.

The remainder of this paper is organized as follows: Section 2 discusses the related studies. Section 3 presents and discusses factors influencing employee awareness of social engineering threats. Finally, the conclusion is presented in Section 4.

2 Related studies

In a recent study covering workplaces and e-learning [15] show that employees who work in the social-based departments have poor knowledge compared to those in the technology-based. However, employees of social-based departments can improve their awareness status by continuing involvement in the enhancement process. This study was impacted by eight factors: "Educational background, working experience, the field of study, gender, age, [nationality], training and area of living." [15]. In addition, the study says that "cyber security can be the collection of best practices, concepts, policies, assurance, guidelines, safeguards, actions, risk management methods, training, tools, and technologies." The study shows that these threats can be risks from this kind of threat that can be lessened if employees' Phishing awareness is raised [15].

The researchers compare employees working in various departments in the same organization. They check their level of cybersecurity awareness through simulation of the phishing activity before the actual training in cybersecurity takes place. Then the second simulation was produced to check employees' actions to Phishing threats. There were various Phishing awareness levels among workers of the same institution. As the collection stage of research has shown — employees from IT were more aware of cyberthreat than employees from the HR department. Additionally, Thai employees working in the social-based department showed a low level of cybersecurity awareness. However, after they went through a cybersecurity awareness training program, their results were improved [15].

Thus, the researchers prove, based on simulations conducted among employees, the hypothesis that Phishing awareness simulations and training help enhance the level of cybersecurity awareness for workers of the organizations. It is essential for employees from social sciences and humanities backgrounds, in fact, for all workers in social-based departments to be trained in cyber activity training programs. So good training is a good safety line for increasing Phishing awareness among all employees of any given organization. Furthermore, the customized programs should be used as a good platform for training and educating employees, raising their level of cybercrime activity. It can protect the organization from all kinds of cyber-attacks [15].

3 Factors Influencing Employee Awareness of Social Engineering Threats

3.1 The End-User's Age

The least crucial variable is the age of end-users who could be potentially exposed to the impact of phishing threats. One of the literature's ideas was that phishing and its alternatives were the most effective with younger Internet users [16, 17, 18, 19, 20, 21]. On the other hand, it was also identified by [22] that people aged from 28 to 40 were the least responsive to Phishing attacks due to the reduced amount of trust toward any specific individuals looking forward to building a close relationship.

3.2 The Gender

Another issue (variable) from the spectrum is the impact of end-user gender on how they interact with attackers and how these could be prevented. Gender is essential to accept and demographic variables related to phishing attacks [19, 20, 21]. There is a significantly tight relationship between the gender of individuals being targeted and the overall success of social engineering attacks, meaning that females

could be, in some cases, more prone to exposing themselves to phishing than males. For example, women are much more prone to becoming victims of phishing attacks because they are more open to communication than their male counterparts and may be susceptible to clicking on suspicious links or replying to junk ads [17].

3.3 The Education

Another important variable that cannot be underestimated is the presence of a certain level of education that ultimately defines the impact of a social engineering attack on an individual or an organization. There is a direct correlation between these notions where individuals with higher levels of study were not as affected by phishing attacks as their counterparts with lower studies [2, 16, 18, 19, 20, 21, 23, 24, 25]. Nevertheless, there is also a hypothesis shared by [22] that the level of education does not associate with proneness to Phishing attacks in any way. Therefore, education level has been placed in the lower half of the list of essential factors. As shown in Fig, demographic variables and their relations.

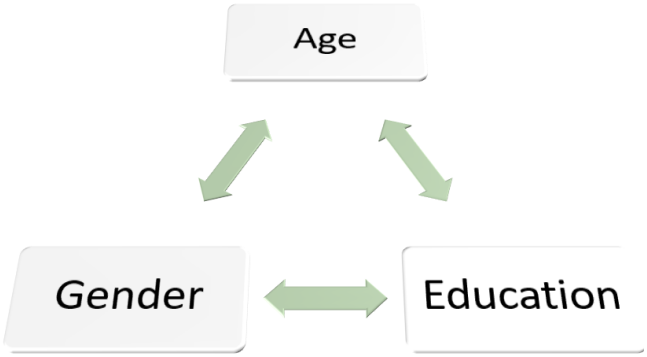

Fig.1: The target list of demographic variables contributing to the emerging threat of Phishing attacks in the public sector.

