Received: 2023-12-23 | Revised: 2024-01-24 | Published: 2024-02-13

DOI: 10.59388/pm00374

PSYCHO MACHINA

Analyzing Influential Psychological Factors in Social Engineering; Human Psyche and Cybersecurity

Hamed Taherdoost

University Canada West, Canada

Correspondence Email:
hamed.taherdoost@gmail.com

Keywords
cybersecurity; human psyche; social engineering

Abstract

To delve into the intricate relationship between cybersecurity and human psychology, this article centers its focus on the psychological aspects of social engineering. Understanding these elements is pivotal, and the analysis explores themes directly relevant to social engineering. While the review refrains from delving into specific real-world instances, it consistently emphasizes the consequences of overlooking psychological dimensions. Furthermore, it advocates for the integration of psychological instruction into cybersecurity training to enhance overall preparedness.

INTRODUCTION

The realm of cyber and network systems involves a complex interplay among various entities, including computer system users, security analysts, cyber assailants, and the computer systems themselves. Within this intricate landscape, the primary objective of cyber attackers is to gain, alter, or sustain unauthorized data (Thompson, 2004). While the bulk of cybersecurity research traditionally concentrates on refining computer network systems, software development, and information technology advancements (Nobles, 2018; Sadkhan, 2019), a noticeable gap exists in exploring the augmentation of system analysts' cognitive abilities and situational awareness (Aggarwal et al., 2018; Barford et al., 2010; Gutzwiller et al., 2015; Knott et al., 2013). Moreover, the psychological tactics employed by cyber assailants, including cognitive hacking and social engineering, enable them to exert influence over computer system users (Fraunholz et al., 2018; King et al., 2018). Social engineering attacks, constituting a significant 28% of all cybersecurity attacks according to Bowen et al. (2011), often leverage tactics like phishing. However, the current exposition lacks a coherent flow and depth, making it challenging for readers to assimilate the multifaceted dynamics presented.

Recognizing the inherent susceptibility of humans to psychological manipulation, a human-centric approach to cybersecurity becomes paramount. This article underscores the critical importance of psychological insights in comprehending and mitigating social engineering risks within the constantly evolving cyber threat landscape. By acknowledging the psychological facets ingrained in cybersecurity, the article advocates for formulating effective defensive measures and educational initiatives. The development of training programs rooted in psychological insights empowers individuals to resist manipulation and heighten their awareness of potential threats.

In navigating the intricate dance between cyber adversaries and the human psyche, organizations and individuals can bolster their security measures. An examination of how social norms, trust, dread, and curiosity impact human behavior provides a foundational understanding for crafting strategies that proactively address the nuanced challenges posed by cyber threats. This cohesive approach ensures a seamless transition from the overarching theme of psychological factors in social engineering to the specific intricacies of cyber and network systems, reinforcing the article's consistency and readability.

The primary objective of this study is not to advocate for or against the role of psychological factors in cybersecurity but, rather, to conduct a thorough examination of their intricate interplay, specifically within the realm of social engineering. Our aim is to illuminate the significance of understanding and incorporating psychological insights into the broader cybersecurity framework, emphasizing their pivotal role in addressing the challenges posed by social engineering tactics.

How to cite this article: Taherdoost, H. (2024). Analyzing Influential Psychological Factors in Social Engineering; Human Psyche and Cybersecurity. *Psychomachina, 1*(1). https://doi.org/10.59388/pm00374

This is an open access article distributed under the Creative Commons Attribution International 4.0 License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. ©2023 by author/s. Psychomachina published by Scidac Plus.

SOCIAL ENGINEERING

The biggest danger to cybersecurity is attempts at social engineering (Breda et al., 2017; Chargo, 2018; Pavković & Perkov, 2011). According to the study by Libicki (2018), these attacks are detectable but cannot be effectively thwarted. Social engineers capitalize on the innate social tendencies of individuals by employing deceit and psychological manipulation to exploit vulnerable individuals and acquire confidential data. This data may subsequently be traded on the dark web or utilized maliciously. As a result of the emergence of Big Data, malicious actors exploit substantial volumes of data for commercial gain, packaging and vending extensive datasets as commodities in contemporary markets (Atwell et al., 2016; Mahmood & Afzal, 2013).

