Social Engineering Attacks: Recent Advances and Challenges

Nikol Mashtalyar(✉), Uwera Nina Ntaganzwa(✉), Thales Santos(✉), Saqib Hakak(✉), and Suprio Ray(✉)

Faculty of Computer Science, University of New Brunswick, Fredericton, Canada
{nmashtal,untaganz,tsantos,saqib.hakak,sray}@unb.ca

Abstract. The world's technological landscape is continuously evolving with new possibilities, yet also evolving in parallel with the emergence of new threats. Social engineering is of predominant concern for industries, governments and institutions due to the exploitation of their most valuable resource, their people. Social engineers prey on the psychological weaknesses of humans with sophisticated attacks, which pose serious cybersecurity threats to digital infrastructure. Social engineers use deception and manipulation by means of human computer interaction to exploit privacy and cybersecurity concerns. Numerous forms of attacks have been observed, which can target a range of resources such as intellectual property, confidential data and financial resources. Therefore, institutions must be prepared for any kind of attack that may be deployed and demonstrate willingness to implement new defense strategies. In this article, we present the state-of-the-art social engineering attacks, their classification and various mitigation strategies.

Keywords: Social engineering attacks · Phishing · Spam · Email fraud

1 Introduction

In the domain of cybersecurity, social engineering is an attack strategy that relies on the exploitation of human vulnerabilities through social manipulation to infiltrate security. [1] The attackers use persuasive tactics to make the victim do what the attacker intends. Social engineers sell sensitive information acquired from victims to underground economies and on the dark web, in order to capitalize on valuable data [2]. Social engineers can also use manipulation and deceit to trick victims into sending them money that cannot be traced (usually by wire) or be destructive for the sake of being destructive.

User susceptibility contributes largely to the success of social engineering attacks. Many users rely on social networking service providers for their security and privacy [3], and are very likely to click on links or provide information to people they trust, people with authority, and people with urgent requests [4].

Social engineering attacks involve a number of steps as shown in Fig. 1 [5]. There are four common phases through which attackers acquire information that

A. Moallem (Ed.): HCII 2021, LNCS 12788, pp. 417–431, 2021.
https://doi.org/10.1007/978-3-030-77392-2_27

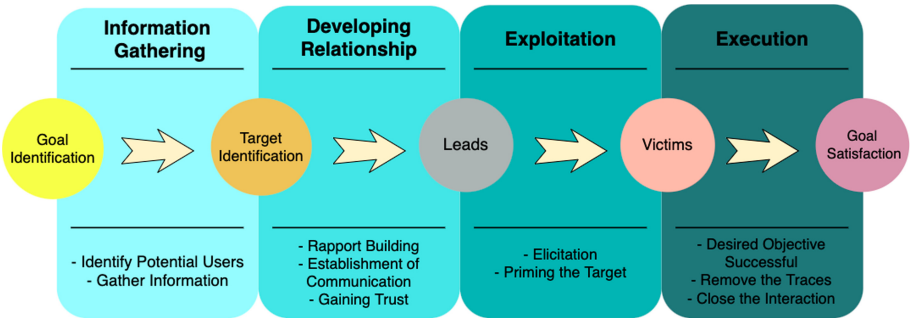

Fig. 1. Social engineering process

would otherwise be inaccessible to them. These phases, also known as the *social engineering attack cycle*, involve "information gathering, developing relationships, exploitation, and execution" [6]. In these four phases, investigation begins by identifying the victims, gathering information, and setting attack methods. Next, attackers engage the victims, obtain information from them over a period of time, and then exit without leaving any trace of their existence.

Social engineering attacks are an urgent security threat, with the number of detected attacks rising each year. In 2011, a global survey of 853 information technology professionals revealed that 48% of large companies have experienced 25 or more social engineering attacks in the past two years [1]. In 2018, the annual average cost of organizations that were targets of social engineering attacks surpassed 1.4 million dollars [1]. The ISACA's State of Cybersecurity report 2018 deemed social engineering as a top cyberthreat for organizations [1]. Over the past decade, research has demonstrated that social engineering threats and expenses are increasing; now it is up to industry to follow appropriate countermeasures in order to avoid such attacks.

During times of crises, social engineering attacks may rise due to the vulnerability of the people. The current COVID-19 pandemic is also no exception with a significant surge in cyber-attacks [7], including social engineering attacks, as shown in Fig. 2. Attackers sent unsolicited emails and telephone calls, claiming to be from a medical office, insurance company, or COVID-19 vaccine center requesting personal and medical information in order to determine eligibility for clinical vaccine trials [8]. Furthermore, the number of COVID-19 spear phishing attempts has increased by 667% [9]. In April 2020, Google reported that it blocked 18 million daily malware and phishing emails related to COVID-19, in addition to 240 million COVID-19 daily spam messages [10]. Palo Alto Networks found that from January to March 2020, there were 116,357 newly registered domains using COVID-19 related keywords. The organisation determined that 34% of those domains posed a high risk rate [11].