3.4 Internet Usage

The concept of Internet usage bounds is the first of seven (7) other factors affecting an organization's proneness to phishing attacks [16, 21]. In line with the evidence presented by [26], it may be claimed that those who use the Internet more often are becoming victims of social engineers due to excessive confidence and risky security behaviors based on overconfidence. The majority of empirical evidence on the subject revolves around the idea that experienced Internet users benefit from weaker security measures instead of establishing the best protection for their assets [27].

This argument is of exceptional importance for the current literature review because modern humanity has become dependent on the Internet and has little to no chance to avoid different cybercrimes that dynamically affect all spheres of human lives. For public sector representatives, excessive confidence might lead to many psychological tricks that take different shapes and sizes that phishing could use to take advantage of employees and steal the data [28]. Therefore, it may be concluded that the current exposure to daily Internet usage turns public sector employees into easy targets because of their belief that phishing is a simple concept that does not affect them in any way.

3.5 Cybersecurity Knowledge

The second of the seven other factors is the presence (or the lack) of strong Cybersecurity knowledge [16, 19, 20, 21, 23, 24]. As Ghafir et al. explain, both experience and education could become the two (2) essential elements contributing to one's ability to point out potential security threats and address them on time. Suppose an organization expects to protect its assets [5]. In that case, it requires to continuously educate its employees and ensure that they have all the skills necessary to safeguard the information assets that could expose the organization or individual users to exceptional cybersecurity threats [29].

In a sense, the organization could establish a lifelong learning initiative to ensure that the executive branch does not just release updated security policies. However, it also makes employees understand and acknowledge the threats and possible ways of resolving them. This kind of reinforcement is essential because security education is on the list of key tasks required to help the given business or organization avoid the costly consequences of overlooking phishing's influence [4]. There is a possibility of improving public sector exposure to social engineering attacks to share cyber threats experiences. This would become a significant factor in the future battle against phishing across the Saudi public sector due to the existence of models suggesting that end-user judgments account for a critical portion of InfoSec challenges [30].

Concurrently, the presence of past experiences or experience exchange sessions might be an opportunity for the organization to capitalize on cybersecurity knowledge and prevent numerous identity theft cases that could have become detrimental for anyone involved with the team. Without respective cybersecurity knowledge, employees would not have the time and experience required to respond to the threats and protect the organization from data theft.

3.6 Cybersecurity-Protective Practices

These may include (but never be limited to) antivirus software installation, firewall enabled, and email validation. These are required for the organization to adequately respond to Phishing attacks and educate every other employee on why phishing could be detrimental, especially across the public sector [3]. The more employees learn about protecting themselves from phishing, the more chances they become victims of phishing looking forward to obtaining their credentials or having the end-users click on infected links. The phishing domain continues to evolve

daily, so it should be crucial to propose numerous solutions to prevent certain Phishing challenges [6].

The public sector should recurrently address employee education to minimize the chances of exposing end-users and citizens to data leaks and identity thefts [16, 18, 19, 20, 21, 23, 24]. This literature review is a direct representation of why security-protective practices are essential for any organization, as [31] and [32] suggest that Phishing attacks lose a great deal of effectiveness under the condition where the perceived targets know how to approach the threats and respond to them. In a sense, when the practice is unsecured, knowledgeable employees have more chances to evade the dangers associated with it and overcome the challenges that could have become real in the case where they would not know what to do with phishing in the first place [33].

Besides, it should be concluded that demographic variables could impact end-users ability to measure and point out potential Phishing attacks when operating within a medium- or high-risk environment. Cybersecurity knowledge is an essential asset that cannot be ignored in the public sector, as more than enough Phishing threats continue evolving daily. Some of the other factors, such as cybersecurity knowledge, Internet usage, and cybersecurity-protective practices affecting employees' susceptibility to various phishing threats, are the presence of security practices rightfully exercised by the workforce [1].