Social engineering operates by manipulating human psychology, as opposed to the technological vulnerabilities that are the primary focus of conventional hacking techniques. Adversaries utilize various psychological strategies, capitalizing on sentiments such as curiosity, dread, and trust, among others, to construct an exceptionally versatile and formidable menace. Acknowledging the wide array of these deceptive strategies is imperative to establish and execute efficient cybersecurity protocols. Phishing, a widely observed type of social engineering, entails the utilization of deceitful emails, messages, or websites that imitate reputable organizations. This practice capitalizes on the victim's sense of urgency and trustworthiness. Pretexting is the fabrication of situations to manipulate others by cultivating a semblance of familiarity and trust. Exploiting individuals' curiosity with enticing offers and baiting induces them to perform compromising actions. Quid pro quo capitalizes on the need for immediate benefit by providing incentives in return for confidential data. Engaging in impersonation entails assuming the identity of a trusted individual to exploit their position of authority. Tailgating exploits social norms and physical proximity to obtain unauthorized access.

PSYCHOLOGICAL FACTORS IN SOCIAL ENGINEERING

Several researchers have formulated psychological theories and frameworks to elucidate social engineering, focusing on individuals operating within institutions, engaging in communication, and gaining access to safeguarded systems. Persuasion is a pivotal element in social engineering, with studies (Bullée et al., 2018; Cialdini & Cialdini, 2007; Komatsu et al., 2013; Muscanell et al., 2014) identifying key persuasive attributes essential for successful attacks. These attributes, including authority, scarcity, affection, reciprocity, commitment, and social proof (Figure 1) (Cialdini & Cialdini, 2007), are harnessed by assailants to exploit psychological characteristics in the target, facilitating unauthorized entry. This section delves into the intricate psychological elements that underpin social engineering assaults, shedding light on the nuanced strategies employed by malicious actors.

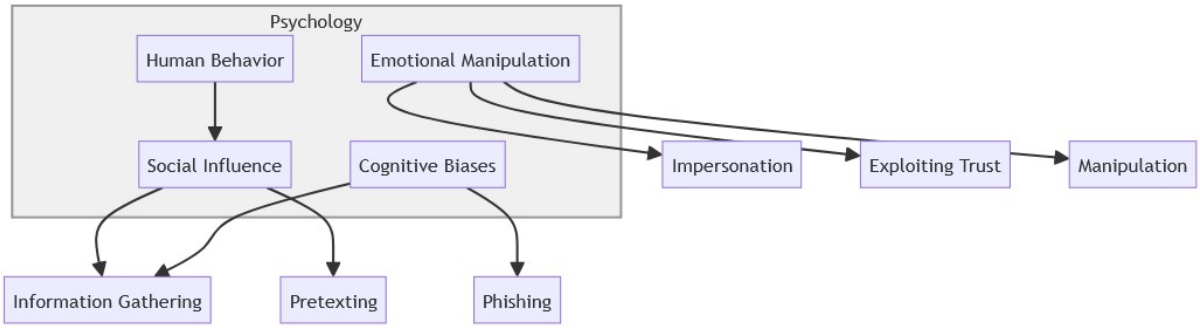

Figure 1. Aspects of psychology influencing social engineering

Reciprocity

Reciprocity, an intrinsic element of social interaction, entails the interchange among numerous participants, frequently to attain reciprocal advantages. Positive forms of reciprocity, which manifest as acts of benevolence in return for prior acts of generosity, are fundamental to forming personal relationships (Gouldner, 1960). The aforementioned reciprocal conduct promotes interdependence and community unity, as emphasized by Putnam (Putnam, 2000), and continues to do so in the dynamic realm of digital engagements (Pelaprat & Brown, 2012). Within this ever-changing milieu, reciprocity is the foundational element that fosters the formation of social connections, thereby enriching the tapestry of interdependent communities.

An investigation into the psychological ramifications of reciprocity by Happ et al. (2016) explores the perception of obligation that some individuals may experience when they perform reciprocal actions. Reciprocity, a principle that transcends interpersonal relationships, is significant in social engineering and cybersecurity dynamics. Capitalizing on the inherent human propensity for reciprocity, malicious actors manipulate trust through reciprocity as a tool, employing strategies such as presenting favors or gifts. To safeguard against reciprocity-based attacks, it is imperative to prioritize vigilance and education, which enable individuals to identify and resist manipulative requests. Comprehensive verification protocols need to be implemented to fortify cybersecurity defenses, and a security culture that values skepticism needs to be fostered. Through a comprehensive understanding of the psychological foundations of reciprocity, organizations, and individuals can enhance their cybersecurity stance, thereby efficiently reducing the potential hazards linked to social engineering.

