Detailed Analysis of Cyber Attacks on Internet Platform

Sonam Chauhan[1], Trapti saxena[2]
[1]MTech Scholar, [2]Assistant Professor, Department of ECE, RKDF University, Bhopal, M.P, India

Abstract: Because of developments in digital communication technology, human communication is now more possible and significant. However, social networks and other internet services without sufficient security measures to protect it may make private and sensitive information accessible. Communication systems are vulnerable spots that malevolent persons might readily exploit through social engineering assaults. These assaults aim to trick individuals or organisations into taking actions that benefit the attackers or provide them with sensitive data like social security numbers, health records, and passwords. One of the biggest security issues networks face today is social engineering, which takes advantage of people's innate tendency to trust. An extensive overview of social engineering assaults is described in this paper, along with information on how to identify the assaults and to secure from them.
Keywords: Cyber attacks, Security systems; Internet scams; baiting; robocalls

1. Introduction

In today's networks, social engineering attacks are rapidly increasing and weakening the cybersecurity chain. They attempt to manipulate individuals and businesses into disclosing valuable and sensitive information about cybercriminals [1].

Increasing the security of all networks using social engineering disregarding the robustness of their firewalls, cryptography techniques, intrusion detection systems, and antivirus software systems. Humans are more likely to trust other humans than computers or other technologies. They are therefore the weakest link in the security chain. Malicious activities carried out through human interaction can psychologically affect a person, leading them to disclose confidential information or breach security protocols [2].

Due to these human interactions, social engineering attacks are the most potent because they destroy all systems and networks. As long as people are not trained to prevent these attacks, they cannot be prevented by software or hardware solutions. When there is no way to compromise a system without technical flaws, cybercriminals choose for these attacks [3].
We present an in-depth survey into social engineering attacks, existing detection methods, and countermeasure techniques in this paper.
The rest of this paper is organized as follows. Section 2 describes Cyber Social attacks. Sections 3and 4gives an overview of detection and prevention techniques which are then discussed and compared in Section 5. Finally, a conclusion is given at the end.

2. Cyber Social Attacks

Currently, social engineering attacks are the biggest threats facing cyber security [4–9]. According to [6]'s authors, they can be detected but not stopped. Social engineers used victims to gather sensitive information that might be used for specific purposes or sold on the black market and dark web. With the Big Data trend, attackers are using big data to capitalise on valuable data for business purposes [10]. They pack up enormous quantities of data to market as things in bulk today [11]. Although social engineering attacks are unique from one another, they share a pattern and go through similar phases. The common pattern entails four phases: (1) gather information about the target; (2) develop a relationship with the target; (3) exploit the available information and carry out the attack; and (4) leave with no trace [12].
Figure1 illustrates the different stages of a social engineering Life Cycle.

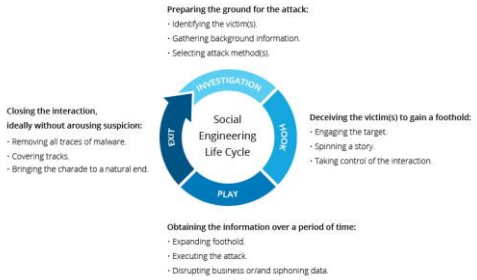

Figure 1. Social Engineering Life Cycle

The attacker chooses a victim based on certain criteria during the research phase, also known as information gathering. In the hook phase, the attacker starts by gaining the victim's trust through direct contact or email communication. The attacker manipulates the victim's emotions during the attack phase so that they give sensitive information or commit security errors. The attacker leaves without leaving any evidence in the exit phase [13].

2.1. Types of Cyber Attacks

As shown in Figure 2, types of cyber attacks are shown.

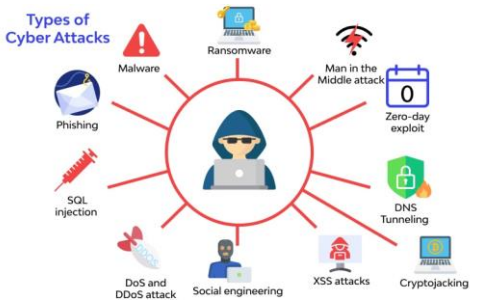

Figure 2. Types of Cyber Attacks.

