# THE PORT Z3R0 EFFECT! HUMAN BEHAVIORS RELATED TO SUSCEPTIBILITY

Henry Collier[1] and Alexandra Collier[2]

[1]College of Graduate and Continuing Studies,
Norwich University, Northfield, Vermont, USA
[2]Southern New Hampshire University, Manchester, New Hampshire, USA

***ABSTRACT***

*Current practices to defend networks against threats involve hardening systems by limiting points of ingress into the system. The most common method of limiting ingress into a system is by limiting which ports are allowed through the firewall. Port limitation as a method of defense is normally effective. Ports in a firewall range from 0 through 65,535 and covers the technical aspects of information security. One method of ingress not covered by technical ports is the human port, coined "port Z3r0" for this paper. To better defend against port Z3r0, we must understand the human better and why they are susceptible. This paper explores the basic human behaviors related to susceptibility and identifies the classifications of traits that increase a person's susceptibility level. Additionally, this paper will address the issue of how the current model of teaching end-users to defend themselves is lacking and needs to be improved.*

***KEYWORDS***

*Information Security, Non-Malicious Insider Threat, Susceptibility, Human Behaviors, Cognition*

## 1. INTRODUCTION

Literature has shown numerous times that humans are a weak link in information security, with many attacks specifically attacking users, e.g., phishing. Current methodologies of preparing the human to defend their network are based on training, but these training methods were not developed using the human behaviors related to susceptibility or proven methods of behavior modification, and have not changed much in the last ten years [1][2][3] [4]. Certainly, some will argue that there needs to be a technical measure put in place to prevent the user from being the reason a system has been compromised. However, it must be pointed out that until there is a mechanism that prevents attachments or links directly from an email, then the end-user will still be the one who decides to click on it or not, and there is no technical measure that will stop this, only behavioral modification will make the user stop and think twice before clicking on the link or attachment.

For end-users to be better prepared to defend themselves in the cyber realm, end-user training needs to work on doing more than just informing the end-user of the threat. The training needs to change the user's behavior [1]. Statistical analysis of security breaches has shown that internal threats cause around 70% of all breaches and that approximately 55 to 70 percent of those breaches are caused by mistakes or incompetence [5]. In fact, during Black Hat 2017, 250 hackers were asked their methods and what was the easiest manner to gain access to sensitive data, and the consensus was that they exploited human weakness more than technical weakness

Dhinaharan Nagamalai et al. (Eds): NATP, ACSTY, ADCOM, SOFE, CCCIOT, MLSC, SVC - 2020
pp. 47-57, 2020. © CS & IT-CSCP 2020 DOI: 10.5121/csit.2020.100404

[2]. According to Christopher Hadnagy [6], author of “Social Engineering: The Science of Human Hacking” in 2017, more than 80% of all breaches had a social engineering element to them.” One of the most common approaches to “hacking” the human is through the use of targeted phishing attacks, aka spear phishing, threat actors don’t need to use sophisticated attacks, they need to send an email to an easily duped end-user [3]. There have been several attempts at identifying why people still fall for phishing attempts [7]. We believe that in order to improve information security, we need to develop a better understanding of the human factors related to susceptibility and then incorporate these factors into our information security awareness programs.

The evidence is pretty clear that the end-user is certainly the weakest link in the chain of information security. With the fact that technical measures are not the most successful method of breaching a system, two questions come to mind: What are the key factors that make the end-user the weakest link? and Why are there so few researchers looking into the reasons and working to develop new methods to mitigate this risk? The answer to the first question is the primary purpose of this paper, and the research this paper is based on. The answer to the second question may never be known, but certain assumptions towards the idea that human-based research makes the average computer science/information security researcher uncomfortable can be made. Most people in the computer/information security industries wear the moniker "computer nerd” with pride, and historically speaking, most computer nerds have preferred to interact with the equipment and not the person. Based on the literature review conducted for this paper, it is clear that people in the realm of computer/information security industry still prefer to interact with the equipment. However, one can see that there is a new trend developing where information security researchers realize that more needs to be done with incorporating behavioral factors into information security [2][3][5][7]. Even with this understanding, most people involved in cybersecurity research would prefer to research something technical in nature, not human in nature [2][3][5].

