

Review

# Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues

Hussain Aldawood \* and Geoffrey Skinner \*

School of Electrical Engineering and Computing, University of Newcastle, Newcastle 2308, Australia

\* Correspondence: hussain.aldawood@uon.edu.au (H.A.); geoff.skinner@newcastle.edu.au (G.S.);

Tel.: +966-565115200 (H.A.)

Received: 7 February 2019; Accepted: 13 March 2019; Published: 18 March 2019



**Abstract:** The idea and perception of good cyber security protection remains at the forefront of many organizations' information and communication technology strategy and investment. However, delving deeper into the details of its implementation reveals that organizations' human capital cyber security knowledge bases are very low. In particular, the lack of social engineering awareness is a concern in the context of human cyber security risks. This study highlights pitfalls and ongoing issues that organizations encounter in the process of developing the human knowledge to protect from social engineering attacks. A detailed literature review is provided to support these arguments with analysis of contemporary approaches. The findings show that despite state-of-the-art cyber security preparations and trained personnel, hackers are still successful in their malicious acts of stealing sensitive information that is crucial to organizations. The factors influencing users' proficiency in threat detection and mitigation have been identified as business environmental, social, political, constitutional, organizational, economical, and personal. Challenges with respect to both traditional and modern tools have been analyzed to suggest the need for profiling at-risk employees (including new hires) and developing training programs at each level of the hierarchy to ensure that the hackers do not succeed.

**Keywords:** cyber security social engineering; training and awareness programs challenges; information security awareness programs

---

## 1. Introduction

Social engineering is defined as a method that seeks to exploit a weakness in human nature and take advantage of the naivety of the average person. Although the techniques of social engineering have evolved over time, the success of such attacks still depends on modern preventive tools and the security systems in place, as well as the availability of trained and skilled personnel dealing with sensitive data in organizations [1]. With innovative and interactive education, training, and awareness programs, corporations seek to prepare their staff with the most current prevention techniques to evade social engineering threats. The measures undertaken are comprised of training materials, policy and regulatory frameworks, and training on the safety measures to be taken before and after attacks. Besides regular training, organizations have the option to conduct timely information security awareness campaigns to stress the importance of maintaining constant vigilance [2].

As employees play the most important role in safeguarding the interest of organizations when it comes to socially engineered attacks, organizations choose to implement information security awareness programs to protect their data. [3,4]. There are some limitations posed in the process of implementing traditional training methods, including financial constraints [5,6]. There may also be

challenges in coordination among different teams in training and awareness programs, and there is a need to monitor the interdependences that may develop among teams during the phase of conducting awareness programs. In addition, the creative skills of hackers to engineer new threats to deceive the human element into revealing crucial information should also be taken in consideration [7–10].

In the last decade, a number of high-profile web services have been compromised. Such social engineering based attacks have resulted in millions of leaked passwords [4,10–12]. Some recent victims include Yahoo, Dropbox, Last.fm, LinkedIn, Weebly, and MySpace [13]. Table 1 lists some details about recent breaches that happened within the last ten years on high usage web services. Additionally, those compromised passwords have been posted (or sold) online months (sometimes years) after they were stolen from those web services, further heightening the impact of social engineering attacks [13].

Considering the fact that social engineering threats are dynamic and constantly evolving, developing mitigation tools should be an ongoing measure. Hence, there is no “perfect” security system against social engineering threats that organizations are subjected to, but training the human element to counter such attacks is essential. As a result, small and large organizations increasingly choose training and awareness programs in addition to developing technical tools to contain the possible damages caused by cyber-attacks [14]. It is imperative to recognize the challenges that organizations may face in the process of implementing training and awareness programs that aim to increase the consciousness level of computer users. This study highlights the challenges faced by an organization using both traditional and modern training and awareness programs as countermeasures.

**Table 1.** Compromised passwords attacks.

| Target  | Attack Date   | Passwords Revealed on | No. of Passwords Compromised |
|---------|---------------|-----------------------|------------------------------|
| Yahoo   | 2013          | October 2017          | 3 billion [15]               |
| Weebly  | February 2016 | October 2016          | 43 million [16]              |
| Dropbox | 2012          | May 2016              | 68 million [17]              |
| Myspace | 2008          | May 2016              | 360 million [18]             |

Most recent catastrophic password breaches revealed months after the actual breach.

## 2. Methodology

For an analysis of challenges faced by companies in training and awareness programs against social engineering, this study utilizes the qualitative method of research. Qualitative research is exploratory in nature and is used to broaden the knowledge of underlying reasons contributing to the phenomenon in the study. An exploratory method of research allows flexibility in research and seeks to establish the boundaries of problems. Using this method helps in overcoming challenges associated with implementing information security training and awareness programs against social engineering deceiving techniques [19].

Qualitative research in this study is based on a secondary analysis of literature. This type of analysis adds strength to the knowledge of the subject [20]. Additionally, as this study reviews traditional as well as recent developments in the field of increasing training and awareness strategies against social engineering, qualitative analysis of literature allows an in-depth analysis of findings of original primary studies. This approach allows a careful analysis of observational records, field notes, and interview transcripts to broaden the understanding in the field [21].

## 3. Challenges of Trying to Keep a Step Ahead

### 3.1. Considerations with Social Engineering Training and Awareness Programs

The efficiency of organizational information systems in countering social engineering threats necessitates the combination of advanced technical measures along with managerial efforts to raise awareness of personnel. One of the most important measures is to provide the right training to employees so that they develop the ability to recognize, flag, evade, and disable malicious attempts of

an attack. However, the road to providing training and awareness programs is fraught with challenges arising from many factors. The factors can be broadly classified as follows.

### 3.1.1. Business Environmental

Business environmental factors include interactive work locations of an employee within a firm as well as outside areas. Environmental changes affecting training and awareness programs provided to employees are comprised of factors such as prevailing technology, organizational culture, employee education, policy, and amendments to physical security controls [22]. Staff could be targeted via email that can be accessed remotely by an outside network. Damages can then take place in organizational digital devices and networks that are accessed remotely. The impacts of remote access have been increasing with the integration of internet in each aspect of a business [23]. Wilcox, Bhattacharya, and Islam [24] highlight that there is an increasing correlation between social engineering and the usage of social media websites such as Twitter, Snapchat, Facebook, etc. Today, business functions such as finance information systems and supply chain information systems are integrated into a combined information system, which increases the vulnerability of an organization. Moreover, social engineering attacks are dynamic and evolving in nature, and with the increasing integration and dependence of working through information technology, a complete isolation of employees from being attacked is very challenging. Studies suggest that the best solution to fight against social engineering threats today is to develop employees' knowledge about common methods of socially engineered attacks [25].

