Including Human Behaviors Into IA Training Assessment: A Better Way Forward!

Henry Collier
Norwich University, Northfield, USA
hcollier@norwich.edu

Abstract: Few can argue against the reality that humans are the weakest link in cybersecurity, and Social Engineers work very hard to take advantage of this human weakness. Many cybersecurity practitioners believe the only way to solve this problem is through a technical solution; however, this solution is elusive because humans are still in control and can circumvent these technical measures. In cybersecurity, the human is the critical component of the human firewall, and it is going to take a multi-disciplinary approach to solve the human problem. The human firewall is the first line of defense for cybersecurity. Historically, the primary solution to the human problem has been the Information Awareness training program, designed to teach the end-user about the risks and assess their risk. The biggest problem with the information awareness training program is that it does not modify behavior. Cybersecurity practitioners need to understand better the human firewall and how it can be strengthened. It is necessary to understand how the human makes security-minded decisions, how these decisions affect the cybersecurity decision-making process, and if there is a way to assess a person's susceptibility level more precisely when working to strengthen the human firewall. Humans are multifaceted, complex beings influenced by both internal and external factors. The most significant internal factor that affects a person's decision-making process is behavior, while Social Media is one of the most significant external factors that impact a person's decision-making capacity. This study presents a new method of assessing a person's susceptibility to cybercrime by including behavioral and social media usage factors into a Dynamic/Adaptable information awareness training assessment tool. This study shows that including human behaviors and social media usage behaviors into an Information Awareness (IA) training assessment tool produces a more precise measure of a person's accurate susceptibility level.

Keywords: cybersecurity, human behaviors, susceptibility, social engineering, information awareness

1. Introduction

Cybersecurity incidents can be classified as either technical or non-technical attacks (McIlwraith, 2006) (Schroeder, 2017). The critical difference between a technical and a non-technical attack is how the threat actor works to access the data on the computer or network system. The technical attack targets a weakness in a system, whereas the non-technical attack targets the human using the system (Ariu et al., 2017). Both forms of cyberattack commonly have one of two desired outcomes, either gaining the attacker profit or causing the target to suffer a service disruption (McIlwraith, 2006) (Schroeder, 2017) (Hallas, 2018). Technical attacks are conducted by malicious outsider threats seeking to take advantage of a technical weakness within a system. The non-technical attacks, also known as social engineering attacks, typically target the individual and work to get the individual to allow the malicious threat actor into their system, making the user a non-malicious insider threat (Ariu et al., 2017). Most social engineering attacks have a technical component to them, but their primary attack surface is the person, not the equipment (Ariu et al., 2017)(Hallas, 2018) (Collier, 2020)(Hadnagy, 2018). Many individuals in the cybersecurity industry want to find a technical means of preventing social engineering attacks. Unfortunately, technical defences can only go so far in preventing social engineering attacks because the attack surface is the human, and humans are complex, multifaceted beings that behave in ways that cannot always be predicted (McIlwraith, 2006)(Schroeder, 2017) (Hadnagy, 2018)(Ayates & Conolly, 2003). For a technical measure to be effective, it needs to apply logic to a situation consistently and manipulate the outcome based on this logic; humans muddle this logic by being non-logical beings.

There is no technical measure that can stop a human from making a poor information security decision, and therefore more needs to be done to mitigate the risk the human creates (McIlwraith, 2006)(Schroeder, 2017 (Wilcox & Bhattacharya, 2019) (American Psychological Association, 2021). The only way to mitigate this problem is to conduct research around the human firewall and better understand the decision-making process, cognition, and what influences a person's decision-making process.

