Why Do People Fall For Scams? A Personality-Based View Using Eysenck's Pen Model

Neethu R Menon
Assistant Professor
Kochi Business School, Edachira, India

Abstract - Social engineering (SE) attacks, which rely more on psychological manipulation than technical flaws, have become one of the most widespread threats in the cybersecurity space. Humans are considered the weakest link when it comes to cyber vulnerability. Though there has been number of studies regarding human errors and social engineering attacks, the influence of different personality traits remains less explored. In this study we try to map personality traits using PEN model Psychoticism, Neuroticism and Extraversion and the sub traits associated with them to susceptibility in different social engineering attacks. The framework emphasises the significance of personality-aware cybersecurity education and risk mitigation techniques while providing a theoretical basis for upcoming empirical research. By going beyond "one-size fits-all" solutions and towards more individualised, psychologically-informed defence mechanisms, this research advances a deeper awareness of the human factors underlying social engineering.

Index Terms - Social Engineering Attacks; Personality Traits; Eysenck's PEN Model; Cybersecurity Behavior; Psychological Vulnerabilities; Conceptual Framework

I. INTRODUCTION

Digital connectivity has become an essential part of our daily lives. As we advance digitally so does the advancement in cybercrimes happen. We have improved features and firewalls for protecting our digital assets but still human error remains the major and undeniable source cyber-attacks. Social engineering relies on the human mind than a system bug in comparison to regular cyberattacks. Phishing, pretexting, baiting, and impersonation are some of the wide array of dirty tricks that fall under the rubric of social engineering that often leverages cruel psychological triggers such as urgency, fear, curiosity, trust, etc. The impact of these attacks in the real world is highlighted by high-profile events such as the Equifax hack (2018), which exposed the personal information of over 145 million people, and the Twitter Bitcoin scam (2020), which damaged the accounts of prominent public figures.

This raises a critical question: Why do some people fall victim to scams with high frequency while others are more vigilant? While situational factors such as stress, distraction, or decision fatigue increase susceptibility, the evidence is increasingly clear that individual attributes play important role over how people perceive and respond to social engineering attacks. Traditional defence methods and awareness initiatives often assume these psychological distinctions don't exist.

This gap is addressed in the present study, where Eysenck's PEN personality model is applied to the examination of scam susceptibility, which classifies traits into the three PEN categories: neuroticism, extraversion, and psychoticism. Sub-traits or facets for a given dimension, such as impulsivity, risk-taking, sociability or anxiety, could lead to individuals being particularly vulnerable to manipulative tactics in different manner. The current study provides a theoretical framework to make sense of how and why individual differences in personality influence vulnerability to fraud, by demonstrating how those traits map onto well-recognised social engineering tactics.

There are theoretical and practical advantages in this person-centred approach: it increases our understanding of the way people experience cybersecurity situations and informs the development of targeted risk reduction interventions. Ultimately the human firewall may hinge on understanding and mitigating individual personality differences.

II. LITERATURE SURVEY

Using a method of psychological manipulation called "social engineering," an attacker can gain unauthorised access to sensitive data or systems or even physical access to a building simply by through different human behaviours. It exploits the unpredictability of the humans (humans are the strongest and weakest link in the computer systems) rather than exploiting the vulnerability of the software (Salahdine & Kaabouch, 2019). Phishing, baiting, pretexting, vishing, spear phishing, and tailgating are examples of traditional strategies.

Information gathering, trust-building, exploitation, and disengagement are the predictable stages of these attacks (Mouton et al., 2014). Due to its ability to effectively exploit psychological and emotional triggers like urgency, fear, empathy, reciprocity, and authority, social engineering persists despite improvements in security tools (Gupta et al., 2016; Mouton et al., 2014).