The objective of this study is to explore the most recent social engineering strategies and current mitigation trends. The organisation of the rest of this article is as follows: literature review is presented in Sect. 2. Section 3 presents

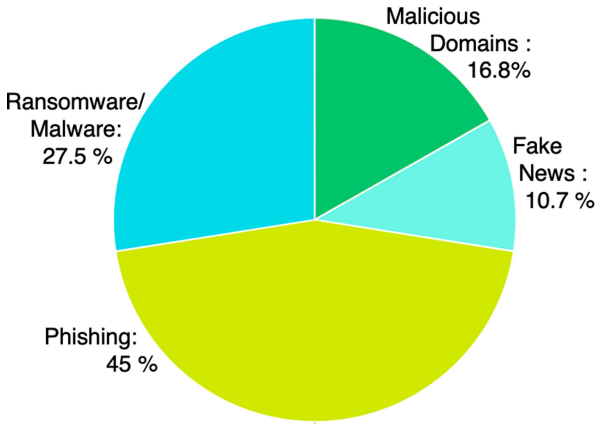

Fig. 2. Social engineering attacks during COVID-19

potential mitigation strategies. Research challenges are highlighted in Sect. 4. Future research directions are explored in Sect. 5. Section 6 concludes the article.

2 Literature Review

In this section, popular social engineering attacks are highlighted and a brief overview of the most recent works is provided. We have categorised the existing approaches into two categories of technical studies and non-technical studies. Both technical and non-technical studies are further sub-categorised into Human-based social engineering attacks and Computer-based social engineering attacks. Figure 3 presents the classification of both these attacks. The social engineering attacks under the technical studies classification, were proposed or created by their respective authors in the forms of code, algorithms, design framework and experiments [12–19]. The attacks are mostly phishing attacks carried out by artificial intelligence (AI) enabled bots [14,15], and by use of persuasion [19]. The attacks under the non-technical studies section of the diagram are defined and elaborately discussed by their respective authors; however, no experiments were conducted to observe their nature. Lastly, suggested solutions for social engineering attacks and countermeasures are summarized in the 'solutions' section of the diagram.

The main approaches used for human-based and computer-based attacks are briefly discussed below.

2.1 Human-Based Social Engineering Attacks

Human-based social engineering requires direct interaction with humans to gain the desired information [9]. Human based methods include impersonation, posing as an important user, posing as a relevant third party, and posing as desktop support, as shown in Fig. 3. An overview of these approaches are provided next.

Persuasion. A unanimous attribute of all social engineering attacks, persuasion, is arguably the key to any profitable attack. Attackers will influence the victims in a positive or negative manner in order to reach their intended goal. For example, a positive influence of persuasion includes the deceit of reward if a certain action is completed. Whereas, a negative influence of persuasion is completed through threat or authoritative intimidation [19].

Impersonation. Impersonation involves pretending to be a valid user, such as an employee, to gain physical access to a system. Similarly, posing as an important user involves impersonating a high-level manager with authority to use computer systems or files while third parties pretend to have permission from authorized users to access systems and files [6].

Tailgating or Piggybacking. During a tailgating or piggybacking social engineering attack, the attackers trick authorised employees to get access into restricted areas (such as company premises) [20]. The attackers use various strategies to fool authorised employees, such as following behind them to gain access, wearing fake identification badges, entering in parking lot doors and other impersonation approaches as mentioned above [21].

Shoulder Surfing. This method of social engineering involves obtaining sensitive information from a victim by means of observation. Attackers watch from a distance, or within proximity, while victims type passwords, identification information and other valuable personal details [2]. Attackers will also observe and listen to conversations between members of companies or institutions, whilst the victims discuss amongst themselves and present information [20].

Dumpster Diving. In this social engineering attack, the attackers attempt to obtain victims' information through physical means. The attackers try to get the personal information such as IP address, bank account details by collecting pieces of trash from the organisation's trash bins [20]. The retrieval of information is not confined to the trash bins alone; the attackers also try to access organisational charts and phone-lists, which might assist them to carry out successful attacks [2].