If humans were entirely logical beings and decisions were made logically, without emotion, the risk posed would be significantly lower than it currently is. The human decision-making process is not entirely logical; rather, it is affected by various behaviours that impact the person's mindset and successively bear upon the decision's effectiveness (Ayates & Conolly, 2003) (Bada et al., 2019). The current method of defending against social engineering attacks is the information awareness (IA) training and assessment program. The IA program is designed to provide the end-user information about cyber risks and then assess the person's risk to an organization (Schroeder, 2017). The problem with this method is that the current information awareness training and assessment model does not consider the behavioural aspect of the person being assessed and therefore does not calculate an accurate measure of a person's risk (McIlwraith, 2006)(Ayates & Conolly, 2003). Current IA training assessments consist of a multiple-question quiz at the end of training. Unfortunately, many of the answers to these questions are readily available on the Internet. Many individuals will seek out these answers to help ensure they meet the minimum grade requirement of 70% (Schroeder, 2017). This process shows that most end users will have a similar susceptibility level calculated for them (Collier, 2021).

This paper presents the results of a mixed qualitative and quantitative study that investigated how human behavioural traits and social media usage behaviours could be used to measure a person's susceptibility level more accurately. This study consisted of a comparative analysis that compared the KnowBe4 information awareness training and assessment program results and a new Dynamic/Adaptable IA training assessment tool. The Dynamic/Adaptable IA training assessment tool consisted of information security questions and behavioral/social media usage questions making the tool's approach new and unique. The KnowBe4 tool is one of the top IA training and assessment programs currently available, and as of the first quarter of 2021, KnowBe4 has over 39,000 customers worldwide (KnowBe4, 2021). In no way is this paper meant to denigrate the KnowBe4 tool; instead, this paper intends to show a different way to assess a person's susceptibility that could prove fruitful in the cybersecurity industry.

2. Humans and their behaviours

Every end-user is a complex and multifaceted human being that holds the key to the success of an organization's information security posture. End users make decisions every day to help protect an organization from cyber threats or open the door to vulnerability and compromise (McIlwraith, 2006). On the surface, the decisions themselves appear to be simple; however, each decision is almost as complex as the person making the decision (Mackinnon & Wearing, 1980). A person's knowledge and logic certainly impact decisions, but they are also influenced by the person's behaviours which significantly increase the intricacy of the decision (Edwards, 1954)(Henderson & Nutt, 1980). Behaviour is the response of an individual to stimuli that can be external or internal (American Psychological Association, 2020). Research has shown that human behaviour results from various interconnected factors that work alone and together, to influence how a person responds to stimuli (UK Parliment, 2020). Understanding which behaviours impact the information security decision-making process is vital as efforts to improve the human firewall continue.

This study was based on the premise that behaviours could be used to improve information awareness training assessment. For this to occur, it was necessary to identify which behaviours have a link to susceptibility. It was essential to identify a list that could be used as a starting point to make this identification. A list of behavioural traits was obtained from an earlier study conducted by MIT's "List Man," Peter Gunkel called The Human Kaleidoscope. Gunkel (Gunkel, 1998) developed a list of 638 traits for his study, where he was looking to see if there were limits on human variability, diversity, and psychogenesis. The evaluation of the behaviours was purely qualitative and did leave room for improvement. The intent of this study was not to identify the behaviours related to susceptibility with absolute mathematical certainty but rather to determine if it is possible to better assess a person's susceptibility by including behavioural factors in the evaluation process. The extensive list of traits was reduced to a shortlist that could be more practically incorporated into an information security assessment tool. A small focus group consisting of a cybersecurity professional, two undergraduate psychology students, and a graduate psychology student was created for this study to assess the traits and specify which traits likely impact a person's susceptibility level. The focus group started with 234 positive traits, 292 negative traits, and 112 neutral traits. Tables 1, 2, and 3 are examples of the three groups of traits from the study.

Table 1: Positive trait example (Collier, 2021) (Collier, 2020)

Accessible	Calm	Dedicated	Fair	Gallant

Table 2: Negative trait example (Collier, 2021) (Collier, 2020)

Aimless	Desperate	Egocentric	Faithless	Gullible

Table 3: Neutral trait example (Collier, 2021) (Collier, 2020)

Absentminded	Busy	Competitive	Emotional	Emotional

The trait assessment process resulted in a revised list of 128 behavioral traits that more closely represented traits that impact a person's decision-making process based on the trait's characteristics. The 128 traits were chosen based on the likelihood that the trait would not only influence the decision-making process but more significantly result in a poor information security decision.