Salahdine and Kaabouch (2019) categorises social engineering attacks into direct and indirect attacks, as involving technical, social, and physical vectors and depending on the nature of interaction, whether it is based on a computer or human. High-profile attacks such as the Twitter Bitcoin scam and Equifax breach are evidence of the massive financial and mental toll of these tactics. The FBI reports that social engineering is responsible for over 84% of successful attacks in the US, resulting in billions of dollars in losses each year.

The first phase in the steps to a social engineering attack involves an information gathering, once this succeeds, the process then shifts to trust, exploitation and clean escape to avoid a mishap (Mouton et al., 2014). Tactics include spear phishing, business email compromise, and more targeted strategies like phishing, vishing and baiting. The attacks exploit emotionally-anchored emotional buttons such as fear, urgency, trust, and reciprocation (Gupta et al, 2016; Salahdine & Kaabouch, 2019). These attacks prey on your emotions such as fear, rush, trust, and obligation.

Although awareness campaigns and technical training are frequently employed to stop these attacks, they frequently overlook more profound psychological elements that increase vulnerability. According to recent psychological and cybersecurity research, some personality traits may increase a person's tendency for dishonesty. People's interpretations and responses to potentially harmful interactions are influenced by a variety of factors, including behavioural tendencies, emotional states, and cognitive biases (Cristescu et al., 2022).

While conditioning and training are often used to prevent these attacks, they often neglect deeper psychological factors that infuence susceptibility. New research suggests certain psychological characteristics can make someone more inclined to be dishonest. Response and interpretation of potential negative interactions People’s response and interpretation of possible negative interactions are determined by several factors including behavioural predispositions, including aggressiveness or intimidation, current emotional
state and cognitive biases (Cristescu et al., 2022). But the sentinels work on us as if they're armed with two crude hammers, seemingly oblivious to the fact that there is a vexing set of individual differences that have created groups of users, some of whom are susceptible and some of whom aren't.

Researchers have also begun examining personality models such as the Myers-Briggs Type Indicator (MBTI) and the Five-Factor Model (FFM) in an attempt to shed light on victim behaviour. Trait correlation to scam susceptibility for these studies There is a significant relationship between susceptibility to scams and traits such as agreeableness, extraversion, and neuroticism based on these works. For instance, those with high neuroticism tend to respond to threat with anxiety and fear; they therefore tend to make hasty or risk-averse decisions. Although agreeable individuals may have a lower tendency to protest when asked for help and to say no, extraverts may be susceptible to socially persuasive messages (Alseadoon et al., 2015; Teodorescu et al., 2019; Cristescu et al., 2022).

Although these models have yielded valuable insights, Eysenck's PEN model, which focusses on three fundamental personality dimensions psychoticism, extraversion, and neuroticism and has a biological foundation, presents a particularly compelling framework for comprehending scam susceptibility (Eysenck & Eysenck, 1975). Impulsivity, risk-taking, and sensation-seeking are traits associated with psychoticism that can lead people to interact with dubious content without doing enough research. Assertiveness and sociability are traits of extraversion that may make people more receptive to socially constructed messages. Anxiety, guilt, and other emotional instability are captured by neuroticism and can result in fear-driven compliance (Cristescu et al., 2022; Primary Traits of Eysenck's PEN System, 2001).

In conclusion, a crucial field of research is the nexus between personality psychology and social engineering. In addition to improving theoretical knowledge, Eysenck's PEN model serves as a basis for more focused and successful interventions. The secret to defeating social engineering attacks might lie in bridging the gap between cybersecurity strategy and personality research.

