National Journal of
Cyber Security Law

ISSN: 2582-9750
Volume 5, Issue 2, 2022
DOI (Journal): 10.37591/NJCSL

http://lawjournals.celnet.in/index.php/njcsl/index

Review NJCSL

Understanding the Growing Issue of Social Engineering: A Legal Take on Human-based Encroachment

Arya Abaranji P.S.*

Abstract

In this era of technological growth and advances, ensuring cyber security becomes one of the greatest challenges everywhere. One such threat to cyber security is social engineering. Social engineering can be defined as wide array of malignant activities which is usually achieved through human interactions. It majorly involves psychological manipulation to a point where the users make security mistakes which generally results in giving away sensitive information. Social engineers are con-artists or fraudsters who mainly rely on gaining the trust of the authorized users in order to steal significant credentials. There are many people who unknowingly deal with this serious and ongoing issue. According to the 2018 Webroot Threat Report, there exist numerous criminals impersonating many financial companies and organizations. One of the most prevalent types of social engineering is phishing. It requires a situation where the fraudster imitates a trusted source and ostensibly devises a rational scenario for delivering login credentials or any other important and delicate data. Though, stopping cybercrimes is the burden of the governmental agencies working on behalf of it, there are certain ways to keep our personal data safe and protected. The study aims to shed light on certain cyber safety tips that could offer protection and might prevent the very activity from happening. More importantly, it is crucial to be aware of all the cyber protection software and options available such as anti-virus software. This study has a pessimistic approach so as to understand the magnitude of effect caused by such deceitful activities and also attempts to suggest and cite solutions pertained to this cyber issue.

Keywords: Social engineering, phishing, cyber security, human psychology, data protection

INTRODUCTION

'Cyberspace' is a notional digital setting that enables interconnectedness of technology and information systems thereby allowing communication, data sharing and data transfer. In simple words, it is also called as the terrain of the internet. Although the origins of the internet are traced back in the USA of the 1950s, it was not until 1982 the term 'cyberspace' was used by an American Canadian author William Gibson in his book 'Neuromancer' [1]. The book described the concept as a virtual space that is filled with artificially intelligent beings. In the 990s, the term was used to denote a 'location' where chat rooms, online games, electronic mode of conversations took place. But it underwent a constructive transformation in relation to social issues and political agenda in the early 21st century. Gradually, the plight of internet and cyberspace lifted where some users grew acquainted to the proper functioning of the virtual space and operated the same to their benefit. During such transformation, it was believed by several users that the domain of cyberspace must be rendered free from laws and regulations [2]. The

***Author for Correspondence**
Arya Abaranji P.S.
E-mail: pattayilaryasuresh@gmail.com

Student, School of Law, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India

Received Date: September 21, 2022
Accepted Date: November 24, 2022
Published Date: November 30, 2022

Citation: Arya Abaranji P.S. Understanding the Growing Issue of Social Engineering: A Legal Take on Human-Based Encroachment. National Journal of Cyber Security Law. 2022; 5(2): 11–19p.

main argument of such a notion was to safeguard and protect the freedom of speech and expression of the individuals using the digital platform and ensure privacy of the abstract personalities in exchanges. However, after the advent of internet and the widespread recognition of the concept of 'cyberspace', the governments of nations mandated regulation of the medium by way of domestic laws and international agreements. The laws and other relevant instruments aimed to govern the physical location of the users and also regarding the type of content that is available to the users. The developed countries of the world have developed multiple safeguard mechanisms that control the actions of the users of the cyberspace because internet has become an integral part of a nation's security systems, global trade grid, emergency services, regular and elementary communications and other public and private activities.

The world is more dependent on internet, technology and software which make life much simple and more convenient. But such convenience does come with its own threats. Taking into account the rapid transformation of technology and the growing number of users of the internet, the need for cyber security is crucial. Any form of technological device is always prone to being hacked, provided protective measures are not taken. It is alarming to witness the rise in different forms of cyber-attacks, each tailored to the intention of the cyber criminals and the type of technology that is aimed to be attacked [3]. The most common forms of cybercrimes are phishing, denial in service, malware, password attack, ransomware, etc. Certain forms of these attacks involve human interactions through which a wide array of malicious activities is achieved. The main element behind the involvement of humans in such attacks is the psychological manipulation in order to deceive and trick users into giving away sensitive information. This act of wrongdoing and ill will is known as Social Engineering. This digital encroachment can be orchestrated in any form, from anywhere as long as there is human interaction.