### 3.1.2. Social

The limitation to prevent socially engineered attacks through training and awareness programs occurs in the process of social communication. On one side, the competition in industry requires a social bond with customers to stay market relevant. On the other side, it may give rise to informal communication. Such informal communication and social bonding could cause a breach in terms of security measures fabricated by staff through training and awareness programs [26]. Social factors leading to challenges in training and awareness programs to counter social engineering include the influence of cultures. According to some cultures that embrace community feeling, interactions are part of work life as well. The trait is carried over by employees into the workplace, making them vulnerable to hacking through the social engineering process [27].

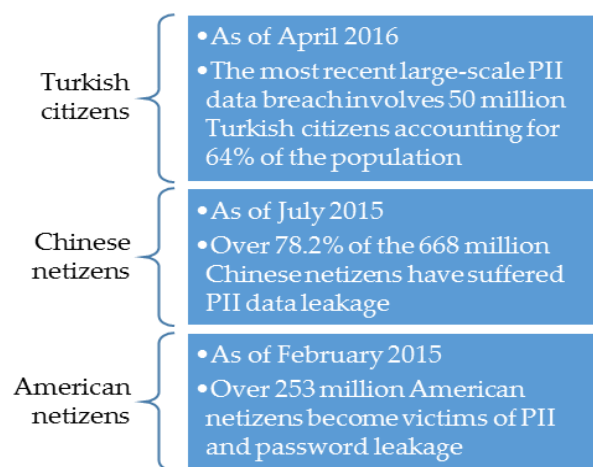
To the best of our knowledge, there is no comparative study indicating the influence of cultural or social factors in limiting the impact of training and awareness programs in literature. However, the findings of a study comparison by Alseadoon [28] highlight that there is only 7% of reported phishing email experiments in Saudi Arabia. The response rate is found to be much higher than reported by various studies across the western countries that report only 3–11% [29–31]. Even though there is a lack of strong relationship between training and awareness programs' effectiveness and social factors, the social factor can be an important one in recording the demographic influence while designing a uniform training method for every employee in an organization.

### 3.1.3. Constitutional

The governmental impact on training and awareness program discourse is very limited in literature. The choices on which the political debates take place are largely to increase security against socially engineered attacks. Furthermore, manipulation based on governmental agendas in the form of spreading misinformation is a common method used by social engineers. Hackers leverage the confirmation prejudice and exploit intellectual dissonance to target like-minded groups and influence specific groups of people to outdo training and awareness programs of personnel [32]. Moreover, Costa and Figueira [33] suggest that governments should legislate more security laws and take actions on organizations to force them to enhance their training and awareness programs against social engineering threats. It is very important to ensure that all staff is in compliance with the various

legal policies to confirm that no security law is broken [34]. The conditions may even lead to trainers reworking educational materials to ensure that the methods of training are constitutionally approved.

Hackers and/or social engineering attack procedures use several up to date methods to obtain personal information, including passwords. Five common contemporary attacks include phishing, baiting, quid pro quo, pretexting, and piggybacking [35,36]. Online guessing is one of these methods, which can be launched against the publicly facing server by anyone using a browser at anytime [37]. This online guessing technique has raised a serious security concern to many governments and organizations as various personally identifiable information (PII) and leaked passwords become readily available. Furthermore, targeted online guessing can exploit not only weak common passwords but also passwords reused across sites and passwords containing personal information [37]. Figure 1 displays some data about PII-based breaches among three nations, Turkey, China, and the USA.



**Figure 1.** Personally identifiable information (PII)-based breaches among three nations [38–40].

### 3.1.4. Organizational

The internal environment of an organization is comprised of the firm-specific limitations to the extent that training and awareness programs will be helpful in controlling socially engineered attacks within the enterprise. The limitation arises from the lack of variety of designed awareness programs targeting specific groups of staff with different levels of awareness [41]. The security training should vary according to the needs of the business, market pressures, business modernization, prerequisites, and budget available to the firm. The dynamic methods that the cybercriminals use to obtain information are continuously updating [26,42]. Unfortunately, once cybercriminals are aware of the preventive measures taken by a targeted firm, they develop and use new techniques that staff is unfamiliar with [43].

### 3.1.5. Economical

Training and awareness programs among employees can be greatly enhanced through interactive content [44]. Jemal [44] indicates that the medium through which awareness material is provided plays a significant role in the overall impact of such training. However, providing cost-effective training with each evolving attack poses a challenge for organizations. Furthermore, to stay relevant with evolving socially engineered threats, an organization has to actively test the readiness of its employees. This process involves evaluating employees on the basis of their readiness and assessing their resilience and ability to follow security contingency plans [45]. Even if the tests are conducted in-house by an IT or security department, it would require funds to be diverted from other divisions of the organization to the training and awareness programs. Briefly, if the required economical resources for training personnel cannot be allocated periodically, business continuity would be at high risk [46,47].

### 3.1.6. Personal

Personality traits are the inherent characteristics of an individual that may pose a threat to training and awareness programs' effectiveness against socially engineered attacks. Social engineers selectively choose their method of attack based on the personality of the targeted employee [48]. Hackers use different psychological methods to specifically recognize the behavioral vulnerabilities of victims. The study by Luo et al. [49] indicates that hackers may even use the technique of moral obligatory guilt to ensure that people act upon the bait. Additionally, the differences in personality of staff even influence the form of reaction that an employee may have to the attempt of social engineering exploits [50]. Reference [51] highlights neuroticism, which is the affinity to experience intimidating emotions easily, such as anxiety, anger, vulnerability, or depression, as being highly correlated to chances of responding to phishing emails. Further, employees who are extroverts and seek excitement are also assertive and may give out information easily. Lastly, openness as a personality trait means that employees are ready to try new things, leaving personal information and digital footprints for hackers to work their way through into their organizations [26,28,52].

The trusting nature of human beings can also be a huge challenge to awareness programs against social engineering threats. Physical and data security of individuals and organizations needs to be taken more seriously by individuals in an organization [48–50]. Because of the amount of trust individuals have in their organizations' IT infrastructures, employees do not consider security as a threat. Organizations need to include training materials to cover the trust gaps that individuals usually have by nature [51]. The trust challenge of staff can be prevented through effective and comprehensive information security training and awareness programs. However, in some cases, organizations provide limited resources to train their staff to cover the minimum harms that can be caused by social engineering attacks [50]. The concept of not needing more security training has become a major factor that challenges effective safety against social engineering threats. As a result, there is a lack of awareness among professionals to cover the trust gap that can be minimized by more awareness campaigns. This gap can create a great opportunity for social engineers to target them easily.