III. THEORETICAL BACKGROUND: EYSENCK’S PEN PERSONALITY MODEL

Why Are Some People More Vulnerable to Scams? To answer why some individuals are more susceptible than others, we need to take into account differences in people’s behavior under manipulation. One of the most famous and biologically based theories in personality psychology is Eysenck's PEN model (Hans J. Eysenck & Sybil B. G. Eysenck, 1975). Three broad categories of personality are identified by the PEN model: neuroticism, extraversion and psychoticism. Each of these categories represents unique patterns of thought, feelings, and action. There are three main factors by the hierarchical personality theory, the PEN model: Psychoticism (P):

This trait reflects a person's tendency toward impulsive, antisocial, manipulative, and tough-minded behaviour, lacks realism, tab-breaking, low empathy, and risk; all are commonly linked with high psychoticism hits. Extraversion (E): Factor includes assertiveness, and the stimulation seeking of the individual. Extraverts, being more sociable or expressive, might be more susceptible to interactive SE attacks and social influencing. Neuroticism (N): Emotional instability, anxiety, feelings of guilt and worry, and vulnerability to stress are characteristics of individuals with high N scores. They often behave irrationally under pressure, and they are more responsive to urgent messages or threatening words. Recent research has advanced the PEN model in Figure 1 by suggesting sub-traits that can reflect more specific behavioural propensities.

PEN Trait	Sub Trait
Psychoticism	Risk Taking Impulsive Irresponsible Manipulative Sensation-seeking Tough Minded Practical
Neuroticism	Inferiority Unhappy Anxiety Guilt Obsessive Dependence Hypochondriacal
Extraversion	Active Sociable Expressive Assertive Ambitious Dogmatic Aggressive

Fig 1. Sub Traits of PEN Models

IV. SOCIAL ENGINEERING ATTACKS

Social engineering is a psychological attack where an attacker tricks and manipulate someone by making them believe that the attacker is someone they are not and gains access to information or systems. Social engineering relies on the weaknesses of people's cognitive and emotional behaviours, and the gullibility, frequently with the practice of deceit, persuasion and impersonation, rather than the technical deficiencies exploited in regular cyber security attacks (Salahdine & Kaabouch, 2019; Gupta, et al., 2016).

Regardless of the variety of these attacks, they all employ the same tactic: taking advantage of psychological shortcuts and human tendencies. A summary of 20 well-known social engineering attack types is provided below. This categorization and explanation of social engineering attacks is based in part on the survey by Salahdine and Kaabouch (2019), which provides a comprehensive classification and description of social engineering techniques and their psychological foundations.

Phishing - a fraudulent message (often an email) that looks authentic and asks the recipient to enter credentials, download a file, or click a link.

Baiting - An attack that uses the promise of something useful (such as USB drives or free downloads) to trick victims into clicking on links or downloading malicious software.

Pretexting - To fool the target into disclosing private or sensitive information, the attacker creates a plausible scenario (a "pretext").

Tailgating - Following someone with permission to enter a secure area without authorisation, frequently by striking up a conversation or taking advantage of social conventions.

Ransomware - Malicious software that encrypts a victim's files and then demands ransom to unlock them.

Impersonation on Help Desk - Posing as an authorised support employee (such as the IT help desk) in order to obtain users' login information or permissions for remote access.

Diversion Theft - Using impersonation or fake instructions to divert a delivery or shipment to a location controlled by the attacker.

Dumpster Diving - Looking through actual trash to find private papers, identification documents, or abandoned electronics that might hold information

Shoulder Surfing - Looking over someone's shoulder, either in person or through cameras, in order to get private information, such as PINs or passwords.

Quid Pro Quo - Providing a service or advantage in return for system access or private data. For instance, asking for login credentials while pretending to be IT support.