Commitment

Evaluating employees' dedication to information security within an organization is essential to scrutiny. This dedication transcends mere recognition of security protocols and encompasses an all-encompassing commitment that persists across all levels of the organization and eventually becomes second nature to its employees. Effectively preventing social engineering assaults requires an organization to establish a culture that strongly emphasizes information security (Budzak, 2016; Harkins, 2016).

Considered a relatively stable personal characteristic, commitment has been the subject of extensive investigation in organizational research. An enduring attitude motivates persistent action (McCaul et al., 1995; Sagie, 1998). Allen and Meyer (1990) classified different categories of commitment according to the context and the object of the commitment. The normative commitment, which results from reciprocal exchanges in which effort is exerted because of customary or obligatory expectations, was included (Beck & Wilson, 2000). Social norms are developed by consistency theories, such as the cognitive dissonance theory proposed by Festinger and Carlsmith (1959), which revolves around perceptions of commitment. In pursuit of a sense of consonance, individuals are motivated to maintain congruence between their attitudes, social norms, and behaviors. As individuals evaluate the "give-and-take," taking into account the value and fairness of the exchange, fairness assessments are of critical importance in social exchange theory (Bergman, 2006). Despite unfavorable circumstances, individuals generally adhere to commitments as part of an implicit social contract, as predicted by the elaboration likelihood model and independent of immediate incentives (Theoharidou et al., 2005).

Social Proof

The cognitive inclination to solicit advice from others during periods of uncertainty, referred to as the principle of social proof in social psychology, originates from the inherent human propensity to perceive the behavior as more suitable when observed in a group setting. Social proof, a subset of social influence, is differentiated from normative social influence, which is motivated by the fear of repercussions or the pursuit of social status. Conversely, social proof is predominantly associated with informational social influence, which underscores the significance of personal decision-making influenced by the behavior of others (Cialdini & Cialdini, 2007).

The psychological occurrence known as social proof carries substantial ramifications in fields such as cybersecurity and social engineering, where individuals tend to imitate the behaviors of others when confronted with uncertain circumstances. Social proof techniques, which cybercriminals utilize, consist of behavioral mimicry and the false consensus effect. To illustrate, phishing emails frequently employ counterfeit logos and testimonials to fabricate an aura of authenticity, capitalizing on the general confidence placed in universally acknowledged messages. By exploiting the false consensus effect, deceptive pop-up messages may erroneously assert a widespread security breach to provoke alarm and elicit rash reactions. To strengthen countermeasures against social proof manipulation, it is critical to educate users about these strategies, foster essential evaluation abilities, and establish verification protocols for sensitive operations (Cialdini & Goldstein, 2004).

Liking

From the elaboration likelihood model perspective, the notion of "liking" is founded upon attributes including physical attractiveness, charisma, appeal, or overall popularity (Cialdini, 2009). Peripheral route persuasion is a psychological phenomenon characterized by individuals complying with requests to gain the favor of those possessing the appealing qualities in question (Cacioppo et al., 1986). Social engineering scenarios typically involve

avoiding physical contact between the perpetrator and the victim. Instead, communication is conducted through alternative channels such as websites, email, postal letters, or telephone calls (Dotterweich & Collins, 2006). Consequently, the social engineer needs help communicating qualities such as appeal or charisma. Conversely, their objective is cultivating a cordial relationship with the prospective target to secure their confidence and favor. This is achieved through various strategies, including confidence schemes, exploiting solitude, capitalizing on the human desire for companionship, fabricating associations with affable celebrities, and more (Gendall, 2005; Mitnick & Simon, 2003).

A reciprocal relationship between trust and liking has been established (Asch, 1946; Casciaro & Lobo, 2005; Guadagno & Cialdini, 2002): individuals tend to trust those they also like, and vice versa. Moreover, trust is frequently correlated with perceived credibility, which may be attributed to a particular skill or expertise extraneous to the object or service the "expert" endorses (Cacioppo et al., 1986). Hence, trust is the fundamental basis for favorability in social engineering and information security (Guadagno & Cialdini, 2002).