DECODING THE CONCEPT OF HUMAN HACKING- THE ART OF DECEPTION

Social engineering as a concept has existed for more than a millennium and currently is one of the biggest threats in the world of cyberspace [4]. Although digital security-based social engineering has seen growth only over the course of few decades, the principles of human psychology have been used for the sly benefit of people for several centuries. The early evidence of using human psychology as a manipulation trick dates back to 1184 BC in the famous novel 'The Odyssey' that discusses the account of using a wooden Trojan horse [5]. The Greeks, in order to conclude the long, apparently never-ending war, built a giant wooden horse and hid some of the members of their army inside the horse. Giving the apprehension of defeat, the Trojans were tricked into thinking that they won the war, and they dragged the wooden statue into their territory as a souvenir of their hard-fought battle. However, after sunset, the Greek army personnel ambushed the Trojans and destroyed the city of Troy with the element of surprise thereby claiming clear victory and formally ending the war [6]. This is the first evidence of a social-engineered act. These deceitful attacks took digital form and received recognition in the 1990s when the infamous hacker Kevin Mitnick, also known as the 'World's Most Wanted Hacker', was arrested for hacking into around 40 high-tech companies including Nokia, IBM, Sun Microsystems, Motorola Corporation, etc. [7]. Citing on instance, using social engineering techniques as a key strategy, Mitnick received the Ultra Lite source code for the MicroTAC Ultra Lite cell phone by Motorola under the pretext that he was an employee of the company. Though he did not do anything using the source code, generally such information is highly confidential and sensitive, and it could have been sold for a much greater profit or could have been used for blackmail purposes. Mitnick's arrest and conviction shed light on the unspoken yet threatening issue of socially engineered activities. However, there was no decline in the number of such malignant activities in the early 2000s.

Though there are several versions of the term 'human hacking', all such definitions form basis on the trusting nature of human beings [8]. Social engineers employ several tactics and elements in order to manipulate users and obtain sensitive data without their consent and knowledge. Malicious activities of this kind occur mainly because of human error rather than the susceptibility of operating system (OS)

and in-built software. According to a cyber security analyst company Cyence, the United States of America was the target country for most of the social engineering attacks and was also ranked highest in terms of attacking cost of an approximate value of $ 121.22 billion, followed by Germany and Japan. As per a report recorded in the year 2005, the United States witnessed more than one million consumer fraud and identity theft complaints that was filed with federal, state, and local law enforcement agencies as well as private organizations [9]. Another survey from the same time period estimated a frightening number of 3.6 million (which constitutes around 3.1% of the American households) being victims of identity theft in 2004 [10]. American high-tech companies are more prone to being attacked by cyber criminals and hackers from almost all the parts of the globe mainly because these companies have a greater impact on worldwide economy and privacy as they manage significant data with international scope [11]. Several statistics and studies show that around 83% of the socially engineered cyber-attacks have a high success rate [12].

The cyber-crime rate in India witnessed a steady increase over the years. Only in the year 2020, there were 4,047 cases of online banking fraud, 2,160 cases of ATM fraud, 1,194 credit/debit card fraud and 1,093 OTP frauds [13]. Vishing, also known as voice phishing, is one of the most common cyber-attacks in India where perpetrators trick the victims into giving away their personal and confidential data. Indian nationals are not the only ones to fall prey to such scams. Several malicious rackets who are highly organized cons have been involved in the 'call center' scamming foreign nationals costing them over Rs. 300 crore, mostly from the United States [14]. Further, the citizens of Madhya Pradesh suffered a loss of around Rs. 51.33 lakh crore during the Covid-19 lockdown as fraudsters used the increased online engagement during COVID-19 lockdown to their advantage [15]. Approximately 60.2% of the cyber-crimes in 2020 were lodged for fraud activities (30,142 out of 50,035 cases), 6.6% complaints for sexual exploitation (3,293 cases), and 4.9% complaints for extortion (2,440 cases). This data shows a startling 11.8% increase in 2020 in the number of cyber-crimes reported in 2020 [16]. All the data and studies presented show the impact and intensity, both economically and psychologically, that social engineering attacks have on the people and governments.

