Heading into the Future: The Dynamic Adaptable IA Training Assessment Tool!

Henry Collier
Marshall University, Huntington, USA

collierh@marshall.edu

Abstract: Information awareness training and assessment have not changed much in the last twenty years. Although most information awareness programs have an assessment, it is used as a check-the-box item. Employees are required to do the training and then take a test of between 10 and 20 questions and achieve a score of at least 70%. The results show that everyone in the organization has some risk, but this information does not help cybersecurity professionals identify and mitigate the risk. With human beings being the primary attack vector, we need to do more to understand people and develop ways of changing behaviour. The Dynamic Adaptable IA Training Assessment Tool developed for this study uses a novel approach to include human behaviours and social media usage factors as part of a susceptibility algorithm designed to assess better an employee's risk of becoming a victim of cybercrime. This study demonstrates that the current methods of assessing risk within an organization lead to a false sense of security. Reinforcing the need to change how we assess risk within an organization.

Keywords: Human behaviours, Social media, IA training assessment, Cybercrime

1. Introduction

Social engineering has historically been the most effective way of gaining access to a system. It takes days, weeks, months, or even years to hack a piece of equipment, but it takes minutes to trick a person and hack them (Hadnagy, 2018) (Mitnick & Simon, 2002) (Schroeder, 2017). This is even more true when you calculate the vast amount of data that is available on social networking sites and the use of Artificial Intelligence to develop more sophisticated social engineering attacks (Weir et al., 2011) (Tsikerdekis & Zeadally, 2014) (Collier, 2024).

Humans are by far the most significant risk to an organization's data (Collier, 2021) (Hallas, 2018) (Hadnagy, 2018) (McIlwraith, 2006). The cybersecurity industry's solution to this problem is Information Awareness (IA) Training and Assessment (McIlwraith, 2006) (Bada, et al., 2019). However, there are a few problems with the current approach to mitigating the human factor in cybersecurity. The first is that humans are complex beings, influenced by many internal and external elements. Emotions and behaviours influence the decision-making process, frequently leading to poor decisions that result in system breaches. One of the problems with trying to mitigate emotions and behaviours is that they are qualitative in nature, and therefore, there is no concrete manner of assessing them and developing mitigation strategies. The second problem with the current IA Training and Assessment process is that it is not designed to change people's behaviour, but rather it is designed to throw a significant amount of information at a person and hope they make good choices (Collier, 2022) (Hallas, 2018) (McIlwraith, 2006). When an employee falls victim to a phishing attempt or other forms of social engineering, the result is typically that they will be terminated from their position, and the reason is 'they were trained' (Collier, et al., 2023). From a cybersecurity perspective, this seems very counterintuitive. Cybersecurity experts should want people to come to them immediately if they fall victim. Knowing a potential breach is happening 5 minutes after the attack is far superior to learning about it six months later, after significant data has already been lost. Certainly, a change in this culture would result in fewer incidents of mass data loss.

One of the primary reasons why cybersecurity specialists don't want to veer away from finding a technical solution and working to develop an interdisciplinary solution is because many individuals in the realm of computer science and cybersecurity fit somewhere in the spectrum of being neurodiverse (Scanlan, et al., 2020)(Wiederhold, 2024). In order to understand how the cyber workforce's neurodiversity plays into this problem, we must first understand what neurodiversity is. Neurodiversity, or someone being neurodivergent, refers to individuals with cognitive differences, which include autism (ASD), Attention-deficit/hyperactivity disorder, dyslexia, and Asperger's syndrome (Wiederhold, 2024). These cognitive differences impact the individuals similarly, resulting in barriers. Autism, Aspergers, and Attention-Deficit/Hyperactivity Disorder present with similar social cognitive impairments that impact the individual's ability to operate in social environments and to understand the behavioural aspects of everyone else (Elements, 2022). In fact, the individuals struggle to read body language read and interpret social cues, and the awkwardness of being in a social setting pushes these individuals into relying on logic and ignoring the behavioural aspects of individuals (Elements, 2022). This sets the stage for the cybersecurity industry to take such a staunch stance on finding a

technical solution to the human problem. The good news is that it is possible to teach these individuals how to operate and be successful in these situations.

Now that one of the primary reasons why we as cybersecurity specialists fail to fix the human firewall problem is understood, it is necessary to understand how to get past this so the community can be more successful at preventing cyber-attacks that originate from a person making poor security-minded decisions. One way is to get the cybersecurity community to see that there is a way to logically and scientifically evaluate the behavioural aspects of susceptibility. By giving this community a better understanding of how internal and external influencing factors can be addressed.