In human-based attacks, the perpetrator carries out the victim's attack by interacting with the target to gather the desired information. Thus, they can influence a limited number of victims. To gather information from the targets, software-based attacks are carried out via tools like computers and mobile phones. They can attack numerous people in a short period of time. The social engineering toolkit (ST) is one of the computer-based attacks used to send out sophisticated phishing emails [15]. According to how the attack is carried out, social engineering attacks can also be classified into three categories, as shown in Figure 3[1, 2]. These categories are based on social, technological, and physical factors.

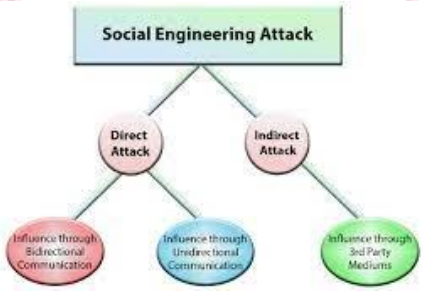

Figure 3. Classification of Social Engineering Attacks.

Relationships with the victims are used to carry out socially motivated attacks in an effort to influence their psychology and emotions. Because they include contacts with people, the attacks are the most hazardous and successful [16]. These attacks, which include phishing and baiting, are examples. Technical-based assaults

use online social networks, online service providers, and their websites to obtain data such as passwords, credit card details, and security questions [1]. Attacks with a physical component involve the attacker taking actual steps to learn more about the victim. One such attacks is searching in dumpsters for valuable documents [2].

Attacks utilising social engineering might incorporate the range of previously discussed elements, including human, computer, technological, social, and physical-based. Social engineering attacks include phishing, impersonating a help desk agent on phone calls, dumpster diving, tailgating, hiding important documents, identity theft, fake software, baiting, quid pro quo, pretexting, Pop-Up windows, Robocalls, ransomware, online social engineering, reference social engineering, and telephone social engineering [1–18].

Figure 4 illustrates the taxonomy of these attacks.

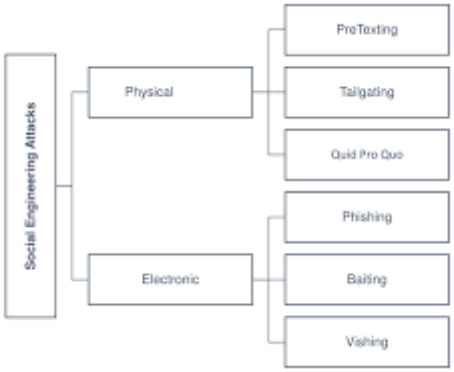

Figure 4. Taxonomy of Social engineering attacks.

Social engineering attacks can be classified into a number of categories depending on a variety of viewpoints. They can be classified into one of two categories depending on what entity is involved: software or humans. The attacks are classified into three categories by how they are carried out: social, technological, and physical-based assaults. We may also classify these attacks into two main categories by analysing the various existing classifications of social engineering: direct and indirgent. Attacks classified under the first category involve direct communication between the attacker and the target of the attack. They carried out physical combative manoeuvres in their attacks.

They may also require the presence of the attacker in the victim's working area toper form 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 appropriate category don't require the attacker to initiate an attack. The attack can be launched remotely using malicious software delivered via email attachments or SMS messages. Examples of software attacks include phishing, fake software, Pop-Up windows, malware downloaders, SMSishing, online social engineering, and reverse social engineering.

2.2. *Description of Attacks*

2.2.1. PhishingAttacks

The most frequent attacks carried out by social engineers are phishing attempts [19, 20]. They attempt to surreptitiously obtain private and confidential information from their intended targets via phone calls or emails. Attackers deceive people to obtain sensitive and private information. They include fake websites, emails, advertisements, viruses, spyware, PayPal websites, alerts, and free offers. For example, the attack could be a phone call or email from a fake lottery department requesting private information or asking the recipient to click on a link attached to the email. 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 into sensitive accounts such as online banking or services [21].

The following categories of phishing attacks are possible, as shown in Figure 5 [15]: spearphishing, whalingphishing, vishing phishing, interactive voice response phishing, and business email compromise phishing.

Figure 5. Phishing attacks.