2.2 Computer-Based Social Engineering Attacks

Computer-based social engineering uses computer software to gain the information from the victims [9]. Computer based methods include phishing, social phishing, spear phishing, baiting, online scams such as brand theft and typosquatting, and email fraud to mention a few. An overview of these approaches is presented next.

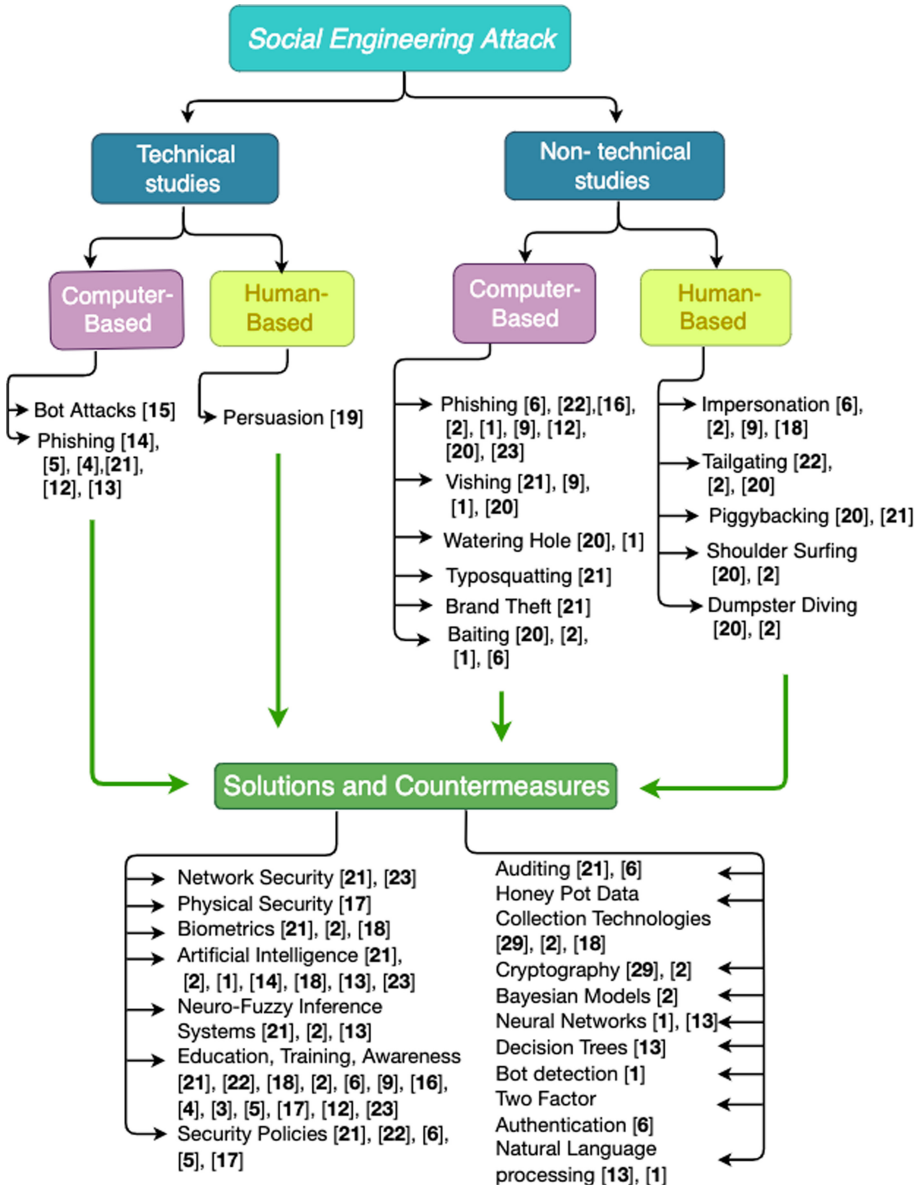

Fig. 3. Taxonomy of existing studies

Phishing. Phishing is the act of gaining access to victim's credentials and then using this data as a way to infect an organization's database or information system with malicious viruses or malware [22,23]. Similarly, social phishing uses techniques involving social media accounts of employees in order to gain access

to organizational networks [21]. Spear phishing is conducted in a similar manner to social phishing, as this attack creates a point of entry into an information system; some of which may even contain other malware, such as Trojan, with the intent of industrial spying and committing financial frauds [6]. Baiting is a similar form of attack whereby attackers lure victims by manipulating them to open links, email attachments or download malware [12].

Vishing. Through Vishing, attackers pretend to be authorised employees of a private/government organisation, which provides essential services (such as healthcare-support, tax-related services and other third-party services) [7,20]. As most of the users heavily rely on phone and Internet, cyber criminals often use this approach to abuse voice over IP (VoIP) services and scam individuals by taking their personal information such as bank account details, social security numbers and other relevant information [7,9].