Another factor that poses a challenge for training and awareness programs against social engineering is the lack of interest found in personnel in general. Individuals often lack personal motivation to be trained on a regular basis to protect themselves and their organizations [52]. The concept of security awareness has most often fallen on deaf ears despite the common occurrence of individuals being attacked for information and data relating to their personal and professional roles. This lack of interest has also been reflected in literature such as Hadnagy [53], who shows that user education relating to security awareness is pointless, as individuals do not show enough interest. Hadnagy also highlights that this lack of interest can be seen as end-users do not think security is their concern. Rather, employees think that security personnel should be in charge and responsible for taking care of any security threat that their organization might face. As a result, lack of interest of individuals relating to social engineering threats becomes a very important factor that challenges effective training and awareness of staff [54].

Different personal capabilities of understanding the types of malicious intent of social engineering attacks creates another big challenge in awareness programs [55]. In the past, the approaches of social engineering techniques were more straightforward than they are today. They used to be poorly veiled, which provided individuals understanding of the nature of such attacks. However, the increased sophistication and complexity of social engineering methods makes it harder for victims to recognize them [56]. In brief, the developments of manipulation tactics might leave individuals unaware of the new methods of social engineering attacks even if they attend awareness programs.

Social engineers often elect to target employees holding a low profile role, which is not as strategic for big organizations. Social engineers start collecting data from the lower personnel level about work activities to gather as much sensitive data as possible before planning to attack the whole firm [51]. Lack of awareness of the seriousness of such attacks, along with the fact that staff may not consider themselves very important in large corporations, make employees very vulnerable [57]. This lack of



self-importance creates a challenge for awareness programs. Covering this lack of self-importance can be included in awareness programs. Employees need to feel the citizenship of themselves to their organizations and feel invested in the safety of the organization.

The last personal challenge is that individuals sometimes face huge work pressures in their professional roles and have limited work-life balance as a result. Several organizations have set strong security policies to force all employees to complete a required security training to increase their knowledge about social engineering threats. When training and awareness programs are conducted, employees attempt to get the required training done in their work hours. However, work pressure can cause a weakness in this matter, as some staff face serious deadlines that challenge the concept of work-life balance [58]. This work pressure leads to a lack of attention from trainees during training and leaves them with a sense of uncaring attitude towards the sessions of the awareness programs [48]. This uncaring attitude creates a challenge for those training sessions to effectively develop the knowledge base of employees for increasing their awareness towards the ever-evolving methods of various social engineering attacks.

One of the most common ways to gain access to information systems and sensitive data is not through forced entry or through electronic theft but through the manipulation of individuals and human intellect. Social engineering is a way of getting unauthorized access to sensitive and confidential information, as it relies on psychological manipulation of individuals. As a result, those individuals reveal such information or provide an access to restricted areas without noticing that they are doing something wrong. They become victims to social engineering and end up doing something illegal as their human nature is being taken advantage of [48].

### *3.2. Review of Challenges Associated with Modern Social Engineering Training and Awareness Programs*

Training and awareness programs have been in development as the threats of social engineering attacks are increasing. Security training and information security awareness programs include techniques of simulations, serious games, virtual labs, and themed awareness videos and modules [59]. However, these modern training techniques have their own limitations in enhancing employee preparedness. Several studies [8,9,60] recommend introducing serious card games as a relevant tool for increasing one's conscious level against social engineering attacks. The card games method, however, presents a challenge of coordination among teams of trainees. A collaborative approach is followed for these types of games during learning phases. It helps to improve the decision-making skills of an employee when targeted with real attacks. However, the differences of personalities in perceiving and adopting learning materials among teams can pose a challenge [9,61].

Recent training methods involving interactive games and virtual labs run into the problem of coordination. As a game involves different steps in both the identification and mitigation of attacks, it is challenging to incorporate everyone in the correct order. It is difficult to control the exposure of an employee to the hacker and to control the spread of possible damage in the organization's information system. The limitation of coordination arises, as it is difficult to determine who should be involved in the security effort. It is also difficult to determine whether there is a correct order in which different teams should do their own specialized work [6].

Recent methods of awareness training such as themed videos and awareness modules are creative approaches. Although awareness modules may be designed to encompass all security measures, there might not be just one single solution. This is because uncertainties in a socially engineered attack are beyond the prediction abilities of the designers of training and awareness programs [61]. Moreover, social engineers are specialized in creating an exceptional need for employees to act upon bait, exploiting the fear of missing out and reverse psychology that awareness programs might be unable to contain [62–64].

Modern training methods, including real-life simulation scenarios, aim to provide awareness of social engineering and how the social engineers actually may operate an attack [58]. Modern training methods use those simulations to help employees think strategically about whether the message is a

social engineering attack or not. However, these simulations are prepared similarly for all employees and do not cater to the understanding of each employee individually [65]. The process of finishing the simulation sessions does not consider how an individual might perceive the message. Different employees may have different reactions to each scenario because each individual has different instincts, different levels of trusting character, and different levels of awareness towards the potential of being tricked or scammed. These different behavioral aspects pose a challenge in effectively discussing how to avoid an attack, as perception of each individual plays a role. Furthermore, because the majority of training sessions are generalized, they might result in a lack of understanding of multi-faceted social engineering attacks and ultimately not meet the objective of the overall goal of implementing such awareness programs [66].

Another challenge that modern techniques of training have is that they are time consuming. Simulations, videos, and interactive games require employees to set aside their normal professional tasks to be able to complete the required training sessions. This extra time for training limits their productivity at work, which might affect employees meeting their work deadlines [49]. If workshops are held outside of working hours, it can create an interference, as staff may or may not attend due to the disruption to work-life balance.

Modern training methods for social engineering attacks are mostly developed by IT professionals. This can create a challenge due to the lack of technical knowledge of the majority of the staff in non-IT organizations [67]. Having a simple design will help trainees focus on the content of the training session rather than try to understand how to work with the modern training method. End-users will appreciate the simplicity of the final design of an interface of these modern training tools. In brief, the simplicity of the designs of modern training methods is important in achieving the overall awareness of staff and ultimately safeguarding the organization's information systems.

### *3.3. Review of Challenges Associated with Traditional Social Engineering Training and Awareness Programs*

Traditional training and awareness programs are mainly used by firms to keep employees updated against socially engineered attacks. Such informative programs include onsite training and awareness camps, screensavers, posters, manual reminders, and online courses [5,68]. Ghafir et al. [69] indicate that shortage of training budgets of firms may pose a challenge to training and awareness camps and other on-site learning methods. This type of challenge is mainly caused by the downward movement of economies, which encourages companies to minimize training budgets. This also opens up the opportunity for social engineering based hackers to devise new techniques to sabotage the outdated systems of the firm. One must also consider the fact that social engineering attacks are not limited to targeting staff electronically. Physical access threats, including dumpster diving, can lead to major damages if organizations stop educating their own employees. Incorporating training and awareness methods for all staff—from high-profile managers to cleaning janitors—poses a challenge, as training material to suit different needs relies on the learning ability of individuals [6,34].

