International Journal of Scientific Engineering and Science
Volume 7, Issue 9, pp. 16-20, 2023. ISSN (Online): 2456-7361

Impact of Teaching Adolescents Social Engineering on Social Media

Ahmed Bukhari[1], Sameer Alqahtani[2], Mohannad Alharbi[3], Abdulaziz Almalki[4], Mohammed Bukhari[5]
[1,2,3]Information Science, University of North Texas, Denton, TX
[4]Emergency Management and Disaster Science, University of North Texas, Denton, TX
[5]Computer Engineering, Al Baha Private College of Science, Al Baha, Saudi Arabia
Email address: ahmed.bukhari@unt.edu

I. Introduction

Social engineering has been identified by Wright (2014), as the engagement of social influence, cultural settings, as well as psychological ploys to facilitate computer consumers with a channel to aid computer hackers in attempting the activities or application of computers systems or connectivity. Social engineering is regraded to be amongst the critical vibrant weapons in the storage room of hackers and malicious code enumerators since it is not complex requesting a person for details which could aid in tracing the passwords than going along way hacking his/her systems or rather accounts. In spite there being some effort by institutions in improving consumer's awareness by doing the sensitization concerning the data security, social engineering has been widely and successfully asserted in spreading malwares in the internet and corrupting number of computer systems (wright, 2014).

By 2007 social engineering techniques was published as the foremost technique applied by intruders in committing e-crimes, however, suspected consumers maintain the stand of being predominant for the undertakers of malicious data.

Social media on the other side like Facebook amongst others was described by Horowitz and Lucero, (2017) as a data mining goldmine over the reliable sources of personal data published in the websites, this is fundamental especially where a number of internet users are operating their devices in default privacy settings (Gregor and Lee-Archer, 2016). The frequent adoption of social media platforms by young generation especially those at adolescent's stage has rampantly resulted to lose of information by companies due to malicious activities undertaken by professionals using the adolescents. The information out there is on data leakage which undermines the compliance policies, user's confidence as well as the competitive benefits.

Having been provided with this detail information pertaining the social engineering and the significant description of social media aspects and concepts, the key aim of this research is sourcing for critical literature review evidence on impacts of teaching adolescents social engineering in social media.

Currently, almost every small and medium or large enterprises are focused on the aspects of data security in their firm and measures through which they can protect huge volume of data by devising paramount and critical measures in seeing that data in the server does not get in anonymous hands. In companies, technical obstruction is not the significant resultant factor to social engineering. The "personnel" through adolescents now days has been detailed by Hur and Gupta, (2013) as the key driving force to cyber securities in organizations and in other small entities. Currently, the adolescents are the targeting groups in extracting sensitive data to hackers for malicious activities through social engineering process. Social engineering from the scrutinized literature peer reviews, it is an element of art used by cyber criminals manipulating the psychology of individuals particularly in this case through the use of the adolescents in getting access to sensitive data.

Social engineering through adolescents have recently registered the foremost success rate in comparison to other cyber insecurity since it diminishes the channel to information security system (wright, 2014). Social engineering activities cannot be easily tracked by the critical security technological packages as well as the hardware since it majorly operates by manipulating man's psychology, and not the established security systems. Particular well known social engineering malwares in the past years that majorly targeted the personnel are such as; Red Pulse attack, 2017; Red Pulse, was the foremost initial Coin Offering (ICO) on the NEO (Gregor and Lee-Archer, 2016). In November 2017, cyber attackers engaged in malicious activities through the use of fake Twitter account in influencing people especially the youths on Phishing internet sites(redpulsetoken.com). making a deal to offer substantial tokens to viewers for a minimal period (Egloff, 2018). By requesting people to key in their private data of their NEO wallet to earn the bonuses, where over this, criminals got away with victim's funds.

II. Method

To collect a sufficient resource that assist this paper in the critique processes, Academic Search Complete database has been used from the library of UNT. There are the two terms has been used "Social Engineering" and "Social Media". Results was around 120 sources. After filtering the search to include just published sources from 2013 to 2021, results changed to 91 sources. Then specifying the type of the source to be a full text, recall was 41 sources. Consequently, abstracts of these 41 sources have been read to make a final decision if the source could be appropriate for this topic or not. Finally, there were 20 sources could be helpful and matching the topic which have been used in this paper. Moreover, some old sources that assist this paper in introducing the social engineering and the history of creating the activity theory.