The 128 traits were then grouped based on how similar the traits were. An example is grouping traits like arrogant, conceited, and egocentric, which represent a state of mind where a person is likely overconfident in their skills. Someone who is overconfident is at risk of becoming a victim of social engineering because they do not believe it will ever happen. Not being aware of the risk of becoming a victim of social engineering could lead to the person becoming a victim of social engineering by making a poor information security decision.

After grouping the list of behavioural traits, the next step was to determine a set of questions that would reflect the underlying behaviour that could lead to a cybersecurity incident. The focus group again took on this qualitative task and developed forty questions related to the eighteen groups of traits. An example of the questions and the associated traits is in Table 4. As can be seen, if a person answers yes to the question, then they likely meet the definition of at least one of the traits. For example, the trait Trusting implies that the person exhibiting the trait tends to believe in someone's honesty or sincerity. Social engineers work very hard to take advantage of their victim's trusting nature (Luo et al., 2011) (Mitnick & Simon, 2002). From an information security perspective, trust needs to be earned, not fully awarded, when you first meet someone. The concept of "trust but verify" promotes the idea of believing what you have been told is accurate but also questioning what you were told and working to verify its truthfulness, rather than simply accepting it blindly as the truth. Information security professionals would rather have an end-user question something than merely take it at face value. In contrast, social engineers would rather have the end-user take it at face value and become their victim.

Table 4: Behavioural question and trait example (Collier, 2021) (Collier, 2020)

Question: Do you believe that people are generally good and trustworthy?
Traits: Gullible, Impressionable, Imitative, Trusting, Dependent, Guileless, Naïve, Soft.

Social engineers develop attacks that target a person's emotions or trigger a particular behavior. For example, social engineers will build a level of urgency in their attacks to trigger an immediate emotional response rather than a thought-out response. A form of attack known as CEO-Fraud is an example whereby an attacker pretends to be an executive of an organization and sends an email to a subordinate ordering them to send money straight away to cover an overdue invoice (Kemp, 2016). The sense of urgency that the attacker imposes in their email prompts the employee to send money to the account information in the phishing email, rather than simply checking with the executive, even when the executive may be in the next room (Kemp, 2016). If the concept of "trust but verify" is applied to this type of attack, the attack's success rate would be significantly reduced, if not eliminated.

The 21st century adds a new level of complexity to the end user's behaviour that has not existed before—Social Media. Social Media was developed to allow individuals to remain connected with others in their familial or social circles, especially when physically displaced. The concept of Social Media supports the social nature of humanity. Unfortunately, social engineers have embraced Social Media and work to use the data held within its digital walls as a goldmine of information (Hallas, 2018) (Collier, 2020). Social influences impact an individual's behaviours, which further impact the security-minded decision (UK Parliment, 2020). There is a constant barrage of social forces bombarding people through Social Media. The continuous connection to Social Media does not allow a person to digest what is happening and then make a conscious decision but instead promotes the instant, knee-jerk reaction that is frequently influenced by emotions and behavioral traits. Add to this how Social Media allows people to connect with others worldwide without ever actually meeting them. Before Social Media, the idea of a group of friends might include 10-20 individuals. Still, with the introduction of Social Media, this group of people called "friends" increases and can do so exponentially. Now, it is possible to have hundreds, thousands, and even millions of so-called friends following you on Social Media (Vishwanath, 2014) (Kayes & Iamnitchi, 2017). This behaviour opens the door to social engineers who will connect with you on social media to work to develop more directed social engineering attacks (Hallas, 2018) (Vishwanath, 2014) (Kayes & Iamnitchi, 2017) (Tsikerdekis & Zeadally, 2014). Before the invention of Social Media and Social Media scraping tools, the reconnaissance process was very labour-intensive, so a social engineer would be limited to targeting a small number of people at a time (Postnikoff & Goldberg, 2018). Now social engineers can gather information on hundreds of potential targets and then develop an increased number of attacks, which increases their likelihood of being successful (Wilcox & Bhattacharya, 2019) (Gharibi & Shaabi, 2012) (Weir et al., 2011).

