future internet

MDPI

Review

Social Engineering Attacks: A Survey

Fatima Salahdine * and **Naima Kaabouch**

School of Electrical Engineering and Computer Science, University of North Dakota, Grand Forks, ND 58202, USA; naima.kaabouch@und.edu
* Correspondence: fatima.salahdine@und.edu; Tel.: +1-701-777-4460

Received: 15 February 2019; Accepted: 27 March 2019; Published: 2 April 2019

Abstract: The advancements in digital communication technology have made communication between humans more accessible and instant. However, personal and sensitive information may be available online through social networks and online services that lack the security measures to protect this information. Communication systems are vulnerable and can easily be penetrated by malicious users through social engineering attacks. These attacks aim at tricking individuals or enterprises into accomplishing actions that benefit attackers or providing them with sensitive data such as social security number, health records, and passwords. Social engineering is one of the biggest challenges facing network security because it exploits the natural human tendency to trust. This paper provides an in-depth survey about the social engineering attacks, their classifications, detection strategies, and prevention procedures.

Keywords: social engineering attacks; cyber security; phishing; vishing; spear phishing; scams; baiting; robocalls

1. Introduction

Social engineering attacks are rapidly increasing in today's networks and are weakening the cybersecurity chain. They aim at manipulating individuals and enterprises to divulge valuable and sensitive data in the interest of cyber criminals [1]. Social engineering is challenging the security of all networks regardless of the robustness of their firewalls, cryptography methods, intrusion detection systems, and anti-virus software systems. Humans are more likely to trust other humans compared to computers or technologies. Therefore, they are the weakest link in the security chain. Malicious activities accomplished through human interactions influence a person psychologically to divulge confidential information or to break the security procedures [2]. Due to these human interactions, social engineering attacks are the most powerful attacks because they threaten all systems and networks. They cannot be prevented using software or hardware solutions as long as people are not trained to prevent these attacks. Cyber criminals choose these attacks when there is no way to hack a system with no technical vulnerabilities [3].

According to the U.S. Department of Justice, social engineering attacks are one of the most dangerous threats over the world. In 2016, the cyber security analyst company Cyence stated that the United States was the country targeted by the most social engineering attacks and had the highest attacking cost followed by Germany and Japan. The estimated cost of these attacks in the US was $121.22 billion. In particular, U.S. companies are highly targeted and impacted by cyber criminals and hackers from everywhere in the world. These companies handle international significant valuable data and when these companies are hacked, it highly impacts the worldwide economy and privacy [4]. For instance, Equifax company was hacked for several months and sensitive costumers 'data were stolen in 2018. This company is a consumer credit reporting and monitoring agency that aggregates data of individuals and business consumers to monitor their credit history and prevent frauds. As a result of this data theft, attackers accessed personal information of 145.5 million American consumers. This data included consumers' full names, birth dates, social security numbers (SSN), driver license numbers, addresses, telephone numbers, credit cards information, and credit scores. This breach was the result of phishing attacks conducted by sending thousands of emails pretending to be from financial institutions or big banks such as Bank of America [5]. Equifax users are still worrying about this breach lunched by cyber attackers [5]. A more recent cyber security attack was reported by Central Bank where an attacker stole over $80 million using a remote access trojans (RAT) installed on the bank's computers [6].

In addition, U.S. Federal Bureau of Investigation (FBI) reported an increase of CEO fraud and email scams where attackers send emails to some employees pretending to be their boss and asking them to transfer funds. These companies lost more than $2.3 billion. Moreover, recent studies and surveys reported that 84% of cyber-attacks are conducted by social engineers with high success rate [7]. Thus, these statistics and others show that social engineering attacks can cost more than a natural disaster, which confirms how important it is to detect and mitigate these cyberattacks.

In this paper, we present an in-depth survey about social engineering attacks, existing detection methods, and countermeasure techniques. The rest of this paper is organized as follows. Section 2 classifies and describes social engineering attacks. Sections 3 and 4 provide an overview of existing detection, prevention, and mitigation techniques. These techniques are then discussed and compared in Section 5. Section 6 represents challenges and future directions. Finally, a conclusion is given at the end.

2. Social Engineering Attacks

Currently, social engineering attacks are the biggest threats facing cybersecurity [4–9]. According to the authors of [6], they can be detected but not stopped. Social engineers take advantage of victims to get sensitive information, which can be used for specific purposes or sold on the black market and dark web. With the Big Data advent, attackers use big data for capitalizing on valuable data for businesses purposes [10]. They package up huge amounts of data to sell in bulk as goods of today's markets [11].

Although social engineering attacks differ from each other, they have a common pattern with similar phases. The common pattern involves four phases: (1) collect information about the target; (2) develop relationship with the target; (3) exploit the available information and execute the attack; and (4) exit with no traces [12]. Figure 1 illustrates the different stages of a social engineering attack.

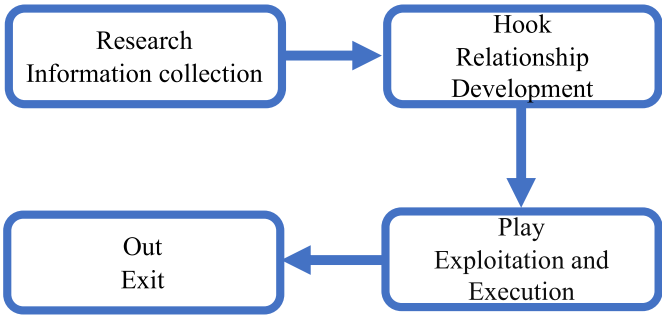

Figure 1. Social engineering attack stages [13].

In the research phase, also called information gathering, the attacker selects a victim based on some requirements. In the hook phase, the attacker starts to gain the trust of the victim through direct contact or email communication. In the paly phase, the attacker influences the victim emotionally to provide sensitive information or perform security mistakes. In the out phase, the attacker quits without leaving any proof [13].

2.1. Attacks Classification

Social engineering attacks can be classified into two categories: human-based or computer-based as illustrated in Figure 2 [14].

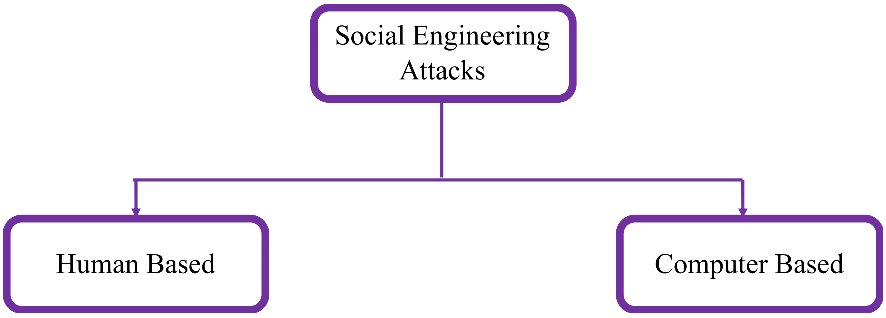

Figure 2. Social engineering attacks classification.

In human-based attacks, the attacker executes the attack in person by interacting with the target to gather desired information. Thus, they can influence a limited number of victims. The software-based attacks are performed using devices such as computers or mobile phones to get information from the targets. They can attack many victims in few seconds. Social engineering toolkit (SET) is one of the computer-based attacks used for spear phishing emails [15]. Social engineering attacks can also be classified into three categories, according to how the attack is conducted: social, technical, and physical-based attacks, as illustrated in Figure 3 [1,2].