Traditional training methods have generally been assessed as boring and tedious, limiting their success. Information security training sessions against social engineering threats sometimes do not focus on the main objective of making staff remember the major manipulation techniques of hackers. Instead, they tend to be very generalized and done in completely formal settings, creating a serious environment that may produce negative results in the final outcome. This type of training environment makes it easy for staff to forget about the important security information they gain during these sessions [20]. Training sessions need to have some fun activities to help employees interact with the customized training materials.

Traditional training methods of social engineering often lack practical exposure for employees [68]. These types of methods do not expose employees to real life scenarios as the ones available in modern training methods do. Employees are introduced by traditional methods to basic knowledge of what the attack is about, but when faced with the real attack itself, they may fail to recognize it easily. Moreover, traditional training methods including printing posters, warnings of social engineering attacks on

screensavers and desktop, and posting critical consequences of leaking sensitive information carry very basic and general information. These traditional methods alone do not create sufficient safe culture among staff [44].

Another challenge that traditional training methods face is that they are not able to address the full critical evaluation of trust. The main weapon used by social engineering attackers is to gain trust of their victims to share sensitive information or help them achieve their goal [48]. Social engineering attackers may become familiar with the employee's personality at first and then carry out an attack at a later stage. This natural trust issue may not alert the employee at an early stage that there is an act of social engineering taking place. Traditional training methods also overlook the behavioral aspect of individuals, which varies from one person to another. One employee may not perceive the attack the same way as another employee, and the resultant behavior might be different [65]. A traditional training session could guide employees to recognize some classic attacks at some point but might not be able to fully demonstrate how to handle such an occurrence. This issue itself poses problems to individuals who are faced with real situations.

Social engineering is innovative in nature, and new methods are being devised to sabotage organizations each day. Technological advancements in designing awareness programs might replace the existing traditional training methods, including manual reminders, posters, and screensavers, as they become outdated. In addition, the uncertainty in the mode of attacks poses a challenge to the traditional approaches of containing socially engineered threats. Caputo et al. [70] highlighted that even though traditional training methods are implemented, employees still react negatively to phishing emails. Regardless of the amount of hours spent on training, employees have the curious nature to check all links in an email. This is why an advanced learning method that includes the option of simulation would work better in the process of developing the knowledge base of an employee.

Another challenge in traditional awareness programs is a lack of attention paid to training sessions or not reading the entire learning module. In addition, high cognitive work load along with work pressure and stress could distract staff from reacting positively against social engineering attacks [25,71]. The subjective mental workload creates memory deficit that leads to the inability of employees to distinguish between real and fake messages. Additionally, Halevi [72] argues that human decisions in general are not entirely logical and can have an emotional bias that tends to influence their reasoning and judgment against serious threats. These cases may include ignorance of employees to a threat, overestimating the security systems of their organizations, or even underestimating the abilities of attackers [25].

#### *3.4. Impacts of Challenges on the Security of Organizations*

Today, most organizations mainly rely on the use of information technology, which obligates them to commit to protect the confidentiality of their consumers [73]. The challenges pose threats to the integrity of enterprises as well as the availability of information data at all times. The misuse of information could cause direct negative impacts on an organization's business continuity [74,75]. If these limitations are not taken into consideration by decision makers to implement the latest training and awareness programs, organizations can suffer from major damages to their information assets. Some of these damages include data leakage, loss of customer confidence, loss of intellectual properties, and denial of information systems services [24,76,77].

The main goal of conducting information security training and awareness programs is to complement the security technical measures, tools, and policies in place to enhance the overall safety of sensitive data. Providing the necessary security awareness programs to staff enhances the overall security to tackle social engineering and other cyber security threats [58]. The reviewed challenges in this study may help organizations avoid such negative impacts on their security. The impacts of these challenges can be either short term or long term. If challenges are not addressed, short term impacts can include wasting the time and efforts of trainers and trainees, resulting in losing the allocated



budget for these training sessions if the overall goal of these programs is not met. Long term impacts may include increased vulnerability of the organization in facing social engineering based attacks [66].

One of the greatest impacts that an organization has due to the challenges faced when conducting effective training and awareness programs is the threat of security of data, personnel, and its social and technological infrastructure [44]. The many types of sensitive data that can be impacted include business plans and procedures, financial data, employees' private information, salary details, and many others. Even though confidential data are usually stored in secured technical servers, social engineers can still take advantage of the impacts of those challenges if not taken into consideration.

The lack of effective training and awareness programs impacts the chances of creating a safe culture among staff. In general, non-IT employees are not suspicious of social engineering attacks, especially when social engineers offer them some help in adjusting their work access or resetting their passwords. Another way a social engineer approaches staff is by offering some rewards or giving a hope of a great opportunity [78]. The lack of awareness of recognizing such a trick may result in a successful breach. The impact can then cause the enterprise a huge cost of recovery if the breach is successful.

The challenges of training and awareness programs also cause an organization to become more vulnerable to social engineering blackmailing. Having unaware employees that have limited information security knowledge can widen the gap for easy social engineering attacks [79]. If staff does not have updated information about the latest fraud techniques in social engineering, they might provide an open road for attackers to get access to the organizational information systems. If social engineers are able to get access through unaware staff, companies might suffer from the recently developed ransomware attacks. Once attackers freeze an organizational workstation or information system, a negotiation process may fail and result in destruction of important data [60]. In brief, ignoring the challenges of training and awareness programs against social engineering attacks may result in being a victim. Well-delivered security training is considered the first line of defense against social engineering attacks [44].

Additionally, the impacts of not getting the required safety training against social engineering techniques of deceiving and misleading individuals may lead to reputational damage to enterprises. Reputation of an organization is crucial for effective relationships with other businesses and customers. Loss of reputation has serious detrimental effects in the performance of the organization and also in retaining employees [66]. If the reputation of an organization is compromised, the overall trust of that firm could be affected as well [80]. In brief, employees' unsafe behaviors as a result of lack of awareness may cause massive consequences and harm to both the users themselves and to the overall reputation of their organizations [81].

#### **4. Strategies for Addressing Social Engineering Education and Awareness Challenges**

One of the major and leading challenges faced by enterprises in providing training and awareness programs against social engineering is the lack of a training budget. The challenge further increases as a result of global economic strikes. In today's competitive economy, many businesses attempt to minimize their expenditures, especially when it comes to costs that are not part of their operation cost. Unfortunately, many organizations do not prioritize training budgets as they should [44,69]. Considering the fact that not all employees have the same level of awareness, training costs could be reduced by many strategies. One strategy to overcoming financial constraints related to training costs is to start testing employees for an understanding of their current vulnerabilities. An assessment test by specialized training officers or phishing email tests can help identify the current level of awareness. Once an employee's specific vulnerability is recognized, organizations can then focus on creating a purpose-focused session to target those who are identified as high risk to the organization. These sessions should be designed specifically for vulnerable users. Alternatively, employees who are less prone to fall for social engineering attempts are then provided with a more specific awareness program,

which is shorter in duration. This method can help in reducing the cost of training and awareness programs in comparison to offering the same sessions for all employees.