III. Literature Review

From the literature articles provided for the study, this research will conduct critical literature analysis on the following subjects; Trends in social engineering malware through the adolescents, common infiltration channels, phases of social engineering, categories of social engineering attacks, prevention and detection measures, methodological strengths and weaknesses then research gap which will be underlined in recommendations for future research then conclusion of the critical literature analysis.

IV. Critical Literature Analysis of Social Engineering

A. Trends in Social Engineering Malware Alongside the Adolescents

Malware is an overall phrase used when referring to viruses, worms and Trojan horses among many more (Egloff, 2018). The reason why this tactic is deemed professionally fit and hard to trace in future, it is due to its nature of operation where it involves technological counter techniques and physiological settings especially the young generation “adolescents” in spreading the malware. The malicious subjects are transformed and spread through certain ways, which has progressively developed while technology advancement keeps growing (Hur and Gupta, 2013).

Consequently, the psychological strategies applied by hackers through kids are as well progressively developing (Lehto, 2013). Instead of depending on anecdotal data, the study sought to speculate on effects of adolescents teaching on social engineering malware theoretically through social media. The data in research is drawn from the variety of literature sources with consideration to social engineering malware and the concepts attached thereto. The primary data source below is from the published evident articles in line with the theme of the study which also facilitates independent directives on protrusion of viruses and anti-virus subjects.

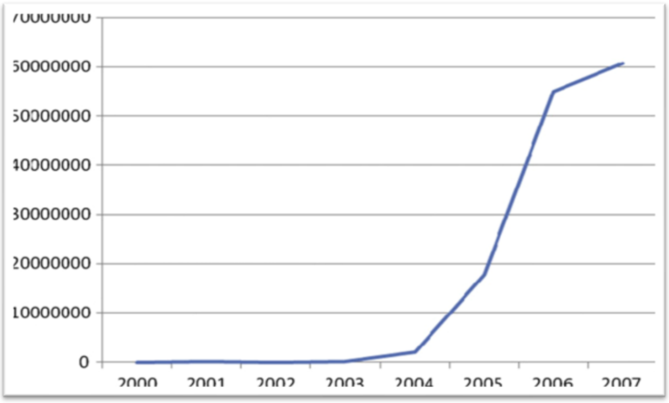

Fig. 1 Reported Security incidents that applied social engineering strategies.

The analysis in this article concerning the malware attack presents certain steps the hackers use in influencing the adolescents to carry out their self-interest activities in the internet. This is what makes the process successfully. Employing technical data for this case of malware, the study constructed a profound list of activities undertaken by hackers to successfully carry out their activities. The literature established four major forms; influence an adolescent victim to activate it; destabilize protective techniques; executive the process, and finally proliferate the exercise. The data in the above diagram represents a cross-section of degree of social engineers whenever they manoeuvre the systems. The diagram has detailed the full course of security incidences as techniques applied by hackers. From the figure, the diagram shows that in 2000, the total number ranged at 0, being a flat rate trend till 2003 when the trend started to rise upto 2007 when the trend was too high and sharp as per the case Figure 2 below presents a flow chart that illustrates the procedure which the social engineering professional use in influencing the young generation to accomplish their mission through the dissemination of system.

Notably, not every social engineering attacker dully follow the processes underlined in figure 2, however, the flowchart presents a general layout with steps that results to successful malware attack to systems. Literature reviewed by Hur and Gupta, (2013) presents that the malware employs a number of contexts like internet sites, social media platforms, electronic mails among others, this is purposely to spread the viruses to user systems. These techniques are engaged alongside other strategies which influence and manipulate the minds of young kids into opening certain infected links, this is made successfully by teaching the adolescents how to go about it without them knowing the consequences attached over it (Dwan, 2001). The actions detailed above results to successful execution and activation of malware spread.