The only way to decrease the success rate of the social engineer is by improving the end user's information security decision-making process. Improving how end-users make information security decisions requires changing how end users are trained and assessed. The current information awareness (IA) training models are based on the idea of simply presenting the end-user with the information, not modifying their behaviour (Schroeder, 2017). Identifying behavioural traits related to susceptibility led to developing a new Dynamic/Adaptable IA Training Assessment Tool for this study. The development of this tool is the first step in validating the concept of including behavioural and social media factors in determining a person's accurate susceptibility level.

3. Dynamic/adaptable assessment tool

The Dynamic/Adaptable IA Training Assessment Tool created for this study was developed to incorporate behavioural and social media usage factors in determining a person's susceptibility level. The tool was designed to improve current information awareness training assessment tools in two distinct ways. The first way is by including human behaviours and social media usage questions which gauge a person's behavioural risk of becoming a victim of social engineering. The second way is by incorporating an adaptive assessment approach to evaluating a person's information security knowledge level. The results of both parts of the tool are then fed into a susceptibility algorithm designed for this study. The tool results are then compared to the results of the KnowBe4 IA Training program completed by the same individuals to determine if there is a statistically significant difference between the two tools.

The Dynamic/Adaptable IA Training Assessment Tool was built around three unique but connected components. The first is the participant registration section, where the participant inputs their demographic information and KnowBe4 score. A unique identification number is assigned to each user to ensure anonymity. For the data from the behavioural and social media section to be valid and usable, the participants needed to answer the questions honestly; therefore, participant anonymity was a must. If participants felt their answers would come back and haunt them, they might answer the questions with a less truthful answer. Anonymity was guaranteed, and not even the researchers could correlate a participant and a specific data set.

The second section of the Dynamic/Adaptable IA Training Assessment Tool is the behavioural questionnaire. The user is presented with forty behavioural questions related to the 128 behavioural traits identified during this study's qualitative portion. The behavioural questions used a Likert scale, and each response was assigned a value from 10 for least risk to 50 for most risk. Upon completing the behavioural questionnaire, the combined total value of the responses is then put into variable Hb for use in the susceptibility algorithm.

Upon completing the behavioural trait-based questions, the individuals are presented with 30 questions related to social media behaviours, representing an enlarged social media footprint. A more prominent social media footprint increases a person's susceptibility to social engineering by providing access to data that could be used to develop a targeted social engineering attack. A person's social media footprint is calculated using two factors—how much data is available and how many people have access to the data. Large amounts of data a person posts to social media increase the amount of information a social engineer can use to create a targeted attack. In addition, an increased number of "friends" raises the probability that a social engineer has gained access to the data. The responses to the social media questions are assigned a value between 50 and 100. The resulting social media score is then placed into the variable SM in the susceptibility algorithm.

Upon completion of the tool's behavioural and social media usage sections, the participants then progress to the information security portion of the tool. Unlike other IA training assessment tools, which only ask between 10 and 20 questions, the Dynamic/Adaptable IA Training Assessment Tool takes a learning approach to question the participants. This learning approach is where the Dynamic/Adaptable IA Training Assessment Tool gets its dynamic/adaptable nature. Furthermore, this approach shows the tool's value in better assessing a person's information security knowledge because the tool does not require the person to "pass it." Instead, the tool measures a person's actual knowledge of information security. Other IA training assessment tools, and their coordinated training programs, provide the end-user with information security information and assess that the person can regurgitate the basic knowledge in a simple quiz (McIlwraith, 2006).

The Dynamic/Adaptable IA Training Assessment Tool is built around seven information security topics: Safe Surfing & Human Firewall, Identity Theft & Privacy, Passwords, Social Engineering, Malware, Physical Security & Policy, and Incident Response & Backup and Recovery. Information security questions, spanning four difficulty levels, were developed for each topic. The individuals who participated in this study were first presented with four level 1 questions related to topic 1. If the participant answered all the questions correctly, the difficulty level increased by 1, and a new set of questions were presented from the same topic. This process continued so long as the participant answered all four questions correctly. If the participant did not answer all four questions correctly or answered the four questions related to the fourth level of difficulty, then the difficulty value reset to 1, and the topic number increased by 1. The process then starts over with the new topic.