Providing all employees with similar training and awareness programs poses additional limitations. Most enterprises still adopt traditional methods of keeping employees aware through the usage of screen savers and posters [5]. However, such common methods may reduce the effectiveness across different organizational hierarchies. Generally speaking, executives are exposed to different types of data hacks with a more sophisticated approach than general employees performing general roles. For example, general employees such as a person in charge of garbage disposal need to be taught about the prevention techniques of avoiding dumpster diving risks of information gathering used by social engineers [6,34]. Penetration testing can be a very helpful strategy to overcoming this type of challenge. It is one of the methods that corporates can adapt to simulate actions of a real attack trying to steal sensitive data [82]. Similarly, the same tools and methods of prevention cannot be applied to managers and board members of an organization, as they are more likely to be targeted with phishing calls. Employers can focus on designing role-specific interventions for identified weak points at each level of hierarchy. To strengthen the outcomes of penetration testing, training and awareness programs need to be effective and up-to-date. Efficiency comes from outlining preventive actions required from employees and helping them frame a preventive attitude by broadening the comprehensibility of why the topic is important [83].

Because social engineering is related to the human capabilities, behavioral limitations of employees pose a challenge to the effectiveness of training and awareness programs. Among all employees, specific behavioral limitations include biases, cultural influence, and cognitive favoritism [27,58,84]. Previous studies [62–64] highlight behavioral limitations among the major causes that increase the chances of socially engineered attacks in organizations. Foremost, noncompliant behaviors observed among employees in the process of training and awareness programs are considered to be one of the challenges that needs to be overcome to create a safe culture. In the case of information security leakage, costs of containment for firms can be a lot higher than if training was considered in the first place. To counter such behavioral limitations and biases, organizations need to establish clear security guidelines and educate all staff about them. One of the key strategies to countering such challenges in training and awareness programs is that employees should learn to avoid overestimating their capabilities to mitigate security risks. Instead, employees should be taught through awareness programs that they could use their security knowledge to yield a positive comprehensive result in the overall security. Awareness campaigns for employees should supersede the individual bias and eliminate thoughts that such attacks “will not happen to me” [70,85–87].

Coordination among team members poses a challenge in the process of training and awareness programs. As social engineering attacks are dynamic and evolving, organizations aim to contain hacking threats using modern training methods. These methods include serious games, virtual labs, and themed awareness videos and modules [59]. Nevertheless, the presence of specialized information security training coordinators who are knowledgeable about recent methods is essential as a preventive measure to mitigate vulnerabilities caused by a lack of security awareness. Training coordinators and instructors should emphasize the importance of design flow diagrams of threat containment to specifically inform all employees regarding who handles what aspect of threat control [9]. Strategies for containing socially engineered threats include the conduction of preparedness exercises based on collaborative incidental response processes. It is very important to map a detailed description of interdependency between different organizational teams. They should specifically include all required activities in sequence for facilitating firm-based training and awareness programs. Briefly, training and awareness programs enhance the development of the capabilities of staff that are expected to see a broader picture towards containing organizational vulnerabilities [31,33,34]. Lastly, to better enhance coordination in handling dynamic socially engineered attacks, training coordinators and instructors need to stay updated and regularly attend the latest conferences to better know how to develop in-house training.

Countering social engineering through new training techniques including simulations faces a challenge of interdependence. Some training exercises specify roles that each member has to perform in coordination as a team to control security risks arising from socially engineered attacks. However, these shared tasks may create interdependencies for certain employees that limit their performances while working alone. In such situations, when employees are trained to work interdependently, they will not know the next responsibility to perform for containment of socially engineered threats, leaving their organization exposed. Interdependency creates loopholes and open doors for social engineers [7,45,88]. Moreover, previous studies [9,89] indicate that social engineers take advantage of interdependencies by synchronizing such activities and sharing resources. Social engineers create a special network that generates a larger scale attack able to impact an entire organization. The trick behind this is to enter into an information system by phishing single employees. Strategies to counter interdependencies could include training and awareness programs that are specifically designed to enhance user-specific engagement and motivate employees to take automatic prediction towards the next step in containing socially engineered attacks. The strategic measure could also include Tabletop exercises that use simulated real-life roles and involve all employees and managers to better contain a possible threat. Tabletop exercises are both online and paper-based and are constructed for identifying involved agents and the correct flow of decision quality. The exercise involves employees getting comfortable with their organization's incident response plan. Simulation of role recognition in a firm's security plan helps in identifying security gaps. These gaps, when addressed by organizations, help improve communication between security stakeholders in firms and help them learn new ways to execute security plans as well.

Another challenge faced by firms is under-preparation for innovative approaches of socially engineered hacking attacks. Even with the latest training and awareness program tools, employees can have vulnerabilities, such as fear of being a victim. Hackers may use reverse psychology to ensure that their chosen targets take the bait [62–64]. The strategies of training should include directions for employees to avoid underestimating hackers' capabilities. Socially engineered attacks rely on such vulnerabilities as socio-emotional perspectives and trust dimensions. Engagement with hackers leaves organizations exposed to more threats. Strategies to counter under-preparation among employees include training and awareness programs involving real case scenarios and case studies. These scenarios can enhance the knowledge base of weaknesses that hackers might prey upon. In brief, implementing training and awareness programs is a crucial step towards having a secure cyber environment in which users of all ages can freely use technology to conduct positive and self-developing activities. It is considered the most effective way to deal with social engineering threats as technology development has made humans potential targets of hackers and cyber criminals [4,6,10–12,44,90–92].

## 5. Conclusions

This study examines factors that may contribute to overcoming the challenges posed from implementing training and awareness programs against social engineering. Today, business functions such as finance and supply chains merge into larger information systems. The integration of information systems increases the vulnerability of an organization. Staff social media access using such interconnected information systems can lead to increased threats of attack by malicious social engineers. Additionally, if the level of information security awareness on the latest techniques used by social engineers is not well maintained, organizations increase their risk of attack. Because social engineering attacks are designed to evolve with both changing technologies and security measures, more categorized training is needed to develop and evolve the knowledge base against such threats.