COMPONENTS OF SOCIAL ENGINEERING

'Interaction' is the key element that a social engineer employs in order to gain sensitive information from victims. By interacting with the targeted user, the attacker initiates the attack on computers, mobile phones or any other non-technical means to get to the victim. Aside from using telephone or internet as means for committing such acts of fraud, perpetrators engage psychological techniques that involve technical, ego, sympathy and intimation attacks [17]. Such attacks, though differ in execution and nature, have the same pattern and components. A socially engineered act generally involves four phases such as: (1) collection of information about the targeted user; (2) development of inappropriate insincere relationship with the targeted user; (3) exploitation of the available information and timely execution of the attack; and (4) quit the attack after obtaining relevant information without leaving any traces [18]. The series of the act essentially starts with adequate extensive data collection by way of OSINT19. Visiting websites of the targeted company or targeted personnel, troves of information can be found as the attacker can find physical areas of interest, email IDs, contact numbers and other communication data of the personnel. Special and unique attributes of the company such as mission and vision statement, policies, agenda, etc. can also be a great source to build credibility and a sense of connection with the user when the attack is in process. Such information can prove to be of great use for a social engineer [20]. Upon collecting sufficient information, the attacker moves to the 'pretexting and elicitation' phase. In this phase, the attacker invents a scenario where the victim is enticed and convinced to release crucial information or perform any act through a cleverly devised pretext. This can be done by way of interaction in person, mobile phone or email. Most of the social engineering attacks are successful because a majority of the people do not arouse suspicion for seemingly obvious information to them [21].

Individuals can be psychologically manipulated for several reasons such as blind trust, gullibility, desire to help, the desire to be liked, etc. When the online users fall for such devious tricks based on the

above-mentioned reasons, it is widely effortless and uncomplicated for the social engineer to make the user perform actions of ill-intent [22]. It is a surprising fact that many online users believe that the chances of being deceived is comparatively low and attacker users such misconception to his/her benefit by making conversations in a polite manner and asking for requests that appear to be reasonable to a common man [23]. The social engineer's ability to convince the target without any doubts is the ultimate token of his/her successful attack. Social engineering activities mainly rely on the emotions rooting from trust and fear. For instance, when the attacker mentions the name of the target's immediate superior, the target, by default, believes that the interaction is genuine since the social engineer knows the superior's name. Adding elements of humour or sympathy is a great way to establish trust, and once a greater level of trust is established, it is too easy for the attacker to successfully complete the attack [24]. Fear is also a highly effective tactic. All that a social engineer has to do is to create a problem and persuade the user that it is their fault. This gives the attacker the opportunity to have the upper-hand over the situation and walk the fearful target through the 'steps' in which the problem can be rectified where the target also obliges. This situation not only allows the attacker to take complete advantage over the situation and gain the required information but also encourages the targeted user to conceal the fact that such a situation occurred at their own fault. Some social engineers master the aspects of micro expressions that allows the perpetrator to study the expressions of the targeted user in an interaction in a physical setting and react accordingly. Understanding emotions of anger, disgust, fear, sadness etc. helps the attacker to gain advantage in the situation [25]. Similarly, the increase in social media usage provides the attacker with a devious way to commence the process of acquiring information about a target [26]. Upon gleaning all the relevant information such as names, relatives, friends, addresses, employers, schools, and other details from social media, social-engineers resort to impersonation. Using all the acquired data about the person, the attacker can easily impersonate the identity of someone else, more easily, over phone [27]. Through a fake profile, the attack can be executed effectively by way of direct communication [28]. It is clear that the outcome of the attack solely depends on how much the attacker manipulates the targeted user without rising suspicion. Social engineers pay attention to all the details, irrespective of trial it could be, and use it accordingly to get the job done [29].