The Dynamic Adaptable Information Awareness Training Assessment tool developed for this study demonstrates that behavioural factors can be used to mitigate the risk associated with the end user and that behavioural factors can be quantified and assessed. This tool puts the logic and science at the forefront, which allows the cybersecurity community to move forward in a positive manner. The tool is built around three pillars of influence/knowledge—behavioural factors, social media usage factors, and a dynamic/adaptable information security questionnaire.

The dynamic/adaptable information security questionnaire is built on seven information security topics at four levels of difficulty for each topic. As the user goes through the process, they are presented with four questions from the lowest level first. If they get all four right, they are then presented with four more questions at a higher difficulty level. This approach makes the tool dynamic and adaptable because it adapts to the user's current information security knowledge base to measure their knowledge more accurately. The results expressed here are the results of an empirical study designed to assess susceptibility to becoming a victim of cybercrime.

2. Behavioural Factors

Patrick Gunkel, known as the idea man, from the Massachusetts Institute of Technology created a list of 638 behavioural traits that every person exhibits (Gunkel, 1998). This list was evaluated and assessed using a focus group that included psychology students, sociology students, computer science and cyberseucrity students. The traits were broken down into positive behavioral traits, negative behavioral traits and neurtral behavioral traits. Tables 1, 2 and 3 below provide examples of each subcategory of behavioral traits.

Table 1: Partial List of Positive Human Behavioral Trait Examples (Collier, 2021)

Accessible	**Admirable**	**Articulate**	**Calm**	**Charming**	**Cheerful**
Constant	Dedicated	Disciplined	Dutiful	Educated	Elegant
Exciting	Fair	Gallant	Gentle	Heroic	Honest
Insightful	Kind	Lovable	Mature	Objective	Passionate
Respectful	Sage	Trusting	Upright	Warm	Wise

Table 2: Partial List of Negative Human Behavioral Trait Examples (Collier, 2021)

Aimless	**Desperate**	**Egocentric**	**Faithless**	**Gullible**
Hedonistic	Ignorant	Impulsive	Lazy	Misguided
Narcissistic	One-sided	Opportunistic	Pompous	Quirky
Reactive	Shortsighted	Sloppy	Tactless	Thoughtless
Uncooperative	Unreliable	Vacuous	Vulnerable	Weak

Table 3: Partial List of Neutral Human Behavioral Trait Examples (Collier, 2021)

Absentminded	**Busy**	**Contradictory**	**Competitive**	**Emotional**
Freewheeling	Guileless	Hurried	Impressionable	Invisible
Mellow	Neutral	Noncommittal	Obedient	Ordinary
Placid	Preoccupied	Restrained	Reserved	Stubborn
Subjective	Tough	Unambitious	Unpredictable	Whimsical

As part of the analysis process, each trait was looked at from the perspective that if someone made a decision influenced by the trait, what was the probability that the result would be a poor information security decision, leading to the individual becoming potentially becoming a victim of cybercrime.

An example of how this analysis was conducted is below using the neutral trait of absentmindedness. The focus group worked through a four-step process as seen below (Collier, 2021).

Step 1. The definition *of absentminded was defined using the 2019 Merriam Webster dictionary—"*lost in thought and unaware of one's surroundings or actions" (Merriam-Webster Incorporated, 2019).

Step 2. Ask the question: *Based on the definition, if someone is experiencing the trait, is there a possibility that the person will make a poor information security decision?* (Collier, 2021)

Step 3. Using the Likert Scale below, the option representing the highest likelihood of a poor information security response was selected (Collier, 2021).

- Very Low Likelihood
- Low Likelihood
- Neutral
- Highly Likely
- Very Highly Likely

Step 4. If the selection was highly likely or very highly likely, the trait is identified as a trait that could impact susceptibility to social engineering. If the selection was neutral, low likelihood or very low likelihood, then the trait does not explicitly qualify as a trait that could impact susceptibility to social engineering.

This assessment process resulted in 128 traits from all three categories that demonstrated a high propensity of influencing the decision-making process, resulting in a poor security minded decision. The behavioral traits were then grouped together based on similarities between the traits. For example, irascible, irritable and miserable can been seen as connected traits.