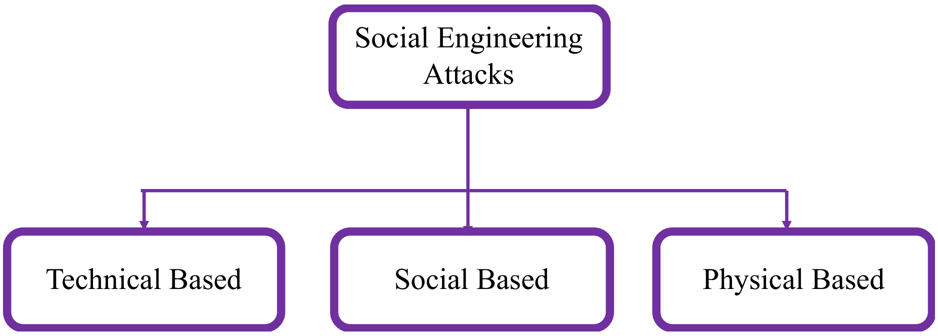

Figure 3. Social engineering attacks classification.

Social-based attacks are performed through relationships with the victims to play on their psychology and emotion. These attacks are the most dangerous and successful attacks as they involve human interactions [16]. Examples of these attacks are baiting and spear phishing. Technical-based attacks are conducted through internet via social networks and online services websites and they gather desired information such as passwords, credit card details, and security questions [1]. Physical-based attacks refer to physical actions performed by the attacker to collect information about the target. An example of such attacks is searching in dumpsters for valuable documents [2].

Social engineering attacks may combine the different aspects previously discussed, namely: human, computer, technical, social, and physical-based. Examples of social engineering attacks include phishing, impersonation on help desk calls, shoulder surfing, dumpster diving, stealing important documents, diversion theft, fake software, baiting, quid pro quo, pretexting, tailgating, Pop-Up windows, Robocalls, ransomware, online social engineering, reverse social engineering, and phone social engineering [1–18]. Figure 4 illustrates the classification of these attacks.

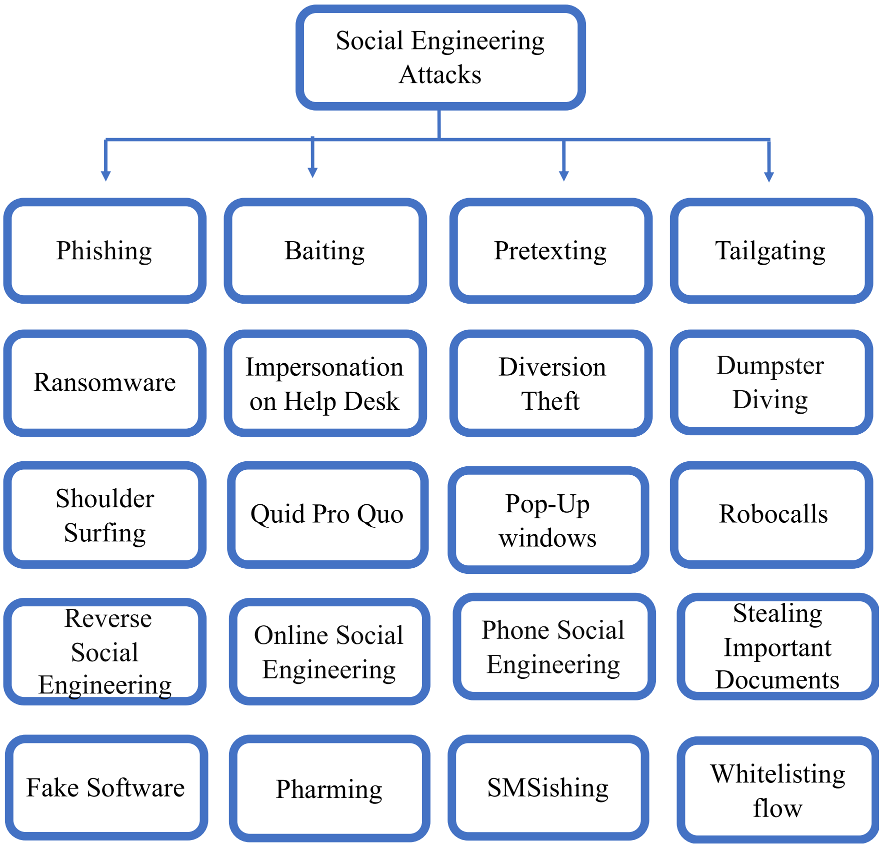

Figure 4. Social engineering attacks.

Social engineering attacks can be classified into several categories depending on several perspectives. They can be classified into two categories according to which entity is involved: human or software. They can also be classified into three categories according to how the attack is conducted: social, technical, and physical-based attacks. Through analyzing the different existing classifications of the social engineering attacks, we can also classify these attacks into two main categories: direct and indirect. Attacks classified under the first category use direct contacts between the attacker and the victim to perform the attack. They refer to attacks performed via physical contact or eye contact or voice interactions. They may also require the presence of the attacker in the victim's working area to perform the attack. Examples of these attacks are: physical access, shoulder surfing, dumpster diving, phone social engineering, pretexting, impersonation on help desk calls, and stealing important documents. Attacks classified under the indirect category do not require the presence of the attacker to launch an attack. the attack can be launched remotely via malware software carried by email's attachments or SMS messages. Examples of these attacks are: phishing, fake software, Pop-Up windows, ransomware, SMSishing, online social engineering, and reverse social engineering.

2.2. Attacks Description

2.2.1. Phishing Attacks

Phishing attacks are the most common attacks conducted by social engineers [19,20]. They aim at fraudulently acquiring private and confidential information from intended targets via phone calls or emails. Attackers mislead victims to obtain sensitive and confidential information. They involve fake websites, emails, ads, anti-virus, scareware, PayPal websites, awards, and free offers. For instance, the attack can be a call or an email from a fake department of lottery about winning a prize of a sum of money and requesting private information or clicking on a link attached to the emails. These data could be credit card details, insurance data, full name, physical address, pet’s name, first or dream job, mother’s name, place of birth, visited places, or any other information the person could use to log in to sensitive accounts such as online banking or services [21].

Phishing attacks can be classified into five categories: spear phishing, whaling phishing, vishing phishing, interactive voice response phishing, and business email compromise phishing as illustrated in Figure 5 [15].