A more in-depth dive into the “how and why” people make the decisions that they make, and what behaviors influence a person’s susceptibility is important for research in the area of cybersecurity. This paper will look at the basics of cognition and the human decision-making process, the behaviors and behavioral characteristics that lead to a person making a decision which results in them becoming a non-malicious insider threat, and the differences between a non-malicious insider threat, a malicious insider threat, and the malicious outsider threat.

## 2. BACKGROUND AND RELATED WORKS

This survey paper is based on research and anecdotal evidence that supports the theory that the human is the weakest link in the chain of information security. That human behaviors and human behavioral characteristics directly affect the level of a person’s susceptibility, and that the current information awareness training models are ineffective because they don’t include a human behavioral analysis component that prepares users to defend themselves from being social engineered. Although the problem of the end-user being the weakest link has been acknowledged extensively over the last 20 years, research into finding an effective solution to the human port has not gone beyond the same old information awareness training that organizations have been using for at least the last 15 years. This paper goes beyond prior work in that it begins the process of looking at behavioral factors related to why humans continue to be susceptible, even after years of information awareness training.

### 2.1. THE WEAKEST LINK

There is significant evidence which shows that threat actors prefer to take advantage of the human factor when attempting to breach an information system [2][3][5][6][7][8][9][10] [11][12]. Very few information security practitioners would argue against the evidence that supports the theory that the human is the weakest link since every single information security plan includes an information awareness training program. The average information awareness training program covers the following topics: Incident Response, Passwords, Malware, Safe Surfing & Human Firewalls, Social Engineering & Phishing, Backup & Preventative Care, Privacy, Identity Theft, Non-Technical & Physical Security, and Policy [13][14]. Each of these topics can be directly related to the human firewall and reinforces that the human is perceived as a significant threat to an organization's network and data.

### 2.2. HUMAN BEHAVIORS

Humans are complex and multifaceted beings. When it comes to the decision-making process, humans have the unique ability to apply critical thinking in their process. The concept of critical thinking should ensure that any decision made by a person is fact-based and sound. However, the decision-making process is subject to being influenced by the array of human behaviors, including, but not limited to: absentmindedness, laziness, carelessness, arrogant, disobedient, confused or foolish [6][15][16][17]. Some information security practitioners have started looking at how human behaviors can be incorporated into their information security plans [3][4][5][18], but more needs to be done. Based on how information security professionals are starting to look at human behaviors and information security, one can see that it is clear that human behaviors influence the critical thinking process and can be directly linked to how easy it is for a social engineer to convert an individual into a non-malicious insider threat.

### 2.3. INFORMATION AWARENESS TRAINING

Information awareness training is the hallmark of end-user security training. Every year, employees are required to go through their annual cyber awareness/information assurance training in order to maintain access to their organization's network [3][5]. If the current version of information awareness training were truly effective, there would be a significant reduction in the success of non-technical attacks like phishing, but there isn't because people still fall for phishing attacks on a regular basis [7][8][10][12][19][20]. Although there has been some research into why cyber awareness campaigns are not as effective as they should be, this research rarely touches on how human behaviors affect a person's decision-making process [1][2][3][5]. As long as the information awareness training programs don't include a human behavioral component to them, end-users will continue to fall for phishing attempts and other forms of social engineering and become non-malicious insider threats.

## 3. THE NON-MALICIOUS INSIDER THREAT

Threats can be categorized into three different categories: malicious outsider threat, malicious insider threat, and non-malicious insider threat. The malicious outsider threat (MOT) is someone who is not in the organization but is attempting to circumvent security controls to gain access to data and do harm. The malicious insider threat (MIT) is an internal employee who is intentionally harming the organization by circumventing the organization's security controls. On the other hand, the non-malicious insider threat (NMIT) is someone who has no ill will towards the organization but has been unwittingly turned into a threat to the organization's network due to their own actions. For this study, only the NMIT will be discussed since their existence is directly