Authority

Social engineers utilize various strategies, including authority and fear tactics, to coerce potential victims into divulging information or performing predetermined actions (Mitnick & Simon, 2003). This manipulation is exemplified in prevalent phishing schemes, which employ disseminating urgent subject lines in emails to captivate the potential victim's attention. Milgram's seminal study (Milgram & Gudehus, 1978) on obedience to authority presents persuasive empirical support for the degree to which members of authority accept directives from others. Deference to those believed to possess coercive authority, such as the ability to withdraw funds from a bank account or revoke a cherished privilege, is frequently the result of obedience (Weatherly et al., 1999).

Within this framework, authority is a mechanism to evoke dread, compelling people to adhere to directives to prevent adverse repercussions, including the deprivation of privileges, disciplinary action, public disgrace, or censure (Milgram & Gudehus, 1978). Social engineers exploit these dynamics by capitalizing on the fear response that is an inherent human reaction to authoritative commands (Cacioppo et al., 1986; Mitnick & Simon, 2003). According to a study by Weatherly et al. (Weatherly et al., 1999), when fear or threats are used to exert authority, those with a greater propensity to submit to authority are more likely to comply with these demands, in contrast to those who adopt a more skeptical and defiant position.

Scarcity

Effective persuasion strategies that revolve around time-based constraints, such as limited-time sales, illustrate the principle of scarcity. These sales aim to generate a feeling of time sensitivity among prospective purchasers, compelling them to complete a transaction before the limited-time offer's termination and the subsequent escalation in product costs (Siddiqi et al., 2022). Conversely, similar to how authority can elicit a reactive response, it has been noted that scarcity can induce a reactive accumulating impulse (Melamed et al., 1998).

Social engineers often utilize strategies that exploit the concept of scarcity to obtain information or induce responses from potential targets. These tactics operate because the target is time-sensitive or risks missing out on obtaining a limited-edition item (Rutte et al., 1987). Individuals who display greater sensitivity to the threat of scarcity are more prone to succumbing to social engineering tactics that exploit this sensitivity, in contrast to those who resist such threats (Guadagno & Cialdini, 2002).

IMPACT ON CYBERSECURITY

Cybersecurity incidents consist of a series of behavioral actions wherein various psychological factors influence each one. Phishing emails are one method by which cyber adversaries frequently attempt to exploit and manipulate the psychological processes of their targets. This reflects the cyber security tenet that humans are the most vulnerable component (Kearney & Kruger, 2016). Nevertheless, despite the acknowledged significance of the human element, cyber security education and training programs frequently fail to tackle the psychological aspects of this complex field comprehensively. Notwithstanding the substantial body of research in psychology that pertains closely to cybersecurity—including but not limited to comprehending motivation, forecasting future actions, developing user-centric policies and interfaces, and influencing organizational culture and behavior—this remains the case (Taylor-Jackson et al., 2020).

There are numerous reasons why integrating psychological education into cybersecurity training is vital. Preceding all else, comprehending the intricacies of human psychology can facilitate the incorporation of key concepts into cybersecurity awareness training, thereby substantially enhancing an organization's security posture. Conventional cybersecurity training programs frequently neglect the development of psychological and soft skills, which are critical for effectively tackling cybersecurity challenges.

By identifying the most pertinent cybersecurity research areas, psychological studies can ensure that provided training is grounded in empirical evidence and psychological knowledge. Integrating psychological principles into cybersecurity education will enhance the proficiency of practitioners in tackling cybersecurity challenges (Taylor-Jackson et al., 2020). Moreover, incorporating learning into one's weekly, daily, or monthly schedule can aid in improving cybersecurity awareness and cognitive readiness.

Psychological approaches to cybersecurity training for employees and consumers can be effectively utilized by organizations, as evidenced by the success of behavioral-based cyber training programs. These programs endeavor to address the issues of phishing and hacking at a broader level by educating and motivating many individuals to abandon undesirable practices. By employing knowledge of human psychology in cybersecurity training, organizations can develop more impactful and effective programs that address the unique challenges of cybersecurity. The advantages, intended recipients, and approaches to incorporating psychological instruction into cybersecurity instruction are succinctly outlined in Table 1.