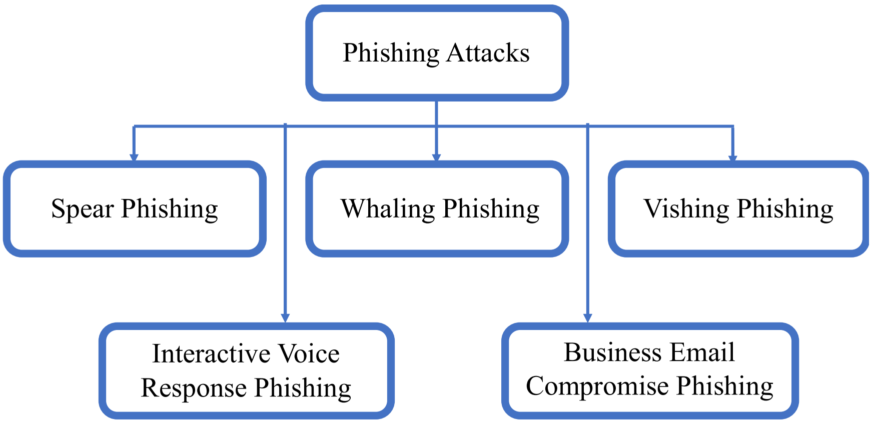
Phishing Attacks
Spear Phishing
Whaling Phishing
Vishing Phishing
Interactive Voice Response Phishing
Business Email Compromise Phishing

Figure 5. Phishing attacks.

Spear phishing attacks refer to specific phishing that target specific individuals or selected groups using their names to make claims or communications. They require collecting information about the victim using available data online. As they attack an entity from inside, it is difficult to detect and distinguish them from legitimate users, which explains the high success rate of these attacks compared to other social engineering attacks [22]. Whaling phishing is a spear phishing attack targeting high profiles in companies named big fishes. Vishing attacks refer to phone phishing to manipulate persons to give their sensitive information for verification like calls from a bank [20]. The name of this attack, ‘vishing’, is derived from voice and phishing to describe the attacks performed via voice over the internet protocol (VoIP) [23]. Interactive voice response phishing is performed by using an interactive voice response system to make the target enter the private information as if it is from a legitimate business or bank [24].

Business email compromise phishing mimics the whaling by targeting big “fishes” in corporate businesses in order to get access to their business emails, calendar, payments, accounting, or other private information [25]. The social engineer uses this data to send emails by mutating past emails, change meeting schedules, read professional information about the enterprise, and contact clients or service providers. The attacker starts by researching high profile employees through social media to know and understand their professional information such as authorized range of money a target can get from the bank [26]. After gaining desired information, the attacker sends a highly convincing business email to get a normal employee to click on a link or download an email attachment to compromise the company’s network. The attacker chooses a specific time according to the target’s calendar and inserts an emergency sense into the email to get the employee act quickly.

2.2.2. Pretexting Attacks

Pretexting attacks consist of inventing fake and convincing scenarios in order to steal a victim’s personal information. They are based on pretexts that make the victim believe and trust the attacker [27]. The attack is performed via phone calls, emails, or physical media. Attackers use publishing information on phone books, public web pages, or conferences where collaborators in the same field meet to carry out their attack. The pretext may be an offer to perform a service or to get a job, asking about personal information, helping a friend to get access to something, or winning a lottery.

2.2.3. Baiting Attacks

Baiting attacks, also called road apples, are phishing attacks that invite users to click on a link to get free stuff. They act like trojan horses where the attack is performed by exploiting unsecured computer materials such as storage media or USB drives containing malware in a coffee shop to be found by victims. When the victims plug the USB drive into their computers, the drive acts like a real world trojan horse and attacks the computer. This attack performs malicious actions in the background without being noticed by the victims.

In [7], the authors described a baiting attack named controller area network (CANDY) to be launched as a trojan horse in the infotainment system of automotive systems. This attack impacts the security capabilities of the vehicle by manipulating the communication between the driver and the vehicle. It is performed by recording the driver's voice which lets the attacker remotely access the victim's vehicle via back door, collect information about the vehicle circulation, and control the operation of the vehicle.

2.2.4. Tailgating Attacks

Tailgating attacks, also called piggybacking or physical access, consist of accessing an area or building by following someone who has the security clearance to that place. They allow attackers access unauthorized buildings. For example, attackers ask a victim to hold the door open because they forgot their company' ID card or RFID (radio-frequency identification) card. They can also borrow a computer or cellphone to perform malicious activities such as installing malware software [14].

For instance, RFID cards attacks are one of the most used attacks to access forbidden spaces for malicious purposes. Due to their wide utilization and low cost, RFID systems are considered as the most emerging technology used by companies to control the access to their facilities. Despite their advantages, they have vulnerabilities that can be exploited to cause serious security issues to companies. RFID attacks can be performed over several layers of the interconnection system model (ISO) [28]. For instance, at the physical layer, the RFID devices and the physical interface are targeted to manipulate an RFID communication. These attacks can cause temporary or permanent damage of the RFID cards. At the network layer level, the attacker manipulates the RFID network such as the communication between the RFID entities and data exchange between these entities.

2.2.5. Ransomware Attacks

Ransomware attack is yet another threat that targets individuals and companies. Recently, the FBI stated that losses due to ransomware attacks were about $1 billion in 2016, which indicates the immense financial damage a ransomware can do to companies. The ramifications of a ransomware attack can be more expensive than the ransom itself [28]. Affected companies may suffer the results of the ransomware attack for years because of loss of business, customers, data, and productivity. Ransomware attacks restrict and block access to the victim's data and files by encrypting them [29]. In order to recover these files, the victim is threatened to publish them unless paying a ransom [13]. This payment must be done with Bitcoins, which is an unregulated digital currency that is hard to track. There are two ways to analyze a ransomware attack: static and dynamic. Static analysis is performed by high skilled engineers and programming language specialists by developing programs to analyze and understand the attack in order to stop it or to get back the encrypted files. Dynamic analysis entails observing the functions of the malware remotely. It requires trusted systems to run untrusted programs without damaging the systems [29].

A Ransomware attack involves six stages: (1) creating the malware; (2) deployment; (3) installation; (4) command and control; (5) destruction; and (6) extortion [13]. The malware creation consists of developing a ransomware or using an existing one to discover any vulnerability in the victim's system in order to create a backdoor. The deployment consists of delivering the ransomware by bypassing the security controls through the created backdoor. The installation consists of running the ransomware and infecting the system. In the command and control stage, the ransomware is active when the victim has internet connection to communicate with the command center or it is passive when it is offline. In the destruction stage, the ransomware starts blocking or encrypting data and freezing screens. Extortion consists of contacting the victim demanding ransom in exchange to release the blocked files with a time limit warning. Getting back the files after the victim's payment is not guaranteed [30,31]. Once a ransomware attack is launched on a computer, the victims have only three choices: (1) paying the ransom to get back the encrypted files; (2) trying to restore the files from backups if any; or (3) losing the data after refusing to pay the ransom [32].

2.2.6. Fake Software Attacks

Fake software attacks, also called fake websites, are based on fake websites to make victims believe they are known and trusted software or websites. The victim enters real login information into the fake website, which gives the attacker the victim's credentials to use on the legitimate website, such as access to online bank accounts. An example of these threats is the tabnabbing attack which consists of a fake web page that looks like the login page of a popular website usually visited by the victim, such as online banking, Facebook, or Twitter for example [33]. The victims enter the login details when focusing on something else. The malicious user exploits the trust the victims have for these websites and gets access to their credential information [34].

2.2.7. Reverse Social Engineering Attacks

Reverse social engineering attackers claim to solve a network's problem. This involves three main steps: causing a problem such as crashing the network; advertising that the attacker is the only person to fix that problem; solving the problem while getting the desired information and leaving without being detected [18].