Spearphishing 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 distinguishthemfromlegitimateusers,which explains the high success rate of these attacks compared to other social engineering attacks [22]. A common phishing attack known as "whaling phishing" targets high-profile companies with the nickname "big fishes." Vishing attacks sometimes involve phone phishing to trick people into providing sensitive information for verification, much as calls from a bank [20]. The term "vishing" is derived from the words "voice" and "phishing" to describe attacks carried out using voice over the internet protocol (VoIP) [23]. Interactivevoiceresponsephishingisperformedbyusinganinteractive voice response system to make the target enter the private information as if it is from a legitimate business or bank[24].
Compromise of business email Phishing imitates whaling by targeting important targets inside of corporate organisations in an effort to obtain their work emails, calendars, payments, accounts, or other personal data [25]. This information is used by the social engineer to send emails, change meeting times, read corporate documents, and contact clients or service suppliers. To learn about and understand high-profile employees' professional information, such as the authorised amount of money a target has stolen from the bank[26], the attacker starts by conducting social media research on them. After gaining desired information, the attackers ends 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. PretextingAttacks

In pretexting assaults, the victim's identifying information is concealed by using fictitious and convincing scenarios. They are baseless pretexts that lead the victim to believe and trust the attacker [27]. Attackers may use physical media, emails, or phone calls to carry out their attacks. Attackers conduct their attacks using material found on phoney publications, public websites, or conferences where professionals from a similar subject assemble. The SMS could be a request for personal information, an offer to help a buddy succeed, a job or service, or even a chance to win the lottery.

Figure 6. Pretexting Attacks

2.2.3. BaitingAttacks

Phishing attacks known as "baiting" encourage users to click on a link in order to receive free goods. They behave like Trojan horses in that the attack is carried out by taking advantage of unsecured computer resources like storage media or USB drives that contain malware and waiting for victims to discover them at a coffee shop. When victims plug in USB drives to their computers, the device behaves like a real-world horse thief and attacks the computer. This attack does heinous acts in the background without the victims seeing.

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 thevehicle.

2.2.4. Tail gating Attacks

Attacks known as tailgating, also known as piggybacking or physical access, involve entering a facility or area by trailing a person who has access to that location's security clearance. They permit attackers to enter unauthorised premises. For instance, attackers might request that a victim hold the door open because they forgot their company ID card or RFID (radio-frequency identification) card. They can even borrow a computer or cell phone to perform illegal activities like installing malicious software[14].

2.2.5. RansomwareAttacks

Ransomware attack is yet another threat that targets individuals andcompanies. Recently, the FBI reported that losses from ransomware attacks totaled almost $1 billion in 2016. This shows the immediate financial harm that a ransomware attack can cause to companies. The consequences of a ransomware attack may be more costly than the ransom itself [28]. Affected businesses may experience the effects of the ransomware attack for years due to lost revenue, clients, 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 performedbyhighskilledengineersandprogramminglanguagespecialistsbydevelopingprograms 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].

The six stages of a ransomware attack are: (1) developing the malware; (2) deploying it; (3) installing it; (4) commanding and controlling it; (5) destroying it; and (6) extorting it [13]. Malware development involves creating new software or utilising existing software to find vulnerabilities. In the victim's system, a backdoor was created. Delivering the software involves passing the security controls through the built-in backdoor. Running the antivirus software and infecting the system constitute the installation. When the victim has an internet connection to communicate with the command centre, the ransomware is active. When it is off-line, it is passive. The ransomware begins freezing screens and blocking or encrypting data in the destruction stage.

Extortionconsistsofcontactingthevictimdemandingransominexchangetoreleasetheblockedfiles 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 rest or get the files from back ups if any;or (3) losing the data after refusing to pay the ransom [32].

2.2.6. Fake SoftwareAttacks

False software attacks, often known as fake websites, rely on false websites to lead victims to believe that they are well-known and reputable software providers or websites. The victim enters real login information onto the fake website, which provides access to the victim's confidential information on the legitimate website, such as online bank accounts. One example of these threats is the tabbing attack, which uses a fake website that

imitates the login page of a popular website that the victim frequently visits, such LinkedIn, Facebook, or Twitter [33]. When concentrating on anything else, the victims overlook the login details. The malicious user takes advantage of the victims' confidence in these websites to gain access to their sensitive information [34].

2.2.7. Phone/Email ScamsAttacks

In this kind of attack, the perpetrator contacts the victim by phone or email and requests specific information or offers a prize or free merchandise. They want to persuade the victim to breach the security system in order to provide personal information. Additionally, cell phone-based attacks, also referred to as SMSishing attacks, can be carried out using calls and short message services (SMS) or text messages [35]. SMSishing attacks involve sending irrational text messages and messages via cell phones to targets in an effort to influence them. They resemble phishing attacks, however they are carried out differently.