related to the human behaviors related to susceptibility and social engineering. For many years, when the average person thought about a threat to their network, they thought about the hacker that was going to target their organization by hacking into the network through an unpatched system or a software backdoor [2] [6] [21] [22]. Hollywood does a great job of presenting the hacker in this way with films like the 1995 film "Hackers" [22] or the 2015 film "Black Hat" [21], which reinforces this belief. These attacks are from malicious outsider threats or individuals who do not have direct access to a network and are malicious in their intent. Although this risk is real, the method by which the malicious outsider gains access to a network is often not how the average person imagines it. One of the most predominant stereotypes associated with hackers (malicious outsider threat) is that they are someone who sits in a darkened room and works tirelessly attacking your network through technical means while drinking highly caffeinated beverages and eating the good old "hot pocket [21] [22]." Although this stereotype might be based on a truth that existed twenty-five years ago, today's malicious outsider threats are highly sophisticated, and their methods have been significantly refined. The fact of the matter is that most malicious outsider threats work to use the end-user to help them conduct their nefarious activity and gain access to the networked resources [2] [4] [5]. Through a process of manipulation and other social engineering techniques, the outsider threat works to turn an unwitting internal end-user into a non-malicious insider threat [2][3][6][7]. Today's threat actors are very good at using social engineering techniques to get what they want. Today's users are too easily duped into giving the threat actor what the threat actor is looking for, either because the end-user is being overloaded by too much data all at once, or because the end-user is too trusting of people, or because there are certain behaviors that the end-user has that makes them more susceptible to becoming an NMIT [2][3][6][7].

## 4. COGNITION AND THE DECISION-MAKING PROCESS

The most basic definition of cognition is "a cognitive mental process" [23]. The term cognitive is further defined as "of, relating to, being, or involving conscious intellectual activity (such as thinking, reasoning, or remembering)" [24]. To further clarify, cognition can be better defined as the mental process of thinking, reasoning, or remembering and is the foundation of the human decision-making process. One of the most important aspects of cognition related to the decision-making process is the concept of thinking, more importantly, critical thinking. Critical thinking can be considered a set of strategies that aid a person's ability to make decisions that are not based on emotion and bias, but rather are based on rational and consideration of our actions and principles [25]. Critical thinking is when the individual focuses more on the "how and why" they know something rather than the "what" they know [25]. Furthermore, critical thinking should not be thought of as "being critical," especially considering that critical thinking is more about having a calm, well-reasoning, intellectual debate about something where you are capable of deconstructing someone else's argument and showing them how and why their point of view is flawed or incorrect [25]. Critical thinking is so much more than simply knowing the facts; it is a process of analyzing and understanding [25]. Unfortunately, as humans, we are not born with the ability to "critically think," but rather, we have to learn how to do it as we grow [25].

The average person doesn't always understand how they came to the decision that they made. What they do know is that they had to make a decision, and they did. In order to better understand how critical thinking works, we need to look at the neuroscience behind the brain and the thinking process in general. First and foremost, humans are complex organisms that have developed over millennia. Taking this into consideration, we need to accept the fact that our brains and our thinking process have also developed over the same millennia. The current scientific theory is that the human brain works on three separate and distinct, but interconnected levels. These three levels are known as the "human brain," the "primate brain," and the "reptilian brain" [25]. The three distinct but connected brains theory is known as the "triune brain model"

and was originally developed by the neuroscientist Paul MacLean [25]. Each level of the brain is thought to have developed during specific stages of human evolution and met each stage's unique requirements for survival. For example, the reptilian brain was most important for surviving in the wild. An example of how the reptilian brain aided in our survival and still does today can be seen when we pick up something to eat, and we smell something that doesn't smell right. Our reptilian brain tells us that whatever it is, it is not good for us to eat, so our reptilian brain takes over and tells the other two to leave it alone and find something else to eat [25]. Now, taking things into consideration, our reptilian brain might have told us that there was danger in the foul-smelling food, it is our human brain that comes to the conscious conclusion that the food has been spoiled and that spoiled food will likely make us ill. In this case, the reptilian brain influenced the human brain without the human brain, even realizing it was being influenced.

In general, the concept of thinking, especially critical thinking, can be broken into three separate bilateral areas: judgment and reasoning, problem-solving and intelligence, conscious thought, and unconscious thought [26]. Critical thinking uses all of these components when applied appropriately to the decision-making process. Judgment and reasoning are the foundation of a normal person's decision-making process. Judgment is something that is developed through experience. Reasoning is the ability to come to a conclusion using the facts presented and an individual's ability to use judgment to determine the strength and viability of the facts. Judgment and reasoning go hand in hand, without one or the other, you would not have a complete decision-making process.