HOW SOCIAL ENGINEERING ATTACKS ARE ORCHESTRATED

Social engineering crimes, like any other crime, have ulterior motive to it. For most of the cases, illicit financial gain is the main reason behind such activities, followed by personal reasons such as revenge, blackmail, etc. One of the most common techniques that the human hacker employs for deceitful purposes is shoulder surfing. This entails the attacker spying on the clueless user in public or in a crowded areas to obtain crucial information such as personal identification numbers (PINs), passwords or other confidential data by looking over the victim's shoulder. Around 97% of the people surveyed claimed the awareness of a shoulder surfing incident on regular basis and in most of the cases, they were unaware that they were been spied on at the moment [30]. Out of all the forms of social engineering attacks, the most common form is phishing [31]. Usually, phishing attacks involves the attacker sending an email containing link to malicious websites to gather personal information by pretending to be a trustworthy organization. This is a malicious attempt by the perpetrator to scam the user into surrendering sensitive information such as bank account login credentials [32]. Approximately, around 36% of the breaches in the past year involved phishing and 95% of business email compromise (BEC)33 losses were ranged between $ 250.00 and 984,855.0033. It is even more appalling to learn that 85% of breaches involved the human element [34]. 96% of the attacks were executed via mail and 46% targets were organisations [35]. 29% of the breaches were caused based on stolen credentials [36]. Overall, phishing activities have caused over $ 54 million annual loss for US consumers and organisations [37]. Dumpster diving, although not very popular, is one of the most effective methods of social engineering. The nature of this malicious activity can be understood by nature of this idiom 'One man's trash is another man's treasure'. It is the process of searching for useful information their trash that can later be used for hacking purposes. A hacker opting for this attack technique might look for phone numbers, passwords, login credentials, sensitive visual components, business secrets or any other information that can be used. It was claimed by identity theft victims that around 87% of the information was obtained by dumpster diving [38].

Social engineers have also resorted to creative means of hacking into systems. For instance, human hackers use tailgating attacks that involves following the concerned personnel who has the security clearance to a specific part of the building. This also gives the hackers an opportunity to install malware software to perform deceitful activities later [39]. Ransomware attacks are also a quietly impending issue. This is a type of malware attack where the attacker seals and encrypts the victim's data which could be important files and then proceeds to demand a payment to unlock and decrypt the data. An estimate of 2,084 ransomware complaints were received by the IC3 in the first half of 2021 that reportedly ranged to over $ 16.8 million in losses [40]. In 2021, health care sector was the third most targeted industry for ransomware attacks in the US and suffered over $ 157 million in losses since 2016 [41]. Apart from the mentioned attack techniques, hackers also prefer hybrid model as it is a combination of two or more attach strategies thereby resulting in sophisticated execution.

SOCIAL ENGINEERING AND INDIAN LAW

Although there is no direct definition of the term 'Social Engineering', Section 415 of the Indian Penal Code, 1860 [42], states a definition for the term 'cheating' which is basically what social engineering entails. It discusses about the fraudulent or the dishonest intention to make a person to act or omit, thereby causing harm to body, mind, reputation or property. The main element of social engineering activities is to gain something by way of deception. Making false documents with deceptive and fraudulent intentions that may contain seal, sign, execution of document, transmission of electronic record or its part, affixing electronic signature, making any mark denoting authenticity of document or made in the name of fictitious person pretending to be real person, are also discussed in the Indian Penal Code [43]. Cheating, impersonation and forgery are penalised under various sections that widely depends on the facts and circumstances of the case.

The Information Technology Act, 2000 also sheds light on prohibited activities that are, by nature, subsets of social engineering. Sections 66 emphasises offences that are committed by way of computers and related devices with 'fraudulent' and 'dishonest' intention [44]. Section 66D in specific discusses the punishment for cheating by personation by using computer resource [45]. The salient feature of this Act is that the IT Act applies for offence or contravention committed outside India by any person irrespective of his nationality [46]. The Act also contains provisions for the creation of nodal agencies that is responsible for the research and development aspects that relates to protection of Critical Information Infrastructure [47]. The Section also defines the term 'Critical Information Infrastructure' that refers to computer resource where the incapacitation or destruction of which will have a debilitating impact on national security, economy, public health or safety. The Act also provides for the Indian Computer Emergency Response Team that will serve as the prominent national agencies ensuring cyber security on the facets such as collection and dissemination of data on cyber incidents, taking emergency measures to combat and give out alerts of cyber security incidents, to issue guidelines, advisories on the matters relating to information security practices, response and prevention of cyber-crime incidents [48]. As a part of India's Digital India initiative under the Ministry of Electronics and Information Technology, the 'Cyber Swachhta Kendra' was launched to detecting botnets and thus to create a secure cyber eco system [49]. This centre works closely with Internet Service Providers and Product/Antivirus companies and is operated by Indian Computer Emergency Response Team [50].