After completing the assessment of the behavioural traits, the focus group started to determine a way of assessing these traits. The focus group worked to develop questions that were reflective of the trait groupings. An example of one of these questions is "*Have you ever driven to work and not remembered the drive?"* This question assesses the traits of absentmindedness, aimlessness, preoccupation, inattention, forgetfulness, busy, sloppy and slow (Collier, 2022). Figure 1 demonstrates a sample of how the behavioral questions were presented to the participants. Figure 2 is an example of the social media usage questions used in this study.

In addition to the behavioral traits being used to evaluate susceptibility, social media usage metrics were also used. With social media playing such a transformative role in today's society, one has to look at how social media usage impacts the security of humans. Certainly, most of the behaviors related to social media use fall within the previously identified categories, it was felt that assessing the level of impact that these behaviors have was valuable. In addition to the behavioral aspects of social media, it is imperative that security researchers understand how the amount of information a person posts to social media and the number of contacts an individual has increased the probability that they will fall victim to cybercrime, specifically social engineering. It is well known that social engineers, and other cyber criminals, are all over social media outlets (Collier, 2020).

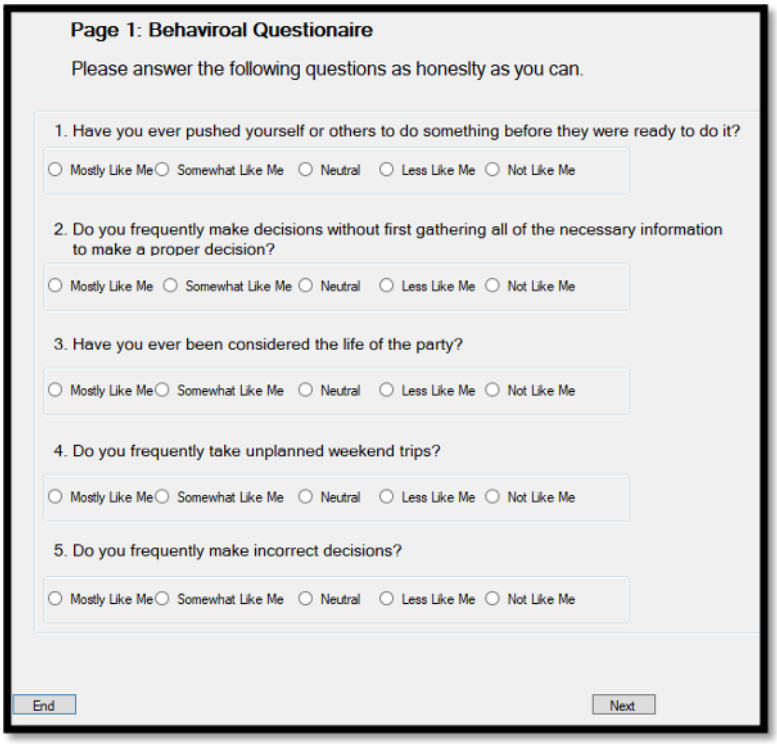

Figure 1: Behavioral Question Examples (Collier, 2021)