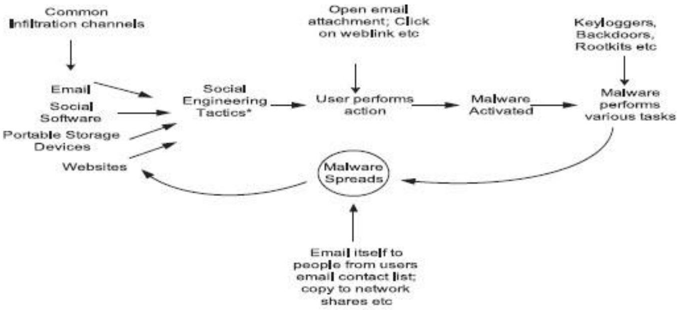
Common Infiltration channels
Email
Social Software
Portable Storage Devices
Websites
Social Engineering Tactics*
Open email attachment; Click on weblink etc
User performs action
Malware Activated
Keyloggers, Backdoors, Rootkits etc
Malware performs various tasks
Malware Spreads
Email itself to people from users email contact list; copy to network shares etc

Fig. 2. Steps taken by malware to infiltrate a system.

B. Privacy Concerns

Social media users interest on aspects of privacy kicked off very long time ago. Subjects of data obstructions have annoyed a number of users which to an extend direct them upon re- considering their interconnections to social media and the safety asserted in their personal sensitive data (Venkatachary, 208). One of the literature articles reviews by Baruh et al., (2017) pinpointed that there was once a narrative of certain consultancy Cambridge analytica which went ahead and started exposing or rather inducing the sensitive information of about 50 million Facebook subscribers to impact the 2016 American presidential campaign. This context and others have rapidly compromised the public trust and made majority of websites subscribers to consult their conscience whether they had lost control against their personal data. With consideration to a research undertaken by Pew Trust, more than 85% of social media consumers file complains concerning the commercial undertakings and the promoters reaching and applying their online posts for other personal selfish gain (Parker, 1993). This emerging privacy concerns have called for advocacy to zero in effective regulations. Furthermore, they filed their complaint against firms rendered the duty to protect their data from being exploited and ordered those underlying firms to be dully speculated. Baruh et al., (2017) coined in his literature article that having the current internet privacy cases and concerns, proficient cyber security personnel will have a fundamental role to play in seeing that personal data for online consumers do not get into the wrong hands. Those with interest of earning the required skills must be equipped with ultimate cyber security knowledge would work smart to get the advanced bachelor's in cyber security management.

What really brings fear to social media consumers? Are their claims genuine? These questions were addressed in the literature reviewed article by Teodorescu, (2015) where he asserted that ideally, the above claims or rather concerns prop-up from the ubiquitous ground of social media in individual's day to day operations. 45% of the global consumers engage social media in most of their operations. This shows a staggering 4 billion personnel interlink to other sites in social media, this is with regards to information gained by Hootesuite and published by Golin, (2012). These aspects can subject consumers to vulnerability in a number of ways. Whenever individuals' data is exposed in the hands of wrong personnel, the results or repercussion can be so alarming. In reference to the Pew Trust, 14% of Americans have experienced in the hard way where their online sites have been undermined and controlled by the anonymous, this is according to a research by Golin, (2012).

Hacks of that nature can encourage the stealing of data and subject users to services which prompt them to malware, amongst the subsequent aspects. Generally, social media sites, that scrutinize and archive huge volume of sensitive user's data with the aid of limited public oversight, will act as significant tools for curbing the contemporary issues around by perpetrators with fraud objectives and theft of personal information of internet subscribers by Teodorescu, (2015). Another contemporary concern, underlined by Cambridge Analytical obstruction of Facebook data system, imparted on ways through which evil minded personnel speculates user's information off the social media sites and any other areas of concern where they use that information for insignificant personal gains (Baruh et al., 2017). For instance, the Russian operation internet Research Agency is reported to have misused their role by compromising the U.S presidential election of 2016 through internet websites by spreading misinformation which awakened the mistrust and conflict in the states.

C. Relationship between Social Engineering and Big Data

First, it interlinks with firms' directors for instance Active Directory and social media sites such as Linkedln to track the connectivity amongst the labor force, and subsequent external contacts. Bell refers to this as the "real org chart" (Olshannikova et al., 2017). Hackers can utilize this data in identifying individuals they plan to impersonate as they try to scam workers. After which AVA consumers can device custom phishing motions, both through the electronic mails and Twitter, to track the comments of employees. This context introduces thereby a white hat instrument, which is the setting of social engineering penetration examination. This comprises of two areas of interest.