3.7 Responsible Departments' Support

Any Saudi public sector that does not have qualified and competent departments responsible for InfoSec planning, training, supporting, and providing the incentives regarding the best employees in the training process is not achieving its security awareness' objectives whatever the level of awareness models it uses. Therefore, this is an important factor that needs to be considered when improving security by enhancing the employees' awareness regarding cybersecurity threats. Another crucial role that cannot be underestimated is linked to the notion of lifelong learning, turning most employees into the pioneers of technical competence and proper studies. The development of technology significantly affects IT security, so it may be reasonable to assume that the team should be well-versed in the current security issues to understand its needs to counter such attacks [34].
Therefore, the ongoing learning and research processes should become the key focus for the management, as complex security issues cannot be resolved without specific theoretical and practical experience. On the other hand, the team should pay closer attention to the communicators' role, meaning that the existing threats must be coordinated with effective correspondence [22]. Based on the above, several responsible departments can support the security training programs and add real (tangible and intangible) to these programs to enhance the Saudi public sector's awareness of cybersecurity threats and specific social engineering threats. However, a standalone role that has to be addressed before discussing the departments is the Chief Information Security Officer (CISO), responsible for top-level reporting and establishing the ultimate architecture for the organization's digital security [35]. In addition, another responsibility for the CISO would be to establish a vision for the organization's security and ensure that all employees follow and promote it by enhancing their knowledge regarding threats and InfoSec policies. Otherwise, any employees' awareness model is not able to succeed. The first department under review should be the senior management unit. Their responsibilities would revolve around managing different types of resources and orchestrating the organization's approach to digital security while serving as the IT evangelists at the same time and promoting cybersecurity values among less trained employees [13]. Their contribution to the ultimate success of cybersecurity initiatives would depend on the practical experience and the complexity of proposed security solutions.

Regarding the intranet and the internal links in the Saudi public sector, the last department under review is the senior security unit that copes with mid-level threats and tasks. According to [28], these specialists are responsible for unconventional threats and relevant technology. Their responsibilities might include (but never be limited to) antivirus software setup, vulnerability assessment and penetration testing, firewall setup, and expert knowledge in Linux-based operating systems. Another unit would include security program managers, whose skill set should also be at the level [36]. The previous note is important for tracking compliance and ensuring regulatory transitions regarding the awareness enhancement process; this unit should possess dedicated technical and human resource management skills to understand the dangers of social engineering attacks. The most basic department included in the discussion is security analysts. Their contribution has to be mentioned because their responsibilities often revolve around training other employees and coordinating most cybersecurity activities on a ground level [34].
These departments are important factors to achieve the awareness training strategy plans' objectives because they relate to how the network and all the data possessed by any given organization could be protected efficiently. They support all kinds of tech projects across the organization and escalate incidents while not requiring any specific knowledge in risk analysis or reporting. Therefore, each of the actors mentioned above plays an important role in enhancing the employees' awareness to counter social engineering threats and ensure that tools and the local network management incentives are effectively applied across the organization [22].

Considering all the required organizational units are trained

appropriately, one may conclude that every department within the bigger team might contribute to an environment with shared responsibilities and timely reporting. If the Saudi public sector expects to take cybersecurity seriously, most employees can empower each other to improve organizational culture to strengthen their workplace efforts [10]. Under the condition where all departments are involved in the prevention measures, it, therefore, be much easier to establish lucrative cybersecurity training sessions and appeal to employees without any false expectations. The departments mentioned above must be adopted in security awareness models because of constant security threats. This means attackers are never ceasing their attempts to find the best way to breach security systems irrespective of the target organizations' cybersecurity tactics [13].

In addition, the existing levels of responsibility and accountability have to be considered because most of the initiatives require specific skills and measures to be implemented. Essentially, security awareness models remain complex not because of the lack of organizational resources but because of the limitations instilled by attackers who are willing to remain at least one step forward [36].

In other words, every department plays its specific role to slow down the progression of hacking efforts and develop a different outlook on digital security among the least trained employees. Finally, there are several tasks that all departments can have to address together if they expect to enhance their employees' awareness regarding phishing from their cybersecurity plan.

3.8 Strategy Training Plans

The importance of training plans aiming to raise employee awareness regarding Phishing threats can be outlined as an opportunity to reduce the prevalence of threats while also building positive relationships with the team [13]. This ultimately shows that social engineering awareness training is statistically significant because it affects the institution's strategy (either short- or long-term) and reduces the team's overt exposure to the biggest threats. Irrespective of the approach, the company should remain dominant and show cybercriminals that access to vital data cannot be easily granted with tricks forming the method of phishing [37]. Accordingly, security awareness strategies cannot be overlooked because of their all-inclusive impact on the given organization.