A value is calculated using the formula (Qr/T)C as each topic is completed. Qr represents the percent of correctly answered questions, divided by the average time (T) it took the participant to answer the questions, which is then multiplied by the highest difficulty level (C) reached by the participant. When all seven topics are completed, each topic's (Qr/T)C values are added together for a cumulative total. The sum value is then put into the variable QrTotal of the algorithm. The last part of the susceptibility algorithm is to multiply the results by 1000, then divide by 2, which converts the results into a numeric value between 0 and 100. The complete susceptibility algorithm is expressed as:

$$S=(QrTotal/(Hb+SM)*1000)/2$$

4. Experiment setup

The experiment for this study was structured around three phases—Tool Development, Beta Testing, and Implementation. Since this study included human subjects, it was necessary to obtain Institutional Review Board (IRB) approval before moving from the prototype phase to implementation. IRB approval was obtained on February 25th, 2021.

This study was limited to participants who were 18 years old or older, with varying levels of information security knowledge. Participants were required to complete the 2021 KnowBe4 IA training and assessment and the Dynamic/Adaptable IA Training Assessment Tool. Participants for this study were recruited from the faculty, staff, and students at Norwich University. The population at Norwich University provided this study with an appropriate level of diversity reflective of the broader United States population. For this study, only three aspects of demographic data were collected and analysed—gender, age, and education level.

5. Data analysis

Forty-seven individuals volunteered to participate in this study. The demographic breakdown for this study is shown in tables 5, 6 and 7.

Table 5: Gender (Collier, 2021)

Male	Female	Transgender
25	21	1

Table 6: Age (Collier, 2021)

18-24	25-34	35-44	45-54	55-64	65-74
7	4	11	11	10	4

Table 7: Education level (Collier, 2021)

High School	College Certificate	Associate Degree	Bachelor Degree	Master Degree	Doctorate/Term
7	4	11	11	10	4

One of the significant problems that current models of IA training assessment present are that the assessment tool tends to group users closely together, implying that all users have approximately the same level of susceptibility. A comparative analysis was conducted comparing the results of the KnowBe4 assessment and the Dynamic/Adaptable IA Assessment tool to show that the Dynamic/Adaptable IA Training Assessment Tool provided a more precise measure of a person's susceptibility. Figure 1 shows a visual comparison between the KnowBe4 results and the Dynamic/Adaptable IA Training Assessments Tool's results. It is easy to see there is a difference between how each of the tools assesses susceptibility. The results for each of the demographic categories are similar where the KnowBe4 tool groups the results together, while the Dynamic/Adaptable IA Training Assessment Tool spreads them apart.

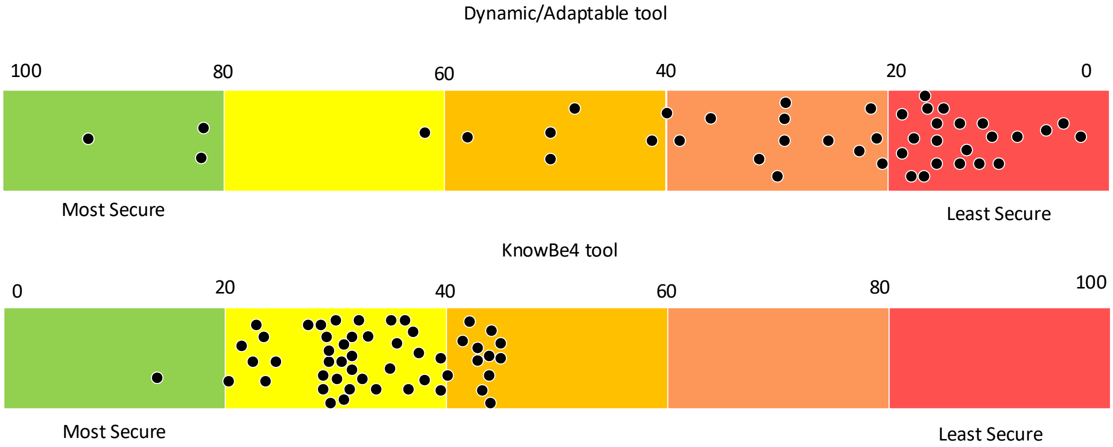

Figure 1: KnowBe4 Compared to Dynamic/Adaptable IA training assessment tool (Collier, 2021)