2.2.8. Pop-Up Windows

Pop-up window attacks refer to windows appearing on the victim's screen informing the connection is lost [35]. The user reacts by re-entering the login information, which runs a malicious program already installed with the window appearance. This program remotely forwards back the login information to the attacker. For instance, pop-ups can be alert messages showing up randomly for online advertising to lure the victim in clicking on that window. Pop-ups also can be fake messages alerting about a virus detection in the victim's computer. The pop up will prompt the victim to download and install the suggested anti-virus software to protect the computer. They can also be fake alerts stating that the computer storage is full and that it needs to be scanned and cleaned to save more space [35]. The victim panics and reacts quickly in order to fix the problem, which activates the malware software carried in the pop-up window.

2.2.9. Phone/Email Scams Attacks

For this type of attacks, the attacker contacts the victim via phone or email seeking specific information or promising a prize or free merchandise. They aim at influencing the victim to break the security rules or to provide personal information. Moreover, cellphone-based attacks can be performed via calls and via short messaging services (SMS) or text messages, which are known as SMSishing attacks [35]. SMSishing attacks consist of sending fraudulent messages and texts via cell phones to victims to influence them. They are similar to phishing attacks but they are performed in different ways. The efficiency of the SMSishing attacks resides in the fact that victims can carry their cellphones anywhere and anytime. A received text message can include a malware even if it was sent from trusted and known transmitter. The malware works as a background process installing backdoors for attackers to have access to information such as contact list, messages, personal email, photos, notes, applications, and calendar. The scammer can install a root kit to control the cellphone completely [20].

2.2.10. Robocalls Attacks

Robocall attacks have recently emerged as massive calls coming from computers to targeted persons with known phone numbers. They target cellphones, residential, and work phones. A robocall is a device or computer program that automatically dials a list of phone numbers to deliver prerecorded messages. It is mainly based on voice over the internet protocol (VoIP) to ensure several VoIP functions such as interactive voice response and text to speech [36]. These calls can be about offering or selling services or solving problems. Helping to solve tax problems is a very known example of attack that has risen in intensity in recent years. In general, when a victim answers the call, the phone number is stored in the attacker's database. Even after blocking these calls, attackers' systems call from other numbers. Robocall attacks have become a serious problem in the USA and other countries. The only way for people to stop these calls is by not answering unknown phone numbers.

2.2.11. Other Attacks

There are many other types of attacks that can be summarized as follows:

- Impersonation on Help Desk attacks: the attacker pretends to be someone with authority or a company's employee and calling the help desk requesting information or services.
- Dumpster Diving attacks: consist of gathering sensitive documents from company's trash or discarded equipment such as old computer materials, drives, CDs, and DVDs [37].
- Quid Pro Quo attacks: baiting attacks offering free services to seduce the victim. They require an exchange of information in return for a service or product [37].
- Diversion Theft attacks: consist of misdirecting a transport company to deliver a courier or package to the desired location.
- Shoulder surfing attacks: consist of watching the victim while entering passwords or sensitive information.
- Stealing important documents attacks: consist of stealing files from someone's desk for personal interests.
- Online social engineering attacks: the attacker pretends to be the network administrator for a company and asks for usernames and passwords.
- Pharming attacks: the attacker steals the traffic coming from a specific website by redirecting it to another fake website in order to get the carried information [38]. This attack works by hacking the domain name system (DNS) server and exploiting any vulnerabilities to change the internet protocol (IP) address of the host machine and the server.

3. Prevention Techniques

Social engineering attacks represent significant security risks and addressing these attacks should be part of the risk management strategy of companies and organizations [39]. Companies should make a commitment to the security awareness culture among their employees. In order to detect and prevent these attacks, a number of techniques have been proposed. A list of defense procedures for social-engineering attacks include: encouraging security education and training, increasing social awareness of social-engineering attacks, providing the required tools to detect and avoid these attacks, learning how to keep confidential information safe, reporting any suspected activity to the security service, organizing security orientations for new employees, and advertising attacks' risks to all employees by forwarding sensitization emails and known fraudulent emails [40].

In order to detect attacks via phone calls, it is necessary to verify the source of calls using a recording contacts' list, being aware of unexpected and unsolicited calls, asking to call back, or asking questions with private answers to check the caller's identity. The most effective way to stop these attacks is by not answering these calls. For help desk attacks, assigning PINs to known callers prevents malicious calls [41]. The help desk is required to stick to the scope while performing a call request. For email-based attacks, some companies use the honeypot email addresses, also called spamtraps, to collect and publish the spams to employees. When an email is sent from one of the spamtraps list, the server considers it as malicious and bans it temporarily. Other procedures that can be done include: verifying emails' sources before clicking on a link or opening an attachment, examining the emails header, calling the known sender if suspicious, and discarding emails with quick rich or prize-winning announcements.

For phishing attacks, anti-phishing tools have been proposed to blacklist and block phishing websites. Examples of these tools are McAfee anti-phishing filter, Microsoft phishing filter, and Web sense [42,43]. In [44], the authors proposed to teach students how the spear phishing attack is performed by learning by doing. They developed a framework in which students learn how phishing emails work by performing attacks on a virtual company. After gathering all the possible information from the company's website, the students launched phishing emails to simulated employees and then scanned all the received emails to decide about their nature.

In [45], the authors proposed a detection technique based on machine learning algorithms. This technique is based on unsupervised learning, in which there is no past knowledge about the observed attacks. The authors compared the performance of six machine learning algorithms for detecting phishing attacks in terms of speed, reliability, and accuracy: support vector machine, biased support vector machine, artificial neural networks, scaled conjugate gradient, and self-organizing map. They showed that the support vector machine algorithm achieves better results compared to the other algorithms. In [22], the authors proposed a method to detect the credential spear phishing attacks in enterprise sittings. The proposed detection method, called anomaly detection (DAS), performs by analyzing the potential characteristics to the spear phishing attacks in order to derive a number of features used by the attacker. It is a non-parametric anomaly scoring method used for ranking alerts.

For tailgating attacks, they may be prevented by training employees to never give access to someone without badge with no exceptions and requiring locks and IDs for all employees [35]. For shoulder surfing attacks, individuals are required to be more aware of what is around them, including persons or cameras when they enter sensitive information. For dumpster diving attacks, sensitive discarded documents and materials must be completely destroyed using shredders, memory devices must be secured or erased, and important files must be locked securely and not left for easy access.

Trojan-based attacks may be prevented by refusing to let someone use other people personal or work computers, using an antivirus for USB scanning before opening it and following the antivirus instructions and warning, examining any unexpected mailing packages, and not picking up and using found digital medias. To prevent fake software attacks, individuals need to check carefully the screen and verify if the software window is legitimate as real websites have always something special than the fake ones. Anti-virus may be limited by human unawareness; they may catch these attacks and send warnings, which most users ignore by closing the window and move on. Other preventions can be considered including verifying if the website has the https logo, not click before examining the URL, and update regularly the computer's operating system and security software.

Some security organizations encourage companies to adopt the defense in depth strategy to monitor their network and prepared themselves for possible attacks while neglecting the human aspect. In [46], the authors proposed to identify the requirements of an anti-social engineering attacks framework capable of analyzing and mitigating attack risks. They developed a new layered defense technique named Social Engineering Centered Risk Assessment (SERA). SERA starts by identifying the critical assets to evaluate the company's information for the next step. Then, each asset is placed in a container and the corresponding social engineering attack vectors are identified. Probability of attack realization is driven by local security experts and the risk analysis is obtained.