Most businesses consider awareness training a top priority; therefore, it cannot be dismissed as insignificant. In other words, the importance of this concept may also be reinforced by the increasing power of manipulation that hackers attain when operating within a fully digital environment. Regardless of either, it comes down to a short- or long-term strategy, and awareness training should be expected to bring the organization to a new digital security level [15]. For instance, short-term strategies to improve awareness among employees can address the most common Phishing threats. Even if they are not as detailed as their long-term alternatives, they are most likely to provide employees with basic attack prevention and mediation [13]. The growing sophistication of attack instruments makes it safe to say that short-term strategies are irreplaceable because they establish the methodological basis for their more complex adherents. As far as conventional Phishing attacks are changing under the influence of digital progression, the strategies responsible for employee awareness to be improved as well, but only in the case where the management recurrently tailors their efforts to the ever-changing conditions set by attackers [37]. Short-term strategies cannot be overlooked because they would be perceived as the defense's frontlines intended to protect vital personal information.

Another reason why short-term strategy is so significant is the human factor that might lead individuals to unconsciously act and give up essential information to strangers without realizing it. In this case, a short-term strategy should be seen as an opportunity to help employees prevent an attack and respond to it reasonably without exposing anything crucial [28]. Therefore, the malicious efforts of Phishing attackers have to be addressed through the prism of short-term strategies only when there are no potentially dangerous long-term losses that could affect the organization. In turn, this affects the company's financial operations and decreases the number of random decisions that might have been made in the past [2]. Either way, organizations should apply short-term awareness training strategies to ensure that social engineering attacks become more evident to employees and have sufficient knowledge and experience to spot them and respond on time [15].

Dialog of long-term strategies included in awareness training; it may be safe to say that they must take a peek at the not so evident attacks. The main reason they have to be introduced is a specific popularization of teaching employees and reducing hackers' chances to exploit organizational data [37]. The growing impact of phishing has to be mitigated with long-term strategies because of attackers' inclination to launch mass data breaches and then sell the acquired information to the black market. The general pattern for most long-term strategies revolves around directing employees toward lifelong education and constant training [13]. Even though malware could be lacking power, human errors are never to be discounted, and long-term strategies require organizations to take care of the possible consequences without exposing the team to negative outcomes. After training more often, the team has developed a collective immunity and protects the company from long-term consequences. The proposed strategies could be beneficial if they teach and evaluate, as only one element of the equation is not enough to respond to social engineering's growing influence [2]. Trustworthiness check-ups become a viable organizational strategy segment only after the management realizes the value behind employee education in digital security. This ultimately creates premises for situations where workers become more skeptical but rarely miss cyberthreats or allow for data

breaches [34]. This directly impacts the success of long-term awareness strategies because employees also might get a chance to learn from each other along the way. Combined, short- and long-term awareness training strategies should be expected to cover the notion of digital security for the organization and prevent individuals from engaging in dangerous behaviors.

There should be no doubt about the importance of awareness training strategies because they might help enterprises of all sizes overcome the lack of IT support or the inability to gain in-depth insights into phishing. Even though most attacks reach an incredible level of sophistication, even a limited series of short-term training sessions might positively affect employee attitudes and practical knowledge use [28]. These strategies' value is proactive and decreases the visibility of protection mechanisms, allowing the team to manage its communication and develop additional cyber defence measures. As a result, the team would most likely convey information quicker and start perceiving digital threats more sensibly [13]. The key to using short- and long-term strategies is the willingness to minimize all kinds of damages and put protection software at the forefront while educating employees about it.

To sum it up, Phishing awareness training strategies cannot be ignored because they serve as some of the most evident examples of how practical knowledge protects corporate assets. Methods used to make these training sessions work are not essential because employee engagement is a much bigger variable for managerial consideration. Threats posed by phishing are nothing but a response to technological development and human error, so it may be safe to say that the core advantage of training strategies is the opportunity to find vulnerabilities within the network and neutralize them. The more information employees know about preventing Phishing attacks, the more chances to minimize the potential damage and engage workers in a prolonged learning process.

3.9 Employee Accountability

The importance of employee accountability regarding the provided security training to enhance the Saudi public sector's awareness regarding Phishing threats can be explained by a specific focus of companies on cybersecurity without paying much attention to employee behaviors. The rationale behind this topic is the growing role of InfoSec training recurrently mentioned in numerous public and private organizations [38]. Therefore, employees should be held accountable and committed because it is their task to access up-to-date information and have enough knowledge to withstand complex cyber threats. Given that mere awareness is not enough to cope with threats, employee accountability catalyzes further education and training [28]. No other positive transformation has been possible without the organization changing employee behaviors. As [39] stated, the right knowledge and skills shall be associated with achieving a higher level of accountability since many workers ignore the importance of cybersecurity and treat phishing as a trivial threat.