Pop-Up Windows - False pop-ups that ask users to install malicious software or enter login credentials, such as "Update required" or "Virus detected."
Robocalls - Automated phone calls with urgent-sounding messages often involving financial or legal threats that are meant to arouse fear or compliance.
Reverse Social Engineering - To gain access and the victim's trust, an attacker creates a perceived or actual problem and then pretends to be the one offering a solution.
Online Social Engineering - Using fictitious identities on the internet (such as social media profiles) to establish a connection, obtain data, or disseminate harmful content.
Phone Social Engineering - Live phone calls in which the attacker poses as a reliable individual (such as a bank employee or colleague) in order to trick the victim into disclosing private information.
Stealing Important Documents - Physically entering and taking sensitive or private documents (such as hard drives, ID cards, and reports) out of unprotected areas.
Fake Software - Applications that look authentic but contain spyware or malware are frequently downloaded willingly by the user.
SMiShing - Via texting applications or SMS, social engineering occurs when hackers send fake messages tempting recipients to click on links or reply with personal information.
Whitelisting Flow - Passing off a malicious application as a normal or legitimate software request in order to fool system administrators into approving it.
Pharming - Transferring a user from a trustworthy website to a fake one, frequently through the use of malware or DNS flaws.

V. CONCEPTUAL FRAMEWORK

The degree of individuals' susceptibility to SE attacks is not randomly predisposed, but instead is highly associated with some psychological attributes, importantly personality. We construct a theoretical model that integrates types of social engineering attacks with Eysenck's PEN model of personality (Psychoticism, Extraversion, and Neuroticism) and its relations with sub traits describing it and explain the variation in vulnerability. This framework theorises how fundamental characteristics affect how people behave in response to different psychological strategies employed by attackers.

Role of Sub-Traits in Framework Development

This study first looked at the sub-traits that underlie each PEN dimension in order to identify the precise psychological weaknesses that are used in social engineering attacks. The problem behaviours commonly exploited by attackers are then directly mapped to underlying sub-traits such as impulsivity, sensation-seeking, sociability, assertiveness, anxiety, and guilt. For instance, the sub-traits under the trait psychoticism like impulsivity are strongly related to being more likely to download unauthorised software without checking it and clicking on unsafe websites. Others are also easier for strangers to approach, which makes them the victims of social attacks such as tailgating and online social engineering. This is accounted for by sociability and expressiveness (under extraversion). Individuals with anxiety and dependency (sub-scale of neuroticism) are more responsive to fear and authority style tactics, leading to their compliance at the moment without thinking. The resultant framework is firmly rooted in sub-trait-based behavioural patterns, even though it is presented at the broader PEN dimension level for simplicity. The conceptual model's theoretical foundations are reinforced by this multi-layered approach, which also provides a way forward for future empirical research to confirm relationships at the trait and sub-trait levels.

Linking PEN Traits with Social Engineering Attacks

A systematic mapping between the two domains is necessary to comprehend how distinct personality traits affect vulnerability to different types of social engineering attacks. A Venn diagram is used in Figure 2 to show this relationship, with attacks arranged according to the dominant PEN trait or traits they target.

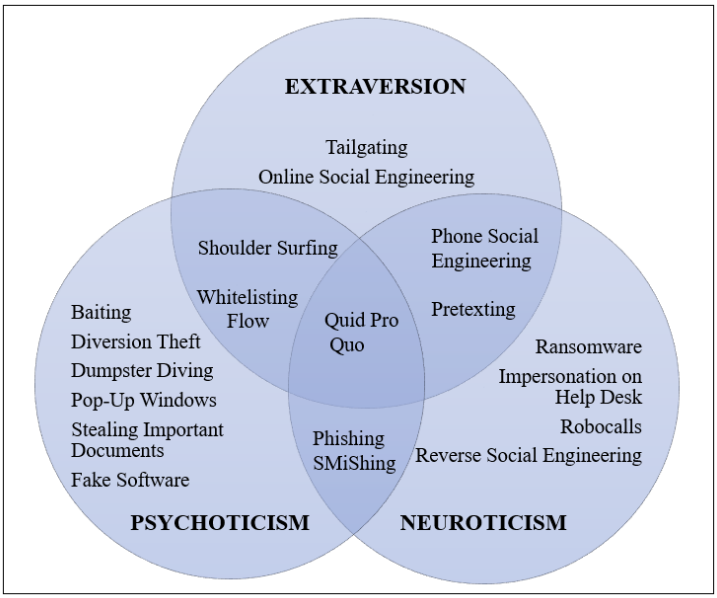

Fig 2: Mapping of Different Social Engineering Attacks to Eysenck's PEN Personality Traits