In [47], the authors proposed a flow whitelisting approach to enhance the network security inside companies. The flow whitelisting approach aims at identifying legitimate traffic from malicious traffic coming to the company's network. Four properties are used to identify these whitelists: address of the client, address of the server, port number of the server, and the protocol used for the traffic transport.

The proposed approach is performed by capturing the network's traffic at a predefined period of time and aggregating that traffic into flows when that traffic is identified as legitimate. It is based on learning to distinguish legitimate traffic from malicious traffic and generating alarms in case of an observed malicious traffic. In [34], the authors proposed a new approach called TabShots to distinguish between legitimate pages from malicious pages. The TabShots is an extension installed in the browser that compares the appearance of the webpages and highlights any observed changes to excite the attention of the user before proceeding.

In [48], the authors discussed the problem of formalizing actions that are a result of social engineering attacks. They proposed to model these actions through probabilities and graphical models such as Bayesian models. They analyzed the user's profile to estimate its vulnerabilities and psychological features. Estimating the protection of a user profile against an attack is obtained through four elements: psychological features (F), critical vulnerabilities (V), attack's actions (A), and user's accountability at successful attacks (C). In [49], the authors proposed to analyze the human's behaviors and perceptions to cope with social engineering attacks. They aim at understanding human weaknesses in being deceived easily by attackers and defining factors and features that influence the human abilities to detect attacks. They also aim at identifying vulnerable users by building a user profile that focuses on security education and training programs.

In [50], the authors evaluated the susceptibility to cybersecurity attacks in cooperative organizations in order to assess the consciousness of social engineering attacks of employees. By performing an attack against the organization based on the available information on the organization's website, employees reacted to the attack in different ways with different awareness degrees. These results were then benchmarked to establish the organization awareness in terms of ignoring the attack and being tricked or recognizing the attack and appropriately responding to it. Attack victims were then directed to intensive training. In [51], a social engineering awareness program (SEAP) was developed for schools aiming at increasing students' awareness by providing significant education and training in early age.

4. Mitigation Techniques

Human-based attacks are sophisticated and hard to detect, making their mitigation necessary. Mitigating techniques for social engineering attacks aim at decreasing the attacks' impact on the individuals or the companies [52]. They aim at saving what can be saved after a human is already attacked or a company's system is already hacked. The cyber security entity needs to minimize the loss as much as possible by defining security actions in case of emergency. For instance, building a corporate security culture among the company's employees is a mitigation technique against the attacks targeting companies or groups of individuals [53]. This positive culture helps the attack's victim not feel ashamed of being manipulated as the social engineer exploits the misplaced trust and not because the victim is unintelligent or foolish.

Being aware of this culture enhances the security responsibilities by reporting all the attacks to the technical staff as soon as possible in order to prevent more damage. This mitigation technique saves valuable time in responding to an attack and stopping the spread of the attack into the company's network. Another mitigation technique for attacks related to calls or emails informing someone of a lottery win is spreading awareness about the psychological triggers of social engineering attacks. If individuals receive this kind of information, they should be aware that they cannot win a lottery or prize they did never entered, and no one gives away a fortune to them by an email or as a donation. Recognizing that can stop people from replying to the attacker with the requested data.

For attacks related to emails or link clicks, software vendors become more aware of the social engineering treats by building strong products with security measures [54]. These software products are very challenging for cyber criminals to penetrate them. Due to these implemented security measures, the attacker cannot get enough data even if a victim is fooled by the attack [55]. The human-based mitigation techniques are based on human judgments in determining if an activity is legitimate or malicious. They involve two approaches: (1) auditing and policy; (2) education, training, and awareness (ETA). The auditing and policy approach refers to a number of security rules and procedures implemented in companies to help employees detect social engineering attacks [56]. These security rules are controlled by policies in order to guide employees to decide about the state of a suspected activity. The policy approach can be considered as a defense strategy to control the employee's reaction while under social engineering attack. The education, training, and awareness approaches refer to the effective application of the auditing and policy approach. They aim at ensuring the deployment of the defined security policies and procedures by the organization. In [57], the authors proposed to introduce these ETA techniques to new employees as a security orientation in order to provide them with the organization prerequisites toward a secure company.

Human-based mitigation techniques are a must for companies to mitigate the social engineering attacks and minimize their impacts in exploiting employees' weaknesses and vulnerabilities. They are mainly related to the effective in decision making and acting to classify an activity as malicious and act as necessary. However, human decisions are relative and thus not efficient as the human judgment is subjective even with strong awareness of social engineering attacks [58]. Technology-based mitigation techniques are required to enhance the accuracy of the human-based mitigation techniques. There are four technology-based mitigation techniques: biometrics, sensors, artificial intelligence, and social honeypot. Biometrics-based techniques aim at counteracting physical impersonation attacks, which refer to impersonating a company's employee by creating a fake profile with his/her identity [59].

Biometrics distinguish real employees from fake profiles through their biological traits. These unique traits can be fingerprint, facial recognition, eye print, and voice. Biometrics-based techniques can be effective only if the malicious user is subjected to biometric tests. Sensor-based technique entails using sensors to identify individuals. For instance, the authors of [60] proposed a prototype based on inter-body communication to check employees using door systems or specific uniforms. The prototype checks the transmitted signal from the system and compares it to the signal used by the genuine uniform. Artificial intelligence-based techniques aim at enhancing the human-based mitigation strategies by adding an additional security layer. As adaptive learning systems, artificial intelligence systems are able to learn, adapt, and change their parameters according to the situation. In [61], a multitier phishing detection and filtering technique was proposed to extract and analyze email features in order to filter them. In [62], the authors proposed a neuro-fuzzy-based technique to mitigate phishing attacks in real time and protect online transactions.

As previously mentioned, ransomware attacks are one of the security risks a company or a user can face. They consider the human as the main target instead of devices or systems, which makes them hard to identify. In [60], the authors focused on mobile ransomware by proposing a new detection technique called HelDroid. According to the authors, this technique efficiently detects any possible ransom activity even if it was never previously experienced. HelDroid was integrated in the cellphones to monitor all the used applications. The technique verifies and scans their activities before proceeding with the utilization or even before the application's installation starts. The authors of [63] focused on designing advanced operation systems and devices resistant to ransomware as a great future interest to deal with these attacks. In [64], the authors proposed an early warning detection system called CryptoDrop that is able to alert the employee in case of suspicious activity on the user data. The CryptoDrop system analyzes several common behavior indicators related to ransomware attacks. It detects the attack rapidly and stops the malicious software with a low data loss.

In [65], the authors proposed several steps to follow to mitigate and handle ransomware attacks. These steps are: (1) preparation; (2) detection; (3) containment; (4) eradication; and (5) recovery. In the preparation step, a company's security staff must eliminate all the vulnerabilities so that the hacker cannot penetrate the company's system. This step is considered as a defense strategy to stop the ransomware from spreading throughout the system and taking sensitive data. The preparation step requires frequent synchronization to protect the company's backups as the hacker destroys all the files (regular files and backup files) before asking for ransom to put the company at risk. These backups must be stored somewhere else than in the company's data centers (cloud and network shared storage), such as offline storage. Moreover, the preparation step requires an incident response to be developed for when an attack occurs. The incident response plan specifies what everyone needs to do when an attack is underway in order to effectively and quickly react to an attack. This plan can be ensured by regular trainings to the employees that teach them how to effectively respond to these attacks.