Nevertheless, all organizational stakeholders should be carefully promoted to remain accountable for protecting the network against social engineering attacks because a small group of individuals would not prevent serious attacks [40]. Furthermore, the role of human error is crucial, and it should be one of the most important tasks for the team to minimize the chances of a worker exposing certain information to attackers. Many organizations switch to digital instruments to reduce the risk, but human personnel's role should never be underestimated.

Employee accountability is important to ensure the provided security training programs' benefits mainly because workers must be encouraged to unlock performance achievements and acquire certain cybersecurity skills. This is a crucial task that depends on employees' personal and professional attitudes, so there is no way any given worker could give up on their accountability in the case of preventing or mitigating a social engineering attack [41].

The knowledge that employees pass down from one to another shall be considered a part of worker accountability. This concept's rationale is the growing rate of damages inflicted by an untrained workforce [38]. The inability to maintain a high level of accountability might lead employees to complicate cybersecurity and make it harder for the management to introduce awareness training programs due to the lack of responsiveness. As it was mentioned by [40], frequent security practices might make employees much more accustomed to responding to phishing, which is going to make the workforce way more accountable as a result. A safe network is a critical layer of cybersecurity that cannot be completed with mere technology, showing that awareness training and employee accountability are intertwined [28].

Cybersecurity's ever-changing nature poses the most threats for many organizations, causing them to give up on employee education and focus on technological advancements instead. The differences in the knowledge possessed by different employees should not serve as an obstacle because most training programs are set up to develop accountable behaviors irrespective of satisfaction, engagement, or experience.

The employees' commitment regarding the provided security tools and training programs is needed to ensure awareness enhancement. This particular premise is based on the idea that different educational materials and practical training might not be as effective as expected if employees are not interested in improving digital protection [41]. Given the objective of protecting the existing data assets and creating a safe digital environment, it may be safe to say that employee commitment is the biggest competitive advantage experienced by any company struggling with social engineering threats [39]. Over time, the workforce

may be expected to become much more flexible and start paying more attention to small details. However, a committed team would be less inclined to data breaches or leakages, as they could be more accountable than their untrained counterparts. Thus, the rightful management of available resources would develop into a multi-factor digital environment where every stakeholder is held accountable for their actions and realizes the importance of adhering to phishing policies [40]. Therefore, strict InfoSec requirements should not be discounted as one of the picks for improved resource management and awareness training.

When explaining why the plans described above are necessary to be adopted in security awareness models, it should be essential to link awareness training to the concept of accountability one more time. Cybersecurity education's effectiveness can be evaluated to measure the rate of successful Phishing attacks, which push employees to become more vigilant [38]. Cyber attacks' prevailing nature makes it safe to say that short- and long-term awareness training plans possess a series of inherent benefits that can only become visible after the implementation. Instead of finding employees responsible for a potential breach, the team should create a team with enough knowledge to dodge every Phishing attack and embrace mentorship [39]. Accordingly, this shows the essential difference between accountability and responsibility; as responsibilities can be shared, accountability is a unique burden for every employee. One possible reason for paying so much attention to the concept of accountability is the link between personal or professional liabilities and recognizing the moment where Phishing awareness can be of assistance. For instance, the team could develop a strong cybersecurity culture to train all the related employees and emphasize the importance of accountability with additional training activities [38]. In other words, the general workforce has to communicate, plan, and execute, while the top-tier management should be accountable for deploying the right tactics and all the on-the-fly changes introduced into the system.

3.10 Employee Satisfaction

To show the importance of employee satisfaction regarding the provided security training to enhance the Saudi public sector's awareness of cybersecurity threats and specific Phishing threats, it may be crucial to thoroughly assess how deeply security is embedded in the organizational culture. While there are numerous generic training classes for employees, they are not benefiting from them in the future unless they feel an inner satisfaction channelled through the process of interactions [33]. Therefore, it is most likely for employees to enjoy shorter training modules (see the discussion on short-term strategies from above), as they would be able to focus on one aspect of digital security at a time. This is an essential value that the management must nurture within the Saudi public sector to reach organizational objectives [42].

It may also be crucial to highlight engaging workers in feedback regarding employee satisfaction. Employee satisfaction shall also be closely associated with the concept of personalization of awareness training efforts. Different tips included in the training program should be seen as a starting point for improved employee education and an opportunity to drive employee attention to social engineering's crucial nature [43]. Personal and professional security also play an important part in developing one's digital personality, allowing the management to elicit employee satisfaction through the stronger link between monetary and behavioral remunerations. In other words, employee satisfaction within Phishing awareness training can be addressed as a dynamic concept contingent on withstanding breaches and responding to them effortlessly [44]. This is an essential concept for the Saudi public sector because it paves the way for more interactive and engaging training formats.