Table 1. Key aspects of integrating psychological education into cybersecurity training

Benefits of Psychological Education in Cybersecurity Training	Target Audience	Implementation Strategies
Enhanced Awareness	All employees	Simulated phishing exercises and regular awareness campaigns.
Behavioral Resilience	Employees in customer-facing roles	Role-playing scenarios, workshops.
Adaptive Defense Strategies	Cybersecurity professionals	Continuous threat intelligence updates and regular training.
Holistic Security Approach	Security teams, decision-makers	Cross-departmental collaboration, integrated security frameworks.
Risk Mitigation	All employees	Regular training sessions and interactive modules.
Cultural Shift Toward Security Consciousness	All employees	Leadership support and ongoing communication.

CONCLUSION

The complex relationship between cybersecurity and human psychology, specifically about social engineering, emphasizes the necessity of adopting a holistic strategy to protect digital environments. It is imperative to develop effective defense mechanisms by recognizing the psychological factors that cyber assailants exploit, including but not limited to reciprocity, commitment, liking, authority, social proof, and scarcity. Disregarding these psychological elements may result in detrimental data intrusions and compromised security, which are concrete repercussions. To mitigate these risks, it is critical to incorporate psychological education into cybersecurity training programs. This will enable participants to identify and withstand attempts at manipulation. Incorporating a comprehensive methodology that integrates technological remedies with a profound comprehension of human conduct is critical in constructing a resilient fortification against social engineering assaults.

REFERENCES

Aggarwal, P., Moisan, F., Gonzalez, C., & Dutt, V. (2018). Understanding cyber situational awareness in a cyber security game involving recommendations. *International Journal on Cyber Situational Awareness*(3 (1)), 29 p.

Allen, N. J., & Meyer, J. P. (1990). The measurement and antecedents of affective, continuance and normative commitment to the organization. *Journal of occupational psychology*, *63*(1), 1-18.

Asch, S. E. (1946). Forming impressions of personality. *The journal of abnormal and social psychology*, *41*(3), 258.

Atwell, C., Blasi, T., & Hayajneh, T. (2016). Reverse TCP and social engineering attacks in the era of big data. 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS),

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., Jha, S., Li, J., Liu, P., & Ning, P. (2010). Cyber SA: Situational awareness for cyber defense. *Cyber Situational Awareness: Issues and Research*, 3-13.

Beck, K., & Wilson, C. (2000). Development of affective organizational commitment: A cross-sequential examination of change with tenure. *Journal of vocational behavior*, *56*(1), 114-136.

Bergman, M. E. (2006). The relationship between affective and normative commitment: review and research agenda. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior*, *27*(5), 645-663.

Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. 2011 IEEE International Conference on Technologies for Homeland Security (HST),

Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. INTED2017 Proceedings,

Budzak, D. (2016). Information security–The people issue. *Business Information Review*, *33*(2), 85-89.

Bullée, J. W. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks—A literature-based dissection of successful attacks. *Journal of investigative psychology and offender profiling*, *15*(1), 20-45.

Cacioppo, J. T., Petty, R. E., Kao, C. F., & Rodriguez, R. (1986). Central and peripheral routes to persuasion: An individual difference perspective. *Journal of personality and social psychology*, *51*(5), 1032.

Casciaro, T., & Lobo, M. S. (2005). Competent jerks, lovable fools, and the formation of social networks. *Harvard business review*, *83*(6), 92-99.

Chargo, M. A. (2018). You've Been Hacked: How to Better Incentivize Corporations to Protect Consumers' Data. *Transactions: Tenn. J. Bus. L.*, *20*, 115.

Cialdini, R. B. (2009). *Influence: Science and practice* (Vol. 4). Pearson education Boston, MA.

Cialdini, R. B., & Cialdini, R. B. (2007). *Influence: The psychology of persuasion* (Vol. 55). Collins New York.

Cialdini, R. B., & Goldstein, N. J. (2004). Social influence: Compliance and conformity. *Annu. Rev. Psychol.*, *55*, 591-621.

Dotterweich, D. P., & Collins, K. S. (2006). The practicality of Super Bowl advertising for new products and companies. *Journal of Promotion Management*, *11*(4), 19-31.