In the detection step, a ransomware attack is detected and blocked using CryptoWall and Locky traffic. When a ransomware is detected earlier, the user can stop it or at least minimize its damage. The quick detection of the ransomware allows companies and individuals contain the situation and act accordingly when the attack is already running. The CryptoWall and Locky traffic are tools integrated in the intrusion detection systems (IDS) and used by companies to limit the attack's propagation over the company's network. The containment step aims at containing the attack on only few devices that are already affected by the attack in order to limit locally the attack. It is mainly based on an endpoint protection system, which is able to kill the process of the attack's execution and deactivate the network connectivity. As a result, the attacker is not able to encrypt the files [66]. The eradication step consists of cleaning the damage resulted once the ransomware attack is contained and identified. It performs by eradicating the attack from the network and replacing infected machines and devices instead of cleaning them in order to get away of any hidden malicious files on the devices.

The last step consists of recovering any damaged or lost files and restoring them from backups after replacing systems and machines. It requires some downtime to run the backup processes and to investigate how the ransomware penetrated the system. These five mitigation steps can be used to handle any other social engineering attacks. They represent the very essential stages a company must have. Moreover, the defense success against any type of social engineering attacks depends on how the individual or the company is prepared [31]. The level to preparation determines the ability to prevent, detect, mitigate, and contain any suspicious activity.

5. Comparison

Social engineering attacks target individuals and even the most complex and secure organizations. Countermeasures and defense strategies aim at protecting them against the social engineering attacks. These techniques can be considered as the minimum an organization or a company should have to defend themselves from the most common social engineering attacks. A company can have one or more mechanisms installed in the company's system. Table 1 compares the human-based and computer-based techniques while Table 2 compares the computer-based countermeasures and mitigation techniques.

Table 1. Human-based versus computer-based countermeasures comparison.

Techniques	Description	Advantages	Limitations
Human Based	Education Training Awareness	- Easy to train humans what to do - Low number of victims	- Humans can be influenced emotionally - Tendency to o trust - Greed - Relative human decisions
Computer Based	Software, systems, and tools	- Efficient - Accurate	- Expensive products - Limited by the human unawareness - Very specific

Through analyzing and comparing these techniques, one can conclude that artificial intelligence-based defense mechanisms are the most effective techniques to reduce the risk of social engineering attacks. In addition, combining two or more defense techniques can ensure better protection. In addition, the level of preparation determines the ability to prevent, detect, mitigate, and contain any suspicious activity.

Table 2. Computer-based countermeasures and mitigation techniques comparison.

Techniques	Description	Advantages	Limitations
Filtering tools	Anti-phishing tools (McAfee filter, Microsoft filter, and Web sense)	- Can block phishing emails and websites	- Not efficient - Attackers can send internally emails - Limited by human unawareness - Expensive tools
Alerting and scanning software	Anti-virus, anti-spams, anti-scams	- Efficient in alerting - Efficient in scanning - Strong products with security measures	- Expensive products - Alerts ignored by Humans
Biometric solutions	Based on biological traits	- Distinguish real profiles from fake profiles through their biological traits - Efficient	- Can be mimicked
Artificial intelligence-based	Based on adaptive learning systems	- Efficient - Adaptive	- Complex
Machine learning-based	Learning-based	- Achieve very good results - Effective -Online learning	- Complex
Anti-social engineering framework	Social Engineering Centered Risk Assessment (SERA)	- Efficient - High probability of attacks' detection	- Very expensive
Threshold-based	Use threshold to detect attacks	- Easy	- Not efficient - Limited by the threshold value
Phone-based	Use phones	- Easy	- Phone companies are still not able to stop Robocalls
Flow whitelisting	Identifying legitimate traffic from malicious traffic coming to the company's network	- Efficient - Learning-based - Able to distinguish between legitimate traffic from malicious traffic	- Limited by the human awareness - Ignoring alarms
IDS-based	Intrusion detection system	- Able to detect suspicious activities	High false alarm rates

6. Challenges and Future Directions

Companies are investing large amounts of money and resources to establish effective strategies against social engineering attacks [67,68]. However, existing detection methods have fundamental limitations and countermeasures are inefficient in coping with the ever-growing number of social engineering attacks. Human-based techniques are limited by humans' subjective decisions. Technology-based techniques can be also limited as the technological vulnerabilities may be exploited. These attacks are evolving day after day and attackers are becoming smarter and stronger. Thus, there is a great need for more effective detection and countermeasure techniques to detect and minimize the impact of these attacks.

Because humans are a challenge for the security of any network, it important to develop training programs for employees and most importantly for K-12 students. Training students at early age can minimize the number of victims in the future. Moreover, countries have to invest in cyber security education [69,70]. Currently, there is a handful of universities in the United States of America that provide quality programs in cybersecurity. Thus, there are numerous jobs in this cyber-security field that are not filled because of the lack of graduates.

7. Conclusions

In this paper, we provided an overview of social engineering attacks, existing detection techniques, and current countermeasure methods. Unfortunately, these attacks cannot be stopped using only technology and a robust security system can be easily overcome by a social engineer with no security knowledge. Social engineering attacks have been increasing in intensity and number and are causing emotional and financial damage to people and companies. Therefore, there is a great need for novel detection techniques and countermeasure techniques as well as programs to train employees and K-12 students. Countries must also invest in cybersecurity education in order to build skilled and trained humans.

Author Contributions: Conceptualization, F.S. and N.K.; methodology, F.S.; formal analysis, F.S.; investigation, F.S. and N.K.; writing—original draft preparation, F.S.; writing—review and editing, N.K; supervision, N.K.

Funding: This research received no external funding.