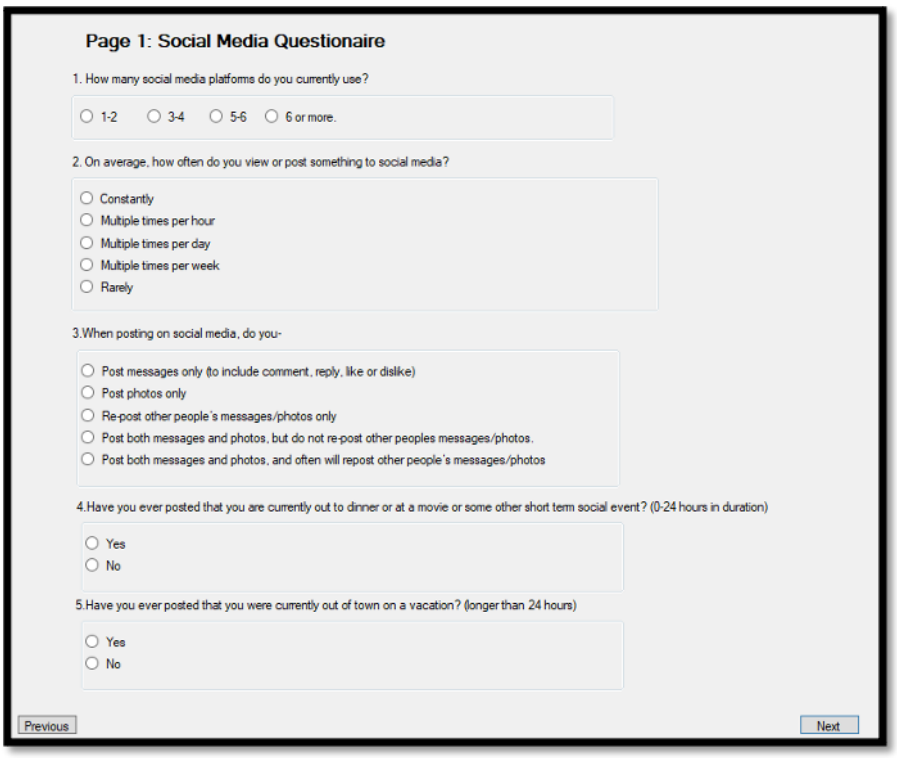

Figure 2: Social Media Questionnaire (Collier, 2021)

3. The Dynamic Adaptable IA Training Assessment Tool

Unlike other forms of IA training assessment, the Dynamic Adaptable IA Training Assessment Tool, built around three distinct components. Behavioural traits, social media usage traits and a dynamic information security questionnaire. Traditional IA assessment tools require that a person achieve a specific score, most frequently a 70 on a 100-point scale. This motivates employees to simply work to pass the test, rather than learn the material. Therefore, individuals will frequently click through the training and then use search engines to find the answers.

From a security perspective, this is ineffective because the training is not actually influencing the individual or working to change their behaviour. The Dynamic Adaptable IA Training Tool does not have a score requirement and therefore removes this condition from consideration. This tool is designed to be an information gathering tool for the security team, which will allow them to change how they are training individuals, rather than being a *check the box* to meet compliance requirements.

Figure 3 is an example of the security questions used in this study.

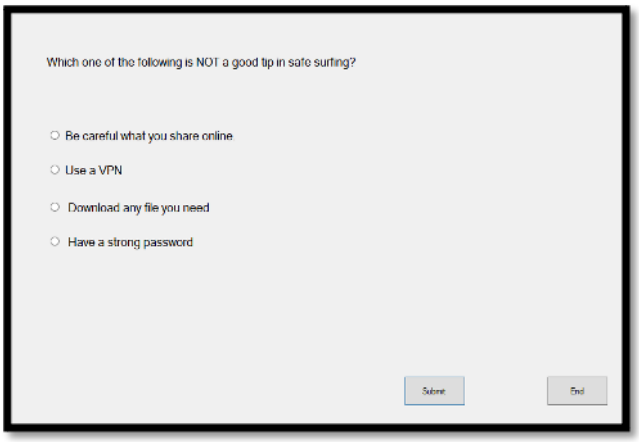

Figure 3: Example of the security questions

For the purpose of this study, the results from the Dynamic Adaptable IA Training Tool were compared to the results of the internationally known KnowBe4 training and assessment. Individuals were required to provide their KnowBe4 scores during the registration process.

KnowBe4 uses a person's job title, the results of phishing tests, and the overall score from the assessment to determine a person's susceptibility. The Dynamic Adaptable IA Training Assessment Tool uses Behaviours, social media usage and the results of the security questionnaire. The KnowBe4 method uses two quantitative factors and one qualitative factor, while this tool uses three quantitative factors.

The Dynamic Adaptable IA Training Assessment Tool's information security questionnaire is built around seven cybersecurity topics, with four levels of difficulty. The participant is presented with a series of questions for the first topic, at the first level of difficulty. If the participant gets all of them correct, they are then presented with new questions based on level two. This process continues until either the participant fails to answer all of the questions correctly or they complete the fourth level of difficulty. At this point, the topic is changed, and the process is restarted.

In order to assess susceptibility with a measure of quantifiable results, a susceptibility algorithm was develoed for this tool. The security algorithm for this study is S = (((((Qr1/T)*C) + ((Qr2/T)*C) + ((Qr3/T)*C) + ((Qr4/T)*C) + ((Qr5/T)*C) + ((Qr6/T)*C) + ((Qr7/T)*C)))/(Hb+SM))*1000. The formula can be simplified to S = QrTotal/(Hb+SM)*1000 where QrTotal is the combined results from the security questionnaire. Hb is representative of the results of the human behavioural questions, and SM is representative of the social media question results.

4. Results

The results of this study are presented below. This study included 47 participants across the spectrum of demographic data to include gender, age, education level. It is important to note the study size was small and that further analysis is needed. However, the results of this study show that the current model of conducting IA training assessment is in need of an overall.