Once we understand the concepts of judgment and reasoning, we need to look at the next components that affect the decision-making process: problem-solving and intelligence. Intelligence should be considered as the ability to obtain and use knowledge [26]. Problem-solving is then the application of intelligence in order to come to a conclusion based on a complex problem [26]. Problem-solving and intelligence provide the glue that holds the decision-making process together.

The last part of thinking that affects the decision-making process is that of conscious thought and unconscious thought. Conscious thought resides at the top level of our minds and is easy to access, while the unconscious thought resides lower in our mind and cannot be readily accessed by the decision-making process, but it certainly does affect the decision-making process. In the Theory of Unconscious Thought, Ap Dijksterhuis and Loran F. Nordgren [17] propose that simple decisions are made by the conscious mind; whereas, complex decisions are better made by the unconscious mind. What is truly the distinguishing factor that differentiates conscious thought and unconscious thought is attention [17].

From an information security process, each of the factors mentioned above is important when understanding why end-users make the decisions that they do. A better understanding of the decision-making process, how cognition works, and the human behaviors behind these decisions will help information security specialists develop more effective training models that will reduce the overall risk of an end-user.

## 5. HUMAN BEHAVIOR AND INFORMATION SECURITY

Information security is normally thought of as the technical approach to securing data/network systems and maintaining the CIA Triad (Confidentiality, Integrity, and Availability). When an information security specialist thinks of the human factor related to information security, they typically only think of the annual information awareness training programs that most organizations incorporate as part of their business model and consider it done [1] [2] [3] [4]. Unfortunately, these models are flawed since they typically only require a person to complete the training annually [3]; furthermore, the training is usually the same, year after year, and the

training was not developed with the reasons why people become security risks in the first place or even developed by someone who has an adult education background [3]. One of the problems with this concept is that information security is a 365-day per year process, not a one-day per year process. Furthermore, some studies show the current method of training end-users to become more security-minded frequently fails to achieve its goal [1]. There are several reasons why the current model of information awareness training is unsuccessful in preparing end-users to defend themselves. To start with, the individuals responsible for developing the information awareness training tools don't take into consideration the human behavioral factors or characteristics that lead to someone making the poor decision that leads to a breach [1] [5] [27] [28]. Secondly, the developers don't fully understand how people think, how the decision-making process works, or anything about the neuroscience behind critical thinking [25]. Additionally, the designers of today's Information Awareness (IA) training programs don't fully understand human nature or how difficult it is to change a person's behaviors [2] [4] [27]. Furthermore, most of the information within an information awareness training program is commonly known and easily found on the Internet [3]. Finally, the individuals developing and running the IA training program at most organizations are neither trained educators nor have a background in adult education [3].

The current policy of conducting information awareness training assumes that by simply informing the end-user of the risk, the end-user will change their behaviors and conduct themselves in a more security-minded manner [1] [5]. As unfortunate as it is, the annual IA training policy only marginally affects cybersecurity because it doesn't really address the issue as to why people continue to be susceptible to becoming the NMIT. Bruce Hallas [2] notes in his book Rethinking the Human Factor that most end-users begin to quickly suffer from cyber fatigue because they are being overwhelmed with the same old IA training programs over and over, and he questions if this is truly the optimal response that we are looking to achieve. If end-users are suffering from cyber fatigue, then one can hypothesize that they have a higher chance of becoming the victim of an attack and converted into an NMIT [2]. As information security professionals, we need to understand better how this can happen and work to identify new, novel methods of preventing this. If we do not, then we are destined to continue to fight the same battles over and over because the end-users go through a cycle of caring, to cyber fatigue, to plain old apathy, and because threat actors are relentless and as long as they are successful, they will continue to target end-users. As long as we don't understand the human behaviors related to someone being susceptible, then we will never develop a better means of preparing the end-users to protect themselves against the threats that exist.