Apparently, research by Banda et al. (2019) shows that intelligent hackers are to date engaging this kind if instrument in finding the profound people to get in touch with, form means of reaching them, and to scrutinize ways of engaging them without any suspicious attempts for them to respond to their interests. The rule of thumb anybody must realize is that at least 70% of the moment are being utilized by hackers through the tools devised by scholars in undertaking the penetration evaluation (Olshannikova et al., 2017). Having in mind that these subjects inhibiting the global space through certain platforms such as twitter, facebook, and many more, a number of them may not be just the next entry to "click farm"-particular a number of them may be click bait for hackers to realize the type of person you are (Thakur et al. 2019). Second, this should ring to every consumers' mind that there is a high chance of them being tricked by hackers. The specific certain strategies detailed in the literature article reviewed is one amongst the obedience to authority, pitting a person's skills of whatever is deemed right and wrong against the personnel the regard as an authority figure (Olshannikova et al., 2017). Although not relatively unrealized as portrayed in other settings, the know-how that we can be tricked in this manner must be very sobering. To position this in alternative ground, it is all about the conjunction of big data era which hackers use in finding out about people, who they offer utmost respect, including whatever they assert their trust at, then utilize them as vulnerabilities to have them act in their own way or as per to their instructions or have trust with particular aspects, perspectives which are critical to review in mind compared to current switch's port count (Olshannikova et al., 2017).

D. Skills and Techniques of Social Engineers

Social engineering as described in this critical literature analysis is a cyber-security attack which take full control of security chain, employees data and even corporate server with view to gain or achieve some selfish interest (Kamenov, 2018). The personnel undertaking these steps apply so much complicated, trickery and physiological influence to make worker and their bosses to let out the sensitive data which could be applied by attackers to succeed in their plans. However, there are a number of ways these crises can be resolved, by understanding its chain and keep up with tight policies which will see that nobody surrender the information from the company or personal to the anonymous.

According the literature articles, Alam, (2017) published that social engineers use majorly phishing attack as the primary technique for sending messages, emails and websites as well as instant texting of employees find critical data from them or trick them through other online links which prompts the victim to click on and ask them to submit their information or after clicking they get attacked by malicious elements created by the social engineers. Phishing prompts attracts the victim's attention into emotional point through tricks from the perpetrators who pretend to be asking for help. This phishing techniques are accompanied by image, logos or special texts to skit the corporates identity, this technique normally make employees believe that the message is from the parent organization directing them to act in a certain manner, this could be crafted to sound like the message is send from the bank or other social official platforms. Majority of phishing messages apply the sense of urgency, making a victim to fear that if no necessary action is taken there will be a negative repercussion.

Another skill detailed by Caldwell, (2013) is that of watering hole technique, this comprise of launching or downloading malicious code from a legal site, which is popular to social media consumers who then become the target of the underlying attack. For instance, attackers may interfere with financial industry report platform, with knowledge that people who operate in finance sectors will easily visit the pages. The team usually prompt the victims to install a backdoor Trojan which enable the attackers to remotely take control of the victims' system.

Conclusively, the research literature article analysed by Caldwell, (2013) pin pointed that whaling technique is another but more superior than other skills available by social engineers, this skill is so critical to an extend that it only focuses on zero-day exploit by targeting the most sensitive and reliable information. For instance, a whaling attack might be undertaken against the managers, the tycoons, or network administrators. This technique is however much sophisticated compared to normal phishing attack. The social engineers undertake a meticulous analysis to device a text that will bring in a particular target to act upon their ploys. The send mails to workers pretending it is from the organization and demanding for certain sensitive information.

V. Theoretical Review

A. History of Activity Theory

This theory is also referred to as the implicit model of aging, normal model of aging, and lay model of aging. The theory as pointed by Alam, (2017) it suggests that profound aging takes place when older individuals remain active and keep up to social engagement with others. It draws the attention of aging as a process which is delayed while old subjects remain socially active. The activity model hence was implemented with view to provide feedback upon the disparity being experienced on the disengagement model.