Apart from several provisions and schemes that impliedly apply to social engineering, the Indian Judiciary has also been opined and propounded judgements that acknowledges the growing number of internet scam complaints. The Delhi High Court conceded that phishing e-mails are becoming increasingly sophisticated. The court recognised that though there is no specific provision, 'misrepresentation' would be an act that amounts to phishing [51]. The Allahabad High Court discussed the ingredients of Section 66-D which are: (a) a person by means of a communication device or computer resource; (b) cheats another by personation. The court also accentuated that while the Information Technology Act does not have a separation definition for the term "personation", it will however originally apply to vast array of phishing attacks [52]. The court also deliberated on what a

'computer system' entails and what could be subjected to online scam and cyber scam. The computer system is entailed to cover one device or a collection of devices, that includes input and output support devices that are capable of being used in conjunction with external files, which also can contain computer programs, electronic instructions, input and output data, data storage and retrieval [53]. The Judiciary has given advanced judgements that are in line with the modern transformation of the society.

CONCLUSION

"Social engineers veil themselves in a cloak of believability" said Kevin Mitnik who is considered to be the world's most famous hacker. Regardless of the high success rate of social engineering activities, there are still several steps that can be taken to combat the issue. Most of the defences depend on equipping individuals with alertness and caution more than fortifying technology. With a comprehensive defensive strategy, both technical and non-technical forms of hacking can be resisted. There is no denial that implementation of such security systems are expensive and key studies show that financial costs of security awareness program can consume up to 20% of the organisation's security budget. However, once a robust level of security is established, that figure could be brought down to 10–15% [54]. Nonetheless, the cost of strengthening the security systems is preferred than having to lose an alarming amount of money to hackers.

In the era of digital transformation, individuals and companies face a variety of threats to data. Such dangers carry significant hazards; thus, organisations and businesses should approach them as part of their risk management plans [55]. Effective security systems must be employed in order to ensure safety and protection. To lower the likelihood of successful social engineering attacks, mandatory training and awareness measures must be implemented. Learning is a continuum that begins with awareness, progresses to training, and finally transforms into education. Basic education about the value of the information assets at their disposal has become imperative for an organization or individual to defend against it [56]. Since social engineering activities are primarily attacks based on human characteristics that are sophisticated and hard to detect, techniques to mitigate such attacks are imperative. Though it is difficult to put an end to all social engineering acts, decreasing the attacks' impact on individuals and companies can be possible with proper mitigation techniques [57]. Encouraging a positive corporate culture among the employees by the way of building corporate security culture is important for the success of such mitigation techniques. What is irrefutable is that human decisions are relative and thus cannot be presumed to bear capability. This is mainly because human judgments are subjective in nature irrespective of there being strong awareness of social engineering attacks and techniques [58]. Therefore, technology-based mitigation techniques like biometrics, sensors, artificial intelligence, and social honeypots are essential [59]. Such security strategies are crucial to the success of fighting social engineering actions.

REFERENCES

1. American Canadian writer of science fiction who was also considered to be the leader of the genre's cyberpunk movement.
2. John Perry Barlow, a cyberspace activist who sought to protect the rights and freedoms of individuals in the virtual space, published a paper on 'A Declaration of the Independence of Cyberspace' followed by the passage of Communications Decency Act of 1996.
3. Kalnin SR, Purin SJ, Alksnis G. Security evaluation of wireless network access points. Appl Comput Syst. 2017; 21: 38–45. Available at https://www.sciendo.com/article/10.1515/acss-2017-0005
4. 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. 2016 Apr 9–10; 1–6. Available at https://ieeexplore.ieee.org/document/7502270
5. An epic poem in 24 books that was traditionally attributed to the presumed Greek poet Homer.
6. Britannica. Trojan horse. [Online]. Available at https://www.britannica.com/topic/Trojan-horse
7. American computer security consultant, author, and convicted hacker.