## 6. BEHAVIORAL CHARACTERISTICS AND SUSCEPTIBILITY

Identifying specific human behaviors that make a person more susceptible to becoming an NMIT is not an easy task since human behavior is quite broad and complex. One method of attempting to categorize human behavior related to susceptibility is to use identifiable personality traits. For the purpose of this paper, 600 different personality traits were initially identified from [29] [30] and incorporated into this paper. Initially, these traits were categorized as generally positive, neutral, and negative traits. These traits were then further evaluated by a team of cybersecurity specialists, undergraduate psychology students and graduate psychology students and then reduced to 128 personality traits that could be associated with behaviors that would probably make someone more susceptible to being socially engineered or put themselves at risk of behaving in a manner that could put their organization's networked data at risk of being compromised. Examples of the 128 personality traits are found in table 1, which demonstrates the breadth of the traits that exist. Although the vast majority of the 128 traits identified came from the negative traits category, several came from the neutral traits category, and some even from the positive traits category.

Table 1. Examples of Human Characteristics/Traits that Lead to Susceptibility

| | | |
|---|---|---|
| Absentminded | Anxious | Busy |
| Careless | Complacent | Confident |
| Disobedient | Disorganized | Freewheeling |
| Hurried | Ignorant | Insecure |
| Misguided | Naïve | Placid |
| Pompous | Trusting | Vulnerable |

The process of analyzing the traits to identify which traits should be considered was completed by a cybersecurity expert, an undergraduate psychology student, and a graduate psychology student. The traits, and actions normally associated with the traits, were analyzed and evaluated to determine if the actions associated with the traits were likely to lead to a potential network breach. Certain traits were easily identified as traits that contributed to someone being more susceptible to contributing to a network breach. For example, the first trait in table 1, "absentminded," clearly represents a trait that will likely lead to someone behaving in a manner that could lead to a network security breach. An absentminded person could be more likely to click on a phishing link or malware-infected attachments simply because they are not being mindful of what they are doing, which could result in the network being infected or compromised [15]. Whereas, a person who was not absentminded, but rather mindful in their day to day tasks, would likely be less inclined to click on the link or attachment and would be more likely to question the authenticity of the email. Being absentminded is considered a negative personality trait; however, confidence, also from table 1, would normally be considered a positive trait, yet this trait also exists in the list of 128 identified traits that can lead to susceptibility. Confidence in itself would normally not lead to increased susceptibility, but overconfidence could. When someone becomes overconfident, they also begin to exhibit secondary traits like arrogance, egocentricity, laziness, narcissism, pompous, prejudiced, unpredictable, and venturesome. This example shows the complexity of human behavior, which leads to the difficulty that exists in identifying ways to mitigate the human factors in information security.

Being susceptible means that an individual is easily influenced or potentially easily harmed. For example, a person who trusts everyone, and believes that every person on the planet is honest, is susceptible to being conned or duped by someone who is not an ethical person. Likewise, a person who walks alone in a darkened alley is at a much higher risk of being mugged than a person who walks as part of a group on a well-lit, densely populated street. In both cases, the individual is susceptible to being influenced or harmed. In the realm of information security, the concept of susceptibility is more like the first example than the second. Threat actors are always trying to find ways to gain access to networked systems. As has been previously mentioned in this paper, hackers prefer to gain access through susceptible end-users over hacking a router or firewall. The reason for this is that the human is the easiest way into the system, and most humans are susceptible to this type of attack.

Organizations spend millions on technical measures to defend their data but skimp on developing better, more effective means of protecting the human port Z3r0. Developing a more effective method of preparing end-users and reducing their susceptibility level would cost organizations more money, but if done right, this would be money well spent. We need to break the mold when it comes to end-user information awareness training and develop a new training model that has a foundation in human behavioral factors and the decision-making process. Changing the training model from a flat, stale model to a dynamic, human behavior and decision-making model should improve the security posture of any organization and reduce the end-user's susceptibility.

## 7. WHY DOES IT MATTER

This paper has already shown that threat actors prefer to gain access to networked systems through the end-user since this method of attack is the easiest and has shown to be the most fruitful method of attack. Criminals prefer to do the least amount of work for the most gain. As long as the end-user is the quickest and easiest way to gain access to a system, threat actors will continue to target the end-user.