The disengagement and activity model were initially the paired key theories which detailed aging in the early 1960's. the model was implemented by Robert J. Havighurst back in 1961. In 1964, Bernice Neugarten imparted that satisfaction among the old group relies on active maintenance of individual relationship and activities. This model presumes a significant correlation between activities and life contentment. One researcher provided that activities aid aged persons adjust to retirement, a norm referred to as "the busy ethic". The undertakings of the activity model provide that it oversights the disparities in health as well as economic which obstruct the capabilities for aging groups to participate in such undertakings. Consequently, particular old ages do not perceive the norm for new challenges.

Activity theory highlights some of the processes and aspects that the equilibrium which people develop while growing to be engaged in future. The model highlight further that aging people who undergo role loss will replace the latter roles with other constituents. The activity model is amongst the key three psychosocial theories that tells how individuals develop while aging. The other two psychosocial models are the disengagement theory, upon which the activity is brought to odds, and the progressive model that entails and highlights upon the activity model.

B. Activity Theory in Information Systems

Consequently, In the beginning of 20th century, activity theory has been adopted and utilized a lot by researchers whose papers about information systems. Vygotsky (1978), is the one of the pioneers that who applied and developed activity theory in the information systems field; also, he described the activity theory well in information science field. Vygotsky (1978), draws a diagram to illustrate the activity system. In summary, any activity needs a doer (subject), the doer has tools to do the activity within theses tools, doer can achieve the purpose of the activity (object). As a result, activity theory assists the activity of the social engineers within some tools to get their goals.

VI. Methodology

The methodology section is an important stage in each papers, so the success of the paper relies on the perfect technique of research methods. Interview with IT security experts would be a perfect idea to gather much significant information about social engineering, particularly social engineers' skills and techniques because employees of IT security department may be encountered such this issue, so their experience assists the paper to better introduce the social engineering for adolescents. In addition, the case study will be better assist this paper, especially if there are a group of adolescents.

A. Methodological Strengths and Weaknesses

Critical literature analysis has both its weaknesses and strengths. This method of data collection and analysis is deemed to provide thorough and general knowledge pertaining a particular theme of the study. The most fundamental area is that of enhancing one's information sourcing skills (which comprise of skills of scanning literature articles published in academic online platforms, scrutinizing skills to identify the only ideal literature resources for the study) (Shewell and Migiro, 2016). The other strength pointed by Schwab, (2006) is that this technique increases the capability for demonstrating critical analysis, this is, skills for establishing and analysing academic material sources with no bias.

Critical literature review has the most identified weakness of not facilitating the researcher with general information technique; especially in the selection and exclusion of literature articles, this is the drawback of the search method as well as the yield of the search procedures (Schwab, 2006). Another limitation is that this method does not give directives on how analysis was undertaken.

B. *Recommendations for Future Research*

A number of current literatures established the concepts underlying social engineering attacks and their remedies that target firms for breaching the scope of defence, influencing its workers to act in their will without knowing they are breaching their data safety. Even though there has been a profound increase in social engineering for corporates and people, very minimal research has been undertaken on social engineering attacks which is after personal sensitive data.

C. *Scholarly Significance*

The consequences of such malicious attack on people and corporates have not been covered in spite of the adversative ramification on financial and mental data of the individuals. This researcher focused on this gap by highlighting certain perspectives of social engineering attacks imparted on people with consideration to measures which can reduce or refute this contemporary issue. Hence, it’s recommendable for future research to consider measures which can be reliable in fighting social engineering attacks. The focus needs to be directed on educating youths and the adolescents on how to identify links purposed maliciously and that which plans to undermine their data security.

D. *Practical Significance*

After conducting this research paper, the researcher would like to recommend that idea: Adoption of a curriculum in the middle school to give those age group (adolescents) some background about social engineers to mitigate the risk of hacking adolescents. This curriculum could be kind of exercises in how to guess this kind of email may be suspicious, such a phishing, and so on, and this curriculum should highlight the important points for social engineering that related to sexual media to which they can through it hack adolescents' devices.

VII. Conclusion

The issues of social engineering attack have been rising and will keep increasing in the life to come. It has been evident that none of the critical security technology innovation can fully prevent the social engineering attacks. Attacks of such kind should be acknowledged that it does not only target the commercial entities but also individuals. After reviewing twenty sources that specified for social engineering, and findings indicate the bad impact of social engineering, particularly with adolescents.

