# A Detailed Review on Engineering Attacks in Social Networking Websites

*Preeti Priyanka[1], Rajesh Sharma[2]*
*[1]Mtech Scholar, [2]Assistant Professor, Department of CSE, RKDF University, Bhopal, M.P, India*

**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.

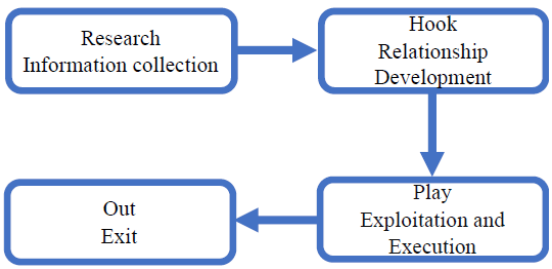


**Figure 1.** Social engineering attack stages [13].

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].

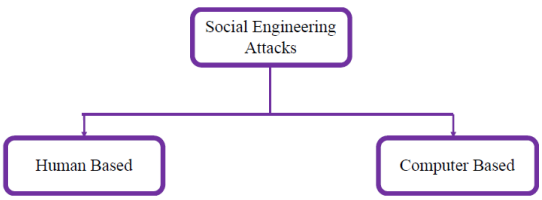


**Figure 2.** Social engineering attacks classification.

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].

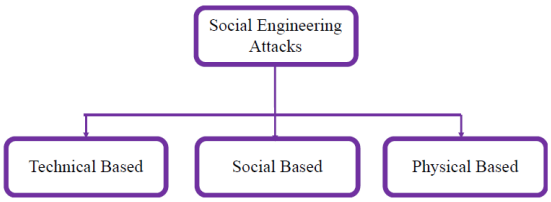


**Figure 3.** Social engineering attacks classification.

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.

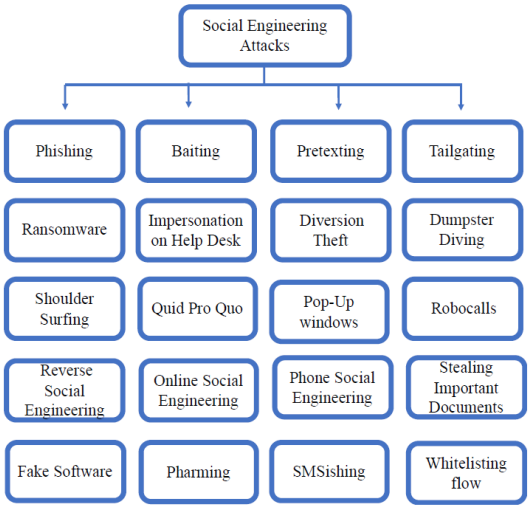


**Figure 4.** Social engineering attacks.

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].

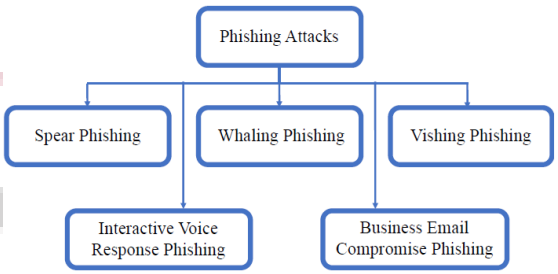


**Figure 5.** Phishing attacks.

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.

## 4. 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.

**References**

1. Kalniņs, R.; Puriņs, J.; Alksnis, G. Security evaluation of wireless network access points. *Appl. Comput. Syst.* **2017**, *21*, 38–45.
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.
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.
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.
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.
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.
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.
12. Mouton, F.; Leenen, L.; Venter, H. Social engineering attack examples, templates and scenarios. *Comput. Secur.* **2016**, *59*, 186–209.
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.
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.
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.
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.
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.
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.
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.
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.

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.
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.
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.
30. Everett, C. Ransomware: To pay or not to pay? *Comput. Fraud Secur.* **2016**, *4*, 8–12.
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.
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.
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.
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.