8. Gaudin S. (2002). Social Engineering: The human side of hacking. [Online]. Earth web. Available at http://itmanagement.earthweb.com/secu/article.php/1860
9. Federal Trade Commission. (2006). Fraud Report for 2006. [Online]. Available at http://www.ftc.gov/opa/2006/01/topten.shtm
10. Lemos R. (2006). Survey: Identity theft hits three percent, Security Focus. [Online]. Available at http//www.securityfocus.com/print/brief/177
11. Arana M. How much does a cyberattack cost companies? Open Data Security. 2017; 1–4.
12. 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. 2018 Jun 3–6; 1–5. Available at https://ieeexplore.ieee.org/document/8417879
13. Orin Basu (2022). Two months of 2022 saw more cyber- crimes than entire 2018: Why e-fraud is a ticking time bomb. [Online]. Available at https://zeenews.india.com/technology/two-months-of-2022-saw-more-cyber-crimes-than-entire-2018-why-e-fraud-is-a-ticking-time-bomb-2458733.html
14. Mahender Singh Manral (2021). When trouble calls: Behind Delhi's call centre scam duping US citizens. [Online]. Available at https://indianexpress.com/article/cities/delhi/when-trouble-calls-behind-delhis-call-centre-scam-duping-us-citizens-7520358/
15. Vivek Trivedi. (2021 Dec 31). Online Fraud of More Than Rs 51 Cr in Last 5 Years in MP, Cyber Cheats Embezzled Rs 38 Cr in Lockdown. [Online]. Available at https://www.news18.com/news/india/online-fraud-of-more-than-rs-51-cr-in-last-5-years-in-mp-cyber-cheats-embezzled-rs-38-cr-in-lockdown-4613105.html
16. The Hindu. (2021 Sep 15). India reported 11.8% rise in cyber- crime in 2020; 578 incidents of 'fake news on social media': Data. [Online]. Available at https://www.thehindu.com/news/national/india-reported-118-rise-in-cyber-crime-in-2020-578-incidents-of-fake-news-on-social-media-data/article36480525.ece
17. Turner T. (2005) Social Engineering–Can Organizations Win the Battle? [Online]. Available at http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_Can_Organizations_Win.pdf
18. 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. 2017 Oct 18–20; 1–6. doi: 10.1109/CHILECON.2017.8229528.
19. Customer Data: Designing for Transparency and Trust [Internet]. Harvard Business Review. 2015 [cited 2023 Jan 20]. Available from: https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.
20. Hadnagy C. Social engineering: The art of human hacking. Indianapolis: Wiley Publishing, Inc; 2011. Available at http://proquest.safaribooksonline.com/book/networking/security/9780470639535
21. Thompson STC. Helping the hacker? Library information, security, and social engineering. Inf Technol Libr. 2006; 25(4): 222–225. Available at http://search.proquest.com/docview/215828364
22. Allsopp W. Unauthorised access physical penetration testing for IT security teams. Chichester, West Sussex, UK: Wiley; 2009.
23. Mitnick K, Simon W. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing, Inc.; 2002.
24. MacDougall S. (2012). Social engineering threats & countermeasures in an overly connected world [Online]. Available at https://media.blackhat.com/ad12/MacDougall/bh-ad-12-social-engineering-threats MacDougall-Slides.pdf
25. Supra note 23.
26. Be'ery T. New tool enables the automation of social engineering attacks on Facebook. Software World. 2011; 42(6): 23.
27. Timm C, Perez R. Seven deadliest social networks attacks. Boston: Syngress/Elsevier; 2010.