As threat actors continue to use social engineering techniques and human behaviors as ways to penetrate a network and gain access to networked resources and data, network security specialists need to work to develop better defense mechanisms built upon the lessons learned from studying the human behavioral characteristics that lead to susceptibility. As long as the status quo continues, threat actors will continue to use the end-user as a means to their nefarious end. This paper shows that information awareness training needs to change and change significantly. Until human behavioral factors related to susceptibility are incorporated into the information awareness training models that are used, breaches through the end-users will continue, and the primary method used to attack a network will be the end-user.

## 8. FUTURE WORK

This survey has identified that more research into the human factors of susceptibility is needed. One of the areas that future work can be conducted involves additional research into the development of a new training and assessment tool based on human behaviors and the decision-making process. Including the human behavioral characteristics that lead to susceptibility into the development of a "new" training and assessment should improve information security by providing information security managers with a better method of assessing an employee's risk to the organization. Once an employee's level of susceptibility has been established, the information security manager can then work to reduce the employee's level of susceptibility by providing specific and directed training.

In addition to incorporating the human behavioral characteristics into the information awareness tools, more research needs to be conducted to understand further the relationship between human behavioral characteristics, the decision-making process, and susceptibility. By better understanding how human behavioral characteristics impact the decision-making process, new methods of reducing an employee's susceptibility could be created. Perhaps a new model of information awareness training can be developed, or perhaps an entirely new model, other than IA training, of preparing end-users to defend themselves against social engineering may be developed.

## 9. CONCLUSIONS

In this paper, we reviewed how easy it is for threat actors to use human behaviors against the end-user, especially as a way of converting the end-user into a non-malicious insider threat. One can clearly see that the threat of the non-malicious insider threat is significant and that the current methods used to help prepare end-users to defend themselves are severely lacking. Furthermore, anyone reading this article can clearly see that a change in how the information security industry approaches the human threat to security needs to occur. We need to better understand the human behavioral factors related to susceptibility and work to identify more effective ways of defending against the human attack vector.

Although there have been some articles regarding the basic reasons why information awareness training programs and information awareness campaigns don't work, very few have looked the behavioral characteristics that are associated with the decision-making process and how these behavioral characteristics and the decision-making process impacts end-user's compliance with information awareness training programs and information awareness campaigns. One of the most important takeaways from this article is that changes in the methodology associated with information awareness training need to occur, and these changes need to incorporate a human behavioral factors components as part of the new methodology. Without incorporating the human behavioral factors related to susceptibility, we, as information security professionals, will never be able to secure port Z3r0.

## ACKNOWLEDGMENTS

We would like to thank Dr. Edward Chow and Dr. Rick White from the University of Colorado, Colorado Springs, Dr. Huw Read and Morgan Woods from Norwich University and Dr. Scott Fisher from New Jersey City University. We would like to also thank Norwich University for providing financial support related to this publication.

## REFERENCES

[1] M. Bada, M. A. Sasse and J. R. Nurse, "Cyber security awareness campaigns: why do they fail to change behavior?" in 1st International Conference on Cyber Security for Sustainable Society, Coventry, 2015.

[2] B. Hallas, Rethinking the Human Factor: A philosophical approach to information security awareness, behavior, and culture, The Hallas Institute, 2018

[3] J. Schroeder, Advanced Persistent Training, Edinburgh: Apress, 2017.

[4] L. Zinatullin, The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour, Cambridgeshire: IT Governance Publishing, 2016.

[5] A. McIlwraith, Information Security and Employee Behaviour: How to Reduce Risk Through Employee Education, Training and Awareness, Hampshire: Gower, 2006.

[6] C. Hadnagy, Social Engineering: The Science of Hacking the Human, Indianapolis: Wiley, 2018.

[7] S. Sheng, M. Holbrook, P. Kumaraguru, L. Crannor and J. Downs, "Who Falls for Phish? A Demographic Analysis of Phishing," in CHI'10, Atlanta, 2010.

[8] R. Griffin, "Arrow@Dublin," June 2018. [Online]. Available: https://arrow.tudublin.ie/scschcomdis/143/. [Accessed 8 September 2019].

[9] R. Broadhurst, K. Skinner, N. Sifniotis, B. Matamoros-Macias, and Y. Ipsen, "Phishing and Cybercrime Risks in a University Student Community," SSRN Electronic Journal, 9 May 2018.