The main objective of information security training and awareness programs is to enable employees to develop skills in identifying, disabling, and reporting any social engineering malicious attempts. One of the primary challenges faced by enterprises in providing training and awareness programs is the lack of training budgets, especially during global economic strikes. This paper lists

some working strategies to reduce the cost of training. Undesirable behavior of an employee or the lack of understanding of information security and organizational security culture counts as confidential vulnerability. This study further recommends strategies for addressing challenges from the point of view of security decision makers in organizations. Some recommendations are presented in this paper, suggesting the conduction of preparedness exercises based on collaborative incidental responses. Enhancing information security training and awareness programs can help organizations achieve better results against social engineering techniques.

**Author Contributions:** Conceptualization, H.A. and G.S.; Methodology, H.A.; Formal Analysis, H.A.; Investigation, H.A.; Resources, H.A.; Writing-Original Draft Preparation, H.A.; Writing-Review & Editing, H.A. and G.S.; Visualization, H.A.; Supervision, G.S.; Project Administration, G.S.; Funding Acquisition, H.A.

**Funding:** This research received no external funding.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

- Smith, A.; Papadaki, M.; Furnell, S.M. Improving awareness of social engineering attacks. In *IFIP Advances in Information and Communication Technology*; Springer: Berlin, Germany, 2013; Volume 406, pp. 249–256.
- Sallai, G. *Social Engineering Audit and Security Awareness Programme*; KPMG: Amstelveen, The Netherlands, 2016.
- Gollan, N.; Carew, N. Why Companies Are Exposed to Social Engineering. Available online: <https://www.senseofsecurity.com.au/pdfs/Sense-of-Security-Whitepaper-Why-Companies-are-Exposed-to-Social%20Engineering-V1.0-09OCT2012.pdf> (accessed on 15 March 2019).
- Aldawood, H.; Skinner, G. A Critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications. In Proceedings of the IEEE 26th International Conference on Systems Engineering, Sydney, Australia, 18–20 December 2018.
- Zulkurnain, A.U.; Hamidy, A.K.B.; Husain, A.B.; Chizari, H. Social engineering attack mitigation. *Int. J. Math. Comput. Sci.* **2015**, *1*, 188–198.
- Kumar, A.; Chaudhary, M.; Kumar, N. Social engineering threats and awareness: A survey. *Eur. J. Adv. Eng. Technol.* **2015**, *2*, 15–19.
- Castellano, G.; Leite, I.; Pereira, A.; Martinho, C.; Paiva, A.; McOwan, P.W. Detecting engagement in hri: An exploration of social and task-based context. In Proceedings of the 2012 International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2012 International Conference on Social Computing (SocialCom), Amsterdam, The Netherlands, 3–5 September 2012; pp. 421–428.
- Shostack, A. *Threat Modeling: Designing for Security*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
- Beckers, K.; Pape, S. A serious game for eliciting social engineering security requirements. In Proceedings of the 2016 IEEE 24th International Requirements Engineering Conference (RE), Beijing, China, 12–16 September 2016; pp. 16–25.
- Aldawood, H.; Skinner, G. Educating and raising awareness on cyber security social engineering: A literature review. In Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE), Wollongong, NSW, Australia, 4–7 December 2018; pp. 62–68.
- Aldawood, H.; Skinner, G. Challenges of implementing training and awareness programs targeting cyber security social engineering. In Proceedings of the International Conferences on Cyber Security and Communication Systems, Melbourne, Australia, 10–12 December 2018.
- Aldawood, H.; Skinner, G. An academic review of current industrial and commercial cyber security social engineering solutions. In Proceedings of the 2019 the 3rd International Conference on Cryptography, Security and Privacy, Kuala Lumpur, Malaysia, 19–21 January 2019.
- Wang, D.; Cheng, H.; Wang, P.; Yan, J.; Huang, X. A security analysis of honeywords. In Proceedings of the 25th Annual Network and Distributed System Security Symposium, San Diego, CA, USA, 18–21 February 2018.
- Gulati, R. The Threat of Social Engineering and Your Defense Against It. Available online: <https://www.scribd.com/document/55172071/The-Threat-of-Social-Engineering-and-Your-Defense-Against-It> (accessed on 15 March 2019).

15. Hackett, R. Yahoo raises breach estimate to full 3 billion accounts, by far biggest known. Available online: <http://fortune.com/2017/10/03/yahoo-breach-mail/> (accessed on 15 March 2019).
16. Ragan, S. Weebly data breach affects 43 million customers. Available online: <https://www.csoonline.com/article/3133031/weebly-data-breach-affects-43-million-customers.html> (accessed on 15 March 2019).
17. Heim, P. Resetting passwords to keep your files safe. Available online: <https://blog.dropbox.com/topics/company/resetting-passwords-to-keep-your-files-safe> (accessed on 15 March 2015).
18. Weir, C. Cracking the Myspace List—First Impressions. Available online: <https://reusablesec.blogspot.com/2016/07/cracking-myspace-list-first-impressions.html> (accessed on 15 March 2019).
19. Dudovskiy, J. Research methodology. *Retr. Febr.* **2016**, *5*, 2017.
20. Long-Sutehall, T.; Sque, M.; Addington-Hall, J. Secondary analysis of qualitative data: A valuable method for exploring sensitive issues with an elusive population? *J. Res. Nurs.* **2011**, *16*, 335–344. [CrossRef]
21. Ruggiano, N.; Perry, T.E. Conducting secondary analysis of qualitative data: Should we, can we, and how? *Qual. Soc. Work* **2017**, *18*, 81–97. [CrossRef]
22. Kpakol, A. Re-Engineering Corporate Culture for Organizational Receptivity to Change. *Eur. J. Bus. Manag.* **2014**, *6*, 167–176.
23. Apăvăloaie, E.-I. The impact of the internet on the business environment. *Procedia Eco. Financ.* **2014**, *15*, 951–958. [CrossRef]
24. Wilcox, H.; Bhattacharya, M.; Islam, R. Social engineering through social media: An investigation on enterprise security. In Proceedings of the International Conference on Applications and Techniques in Information Security, Lisbon, Portugal, 16–20 November 2014; pp. 243–255.
25. Greitzer, F.L.; Strozer, J.R.; Cohen, S.; Moore, A.P.; Mundie, D.; Cowley, J. Analysis of unintentional insider threats deriving from social engineering exploits. In Proceedings of the 2014 IEEE Security and Privacy Workshops (SPW), San Jose, CA, USA, 17–18 May 2014; pp. 236–250.
26. Airehrour, D.; Vasudevan Nair, N.; Madanian, S. Social engineering attacks and countermeasures in the new zealand banking system: Advancing a user-reflective mitigation model. *Information* **2018**, *9*, 110. [CrossRef]
27. Wilcox, H.; Bhattacharya, M. Countering social engineering through social media: An enterprise security perspective. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Cham, Switzerland, 2015; Volume 9330, pp. 54–64.
28. Alseadoon, I.; Chan, T.; Foo, E.; Gonzales Nieto, J. Who is more susceptible to phishing emails? A saudi arabian study. In Proceedings of the 23rd Australasian Conference on Information Systems, Geelong, Australia, 3–5 December 2012; pp. 1–11.
29. Mohebzada, J.G.; El Zarka, A.; BHoijani, A.H.; Darwish, A. Phishing in a university community: Two large scale phishing experiments. In Proceedings of the 2012 International Conference on Innovations in Information Technology (IIT), Abu Dhabi, UAE, 18–20 March 2012; pp. 249–254.
30. Dhamija, R.; Tygar, J.D.; Hearst, M. Why phishing works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA, 22–27 April 2006; pp. 581–590.
31. Sheng, S.; Holbrook, M.; Kumaraguru, P.; Cranor, L.F.; Downs, J. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, New York, NY, USA, 10–15 April 2010; pp. 373–382.
32. Justin, S.; Anastasios, A. Social engineering as a threat to societies: The cambridge analytica case. Available online: [https://www.realcleardefense.com/articles/2018/07/18/social\\_engineering\\_as\\_a\\_threat\\_to\\_societies\\_the\\_cambridge\\_analytica\\_case\\_113620.html](https://www.realcleardefense.com/articles/2018/07/18/social_engineering_as_a_threat_to_societies_the_cambridge_analytica_case_113620.html) (accessed on 15 March 2019).
33. Costa, L.P.d.S.; Figueira, A.C.R. Political risk and internationalization of enterprises: A literature review. *Cadernos EBAPE* **2017**, *15*, 63–87. [CrossRef]
34. Gardner, B.; Thomas, V. *Building an Information Security Awareness Program: Defending against Social Engineering and Technical Threats*; Elsevier: Amsterdam, The Netherlands, 2014.
35. Chappell, S. Turkey: Personal data of 50 million citizens leaked online, hackers claim. *Euronews*, 6 April 2016.
36. Yan, W. Nearly 80 Percent of Internet Users Suffer Identity Leaks. Available online: [http://www.chinadaily.com.cn/china/2015-07/24/content\\_21400381.htm](http://www.chinadaily.com.cn/china/2015-07/24/content_21400381.htm) (accessed on 18 March 2019).
37. Pham, T. Four Years Later, Anthem Breached Again: Hackers Stole Credentials. Available online: <https://duo.com/blog/four-years-later-anthem-breached-again-hackers-stole-employee-credentials> (accessed on 15 March 2019).



38. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
39. Thomas, K.; Li, F.; Zand, A.; Barrett, J.; Ranieri, J.; Invernizzi, L.; Markov, Y.; Comanescu, O.; Eranti, V.; Moscicki, A. Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 1421–1434.
40. Wang, D.; Zhang, Z.; Wang, P.; Yan, J.; Huang, X. Targeted online password guessing: An underestimated threat. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1242–1254.
41. Butavicius, M.; Parsons, K.; Pattinson, M.; McCormac, A. Breaching the human firewall: Social engineering in phishing and spear-phishing emails. *arXiv*, 2016; arXiv:1606.00887.
42. Financial Services Sector—Specific Plan 2015. Available online: <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-financial-services-2015-508.pdf> (accessed on 15 March 2019).
43. Atkins, B.; Huang, W. A study of social engineering in online frauds. *Open J. Soc. Sci.* **2013**, *1*, 23. [CrossRef]
44. Abawajy, J. User preference of cyber security awareness delivery methods. *Behav. Inf. Technol.* **2014**, *33*, 237–248. [CrossRef]
45. Frumento, E.; Puricelli, R.; Freschi, F.; Ariu, D.; Weiss, N.; Dambra, C.; Cotoi, I.; Rocchetti, P.; Rodriguez, M.; Adrei, L. The Role of Social Engineering in Evolution of Attacks. Available online: [https://www.dogana-project.eu/images/PDF\\_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf](https://www.dogana-project.eu/images/PDF_Files/D2.1-The-role-of-SE-in-the-evolution-of-attacks.pdf) (accessed on 15 March 2019).
46. Hadnagy, C.; Aharoni, M.; O’Gorman, J. Social Engineering Capture the Flag Results. In Proceedings of the Defcon 18, Las Vegas, NV, USA, 30 July–1 August 2010.
47. Magee, T. The Most Common Social Engineering Attacks. Available online: <https://www.techworld.com/picture-gallery/security/most-common-social-engineering-attacks-3681385/> (accessed on 15 March 2019).
48. Reicher, H. Building inclusive education on social and emotional learning: Challenges and perspectives—a review. *Int. J. Inclus. Educ.* **2010**, *14*, 213–246. [CrossRef]
49. Conteh, N.Y.; Schmick, P.J. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *Int. J. Adv. Comput. Res.* **2016**, *6*, 31. [CrossRef]
50. Pazey, B.L.; Cole, H.A. The role of special education training in the development of socially just leaders: Building an equity consciousness in educational leadership programs. *Educ. Admin. Q.* **2013**, *49*, 243–271. [CrossRef]
51. Jansson, K. A Model for Cultivating Resistance to Social Engineering Attacks. Ph.D. Thesis, Nelson Mandela Metropolitan University, Port Elizabeth, South Africa, September 2011.
52. Mann, I. *Hacking the Human: Social Engineering Techniques and Security Countermeasures*; Routledge: London, UK, 2017.
53. Hadnagy, C. *Social Engineering: The Art of Human Hacking*; John Wiley & Sons: Hoboken, NJ, USA, 2010.
54. Jacobs, J.R. *Measuring the Effectiveness of the Usb Flash Drive as a Vector for Social Engineering Attacks on Commercial and Residential Computer Systems*; Embry Riddle Aeronautical University: Cadiz, Spain, 2011.
55. Bhakta, R.; Harris, I.G. Semantic analysis of dialogs to detect social engineering attacks. In Proceedings of the 2015 IEEE International Conference on Semantic Computing (ICSC), Anaheim, CA, USA, 7–9 February 2015; pp. 424–427.
56. Fujikawa, M.; Nishigaki, M. A study of prevention for social engineering attacks using real/fake organization. In Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security, Vienna, Austria, 22–26 August 2011; pp. 597–602.
57. Irani, D.; Balduzzi, M.; Balzarotti, D.; Kirda, E.; Pu, C. Reverse social engineering attacks in online social networks. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Amsterdam, The Netherlands, 7–8 July 2011; pp. 55–74.
58. Bullée, J.-W.H.; Montoya, L.; Pieters, W.; Junger, M.; Hartel, P.H. The persuasion and security awareness experiment: Reducing the success of social engineering attacks. *J. Exp. Criminol.* **2015**, *11*, 97–115. [CrossRef]
59. Peery, J.; Pasalar, C. *Designing the Learning Experiences in Serious Games: The Overt and the Subtle—The Virtual Clinic Learning Environment*; Informatics; Multidisciplinary Digital Publishing Institute: Basel, Switzerland, 2018; p. 30.