Watering Hole. Attackers will find a suitable target by stalking the cyber activity of an organization to determine which websites or domains are regularly visited. Social engineers will then infect these specific websites with malware or viruses. The victims unknowingly access the now compromised websites and their devices will download malicious scripts in the background, which have the potential to spread to other devices in the organization [1,20].

Bot Attacks. With the surge of online users and increase in use of social-media platforms, attackers have started exploiting social-bots for malicious activities [15]. A social bot is an automated software that mimics human-behaviour. Numerous organisations implement social bots for different purposes such as interacting with customers. Attackers have started exploiting these social-bots in combination with other strategies such as vishing, whereby an automated social-bot interacts with and targets victims. This strategy saves attackers a lot of time due to the automated nature of setting up bots [15].

Brand Theft and Typosquatting. Brand theft and typosquatting hackers automate exploits such as brand theft to lure staff [21]. In brand theft, employees are tricked into believing that they are interacting with legitimate services or websites [21]. Additionally, typosquatting can lead to trademark infringement and loss of trust in the original organizations, according to Aldawood and Skinner.

2.3 Recent Advances

For the many social engineering attacks that exist today, countermeasures have been established. Depending on the nature of the attack, the countermeasures range from non-technical actions such as training and awareness, to more technical actions like endpoint security measures, which include two-factor authentication, use of antiviruses, and host-based intrusion detection systems.

A recurring theme in the discussion of challenges in dealing with social engineering attacks is what Parthy and Rajendran refer to as the carelessness of the human mind [20]. Humans always find a way to circumvent security measures especially when they interfere with the performance of the software artifacts in question. As a result, procedures and policies need to be in place to ensure that security measures are observed. Table 1 presents a snapshot of recent advances in the area of social engineering attacks.

Lansley et al. [13] designed an automated system (referred to as SEADer++ v2) in order to detect social engineering attacks in online chat environments. The proposed system examined the dialogue using natural language processing and uses an artificial neural network multi-layer perceptron classifier to classify possible attacks. In order to determine which dialogues contained a social engineering attack, the study categorized the criteria as features; this ranged from malicious links to the history of the attacker. The classification techniques used to detect and extract the various features included decision trees, random forest, fuzzy logic prediction, topic blacklists and neural networks. The authors evaluated their proposed method using real and semi-synthetic data sets and the system was able to detect social engineering attacks with very high accuracy.

Table 1. A snapshot of social engineering technical studies

Study	Attack experiments			Detection/Defense experiments			Proposed model solution		
	Spear phishing	Socio-technical attacks	Drive-by-downloads	Artificial intelligence	Natural language processing	Anomaly detection (DAS)	User-centric framework	Susceptibility model	Awareness, training and policy
E. J. Williams et al. [4]	✓	✗	✗	✗	✗	✗	✗	✗	✓
F. Breda et al. [5]	✗	✓	✗	✗	✗	✗	✗	✗	✓
R. Heartfield et al. [24]	✓	✗	✓	✗	✗	✗	✗	✓	✓
S. M. Albladi and G. R. Weir [3]	✗	✗	✗	✗	✗	✗	✓	✓	✓
F. Salahdine and N. Kaabouch [2]	✓	✓	✓	✓	✗	✓	✓	✓	✓
M. Lansley et al. [13]	✗	✗	✗	✓	✓	✗	✗	✗	✗
S. M. Albladi and G. R. Weir [12]	✗	✗	✗	✗	✗	✗	✗	✓	✓
A. Basit et al. [14]	✓	✓	✗	✓	✗	✗	✗	✗	✓

In [12], the authors developed a novel conceptual model to predict user vulnerability to social engineering victimisation. The study conducted a scenario-based experiment whereby the model tested the weakest points of detection behaviour in users and predicted vulnerable individuals. The model used several perspectives of user characteristics such as motivation, level of involvement, and competence regarding network threats. The most significant behaviour predictor was perceived trust, and the conceptual model supports the finding that vulnerable users can be identified by their characteristics. The following should be taken into consideration for the design of comprehensive awareness and training programs. The metrics used to evaluate the results included reliability and convergent validity tests, assessment of collinearity and path coefficients, hypothesis

testing, bootstrap re-sampling procedure and regression analysis. The main limitation of the study was the restriction of conducting a scenario-based experiment rather than a live attack study, however it was considered unavoidable due to ethical considerations.