Comparing specific KnowBe4 scores to their associated Dynamic/Adaptable scores makes it clear that the Dynamic/Adaptable tool measures susceptibility more precisely. Table 8 is an example of three users who score virtually the same when assessed by the KnowBe4 assessment tool. In contrast, the Dynamic/Adaptable IA Training Assessment Tool assesses their risk level significantly differently.

Table 8: Similar KnowBe4 Scores example 1 (Collier, 2021)

KnowBe4	Dynamic/Adaptable
25.9	65.5
25.9	19.5
26	6.4

Although the KnowBe4 assessment tool scored the three users in Table 8 as having virtually the same score, the Dynamic/Adaptable IA Training Assessment Tool evaluated those same three users with significantly different levels of susceptibility. The Dynamic/Adaptable IA Training Assessment Tool assessed the user with the higher KnowBe4 score with the lowest susceptibility rating. The results of this comparison show the disparity that exists between the results of the two tools and further show that the current method of assessing someone's susceptibility is not as precise as it could be

6. Future work

This study consisted of both qualitative and quantitative aspects. To solidify the value of the qualitative approach to identifying the behaviors related to susceptibility, a more quantitative approach to assessing the behavioral traits is an area to conduct future research. The Covid-19 pandemic placed limitations on this study by not allowing the researchers to observe body language responses to the behavioral questions or include biometric data related to the behavioral or social media usage questions. Both an observational approach and a data collection approach would have increased the viability of the qualitative methodology of identifying the validity of the behavioral factors and their relationship to susceptibility.

Taking this research to the next level will include identifying what role culture plays in the information security decision-making process. Do people from western countries perceive the threat of social engineering differently than those from eastern countries? Is there an impact from different cultures within a single country where multiple sub-cultures exist? Does culture support or block improved information security responses? These are but a few questions that need to be answered to understand better how culture impacts a person's perception of cyber threats.

Another area where this study opens the door is finding ways to alter the current model of information awareness training, so the training modifies a person's behavior, rather than simply teaching them about risks. Taking what has been learned from this study and working with an interdisciplinary team of information security professionals and behavioral modification professionals, it could be possible to develop a new form of IA training that incorporates behavioral modification techniques like Cognitive Behavioral Therapy(CBT). CBT works to change the person's behavior, which would improve their response to a cyber-attack.

7. Conclusion

Humans are certainly the most vulnerable part of any information security chain. Although technical solutions are great at preventing many forms of cybercrime, humans can still bypass those technical solutions, opening themselves and their employers to become victims of cybercrime. People are complex, multifaceted beings, and their decision-making process is also intricate and influenced by many factors. The current method of assessing a person's susceptibility to becoming a victim of cybercrime does not include the behavioural or social media usage factors that influence a person's ability to make a good information security decision. Since necessary behavioural data is not used in the current IA training assessment tools, these tools artificially group users, giving the impression that users all have approximately the same level of susceptibility. This study showed that human behaviours and social media usage behaviours could and should be included in the information awareness training assessment tools used by organizations around the world to assess better the risk their employees pose.

Acknowledgements

I would like to thank the following people for their support of my research. Dr. Edward Chow, Dr. Yanyan Zhuang, and Dr. Rick White—University of Colorado, Colorado Springs, Dr. Huw Read, Dr. Matthew Thomas and Dr. Mich Kabay—Norwich University. Alexandra Collier, Southern New Hampshire University, Morgan Woods, Elizabeth Gregory, Aiden Cruz, Charles Grunert, Nicole Folib—Norwich University.

References

American Psychological Association, 2020. *APA Dictionary of Psychology.* [Online] Available at: https://dictionary.apa.org/behavior [Accessed July 28th, 2021].