References

[1]. Alam, F. (2017). Usage of data Data Mining Techniques for combating cyber security. International Journal of Engineering and Computer Science. https://doi.org/10.18535/ijecs/v6i1.31

[2]. Banda, R., Phiri, J., Nyirenda, M., & Kabemba, M. M. (2019). Technological Paradox of Hackers Begetting Hackers: A Case of Ethical and Unethical Hackers and their Subtle Tools. Zambia ICT Journal, 3(1), 40. https://doi.org/10.33260/zictjournal.v3i1.74

[3]. Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta-Analytical Review. Journal of Communication, 67(1), 26–53. https://doi.org/10.1111/jcom.12276

[4]. Caldwell, T. (2013). Plugging the cyber-security skills gap. Computer Fraud & Security, 2013(7), 5–10. https://doi.org/10.1016/s1361-3723(13)70062-9

[5]. Dwan, B. (2001). Nice Kids Need Cyber-angels. Computer Fraud & Security, 2001(7), 7. https://doi.org/10.1016/s1361-3723(01)00715-1

[6]. Egloff, F. J. (2018). Cyber mercenaries: the state, hackers, and power. Journal of Cyber Policy, 3(3), 467–468. https://doi.org/10.1080/23738871.2018.1523443

[7]. Golin, C. (2012). Impressions of Privacy in the Media: Does Greater Public Awareness of Privacy Concerns Influence Legislative Action? SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2204447

[8]. Gregor, S., & Lee-Archer, B. (2016). The digital nudge in social security administration. International Social Security Review, 69(3-4), 63–83. https://doi.org/10.1111/issr.12111

[9]. Horowitz, B. M., & Lucero, D. S. (2017). System-Aware Cyber Security: A Systems Engineering Approach For Enhancing Cyber Security. Insight, 20(3), 66–68. https://doi.org/10.1002/inst.12165

[10]. Hur, J., & Gupta, M. (2013). Growing up in the Web of Social Networking: Adolescent Development and Social Media. Adolescent Psychiatry, 3(3), 233–244. https://doi.org/10.2174/2210676611303030004

[11]. Kamenov, D. (2018). Intelligent Methods for Big Data Analytics and Cyber Security. Information & Security: An International Journal, 39(3), 255–262. https://doi.org/10.11610/isij.3921

[12]. Lehto, M. (2013). The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies. International Journal of Cyber Warfare and Terrorism, 3(3), 1– 18. https://doi.org/10.4018/ijcwt.2013070101

[13]. Olshannikova, E., Olsson, T., Huhtamäki, J., & Kärkkäinen, H. (2017). Conceptualizing Big Social Data. Journal of Big Data, 4(1). https://doi.org/10.1186/s40537-017-0063-x

[14]. Parker, D. B. (1993). Confidentiality of Information and Personal Privacy. Information Systems Security, 2(1), 13–17. https://doi.org/10.1080/19393559308551337

[15]. Schwab, D. P. (2006). Book Review: Research Methods for Organizational Studies. Organizational Research Methods, 9(4), 572–574. https://doi.org/10.1177/1094428106290197

[16]. Shewell, P., & Migiro, S. (2016). Data envelopment analysis in performance measurement: a critical analysis of the literature. Problems and Perspectives in Management, 14(3), 705–713. https://doi.org/10.21511/ppm.14(3-3).2016.14

[17]. Teodorescu, H.-N. (2015). Using Analytics and Social Media for Monitoring and Mitigation of Social Disasters. Procedia Engineering, 107, 325–334. https://doi.org/10.1016/j.proeng.2015.06.088

[18]. Thakur, K., Hayajneh, T., & Tseng, J. (2019). Cyber Security in Social Media: Challenges and the Way Forward. IT Professional, 21(2), 41–49. https://doi.org/10.1109/mitp.2018.2881373

[19]. Venkatachary, S. K., Prasad, J., & Samikannu, R. (2018). Cybersecurity and cyber terrorism - in energy sector – a review. Journal of Cyber Security Technology, 2(3-4), 111–130. https://doi.org/10.1080/23742917.2018.1518057

[20]. Vygotsky, L. S. (1978). Mind in Society: the Development of Higher Psychological Processes. Cambridge, MA: Harvard University Press. ISBN 978-0-67457629-2.

[21]. Wright, O. (2014). Social Engineering. Engineering & Technology Reference. https://doi.org/10.1049/etr.2014.0013