KnowBe4 groups individuals together on the spectrum of susceptibility with a standard deviation of 12.47. This close proximity is demonstrated in the rainbow diagram found in figure 4.

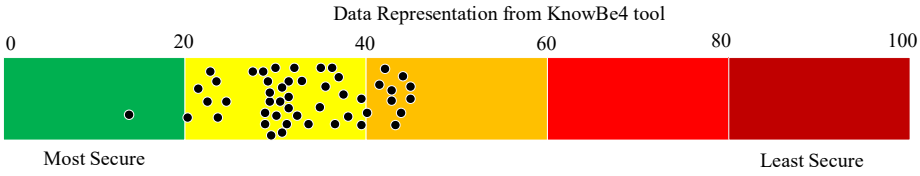

Figure 4: The rainbow diagram

Green (0-20) represents that someone is more secure, while yellow (20-40) and orange (40-60) represent some risk, and red (60-80) and maroon (80-100) represent significant risk. As can be seen, the 47 participants of this study all fell within a 33-point range, that falls within the area of *some risk*. This gives the cybersecurity professionals a false sense of security as it does not accurately reflect the complex nature of the human component.

Regarding the demographic data collected, it was used to attempt to confirm or deny previous studies. Prior research has attempted to determine if things like gender, age, education level impact a person's propensity to clicking on a malicious link in a phishing email. Some early studies have shown that women are more susceptibility, while others have shown the older population is more susceptible (Sheng, et al., 2010). The results of this study made no determination as whether gender or age made a significant difference. However, this study did show that individuals who were more educated, tended to do better and were less susceptible.

The Dynamic Adaptable IA Training Assessment Tool's results show a different picture. Figure 5 shows that when behavioural and social media factors are incorporated into the susceptibility algorithm, the result is that individuals are better spread across the spectrum, clearly identifying that its results demonstrate a more realistic interpretation of susceptibility.

The demographic data analysed consisted of age, gender, and education level. The study showed that neither age or gender significantly impacted a person's susceptibility, but education did. Individuals with higher levels of education tended to do better than those will less education (Collier, 2021).

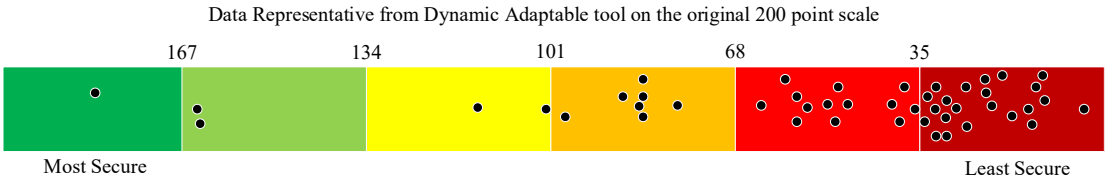

Figure 5: Data (Collier, 2021)

To further demonstrate the importance of this study, we must look deeper at the data. Four separate groupings of individuals who scored the same or approximately the same on the KnowBe4 tool were looked at in deeper detail. Tables 4, 5, 6 and 7 below show the difference in how each tool assessed these individuals' susceptibility levels. KnowBe4 is based on a 100-point scale, with 0 being best and 100 being worst, while the Dynamic Adaptable IA Training Too uses the reverse 100-point scale. When the data is observed, it is clear that the KnowBe4 assessment too falsely groups people together while the Dynamic Adaptable IA Training Tool more precisely evaluates the individual's susceptibility levels.

Table 4: Similar KnowBe4 scores example 1(Collier, 2021)

KnowBe4	Dynamic/Adaptable
25.9	65.5
25.9	19.5
26	6.4

Table 5: Similar KnowBe4 scores example 2(Collier, 2021)

KnowBe4	Dynamic/Adaptable
29.5	24.86
29.5	28.35

KnowBe4	Dynamic/Adaptable
29.5	81

Table 6: Similar KnowBe4 scores example 3(Collier, 2021)

KnowBe4	Dynamic/Adaptable
39.4	24.27
39.4	94.79

Table 7: Similar KnowBe4 scores example 4(Collier, 2021)

KnowBe4	Dynamic/Adaptable
46	34.5
46	61.56

The data clearly shows the difference in how KnowBe4 and the Dynamic Adaptable IA Training Assessment Tool calculates susceptibility. Although KnowBe4 has been a leader in IA training and assessment, the results show that there is room for improvement, and it is possible to get a more finite measure of susceptibility.