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

References

1. Kalniņs, R.; Puriņs, J.; Alksnis, G. Security evaluation of wireless network access points. *Appl. Comput. Syst.* **2017**, *21*, 38–45. [CrossRef]
2. Pokrovskaia, N. Social engineering and digital technologies for the security of the social capital' development. In Proceedings of the International Conference of Quality Management, Transport and Information Security, Petersburg, Russia, 24–30 September 2017; pp. 16–19. [CrossRef]
3. Aroyo, A.M.; Rea, F.; Sandini, G.; Sciutti, A. Trust and social engineering in human robot interaction: Will a robot make you disclose sensitive information, conform to its recommendations or gamble? *IEEE Robot. Autom. Lett.* **2018**, *3*, 3701–3708. [CrossRef]
4. Arana, M. How much does a cyberattack cost companies? *Open Data Security* **2017**, 1–4.
5. Chargo, M. You've been hacked: How to better incentivize corporations to protect consumers' data. *Trans. Tenn. J. Bus. Law* **2018**, *20*, 115–143.
6. Libicki, M. Could the issue of DPRK hacking benefit from benign neglect? *Georg. J. Int. Aff.* **2018**, *19*, 83–89. [CrossRef]
7. Costantino, G.; La Marra, A.; Martinelli, F.; Matteucci, I. CANDY: A social engineering attack to leak information from infotainment system. In Proceedings of the IEEE Vehicular Technology Conference, Porto, Portugal, 3–6 June 2018; pp. 1–5. [CrossRef]
8. Pavković, N.; Perkov, L. Social Engineering Toolkit—A systematic approach to social engineering. In Proceedings of the 34th IEEE International Convention MIPRO, Opatija, Croatia, 23–27 May 2011; pp. 1485–1489.
9. Breda, F.; Barbosa, H.; Morais, T. Social engineering and cyber security. In Proceedings of the International Conference on Technology, Education and Development, Valencia, Spain, 6–8 March 2017.
10. Atwell, C.; Blasi, T.; Hayajneh, T. Reverse TCP and social engineering attacks in the era of big data. In Proceedings of the IEEE International Conference of Intelligent Data and Security, New York, NY, USA, 9–10 April 2016; pp. 1–6. [CrossRef]
11. Mahmood, U.; Afzal, T. Security analytics: Big Data analytics for cybersecurity: A review of trends, techniques and tools. In Proceedings of the IEEE National Conference on Information Assurance, Rawalpindi, Pakistan, 11–12 December 2013; pp. 129–134. [CrossRef]
12. Mouton, F.; Leenen, L.; Venter, H. Social engineering attack examples, templates and scenarios. *Comput. Secur.* **2016**, *59*, 186–209. [CrossRef]
13. Segovia, L.; Torres, F.; Rosillo, M.; Tapia, E.; Albarado, F.; Saltos, D. Social engineering as an attack vector for ransomware. In Proceedings of the Conference on Electrical Engineering and Information Communication Technology, Pucon, Chile, 18–20 October 2017; pp. 1–6. [CrossRef]
14. Xiangyu, L.; Qiuyang, L.; Chandel, S. Social engineering and Insider threats. In Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Nanjing, China, 12–14 October 2017; pp. 25–34. [CrossRef]

15. Koyun, A.; Aljanaby, E. Social engineering attacks. *J. Multidiscip. Eng. Sci. Technol.* **2017**, *4*, 1–6.
16. Patil, P.; Devale, P. A literature survey of phishing attack technique. *Int. J. Adv. Res. Comput. Commun. Eng.* **2016**, *5*, 198–200.
17. Masoud, M.; Jaradat, Y.; Ahmad, A. On tackling social engineering web phishing attacks utilizing software defined networks approach. In Proceedings of the International Conference on Open Source Software Computing, Beirut, Lebanon, 1–3 December 2016; pp. 1–6. [CrossRef]
18. Beckers, K.; Pape, S. A serious game for eliciting social engineering security requirements. In Proceedings of the International Requirements Engineering Conference, Beijing, China, 12–16 September 2016; pp. 16–25. [CrossRef]
19. Gupta, S.; Singhal, A.; Kapoor, A. A literature survey on social engineering attacks: Phishing attack. In Proceedings of the International Conference on Computing, Communication, and Automation, Noida, India, 29–30 April 2016; pp. 537–540. [CrossRef]
20. Yeboah-Boateng, E.O.; Amanor, P.M. Phishing, SMiShing & Vishing: An assessment of threats against mobile devices. *J. Emerg. Trends Comput. Inf. Sci.* **2014**, *5*, 297–307.
21. Peotta, L.; Holtz, M.D.; David, B.M.; Deus, F.G.; De Sousa, R.T. A formal classification of internet banking attacks and vulnerabilities. *Int. J. Comput. Sci. Inf. Technol.* **2011**, *3*, 186–197. [CrossRef]
22. Ho, G.; Sharma, A.; Javed, M.; Paxson, V.; Wagner, D. Detecting credential spearphishing in enterprise settings. In Proceedings of the 26th USENIX Security Symposium, Vancouver, BC, Canada, 15–17 August 2017; pp. 469–485.
23. Hofbauer, S.; Beckers, K.; Quirchmayr, G. Defense Methods against VoIP and Video Hacking Attacks in Enterprise Networks. In Proceedings of the 10th International Conference on e-Business, Bangkok, Thailand, 23–24 November 2015; pp. 1–10.
24. Braun, T.; Fung, B.C.; Iqbal, F.; Shah, B. Security and privacy challenges in smart cities. *Sustain. Cities Soc.* **2018**, *39*, 499–507. [CrossRef]
25. Opazo, B.; Whitteker, D.; Shing, C. Email trouble: Secrets of spoofing, the dangers of social engineering, and how we can help. In Proceedings of the International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery, Guilin, China, 29–31 July 2018; pp. 2812–2817. [CrossRef]
26. Wilcox, H.; Bhattacharya, M. A framework to mitigate social engineering through social media within the enterprise. In Proceedings of the IEEE International Conference on Industrial Electronics and Applications, Hefei, China, 5–7 June 2016; pp. 1039–1044. [CrossRef]
27. Ghafir, I. Social engineering attack strategies and defence approaches. In Proceedings of the IEEE International Conference on Future Internet of Things and Cloud, Vienna, Austria, 22–24 August 2016; pp. 1–5. [CrossRef]
28. Wang, S.; Zhu, S.; Zhang, Y. Blockchain-based mutual authentication security protocol for distributed RFID systems. In Proceedings of the 2018 IEEE Symposium on Computers and Communications, Natal, Brazil, 25–28 June 2018; pp. 74–77.
29. Kim, H.; Yoo, D.; Kang, J.; Yeom, Y. Dynamic ransomware protection using deterministic random bit generator. In Proceedings of the IEEE Conference on Applications, Information and Network Security, Miri, Malaysia, 13–14 November 2017; pp. 1–6. [CrossRef]
30. Everett, C. Ransomware: To pay or not to pay? *Comput. Fraud Secur.* **2016**, *4*, 8–12. [CrossRef]
31. Kharraz, A.; Robertson, W.; Balzarotti, D.; Bilge, L.; Kirda, E. Cutting the gordian knot: A look under the hood of ransomware attacks. In Proceedings of the International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Saclay, France, 29–29 July 2016; pp. 3–24.
32. Sittig, D.F.; Singh, H. A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. *Appl. Clin. Inform.* **2016**, *72*, 624–632.
33. De Ryck, P.; Nikiforakis, N.; Desmet, L.; Joosen, W. Tabshots: Client-side detection of tabnabbing attacks. In Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, Hangzhou, China, 8–10 May 2013.
34. Suri, R.K.; Tomar, D.S.; Sahu, D.R. An approach to perceive tabnabbing attack. *Int. J. Sci. Technol. Res.* **2012**, *1*, 1–4.
35. Ivaturi, K.; Janczewski, L. A taxonomy for social engineering attacks. In Proceedings of the International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, Ontario, Canada, 18–20 June 2011; pp. 1–12.