American Psychological Association, 2021. *Personality.* [Online] Available at: https://www.apa.org/topics/personality [Accessed July 27th, 2021].

Ariu, D., Frumento, E. & Fumera, G., 2017. *Social Engineering 2.0: A Foundational Work.* Sienna, s.n.

Ayates, K. & Conolly, T., 2003. *A Research Model for Investigating Human Behavior Related to Computer Security.* Tampa, s.n.

Bada, M., Sasse, A. M. & Nurse, J. R., 2019. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. *CoRR,* Volume abs/1901.02672.

Collier, H. D., 2020. *Social Media: A Social Engineer's Goldmine.* Larnaca, s.n.

Collier, H. D., 2021. *Enhancing Information Security By Identifying and Embracing Executive Functioning and the Human Behaviors Related to Susceptibility.* Colorado Springs: s.n.

Edwards, W., 1954. The Theory of Decision Making. *Psychological Bulletin,* pp. 380-417.

Gharibi, W. & Shaabi, M., 2012. Cyber Threats in Social Networking. *International Journal of Distributed and Parallel Systems,* Volume 3, pp. 119-126.

Gunkel, P., 1998. *638 Primary Personality Traits - Ideonomy.* [Online] Available at: http://ideonomy.mit.edu/essays/traits.html [Accessed 2019].

Hadnagy, C., 2018. *Social Engineering: The Science of Human Hacking.* Indianapolis: Wiley.

Hallas, B., 2018. *Rethinking the Human Factor.* s.l.: The Hallas Institute.

Henderson, J. C. & Nutt, P. C., 1980. The Influence of Decision Style on Decision Making Behavior. *Management Science,* pp. 119-126.

Kayes, I. & Iamnitchi, A., 2017. Privacy and security in online social networks: A survey. *Online Social Networks and Media,* 3(4), pp. 1-21.

Kemp, T., 2016. Social Engineering Fraud: A Case Study. *Risk Management,* 63(6), pp. 8-9.

KnowBe4, 2021. *KnowBe4 Human Error Conquered.* [Online] Available at: https://www.knowbe4.com/knowbe4-timeline/#:~:text=Now%20647%20employees%2C%20and%2023%2C000,is%20going%20stronger%20than%20ever.[Accessed 19 04 2021].

Luo, X., Brody, R., Seazzu, A. & Burd, S., 2011. Social Engineering: The Neglected Human Factor for Information Security Management. *Information Resources Management Journal,* pp. 1-8.

Mackinnon, A. J. & Wearing, A. J., 1980. Complexity and Decision Making. *Behavioral Science,* pp. 285-296.

McIlwraith, A., 2006. *Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness.* Burlington: Gower Publishing Company.

Mitnick, K. D. & Simon, W. L., 2002. *The Art of Deception.* Indianapolis: Wiley Publishing Inc.

Postnikoff, B. & Goldberg, I., 2018. *Robot Social Engineering Attacking Human Factors with Non-Human Actors.* Chicago, s.n.

Schroeder, J., 2017. *Advanced Persistent Training: Take your Security Awareness Program to the Next Level.* Edinburgh: Apress.

Tsikerdekis, M. & Zeadally, S., 2014. Online Deception in Social Media. *Communications of the ACM,* 57(9), pp. 72-80.

UK Parliament, 2020. *Science and Technology Committee - Second Report Behaviour Change.* [Online] Available at: https://publications.parliament.uk/pa/ld201012/ldselect/ldsctech/179/17902.htm [Accessed July 27th, 2021].

Vishwanath, A., 2014. Habitual Facebook Use and its Impact on Getting Deceived on Social Media. *Journal of Computer-Mediated Communication,* 20(1), pp. 83-98.

Weir, G. R., Toolan, F. & Smeed, D., 2011. The Threats of Social Networking: Old Wine in New Bottles?. *The Herald*, August 11th, p. 3.

Wilcox, H. & Bhattacharya, M., 2019. *A Human Dimension of Hacking: Social Engineering through Social Media.* Guangzhou, s.n.