The effectiveness of the SMS attacks lies on the fact that victims can use their cell phones whenever they choose. Received text messages can contain important information that was sent by a reliable and reputable sender. The use of theme-based software serves as a back-end procedure for opening doors for attackers to access information such as a contact list, messages, personal email, images, notes, applications, and a calendar. The scammer can install a root kit to control the cell phone completely [20].

3. PreventionTechniques

Social engineering attacks represent significant security risks, and organisations' risk management strategies should include dealing with them [39]. Companies should commit to fostering a culture of security awareness and responsibility among their staff. A number of techniques have been suggested in order to detect and prevent these attacks. A list of defence procedures against social engineering attacks includes: encouraging security education and training, raising societal awareness of social engineering attacks, providing the necessary tools to detect and prevent attacks, teaching people how to keep confidential information safe, organising security orientations for new hires, and promoting the risks of attacks to all employees by forewarning them of sensitization emails and well-known threats.

In order to detect attacks via phone calls, it is necessary to verify the source of calls using a recordingcontacts'list,beingawareofunexpectedandunsolicitedcalls,askingtocallback,orasking 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 [40]. 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 spam traps,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-winningannouncements.

Anti-phishing tools are used in phishing attacks. phishing websites have been proposed to be blacklisted and blocked. Examples of these products are the Microsoft phishing filter, the McAfee anti-phishing filter, and Web Sense [42,43]. The authors of [44] suggested that students be taught how to perform a sophisticated phishing attack by learning via practise. They created a course that teaches students how phishing emails operate through performing an attack on a virtual company. After gathering all the information possible from the company's website, the students launched phishing emails to impersonate employees before scanning all the received emails to determine the sender's identity.

4. Conclusions

We provided a novel review of social engineering attacks, as well as current ways for countermeasures, in this research paper. A sophisticated security system that can be easily handled by a social engineer without security experience is unfortunately not enough to stop these attacks. Attacks by social engineers have increased in ferocity and frequency, damaging individuals and organisations both psychologically and financially. New detection methods, countermeasure methods, and training programmes for workers and K–12 students are therefore desperately needed. To develop qualified and trained people, nations must also invest in cybersecurity education.

References

1. Kalniņs,R.;Purinš,J.;Alksnis,G.Securityevaluationofwirelessnetworkaccesspoints.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,Transportand 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 informationfrominfotainmentsystem.InProceedingsoftheIEEEVehicularTechnologyConference,Porto, Portugal, 3–6 June 2018; pp. 1–5.
8. Pavković,N.;Perkov,L.SocialEngineeringToolkit 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, techniquesandtools.InProceedingsoftheIEEENationalConferenceonInformationAssurance,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.Socialengineeringasanattackvectorfor ransomware.InProceedingsoftheConferenceonElectricalEngineeringandInformationCommunication 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.Ontacklingsocialengineeringwebphishingattacksutilizingsoftware 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.Aseriousgameforelicitingsocialengineeringsecurityrequirements.InProceedingsof 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:Anassessmentofthreatsagainstmobile 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 EnterpriseNetworks.InProceedingsofthe10thInternationalConferenceone-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.Emailtrouble:Secretsofspoofing,thedangersofsocialengineering,and howwecanhelp.InProceedingsoftheInternationalConferenceonNaturalComputation,FuzzySystems andKnowledgeDiscovery,Guilin,China,29–31July2018;pp.2812–2817.
26. Wilcox, H.; Bhattacharya, M. A framework to mitigate social engineering through social media within the enterprise.InProceedingsoftheIEEEInternationalConferenceonIndustrialElectronicsandApplications, 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-basedmutualauthenticationsecurityprotocolfordistributedRFID 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.InProceedingsoftheIEEEConferenceonApplications,InformationandNetworkSecurity,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 hoodofransomwareattacks. InProceedingsoftheInternationalConferenceonDetectionofIntrusionsand Malware,andVulnerabilityAssessment,Saclay,France,29–29July2016;pp.3–24.
32. Sittig,D.F.;Singh,H.Asocio-technicalapproachtopreventing,mitigating,andrecoveringfromransomware 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 May2013.
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 ConferenceonInformationResourcesManagement,CentreforInformationTechnology,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 IEEEInternationalConferenceonCircuit,PowerandComputingTechnologies(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.