Employee satisfaction is important to meet the security objectives related to the security strategy plans, and it can also be an embedded value to security strategy plans because it significantly influences the engagement rate among workers. The so-called gamification of the process typical of many awareness initiatives is one of the key opportunities to help workers learn and increase their self-motivation [45]. The role of employee satisfaction within the framework of meeting security objectives may also be explained via the possibility of taking on the role of hackers and seeing the Phishing issue from a completely different perspective. The stakes in the public sector are very high when it comes to digital security, so it should be noted that every policy and procedure across the organization should respond to employee needs and aspirations [43]. In a sense, phishing awareness initiatives' overall success depends on the ultimate employee satisfaction because the absence of commitment and content would extinguish the company's long-term plans.

Another crucial element that cannot be ignored when discussing security objectives is the prevalence of testing procedures. Allowing employees to see real-life outcomes of their training is one of the best ways to achieve greater results and let them see the evident progress they have achieved with additional training [42]. Employee encouragement might be seen as one of the few drivers of worker performance and willingness to engage in training. This concept also brings the issue of rewarding employees to the forefront, showing that organizational penalties do not create a lucrative workplace environment and hinder employee engagement attempts [33]. The embedded value of employee satisfaction may also be defined with additional training intended to build stronger connections between employees and make the supervisor's life easier at the end of the day, allowing for a more detailed Phishing awareness education.

Another hypothesis that has to be validated here is that the quality and the usability of the training tools and programs can increase employee satisfaction. The main reason to consider it is that many workers merely do not have the

time and enough mental resources to keep track of various unique passwords, so they choose to go down the easiest route and reuse their personal information repeatedly [44]. Therefore, it has positively changed the organization by taking a proactive approach and implementing more awareness training sessions paired with technology investments. Instead of taking shortcuts, employees have reached different satisfaction levels while using digital instruments to complete the tasks recently done by hand [43]. This difference is an essential contributor to how the management perceives employee satisfaction and whether it has strengthened its security posture. Network vulnerabilities should not be seen as unexpected or incredible, as human errors are relatively common. Accordingly, specific training initiatives might affect employee satisfaction to an extent where they would personally engage in more activities and pay more attention to the team morale [42]. The team should use awareness training to reduce embarrassment and enhance employee satisfaction through a digital instruments' interface with a validated history of successful implementation.

Speaking of employee satisfaction, one might also mention the importance of improved productivity in raising awareness. Employees can better understand how to enrich data security, leave them more contented, and increase their productivity [33]. As a result, the overall costs of data breaches might be reduced, creating a financial cushion for the organization and paving the way for employee benefits. A potential data breach negatively influences the Saudi public sector, but social engineering awareness training and satisfied employees might go a long way together, helping organizations avoid threats and identify the best ways to respond to attacks. In this case, the significance of employee satisfaction may be explained through the lens of lifelong education that has to be paired with constant engagement and practical experience [45]. There are no perfect employees, but the human error could be significantly reduced with digital tools, awareness training, and initiatives to reach the highest possible employee satisfaction level. Table 1 summarizes the study's demographic and other factors.

Table 1: Demographic factors (personality variables) and other factors' references.

No.	Demographic variables/Other Factors	References
1	Age	[16, 17, 18, 19, 20, 21, 22]
2	Gender	[17, 19, 20, 21]
3	Education	[2, 16, 18, 19, 20, 21, 22, 23, 24, 25]
4	Internet Usage	[16, 21, 26, 27, 28]
5	Cybersecurity Knowledge	[4, 5, 16, 18, 19, 20, 21, 23, 24, 29, 30]
6	Cybersecurity-Protective Practices	[1, 6, 16, 18, 19, 20, 21, 23, 24, 31, 32, 33]
7	Responsible Departments' Support	[10, 13, 22, 28, 34, 35, 36]
8	Strategy Training Plans	[2, 13, 28, 34, 37]
9	Employee Accountability	[28, 38, 39, 40, 41]
10	Employee Satisfaction	[33, 42, 43, 44, 45]

5 Conclusion

The skills of phishing attackers have improved dramatically over the previous decade, allowing for more high-profile situations in which millions of passwords have been exposed. Due to the presence of the human aspect, IT giants have also been involved in identity theft instances, implying that IT behemoths are just as vulnerable to social engineering difficulties as their smaller counterparts. The nature of Phishing threats makes it more difficult for businesses to respond, as many businesses miss the benefits of developing training programmes and preventing future data breaches and identity thefts. This research looked at relevant studies to see what factors might influence employee awareness of social engineering threats. According to the literature, three demographic factors including age, gender, and education and seven other aspects including internet usage, cybersecurity knowledge, cybersecurity-protective practices, responsible departments' support, strategy training plans, employee accountability, and employee satisfaction. The reviewed factors could influence employee awareness of social engineering concerns. Further empirical work is needed to confirm the influence of these factors.