As shown in the figure,

Being impulsive, risk-taking, irresponsible, and pragmatic attitudes can be related to the psychoticism factor. Such people are often susceptible to attacks like baiting, diversion theft, dumpster diving, fake software, and pop-up. Sociability, expressiveness, and assertiveness are characteristics of extroverts. They are the most susceptible to people-based attacks, which are more focused on interaction and trust, such as tailgating and online social engineering.

Attacks on emotional instability, anxiety, and dependency are related to neuroticism. Fear-based, urgency-driven attacks like ransomware, help desk impersonation and robocalls are in particular meant to take advantage of people with a high level of neuroticism.

Some attacks, such as Quid Pro Quo, SMiShing, and Phishing, show up at the intersection of several characteristics, suggesting that they take advantage of several psychological weaknesses at once.

Mapping Attack Themes to PEN Traits

We further map these attack themes to particular vulnerabilities linked to Eysenck's PEN personality traits, building on the categorisation of social engineering attacks by psychological mechanisms. This mapping demonstrates how an individual's vulnerability to specific kinds of deception is influenced by various cognitive and emotional traits that are as identified by the PEN model.

The broad categories of social engineering attack techniques are grouped in Figure 3 according to the psychological trigger that they mostly target.

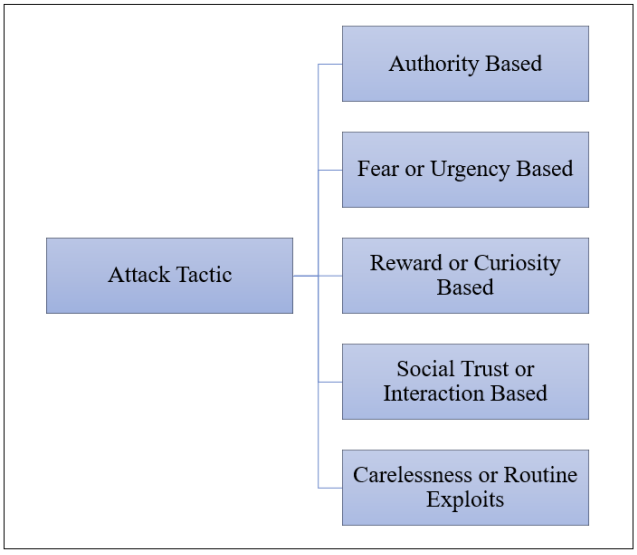

Fig 3: Types of Attacks Tactics

Here are the primary themes of attack:

Authority Based: Convince others by appealing to their sense of trust or fear for those in power.

Fear & Urgency Based: To scare or rush you into hasty and thoughtless action.

Reward or Curiosity Based: Motivate and trick victims with rewards, offers, or invitations.

Social Trust/ Interaction Based: Employ friendliness, trust, or a pose of helpfulness to deceive victims.

Carelessness/ Routine Exploits: Exploit a habit, carelessness or any form of accidental or focused slip of the mind.

These themes generate certain psychological responses among certain individuals, these may vary according to the personality profile of the individuals, which make them more prone to risk.

A detailed mapping of the attack themes, attack techniques, vulnerable attributes, and psychological cause of vulnerability is depicted in Figure 4.