36. Tu, H.; Doupé, A.; Zhao, Z.; Ahn, G.J. Sok: Everyone hates robocalls: A survey of techniques against telephone spam. In Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2016; pp. 320–338.
37. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2014**, *22*, 113–122. [CrossRef]
38. Arya, B.; Chandrasekaran, K. A client-side anti-pharming (CSAP) approach. In Proceedings of the 2016 IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), Nagercoil, India, 23–24 November 2015; pp. 1–10.
39. Osuagwu, E.; Chukwudebe, G.; Salihu, T.; Chukwudebe, V. Mitigating social engineering for improved cybersecurity. In Proceedings of the IEEE Conference on Cyberspace, Abuja, Nigeria, 4–7 November 2015; pp. 91–100.
40. Foozy, C.F.M.; Ahmad, R.; Abdollah, M.F.; Yusof, R.; Mas'ud, M.Z. Generic taxonomy of social engineering attack and defence mechanism for handheld computer study. In Proceedings of the Malaysian Technical Universities International Conference on Engineering and Technology, Batu Pahat, Malaysia, 13–15 November 2011; pp. 1–6.
41. Kaushalya, S.A.; Randeniya, R.M.; Liyanage, A.D. An Overview of Social Engineering in the Context of Information Security. In Proceedings of the 5th IEEE International Conference on Engineering Technologies and Applied Sciences, Bangkok, Thailand, 22–23 November 2018; pp. 1–6. [CrossRef]
42. Lohani, S. Social Engineering: Hacking into Humans. *Int. J. Adv. Stud. Sci. Res.* **2019**, 5.
43. Mohammed, S.; Apeh, E. A model for social engineering awareness program for schools. In Proceedings of the IEEE International Conference on Software, Knowledge, Information Management and Applications, Abuja, Nigeria, 4–7 November 2016; pp. 392–397. [CrossRef]
44. Chothia, T.; Stefan-Ioan, P.; Oultram, M. Phishing Attacks: Learning by Doing. In Proceedings of the USENIX Workshop on Advances in Security Education, Baltimore, MD, USA, 13 August 2018; pp. 1–2.
45. Smutz, C.; Stavrou, A. Malicious PDF detection using metadata and structural features. In Proceedings of the 28th ACM annual computer security applications conference, Orlando, FL, USA, 3–7 December 2012; pp. 239–248.
46. Abeywardana, K.; Tunnicliffe, M. A layered defense mechanism for a social engineering aware perimeter. In Proceedings of the SAI Computing Conference, London, UK, 13–15 July 2016; pp. 1054–1062. [CrossRef]
47. Barbosa, R.R.R.; Sadre, R.; Pras, A. Flow whitelisting in SCADA networks. *Int. J. Crit. Infrastruct. Prot.* **2013**, *6*, 150–158. [CrossRef]
48. Abramov, M.; Azarov, A. Social engineering attack modeling with the use of Bayesian networks. In Proceedings of the IEEE International Conference on Soft Computing and Measurements, Petersburg, Russia, 25–27 May 2016; pp. 58–60. [CrossRef]
49. Albladi, S.; Weir, G. Vulnerability to social engineering in social networks: A proposed user centric framework. In Proceedings of the IEEE International Conference on Cybercrime and Computer Forensic, Vancouver, BC, Canada, 12–14 June 2016; pp. 1–6. [CrossRef]
50. Bakhshi, T. Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors. In Proceedings of the IEEE International Conference on Emerging Technology, Islamabad, Pakistan, 27–28 December 2017; pp. 1–6. [CrossRef]
51. Algarni, A.; Xu, Y.; Chan, T. Measuring source credibility of social engineering attackers on Facebook. In Proceedings of the IEEE Hawaii International Conference on System Sciences, Koloa, HI, USA, 5–8 January 2016; pp. 3686–3695. [CrossRef]
52. Nagrath, P.; Aneja, S.; Gupta, N.; Madria, S. Protocols for mitigating blackhole attacks in delay tolerant networks. *Wirel. Netw.* **2016**, *22*, 235–246. [CrossRef]
53. Thomson, K.L.; Niekerk, J.V. Towards Culturally Sensitive Policy: Africanising Approaches to Prevent Social Engineering. *Adv. Sci. Lett.* **2018**, *24*, 2499–2503. [CrossRef]
54. Ali, B.; Awad, A. Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors* **2018**, *18*, 817. [CrossRef]
55. Smith, A.; Papadaki, M.; Furnell, M. Improving awareness of social engineering attacks. In Proceedings of the 8th World Conference on Information Security Education and Training, Auckland, New Zealand, 8–10 July 2013; pp. 249–256.

56. Campbell, C.C. Solutions for counteracting human deception in social engineering attacks. *Inf. Technol. People* **2018**. [CrossRef]
57. Algarni, A.; Yue, X.; TaizaN, C.; Yu-Chu, T. Social engineering in social networking sites: Affect-based model. In Proceedings of the 8th IEEE International Conference for Internet Technology and Secured Transactions, London, UK, 9–12 December 2013; pp. 508–515.
58. Hadlington, L. The "human factor" in cybersecurity: Exploring the accidental insider. In *Psychological and Behavioral Examinations in Cyber Security*; IGI Global: Hershey, PA, USA, 2018; pp. 46–63.
59. 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.
60. Rashid, A.; Danezis, G.; Chivers, H.; Lupu, E.; Martin, A.; Lewis, M.; Peersman, C. Scoping the Cyber security body of knowledge. *IEEE Secur. Priv.* **2018**, *16*, 96–102. [CrossRef]
61. Parekh, S.; Parikh, D.; Kotak, S.; Sankhe, S. A new method for detection of phishing websites: Url detection. In Proceedings of the Second IEEE International Conference on Inventive Communication and Computational Technologies, Coimbatore, India, 20–21 April 2018; pp. 949–952.
62. Andronio, N.; Zanero, S.; Maggi, F. Heldroid: Dissecting and detecting mobile ransomware. In Proceedings of the International Springer workshop on recent advances in intrusion detection, Kyoto, Japan, 2–4 November 2015; pp. 382–404.
63. Anwar, S.; Mohamad Zain, J.; Zolkipli, M.F.; Inayat, Z.; Khan, S.; Anthony, B.; Chang, V. From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions. *Algorithms* **2017**, *10*, 39. [CrossRef]
64. Scaife, N.; Carter, H.; Traynor, P.; Butler, K.R. Cryptolock (and drop it): Stopping ransomware attacks on user data. In Proceedings of the 2016 IEEE 36th International Conference on Distributed Computing Systems, Nara, Japan, 27–30 June 2016; pp. 303–312.
65. Brewer, R. Ransomware attacks: Detection, prevention and cure. *Netw. Secur.* **2016**, *9*, 5–9. [CrossRef]
66. Kharaz, A.; Arshad, S.; Mulliner, C.; Robertson, W.; Kirda, E. A large-scale, automated approach to detecting ransomware. In Proceedings of the 25th USENIX Security Symposium, Austin, TX, USA, 10–12 August 2016; pp. 757–772.
67. Cullen, A.; Armitage, L. The social engineering attack spiral. In Proceedings of the IEEE International Conference on Cyber Security and Protection of Digital Services, London, UK, 13–14 June 2016; pp. 1–6. [CrossRef]
68. Conteh, N.Y.; Schmick, P.J. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *Int. J. Adv. Comput. Res.* **2016**, *6*, 1–31. [CrossRef]
69. Heartfield, R.; Loukas, G. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Comput. Surv.* **2016**, *48*, 1–37. [CrossRef]
70. Madain, A.; Ala, M.A.; Al-Sayyed, R. Online social networks security: Threats, attacks, and future directions. In *Social Media Shaping e-Publishing and Academia*; Springer International Publishing: New York, NY, USA, 2017; pp. 121–132.