Reference

[1] A. Kumar, M. Chaudhary, and N. Kumar, "Social engineering threats and awareness: a survey," *Eur. J. Adv. Eng. Technol.*, **2(11)**, pp. 15-19, 2015.

[2] H. Aldawood and G. Skinner, "Educating and raising awareness on cyber security social engineering: A literature review," in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 2018, pp. 62-68.

[3] H. Wilcox and M. Bhattacharya, "Countering social engineering through social media: An enterprise security perspective," in *Computational Collective Intelligence*, Springer, 2015, pp. 54-64.

[4] W. R. Flores and M. Ekstedt, "Shaping intention to resist social engineering through transformational leadership, information security culture and awareness," *Comput. Secur.*, **59**, pp. 26-44, 2016.

[5] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in *2016 IEEE 4th international conference on future internet of things and cloud (FiCloud)*, 2016, pp. 145-149.

[6] H. Wilcox, M. Bhattacharya, and R. Islam, "Social engineering through social media: an investigation on enterprise security," in *International Conference on Applications and Techniques in Information Security*, 2014, pp. 243-255.

[7] W. D. Kearney and H. A. Kruger, "Considering the influence of human trust in practical social engineering exercises," in *2014 Information Security for South Africa*, 2014, pp. 1-6.

[8] M. K. N. Alotaibi, "Employees' interest in professional advancement on LinkedIn increases susceptibility to cyber-social engineering: An empirical test," in *International Symposium on Human Aspects of Information Security and Assurance*, 2020, pp. 85-96.

[9] R. Tromble and S. C. McGregor, "You break it, you buy it: The naiveté of social engineering in tech–and how to fix it," *Polit. Commun.*, **36(2)**, pp. 324-332, 2019.

[10] M. Edwards, R. Larson, B. Green, A. Rashid, and A. Baron, "Panning for gold: Automatically analysing online social engineering attack surfaces," *Comput. Secur.*, vol. 69, pp. 18-34, 2017.

[11] M. Silic and A. Back, "The dark side of social networking sites: Understanding phishing risks," *Comput. Human Behav.*, **60**, pp. 35-43, 2016.

[12] N. Shindarev, G. Bagretsov, M. Abramov, T. Tulupyeva, and A. Suvorova, "Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities," in *International Conference on Intelligent Information Technologies for Industry*, 2017, pp. 441-447.

[13] H. Aldawood and G. Skinner, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," *Futur. Internet*, **11(3)**, p. 73, 2019.

[14] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios," *Comput. Secur.*, **59**, pp. 186-209, 2016.

[15] T. Daengsi, P. Wuttidittachotti, P. Pornpongtechavanich, and N. Utakrit, "A Comparative Study of Cybersecurity Awareness on Phishing Among Employees from Different Departments in an Organization," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2021, pp. 102-106.

[16] A. Shargawi, *Understanding the Human Behavioural Factors behind Online Learners' Susceptibility to Phishing Attacks*. Lancaster University (United Kingdom), 2017.

[17] S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Human-centric Comput. Inf. Sci.*, **8(1)**, pp. 1-24, 2018.

[18] E. J. Williams, J. Hinds, and A. N. Joinson, "Exploring susceptibility to phishing in the workplace," *Int. J. Hum. Comput. Stud.*, **120**, pp. 1-13, 2018.

[19] M. S. bin Othman Mustafa, M. N. Kabir, F. Ernawan, and W. Jing, "An enhanced model for increasing awareness of vocational students against phishing attacks," in *2019 IEEE international conference on automatic control and intelligent systems (I2CACIS)*, 2019, pp. 10-14.

[20] S. Anawar, D. L. Kunasegaran, M. Z. Mas'ud, and N. A. Zakaria, "Analysis of phishing susceptibility in a workplace: a big-five personality perspectives," *J Eng Sci Technol*, **14(5)**, pp. 2865-2882, 2019.