[10] Q. Cui, G.-V. Jourdan, G. V. Bochmann, R. Couturier and I.-V. Onut, "Tracking Phishing Attacks Over Time," WWW'17 Proceedings of the 26th International Conference on World Wide Web, pp. 667-676, 2017.

[11] B. E. Gavett, R. Zhao, S. E. John, C. A. Bussell, J. R. Roberts, and C. Yue, "Trustworthy and effective communication of cybersecurity risks: A review," Plos One, vol. 12, no. 2, March 2017.

[12] R. Zhau, S. John, S. Karas, C. Bussell, J. Roberts, D. Six, B. Gavett and C. Yue, "Design and Evaluation of the Highly Insidious Extreme Phishing Attacks," Computer & Security, vol. 70, pp. 634-647, 2017.

[13] KnowBe4, "Security Awareness Fundamentals," KnowBe4, 2019. [Online]. Available: https://www.knowbe4.com/security-awareness-training-features/.

[14] US Department of Defense, "Department of Defense (DoD) Cyber Awareness Challenge 2019," US Department of Defense, 2019. [Online]. Available: https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf. [Accessed 08 09 2019].

[15] J. Reb, Z. W. Ho and J. Narayanan, "Mindfulness at Work: Antecedents and Consequences of Employee Awareness and Absent-mindedness," Mindfulness, vol. 6, no. 1, pp. 111-122, February 2019.

[16] J. Cheyne, J. Carrier and D. Smilek, "Absentmindedness: Lapses of conscious awareness and everyday cognitive failures," Consciousness and cognition, vol. 15, pp. 578-592, 2006.

[17] A. Dijksterhuis and L. F. Nordgren, "A Theory of Unconscious Thought," Perspectives on Psychological Science, vol. 1, no. 2, pp. 95-109, 2006.

[18] J. Mcalaney, S. Faily and J. Taylor, "The Social Psychology of Cybersecurity," in 1st International Conference on Cyber Security for Sustainable Society, Coventry, 2015.

[19] A. Ferreira and S. Teles, "Persuasion: How phishing emails can influence users and bypass security measures," International Journal of Human-Computer Studies, vol. 125`, pp. 19-31, 2019.

[20] C. Yue and H. Wan, "BogusBiter: A transparent protection against phishing attacks.," ACM Trans. Internet Technology, vol. 10, 2010.

[21] M. Mann, Director, Black Hat. [Film]. Universal Studios, 2015.

[22] L. Softely, Director, Hackers. [Film]. United States of America: MGM/UA Home Video, 1996.

[23] "Cognition," Webster's Dictionary, [Online]. Available: https://www.merriamwebster.com/dictionary/cognition#other-words. [Accessed 20 07 2019].

[24] "Cognitive," Webster's Dictionary, [Online]. Available: https://www.merriamwebster.com/dictionary/cognitive. [Accessed 20 07 2019].

[25] A. Rutherford, Neuroscience and Critical Thinking, Albert Rutherford, 2019.

[26] D. Reisberg, Cognition: Exploring the Science of the Mind, New York: W.W. Norton & Company, 2013.

[27] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Guidelines for usable cybersecurity: Past and present," in 2011 Third International Workshop on Cyberspace Safety and Security (CSS), Milan, 2011.

[28] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Trustworthy and Effective Communication of Cybersecurity Risks: A Review," in 2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST), Milan, 2011.

[29] MIT, "638 Primary Personality Traits - Ideonomy," [Online]. Available: http://ideonomy.mit.edu/essays/traits.html. [Accessed 06 07 2019].

[30] B. Davenport, "Live Bold and Bloom," 16 May 2019. [Online]. Available: https://liveboldandbloom.com/02/self-awareness-2/list-of-personality-traits. [Accessed 06 07 2019].

## AUTHORS

Henry Collier is an Assistant Professor of cybersecurity and the Program Manager for the BS in Cybersecurity at Norwich University's College of Graduate and Continuing Studies. Mr. Collier is a Ph.D. Candidate in the Security Engineering program at the University of Colorado, Colorado Springs. His main research areas are human factors in cybersecurity and networking.

Alexandra Collier is a graduate of Norwich University's Bachelor of Art in Psychology degree and a Master's degree student at Southern New Hampshire University studying Clinical Mental Health Counselling.