Heartfield et al. [24] conducted two experiments, which consisted of a survey and exhibit-based test, to explore user susceptibility of deception based attacks. Participants were exposed to spear-phishing, obfuscated URLs, drive-by downloads, spoofed websites and scareware. In both experiments, participants were asked to categorize examples as attacks or non-attacks. The authors identified a set of features and produced logistic regression and random forest models for predicting susceptibility to attacks, with accuracy rates of .68 and .71. The authors observed that a general aptitude in security awareness creates a significant difference in users' ability to distinguish deception attempts, specifically if the user has strong computer literacy, familiarity and high frequency of use.

Basit et al. [14] explored four Artificial Intelligence (AI) techniques: deep learning, machine learning, hybrid learning, and scenario based techniques to detect social engineering attacks. For each AI technique, the authors examined and compared different studies conducted in the detection of phishing attacks. The deep learning technique described used data sets with two main threshold frequencies and rules strength. Similarly, machine learning techniques used testing and training data sets to develop algorithms and evaluation techniques. For deep learning techniques, the products of the data set evaluation techniques lead to the development of models that detect phishing attacks. The proposed scenario-based detection techniques are different, however. Topical and game-based techniques were employed to understand social engineering attack scenarios. Based on the outcome of the games, users gained better understanding of phishing attacks and so, allowed them to take "preventive" activities against phishing attacks. Suggested hybrid learning techniques coupled machine learning with approaches such as Search and Heuristic Rule and Logistic Regression (SHLR) to distinguish legitimate web information from that intended to carry out phishing attacks.

3 Potential Mitigation Strategies

Based on the discussion from the above-mentioned related studies, the following mitigation strategies will prove helpful in mitigating social engineering attacks.

3.1 Awareness Programs

Protection measures such as awareness programs and training of staff are a non-technical approach to addressing social engineering attacks. Since one of the factors that leads to social engineering is the deficiency of ongoing education [18,23], security awareness measures equip users with the knowledge and tools to identify and report social engineering attacks. Awareness programs include conferences, awareness campaigns, and theme-based training. Training methods

include virtual labs, simulations, games, and use of modern applications. Both awareness programs and training methods can be offered through workshops, lectures, and other virtual learning tools [22]. Enhanced information security awareness programs on password protection, non-sharing of any work-related information on social media and other gaming websites can all be included in an organisation's counterattack strategy [21].

3.2 Endpoint Security

Endpoint security is a significant method of mitigating social engineering attacks done by securing the entry points, or endpoints, of end-user devices such as phones and computers. Endpoint security includes the use of updated anti-viruses, anti-malware, and host-based intrusion detection systems (HIDS) [22]. Biometric and two-factor authentication, safe web browsing, and application of artificial intelligence techniques to detect threats are also components of endpoint security and these methods are crucial because they warrant access control.

3.3 Blockage of Phishing Attacks

A new generation of malicious email blockers can be applied by each email service provider in order to prevent malicious emails from reaching their clients. For example, Google blocks 100 million malicious emails, in the form of spam, phishing attempts and malware, every day [10]. The company's techniques can block 99.9% of threats from reaching Gmail inboxes [25]. Google implements a Tensor Flow deep-learning model trained with TFX. These document analyzers are responsible for parsing the document, identifying common attack patterns, extracting macros, de-obfuscating content, and performing feature extraction.

3.4 Validate Information

As discussed earlier, a lack of knowledge on the part of the victim can lead to social engineering attacks. In order to help combat this, governments and organizations are attempting to validate information. For example, on the World Hearth Organization's website, users may report misinformation about various social media platforms [26], as well as read which information is currently valid or invalid [27]. The FBI has released a list of fraud schemes that are currently active in relation to COVID-19 vaccines [8]. The Government of the United Kingdom and the University of Cambridge have created a game called, "Go Viral", which users can play to learn more about accurate information related to COVID-19 [28]. Various valid sources can also run joint campaigns in order to stop the spread of misinformation. The World Health Organization and the UK government have run a joint campaign to stop the spread of misinformation related to COVID-19 [29].

4 Research Challenges

In this section, we highlight emerging research challenges within the domain of cybersecurity (Table 2).