Festinger, L., & Carlsmith, J. M. (1959). Cognitive consequences of forced compliance. *The journal of abnormal and social psychology*, *58*(2), 203.

Fraunholz, D., Anton, S. D., Lipps, C., Reti, D., Krohmer, D., Pohl, F., Tammen, M., & Schotten, H. D. (2018). Demystifying deception technology: A survey. *arXiv preprint arXiv:1804.06196*.

Gendall, P. (2005). Can you judge a questionnaire by its cover? The effect of questionnaire cover design on mail survey response. *International journal of public opinion research*, *17*(3), 346-361.

Gouldner, A. W. (1960). The norm of reciprocity: A preliminary statement. *American sociological review*, 161-178.

Guadagno, R. E., & Cialdini, R. B. (2002). Online persuasion: An examination of gender differences in computer-mediated interpersonal influence. *Group dynamics: Theory, research, and practice*, *6*(1), 38.

Gutzwiller, R. S., Fugate, S., Sawyer, B. D., & Hancock, P. (2015). The human factors of cyber network defense. Proceedings of the human factors and ergonomics society annual meeting,

Happ, C., Melzer, A., & Steffgen, G. (2016). Trick with treat–Reciprocity increases the willingness to communicate personal data. *Computers in Human Behavior*, *61*, 372-377.

Harkins, M. (2016). The cause is also the cure. *People & Strategy*, *39*(1), 7-9.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security*, *61*, 46-58.

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in psychology*, *9*, 39.

Knott, B. A., Mancuso, V. F., Bennett, K., Finomore, V., McNeese, M., McKneely, J. A., & Beecher, M. (2013). Human factors in cyber warfare: Alternative perspectives. Proceedings of the Human Factors and Ergonomics Society Annual Meeting,

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security: An empirical study of intentional versus actual behavior. *Information Management & Computer Security*, *21*(1), 5-15.

Libicki, M. (2018). Could the issue of DPRK hacking benefit from benign neglect? *Georgetown Journal of International Affairs*, *19*, 83-89.

Mahmood, T., & Afzal, U. (2013). Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools. 2013 2nd national conference on Information assurance (ncia),

McCaul, H. S., Hinsz, V. B., & McCaul, K. D. (1995). Assessing organizational commitment: An employee's global attitude toward the organization. *The Journal of applied behavioral science*, *31*(1), 80-90.

Melamed, Y., Szor, H., Barak, Y., & Elizur, A. (1998). Hoarding-What does it mean? *Comprehensive psychiatry*, *39*(6), 400-402.

Milgram, S., & Gudehus, C. (1978). Obedience to authority. In: Ziff-Davis Publishing Company New York, NY.

Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Muscanell, N. L., Guadagno, R. E., & Murphy, S. (2014). Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass*, *8*(7), 388-396.

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA–Journal of Business and Public Administration*, *9*(3), 71-88.

Pavković, N., & Perkov, L. (2011). Social Engineering Toolkit—A systematic approach to social engineering. 2011 Proceedings of the 34th International Convention MIPRO,

Pelaprat, E., & Brown, B. (2012). Reciprocity: Understanding online social relations. *First Monday*.

Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. Simon and schuster.

Rutte, C. G., Wilke, H. A., & Messick, D. M. (1987). Scarcity or abundance caused by people or the environment as determinants of behavior in the resource dilemma. *Journal of Experimental Social Psychology*, *23*(3), 208-216.

Sadkhan, S. B. (2019). Cognition and the future of information security. 2019 International Conference on Advanced Science and Engineering (ICOASE),

Sagie, A. (1998). Employee absenteeism, organizational commitment, and job satisfaction: Another look. *Journal of vocational behavior*, *52*(2), 156-171.

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences*, *12*(12), 6042.

Taylor-Jackson, J., McAlaney, J., Foster, J. L., Bello, A., Maurushat, A., & Dale, J. (2020). Incorporating psychology into cyber security education: a pedagogical approach. Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24,

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers & Security*, *24*(6), 472-484.

Thompson, P. (2004). Cognitive hacking and intelligence and security informatics. Enabling Technologies for Simulation Science VIII,

Weatherly, J. N., Miller, K., & McDonald, T. (1999). Social influence as stimulus control. *Behavior and Social Issues*, *9*, 25-45.