[21] S. Back and R. T. Guerette, "Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks," *J. Contemp. Crim. Justice*, **37(3)**, pp. 427-451, 2021.

[22] M. Junger, L. Montoya, and F.-J. Overink, "Priming and warnings are not effective to prevent social engineering attacks," *Comput. Human Behav.*, **66**, pp. 75-87, 2017.

[23] R. Poepjes and M. Lane, "An information security awareness capability model (ISACM)," 2012.

[24] M. R. Endsley, "Situation awareness misconceptions and misunderstandings," *J. Cogn. Eng. Decis. Mak.*, **9(1)**, pp. 4-32, 2015.

[25] H. Heizmann and M. R. Olsson, "Power matters: the importance of Foucault's power/knowledge as a conceptual lens in KM research and practice," *J. Knowl. Manag.*, 2015.

[26] A. Algarni, Y. Xu, and T. Chan, "An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook," *Eur. J. Inf. Syst.*, **26(6)**, pp. 661-687, 2017.

[27] S. Mohammed and E. Apeh, "A model for social engineering awareness program for schools," in *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*,

2016, pp. 392-397.

[28] F. Salahdine and N. Kaabouch, "Social Engineering Attacks: A Survey. Future Internet", **11**, 89. 2019.

[29] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Advanced social engineering attacks," *J. Inf. Secur. Appl.*, **22**, pp. 113-122, 2015.

[30] S. Uebelacker and S. Quiel, "The social engineering personality framework," in *2014 Workshop on Socio-Technical Aspects in Security and Trust*, 2014, pp. 24-30.

[31] A. Suleimanov, M. Abramov, and A. Tulupyev, "Modelling of the social engineering attacks based on social graph of employees communications analysis," in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, 2018, pp. 801-805.

[32] I. Ghafir *et al.*, "Security threats to critical infrastructure: the human factor," *J. Supercomput.*, vol. **74(10)**, pp. 4986-5002, 2018.

[33] W. Fan, L. Kevin, and R. Rong, "Social engineering: IE based model of human weakness for attack and defense investigations," *IJ Comput. Netw. Inf. Secur.*, **9(1)**, pp. 1-11, 2017.

[34] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Comput. Secur.*, **73**, pp. 102-113, 2018.

[35] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, "The influence of a good relationship between the internal audit and information security functions on information security outcomes," *Accounting, Organ. Soc.*, **71**, pp. 15-29, 2018.

[36] K. Njenga, "Social media information security threats: Anthropomorphic emoji analysis on social engineering," in *IT Convergence and Security 2017*, Springer, 2018, pp. 185-192.

[37] A. Rege, T. Nguyen, and R. Bleiman, "A social engineering awareness and training workshop for STEM students and practitioners," in *2020 IEEE Integrated STEM Education Conference (ISEC)*, 2020, pp. 1-6.

[38] A. Caballero, "Security education, training, and awareness," in *Computer and information security handbook*, Elsevier, 2017, pp. 497-505.

[39] N. B. Kurland, "Accountability and the public benefit corporation," *Bus. Horiz.*, **60(4)**, pp. 519-528, 2017.

[40] M. J. A. Miranda, "Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach," *Int. Manag. Rev.*,**14(2)**, pp. 5-10, 2018.

[41] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Comput. Secur.*, **70**, pp. 663-674, 2017.

[42] I. G. P. Kawiana, L. K. C. Dewi, L. K. B. Martini, and I. B. R. Suardana, "The influence of organizational culture, employee satisfaction, personality, and organizational commitment towards employee performance," *Int. Res. J. Manag. IT Soc. Sci.*, **5(3)**, pp. 35-45, 2018.

[43] T. Bakhshi, "Social engineering: revisiting end-user awareness and susceptibility to classic attack vectors," in *2017 13th International Conference on Emerging Technologies (ICET)*, 2017, pp. 1-6.

[44] L. Khanal and S. R. Poudel, "Knowledge management, employee satisfaction and performance: Empirical evidence from Nepal," *Saudi J. Bus. Manag. Stud.*, **2(2)**, pp. 82-91, 2017.

[45] J. J. Li, M. A. Bonn, and B. H. Ye, "Hotel employee's artificial intelligence and robotics awareness and its impact on turnover intention: The moderating roles of perceived organizational support and competitive psychological climate," *Tour. Manag.*, vol. 73, pp. 172-181, 2019.