Table 2. Research challenges and possible solutions

	Challenges	Possible solutions
5G technology	High-data rate, low latency, more bandwidth, assisted botnet networks create and increase attack surfaces for attackers. Denial of service attacks are accelerated	Use AI enabled bot detectors, endpoint security measures and educate people on network security threats and defense mechanisms
Cyborgs	Automated, follow no fixed pattern, and can sometimes be controlled by humans which makes them difficult to detect	Use machine learning and neuro-fuzzy and inference systems to learn about and predict cyborg behaviour
Edge computing	Low bandwidth costs and cast amounts of data processed attract attackers	Use two-factor authentication and endpoint security measures such as anti-viruses and anti-malware.
Blockchain and cryptocurrency	Use of cryptocurrency is a new and attractive way to capitalize on data.	Encourage individuals to educate themselves on personal security and practice it

4.1 Attack Surfaces Using 5G Technology

5G or fifth generation cellular technology is designed to provide high-data speed compared to existing 4G networks with reduced latency. 5G networks are expected to provide data rates of up to 10 Gbps and thousands of devices can maintain reliable connection at the same time [30]. Although high-data rate, low latency, and more bandwidth has its own advantages for users, ultimately it will also create more attack surfaces for the attackers. The attackers will be able to create more computational bots to carry out social engineering attacks. This malicious network can be further accelerated using 5G assisted botnet networks. Attackers can also accelerate denial of service attacks by disrupting the services of the users and simultaneously launch vishing attacks to manipulate the victims.

4.2 Detection of Cyborgs

There are a variety of tools available for attackers to implement social engineering attacks such as spam bots for phishing activities, wardialing for vishing activities and so on. Bots are the automated computational programs that

are created for repetitive tasks. Numerous research studies have focused on bot detection such as [31–35]. However, with the emergence of cyborgs, detection has become more difficult. Cyborgs are also automated programs, yet to evade detection, the human behind the program can take control. Compared to social bots, cyborgs follow no specific or fixed pattern which makes detection one of the key challenges. Therefore, combating attackers that use cyborgs to carry out social engineering on social media platforms needs immediate countermeasures.

4.3 Edge Computing Security Risks

Edge computing allows for data to be analyzed and processed at the edge of the network and within a terminal device [36]. This technology was developed as a result of the increasing number of IoT (Internet of Things) devices, which use the Internet to deliver and receive information and data to and from the cloud. One of the main goals for advancing edge computing was to reduce bandwidth costs for IoT devices and other devices that require extensive data processing, in addition to improving reliability and reducing response times [36]. While edge computing was developed to better handle the increasing volume of data from IoT devices, edge computing is also very susceptible to security threats such as social engineering. Therefore, it is of utmost importance to prevent attackers from obtaining these vast quantities of data for illegal purposes, and organisations must ensure that their edge environments are meticulously protected [36].

4.4 Blockchain and Cryptocurrency Cautions

In 2008, blockchain was created to act as a decentralized ledger for Bitcoin [37]. Today, this technology is being used by many established and aspiring cryptocurrencies. As with regular social engineering attacks, scammers are able to use social engineering techniques to exploits users, instead of the technical aspects surrounding blockchain and cyrptocurrency. Attackers created a fake twitter account with a name similar to that of Elon Musk, and proceeded to manipulate victims to send 0.5–1 ether (the cryptocurrency of the Ethereum) in order to receive 5–10 ether as a reward [38]. Moreover, there have been COVID-19 cryptocurrency scams detected, whereby attackers pretend to be health-related organizations and deceive victims to send them cryptocurrency. Such attacks will continue as blockchain technology and the adoption of cryptocurrency becomes ubuiqitious.

5 Future Directions and Recommendations

With the rapid increase of cyber-crime, and its impact on the global market, organizations are beginning to recognize the importance of strategies to mitigate social engineering [22]. Cyber-attacks are continuously evolving each day and social engineers are using new and sophisticated strategies for deception.

Consequently, there is a great need for robust detection and countermeasure techniques to rectify these attacks [2].

As previously stated, awareness for the general population is a key component in defense against social engineering. Many modern employees are not aware of the basic protection measures to ensure they remain safe and vigilant in the digital workplace and at home. Therefore, training programs must begin at an early age, even in schools for K-12 students. Training students at a younger age can decrease the number of victims in the future while unloading the need for further training later in life [2].

One of the main reasons for lack of security training is due to budget constraints [2]. Wherever possible, management must realize that security is of top concern, and that organizations could lose profit and reputation if their staff members are victims of social engineering. One study found that the length of time since the last security training is significant; accordingly, institutions must recognize the importance of conducting regular training [24].

We would also stress that further research is required to delve deeper into the aforementioned problems. While we recognize that awareness is the key component in battling social engineering, there are still cases where employees can fall prey to these techniques. Thus, we recommend further study into methods of training, as well as exploring other emerging technologies such as edge-computing [36,39], artificial intelligence based approaches (such as machine learning, federated learning) [40] and blockchain-technology [40,41] to mitigate social engineering attacks.