Statistical analysis was conducted on tables 4-7 and the results in a two tailed t-test a t value of 1.15, and a p value of <.2785. The statistical results, when added to the comparative analysis results demonstrates how different the two tools evaluate a person's susceptibility level. The evidence gives the impression that the Dynamic Adaptable IA Training Tool measures a person's susceptibility level more accurately than the KnowBe4 tool.

Additional statistical analysis was performed comparing the entirety of the data for both tools and the results are found in table 8 below.

Table 8: Unpaired T-Test results between KnowBe4 and Dynamic/Adaptable tool

Group	Dynamic/Adaptable	KnowBe4
Mean	51.92	33.79
SD	39.52	7.96
SEM	5.76	1.16
N	47	47

The test completed was a paired T-test, which resulted in a t value of 3.128 and a p value of <.0031, which is very statistically significant based on the conventional criteria. The difference between the mean values is 18.134, while the 95% confidence interval is 6.4648 to 29.8033. Since the difference between the means falls within the 95% confidence interval, it is proven that the mean difference is true to the 95% confidence interval. To reinforce the benefits of including behavioural and social media usage factors in determining a secondary test was conducted. The results of each participant's behavioural and social media usage factors were calculated using the KnowBe4 results. The same susceptibility algorithm was used, but in this test case, the KnowBe4 scores were used in lieu of the original QrTotal value.

When calculated, the new T-test results showed that the t value was 4.85 and the p value was <.0001, which based on conventional criteria makes this result extremely significant. This secondary result shows that adding human behavioural and social media factors into calculating someone's risk, the results are vastly improved over the KnowBe4 results alone.

5. Future Work

Humans are very complex beings and more needs to be done to evaluate this complexity as it relates to an individual becoming a victim of social engineering and cybercrime. To expand on this study, we will investigate how culture plays a role in influencing the decision-making process. It is hypothesised that by adding a cultural component to the Dynamic Adaptable IA Training Assessment Tool that an even more precise measure of someone's susceptibility will be identified. Current information awareness training fails to change behaviour (Bada, et al., 2019) (Hallas, 2018) (McIlwraith, 2006) (Schroeder, 2017). The results from this study and future studies will be the feeder to developing a new form of Information Awareness training the works to modify

behaviour by incorporating psychological techniques like Cognitive Behavioural Therapy, which has shown significant progress in changing people's behaviour in a positive manner.

6. Summary

This study has clearly shown that there is an advantage to including behavioural and social media factors when attempting to calculate a precise measure of someone's susceptibility to becoming a victim of social engineering and cybercrime. It can easily be envisioned that as this tool is further developed, to include additional data points, that the results will improve and become a vital tool for cybersecurity professionals all around the world. Imagine a world where cybersecurity professionals can predict the likelihood that an end user is going to fall for a specific attack, and then implement proactive strategies to stop the attack before it leads to a breach. As nefarious threat actors continue to develop better, more effective attacks, cybersecurity professionals need to adopt new techniques to defend against these attacks.

References

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

Collier, H., 2022. *Including Human Behaviors into IA Training Assessment: A Better Way Forward!.* Chester, European Conference on Cyber Warfare and Security (.

Collier, H., 2024. *AI: The Future of Social Engineering.* Johannesburg, Academic Conferences International.

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.

Collier, H., Morton , C., Altharhi, D. & Kliener, J., 2023. *Cultural Influences on Information Security.* Athens, European Conference on Cyber Warfare and Security.

Elements, 2022. *10 Neurodvidrsity Symptoms Every Employer Should Know..* [Online] Available at: https://www.weareelements.io/insight/10-neurodiversity-symptoms-every-employer-should-know/#:~:text=Those%20with%20neurodivergence%20may%20find,one%2Doption%2C%20linear%20approach.[Accessed 10 11 2024].

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.

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

Merriam-Webster Incorporated, 2019. *Merriam-Webster Online Dictionary.* [Online] Available at: https://www.merriam-webster.com/dictionary/ [Accessed 19 September 2019].

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

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

Scanlan, J. et al., 2020. *Neurodiverse Knowledge, Skills and Ability Assessment for Cyber Security.* Wellington, AIS eLibrary.

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.

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*, 11 August, p. 3.

Wiederhold, B. K., 2024. Diverse Minds, Secure Networks: Embracing Neurodiversity in Cybersecurity. *Cyberpsychology, Behavior, and Social Networking,* 27(9), pp. 609-676.