60. Shostack, A. Elevation of Privilege: Drawing Developers into Threat Modeling. In Proceedings of the 3GSE, San Diego, CA, USA, 18 August 2014.
61. Line, M.B.; Moe, N.B. Understanding collaborative challenges in it security preparedness exercises. In Proceedings of the IFIP International Information Security Conference, Hamburg, Germany, 26–28 May 2015; pp. 311–324.
62. Hadnagy, C. *Unmasking the Social Engineer: The Human Element of Security*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
63. Gil, F.; Chamarro, A.; Oberst, U. Po-14: Addiction to online social networks: A question of "fear of missing out"? *J. Behav. Addict.* **2015**, *4*, 51–52.
64. Beckers, K.; Krautsevich, L.; Yautsiukhin, A. Analysis of social engineering threats with attack graphs. In *Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance*; Springer: Cham, Switzerland, 2015; pp. 216–232.
65. Molok, N.N.A.; Chang, S.; Ahmad, A. Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats. In Proceedings of the 8th Australian Information Security Management Conference, Perth, Australia, 30 November 2010.
66. Kim, E.B. Recommendations for information security awareness training for college students. *Inf. Manag. Comput. Secur.* **2014**, *22*, 115–126. [[CrossRef](#)]
67. Talib, S.; Clarke, N.L.; Furnell, S.M. An analysis of information security awareness within home and work environments. In Proceedings of the 2010 International Conference on Availability, Reliability and Security, Krakow, Poland, 15–18 February 2010; pp. 196–203.
68. Olusegun, O.J.; Ithnin, N.B. People Are the Answer to Security: Establishing a Sustainable Information Security Awareness Training (ISAT) Program in Organization. *arXiv*, 2013; arXiv:1309.0188.
69. Ghafir, I.; Prenosil, V.; Alhejailan, A.; Hammoudeh, M. Social engineering attack strategies and defence approaches. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, 22–24 August 2016; pp. 145–149.
70. Caputo, D.D.; Pfleeger, S.L.; Freeman, J.D.; Johnson, M.E. Going spear phishing: Exploring embedded training and awareness. *IEEE Secur. Privacy* **2014**, *12*, 28–38. [[CrossRef](#)]
71. Vishwanath, A.; Herath, T.; Chen, R.; Wang, J.; Rao, H.R. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decis. Support Syst.* **2011**, *51*, 576–586. [[CrossRef](#)]
72. Halevi, T.; Lewis, J.; Memon, N. Phishing, personality traits and facebook. *arXiv*, 2013; arXiv:1301.7643.
73. Kansal, P. Online privacy concerns and consumer reactions: Insights for future strategies. *J. Indian Bus. Res.* **2014**, *6*, 190–212. [[CrossRef](#)]
74. Hardy, C.A.; Williams, S.P. Managing information risks and protecting information assets in a web 2.0 era. In Proceedings of the Bled eConference, Bled, Slovenia, 20–23 June 2010; p. 25.
75. Workman, M.; Bommer, W.H.; Straub, D. Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput. Hum. Behav.* **2008**, *24*, 2799–2816. [[CrossRef](#)]
76. Colwill, C. Human factors in information security: The insider threat—who can you trust these days? *Inf. Secur. Tech. Rep.* **2009**, *14*, 186–196. [[CrossRef](#)]
77. Young, K. Policies and procedures to manage employee internet abuse. *Comput. Hum. Behav.* **2010**, *26*, 1467–1471. [[CrossRef](#)]
78. Abraham, S.; Chengalur-Smith, I. An overview of social engineering malware: Trends, tactics, and implications. *Technol. Soc.* **2010**, *32*, 183–196. [[CrossRef](#)]
79. Luo, X.; Brody, R.; Seazzu, A.; Burd, S. Social engineering: The neglected human factor for information security management. *Inf. Resour. Manag. J.* **2011**, *24*, 1–8. [[CrossRef](#)]
80. Chitrey, A.; Singh, D.; Singh, V. A comprehensive study of social engineering based attacks in india to develop a conceptual model. *Int. J. Inf. Netw. Secur.* **2012**, *1*, 45. [[CrossRef](#)]
81. Alavi, R.; Islam, S.; Mouratidis, H.; Lee, S. Managing social engineering attacks-considering human factors and security investment. In Proceedings of the HAISA, Lesvos, Greece, 1–3 July 2015; pp. 161–171.
82. Shah, S.; Mehtre, B.M. An overview of vulnerability assessment and penetration testing techniques. *J. Comput. Virol. Hack. Tech.* **2015**, *11*, 27–49. [[CrossRef](#)]

83. Parsons, K.; McCormac, A.; Butavicius, M.; Pattinson, M.; Jerram, C. Determining employee awareness using the human aspects of information security questionnaire (hais-q). *Comput. Secur.* **2014**, *42*, 165–176. [[CrossRef](#)]
84. Bosworth, S.; Kabay, M.E.; Whyne, E. *Computer Security Handbook*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
85. Tsohou, A.; Karyda, M.; Kokolakis, S. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Comput. Secur.* **2015**, *52*, 128–141. [[CrossRef](#)]
86. Glaspie, H.W.; Karwowski, W. Human factors in information security culture: A literature review. In Proceedings of the International Conference on Applied Human Factors and Ergonomics, Orlando, FL, USA, 21–25 July 2017; pp. 269–280.
87. Tsohou, A.; Karyda, M.; Kokolakis, S.; Kiountouzis, E. Managing the introduction of information security awareness programmes in organisations. *Eur. J. Inf. Syst.* **2015**, *24*, 38–58. [[CrossRef](#)]
88. Bartnes, M.; Moe, N.B. Challenges in it security preparedness exercises: A case study. *Comput. Secur.* **2017**, *67*, 280–290. [[CrossRef](#)]
89. Beckers, K.; Fries, V.; Groen, E.C.; Pape, S. Creativity techniques for social engineering threat elicitation: A controlled experiment. In Proceedings of the REFSQ Workshops, Essen, Germany, 27 February 2017.
90. Bhardwaj, T.; Sharma, T.K.; Pandit, M.R. Social engineering prevention by detecting malicious urls using artificial bee colony algorithm. Available online: [https://link.springer.com/chapter/10.1007/978-81-322-1771-8\\_31](https://link.springer.com/chapter/10.1007/978-81-322-1771-8_31) (accessed on 15 March 2019).
91. Knowbe4. Security Awareness Training. Available online: <https://www.itsecuritytraining.com.au/resources/knowbe4-security-awareness-training> (accessed on 15 March 2019).
92. Mataracioglu, T.; Ozkan, S. User awareness measurement through social engineering. *arXiv*, 2011; arXiv:1108.2149.



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).