Lastly, cybersecurity is an immense field with a growing demand. Currently, there are only a handful of universities in North America that provide quality programs in cybersecurity. Thus, this leads to numerous jobs in the cybersecurity field that are not filled due to the lack of graduates [2]. Governments and organizations need to fund and stress the importance of these programs and employment opportunities in order to acquire a greater number of qualified specialists in the field.

6 Conclusion

In conclusion, with the increasing rate of cybercrime, awareness and prevention methods are more important than ever for individuals and organizations. This paper familiarized the reader with the main types of social engineering attacks, explained the common techniques to mitigate or possibly eliminate the risks caused by those same attacks, and finally discussed the areas which can be improved by businesses and users. Recommendations were then made in order to provide the reader with a sense of how to keep alert, prepared and safe in this ever-changing era of cyberspace.

References

1. Wang, Z., Sun, L., Zhu, H.: Defining social engineering in cybersecurity. IEEE Access **8**, 85094–85115 (2020)

2. Salahdine, F., Kaabouch, N.: Social engineering attacks: a survey. Future Internet **11**(4), 89 (2019)
3. Albladi, S.M., Weir, G.R.S.: User characteristics that influence judgment of social engineering attacks in social networks. Hum.-Cent. Comput. Inf. Sci. **8**(1), 1–24 (2018). https://doi.org/10.1186/s13673-018-0128-7
4. Williams, E.J., Hinds, J., Joinson, A.N.: Exploring susceptibility to phishing in the workplace. Int. J. Hum. Comput. Stud. **120**, 1–13 (2018)
5. Breda, F., Barbosa, H., Morais, T.: Social engineering and cyber security. In: Proceedings of International Technology, Education and Development Conference (2017)
6. Kumar, A., Chaudhary, M., Kumar, N.: Social engineering threats and awareness: a survey. Eur. J. Adv. Eng. Tech. **2**(11), 15–19 (2015)
7. Hakak, S., Khan, W.Z., Imran, M., Choo, K.-K.R., Shoaib, M.: Have you been a victim of COVID-19-related cyber incidents? Survey, taxonomy, and mitigation strategies. IEEE Access **8**, 124134–124144 (2020)
8. FBI. Federal agencies warn of emerging fraud schemes related to COVID-19 vaccines. [Online]. Available: https://www.fbi.gov/news/pressrel/press-releases/federal-agencies-warn-of-emerging-fraud-schemes-related-to-covid-19-vaccines
9. Alzahrani, A.: Coronavirus social engineering attacks: issues and recommendations. Int. J. Adv. Comput. Sci. Appl. **11**(5), 9 (2020). https://doi.org/10.14569/IJACSA.2020.0110523
10. Google. Protecting businesses against cyber threats during COVID-19 and beyond. [Online]. Available: https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
11. Szurdi, J., Starov, O., McCabe, A., Chen, Z., Duan, R.: Studying how cybercriminals prey on the COVID-19 pandemic. [Online]. Available: https://unit42.paloaltonetworks.com/how-cybercriminals-prey-on-the-covid-19-pandemic/
12. Albladi, S.M., Weir, G.R.: Predicting individuals' vulnerability to social engineering in social networks. Cybersecur. **3**(1), 1–19 (2020)
13. Lansley, M., Kapetanakis, S., Polatidis, N.: SEADer++ v2: detecting social engineering attacks using natural language processing and machine learning. In: 2020 International Conference on Innovations in Intelligent Systems and Applications (INISTA), pp. 1–6. IEEE (2020)
14. Basit, A., Zafar, M., Liu, X., Javed, A.R., Jalil, Z., Kifayat, K.: A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun. Syst. **76**(1), 139–154 (2020). https://doi.org/10.1007/s11235-020-00733-2
15. Abreu, J.V.F., Fernandes, J.H.C., Gondim, J.J.C., Ralha, C.G.: Bot development for social engineering attacks on Twitter. arXiv preprint arXiv:2007.11778 (2020)
16. Smith, A., Papadaki, M., Furnell, S.M.: Improving awareness of social engineering attacks. In: Dodge, R.C., Futcher, L. (eds.) WISE 2009/2011/2013. IAICT, vol. 406, pp. 249–256. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39377-8_29
17. Saleem, J., Hammoudeh, M.: Defense methods against social engineering attacks. In: Daimi, K. (ed.) Computer and Network Security Essentials, pp. 603–618. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-58424-9_35
18. Zulkurnain, A.U., Hamidy, A., Husain, A.B., Chizari, H.: Social engineering attack mitigation. Int. J. Math. Comput. Sci. **1**(4), 188–198 (2015)
19. Bullée, J.-W., Montoya, L., Pieters, W., Junger, M., Hartel, P.H.: The persuasion and security awareness experiment: reducing the success of social engineering attacks. J. Exp. Criminol. **11**, 97–115 (2015)