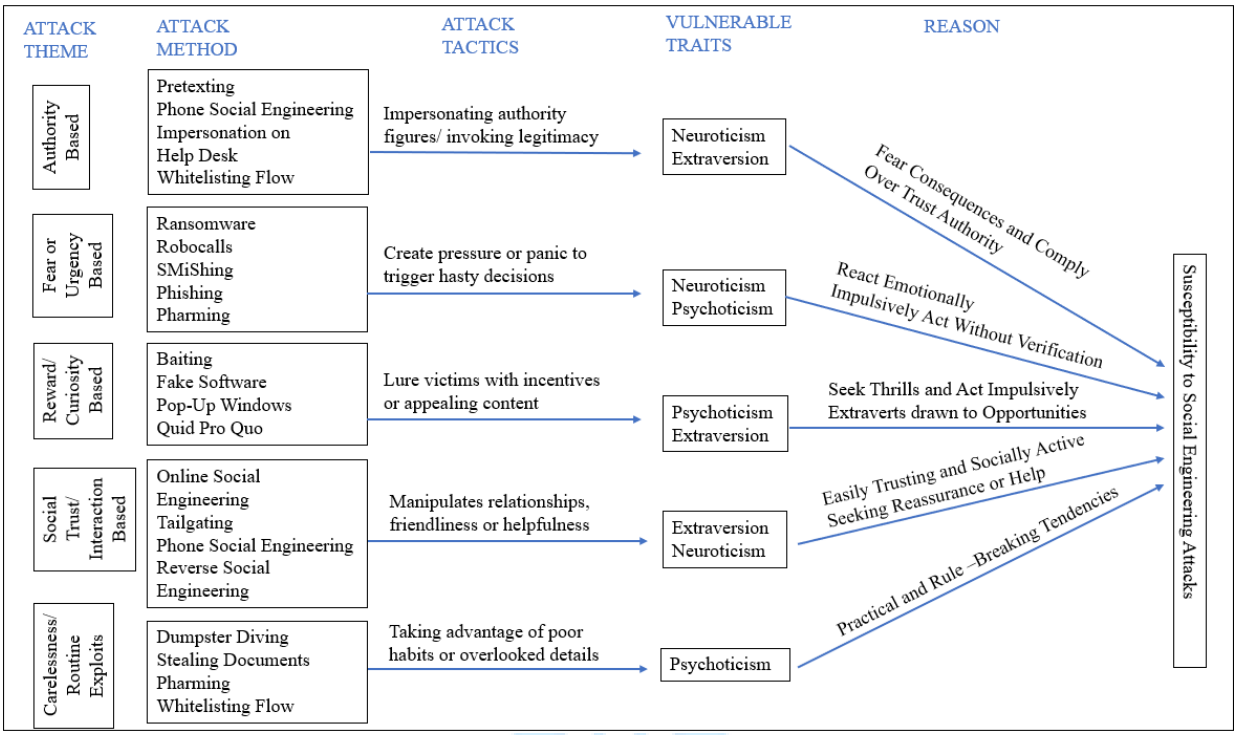

Fig 4 : Mapping of Attack Themes to Vulnerable Traits and Reasons for Susceptibility

Among the mapping's key findings are:

It is people with high levels of neuroticism and extraversion who are the main targets of authority-based attacks. Extraverts may be quite trusting while neurotic people are highly nervous of bad happenings and therefore easily submit to authority.

Attacks motivated by fear or urgency are more likely to occur in people who exhibit high levels of neuroticism and psychoticism. Psychotic people act impulsively without enough evidence, while neurotics react emotionally when under pressure.

People with high levels of extraversion and psychoticism who are impulsive, thrill-seeking, and drawn to new experiences respond best to reward or curiosity-based attacks. Because of their propensity to seek assistance or reassurance, extraverts and neurotics are the targets of social trust or interaction-based attacks. Figure 5 summarises the PEN traits susceptible to various attack themes.