28. Brian Prince. (2009). Using Facebook to Social Engineer Your Way Around Security. [Online]. E Week. Available at https://www.eweek.com/security/using-facebook-to-social-engineer-your-way-around-security/
29. Charles Snyder. Defense against Social Engineering. Handling Human Hacking-Creating a Comprehensive Defensive Strategy Against Modern Social Engineering. Thesis. USA: Liberty University; 2015. Available at https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1510&context=honors
30. NYU Tandon School of Engineering. (2017). Tricking the Eye to Defeat Shoulder Surfing Attacks. [Online]. Available at https:// engineering.nyu.edu/news/tricking-eye-defeat-shoulder-surfing-attacks#:~:text=And%20while%20there%20are%20no,a%202017%20study%20of%20shoulder
31. Granger S. (2006). Social engineering reloaded. [Online]. Available at http://www.securityfocus.com/print/infocus/1860
32. Peotta L, Holtz MD, David BM, Deus FG, De Sousa RT. A formal classification of internet banking attacks and vulnerabilities. Int J Comput Sci In Technol. 2011; 3(1): 186–197. Available at http://www.airccse.org/journal/jcsit/0211ijcsit13.pdf
33. Business Email Compromise (BEC) [Online]. Proofpoint. 2021 [cited 2023 Jan 20]. Available from: https://www.proofpoint.com/us/threat-reference/business-email-compromise.
34. Verizon. (2021). Data Breach Investigations Report (DBIR) – 2021. [Online]. Available at https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-DBIR-2021.pdf
35. Verizon. (2020). Data Breach Investigations Report (DBIR) 2020. [Online]. Available at https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-DBIR-2020.pdf
36. Symantec. (2019). Internet Security Threat Report (ISRT) for 2019. [Online]. Available at https://www.phishingbox.com/downloads/Symantec-Security-Internet-Threat-Report-ISRT-2019.pdf
37. Verizon. (2019). Data Breach Investigations Report (DBIR). [Online]. Available at https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-DBIR-2019.pdf
38. Express. (2013 Sep 18). Dumpster Diving and Identity Theft. [Online]. Available at https://expressrecyclingandsanitation.com/2013/09/18/dumpster-diving-and-identity-theft/
39. 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. 2017 Oct 12–14; 25–34. Available at https://ieeexplore.ieee.org/document/8250331
40. CISA. (2021 Aug 31). Alert (AA21-243A): Ransomware Awareness for Holidays and Weekends. [Online]. Available at https://www.cisa.gov/uscert/ncas/alerts/aa21-243a
41. Steve Alder. (2020 Feb 13). Ransomware Attacks Have Cost the Healthcare Industry at Least $157 Million Since 2016. [Online]. HIPAA Journal. Available at https://www.hipaajournal.com/ransomware-attacks-have-cost-the-healthcare-industry-at-least-157-million-since-2016/
42. Cheating: Section 415 in The Indian Penal Code. Available at https://indiankanoon.org/doc/1306824/
43. Making a false document. Section 464 in The Indian Penal Code. Available at https://indiankanoon.org/doc/1745798/
44. Computer related offences: Section 66 in The Information Technology Act, 2000. Available at https://indiankanoon.org/doc/326206/
45. Punishment for cheating by personation by using computer resource': Section 66D in The Information Technology Act, 2000. Available at https://indiankanoon.org/doc/121790054/
46. Act to apply for offence or contravention committed outside India. Section 75 in The Information Technology Act, 2000. Available at https://indiankanoon.org/doc/576992/
47. Protected system: Section 70 in The Information Technology Act, 2000. Available at https://indiankanoon.org/doc/1680277/

48. Indian Computer Emergency Response Team to serve as national agency for incident response': Section 70B in The Information Technology Act, 2000. Available at https://indiankanoon.org/doc/80680324/
49. CSK C-I. Cyber Swachhta Kendra [Internet]. Csk.gov.in. 2023 [cited 2023 Jan 20]. Available from: https://www.csk.gov.in/.
50. Ibid
51. National Association of Software ... vs Ajay Sood and Ors. 119 (2005) DLT 596, 2005 (30) PTC 437 Del.
52. Achin Sharma And 2 Others vs State of U. P. And 2 Ors. Criminal Misc. Writ Petition No. - 5755 of 2020.
53. Gagan Harsh Sharma and Anr vs The State of Maharashtra and Anr. Criminal Writ Petition NO.4361 OF 2018.
54. McBride P. (2000 Nov 9). How to spend a dollar on security. [Online]. Computerworld.
55. Osuagwu E, Chukwudebe G, Salihu T, Chukwudebe V. Mitigating social engineering for improved cybersecurity. Proceedings of the IEEE Conference on Cyberspace, Abuja, Nigeria. 2015 Nov 4–7; 91–100.
56. Okenyi Peter O (CISSP and CISM), Owens Thomas J (CEng and C Math). On the Anatomy of Human Hacking. Inf Syst Secur. 2007; 16(6): 302–314. Available at https://www.tandfonline.com/doi/pdf/10.1080/10658980701747237
57. Nagrath P, Aneja S, Gupta N, Madria S. Protocols for mitigating blackhole attacks in delay tolerant networks. Wirel Netw. 2016; 22(1): 235–246.
58. Hadlington L. The "human factor" in cybersecurity: Exploring the accidental insider. In: Psychological and Behavioral Examinations in Cyber Security. Hershey, PA, USA: IGI Global; 2018; 46–63.
59. Zulkurnain AU, Hamidy AKB, Husain AB, Chizari H. Social engineering attack mitigation. Int J Math Comput Sci. 2015; 1(4): 188–198.