20. Parthy, P.P., Rajendran, G.: Identification and prevention of social engineering attacks on an enterprise. In: 2019 International Carnahan Conference on Security Technology (ICCST), pp. 1–5. IEEE (2019)
21. Aldawood, H.A., Skinner, G.: A critical appraisal of contemporary cyber security social engineering solutions: measures, policies, tools and applications. In: 2018 26th International Conference on Systems Engineering (ICSEng), pp. 1–6. IEEE (2018)
22. Aldawood, H., Skinner, G.: An academic review of current industrial and commercial cyber security social engineering solutions. In: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 110–115 (2019)
23. Campbell, C.C.: Solutions for counteracting human deception in social engineering attacks. Inf. Technol. People **32**(5), 1130–1152 (2019)
24. Heartfield, R., Loukas, G., Gan, D.: You are probably not the weakest link: towards practical prediction of susceptibility to semantic social engineering attacks. IEEE Access **4**, 6910–6928 (2016)
25. Google. Improving malicious document detection in gmail with deeplearning (2020). [Online]. Available: https://security.googleblog.com/2020/02/improving-malicious-document-detection.html. Accessed 16 January 2021
26. World Health Organisation. How to report misinformation online (2020). [Online]. Available: https://www.who.int/campaigns/connecting-the-world-to-combat-coronavirus/how-to-report-misinformation-online. Accessed 16 January 2021
27. W.H.O. Coronavirus disease (COVID-19) advice for the public: mythbusters (2020). [Online]. Available: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/advice-for-public/myth-busters. Accessed 16 January 2021
28. U.Gov. (2020) Go viral! a 5 minute game that helps protect you against COVID-19 misinformation. [Online]. Available: https://www.goviralgame.com/en?utm_source=EO&utm_medium=SocialMedia&utm_campaign=goviral&utm_content=Eng. Accessed 16 January 2021
29. WHO. Countering misinformation with the government of the United Kingdom (2020). [Online]. Available: https://www.who.int/news-room/feature-stories/detail/countering-misinformation-about-covid-19. Accessed 16 January 2021
30. Shafi, M., et al.: 5g: a tutorial overview of standards, trials, challenges, deployment, and practice. IEEE J Sel. Areas Commun. **35**(6), 1201–1221 (2017)
31. Cresci, S.: A decade of social bot detection. Commun. ACM **63**(10), 72–83 (2020)
32. Heidari, M., Jones, J.H.: Using bert to extract topic-independent sentiment features for social media bot detection. In: 11th IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON), vol. 2020, pp. 0542–0547. IEEE (2020)
33. Kudugunta, S., Ferrara, E.: Deep neural networks for bot detection. Inf. Sci. **467**, 312–322 (2018)
34. Wu, W., Alvarez, J., Liu, C., Sun, H.-M.: Bot detection using unsupervised machine learning. Microsyst. Technol. **24**(1), 209–217 (2018)
35. Abou Daya, A., Salahuddin, M.A., Limam, N., Boutaba, R.: A graph-based machine learning approach for bot detection. In: IFIP/IEEE Symposium on Integrated Network and Service Management (IM), vol. 2019, pp. 144–152. IEEE (2019)
36. Huh, J.-H., Seo, Y.-S.: Understanding edge computing: engineering evolution with artificial intelligence. IEEE Access **7**, 164229–164245 (2019)
37. Xia, P., et al.: Don't fish in troubled waters! characterizing coronavirus-themed cryptocurrency scams (2020)

38. Weber, K., Schütz, A., Fertig, T., Müller, N.: Exploiting the human factor: social engineering attacks on cryptocurrency users **07**, 650–668 (2020)
39. Khan, W.Z., Ahmed, E., Hakak, S., Yaqoob, I., Ahmed, A.: Edge computing: a survey. Future Gener. Comput. Syst. **97**, 219–235 (2019)
40. Hakak, S., Ray, S., Khan, W.Z., Scheme, E.: A framework for edge-assisted healthcare data analytics using federated learning. In: IEEE International Workshop on Data Analytics for Smart Health (DASH) 2020. IEEE BigData (2020)
41. Hakak, S., Khan, W.Z., Gilkar, G.A., Haider, N., Imran, M., Alkatheiri, M.S.: Industrial wastewater management using blockchain technology: architecture, requirements, and future directions. IEEE Internet of Things Mag. **3**(2), 38–43 (2020)