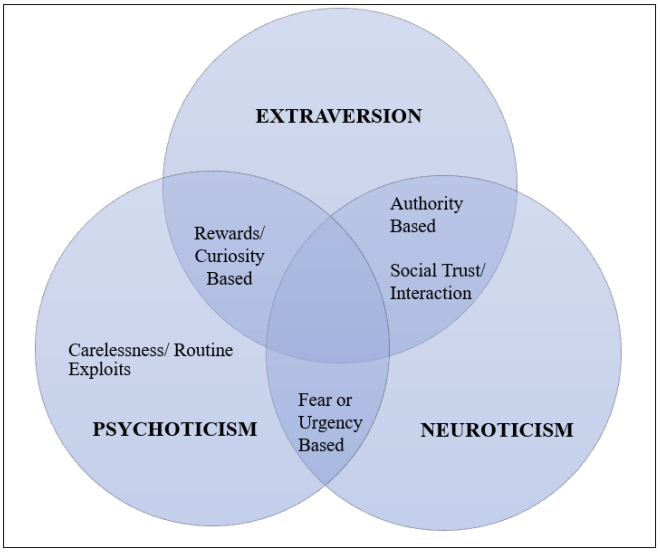

Fig 5: Mapping of Attack Themes to Eysenck's PEN Personality Traits

VI. CONCLUSION

In this study we created a conceptual model that provides the relationship between psychological traits in the PEN model which are Psychoticism, Neuroticism and Extraversion and different types of social engineering attacks. The sub traits associated with PEN traits were also used in the analysis to provide more comprehensive results.

The model links attack mechanisms to specific vulnerabilities rooted in fundamental personality traits and categorises them into five psychological themes: authority-based, fear-based, reward-based, social trust-based, and carelessness-based.

The findings imply that:

Because of their emotional reactivity and dependence, neurotic people are more likely to use fear and authority-based strategies.

Because extraverted people are more gregarious and expressive, they are more susceptible to reward-based attacks and social trust issues.

Attacks based on reward, urgency, and carelessness that are motivated by impulsivity, risk-taking, and a lack of respect for protocol are all associated with psychoticism.

This framework highlights the fact that social engineering attacks take advantage of particular, predictable psychological tendencies rather than being completely random occurrences. By being aware of these trends, cybersecurity professionals can create more individualised and successful training programs, identify risky behaviours, and create behavioural as well as technical interventions.

Although this study offers a solid theoretical framework, it also encourages more empirical research to support the suggested connections. The predictive power of the model can be improved and strengthened by quantifying the true influence of personality traits on cybersecurity vulnerabilities through longitudinal research, behavioural experiments, and real-world simulations.

To sum up, incorporating personality psychology into information security presents a viable way to create a more human-centred defence against the constantly changing threat of social engineering attacks.

VII. REFERENCES

[1] Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183–196.

[2] Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1).

[3] Arabia-Obedoza, M. R., Rodriguez, G., Johnston, A., Salahdine, F., & Kaabouch, N. (2020). Social Engineering Attacks A Reconnaissance Synthesis Analysis. *11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA*, 0843–0848.

[4] Costa, P. T., & McCrae, R. R. (1995). Primary traits of Eysenck's P-E-N system: Three- and five-factor solutions. *Journal of Personality and Social Psychology*, *69*(2), 308–317.

[5] Cristescu, I., Ciuperca, E. M., & Cirnu, C. E. (2022). Exploiting personality traits in social engineering attacks. *Romanian Journal of Information Technology and Automatic Control*, *32*(1), 113–122.
[6] Cullen, A., & Armitage, L. (2018). A Human Vulnerability Assessment Methodology. *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA)*, 1–2.
[7] Eysenck, H. J., Barrett, P., Wilson, G., & Jackson, C. (1992). Primary trait measurement of the 21 components of the P-E-N system. *European Journal of Psychological Assessment*, 109–117.
[8] Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *International Conference on Computing, Communication and Automation (ICCCA2016*, 537–540.
[9] Koyun, A., & Al Janabi, E. (2017). Social engineering attacks. *Journal of Multidisciplinary Engineering Science and Technology (JMEST)*, 7533–7538.
[10] Mouton, F., Malan, M. M., Leenen, L., & Venter, H. (2014). Social engineering attack framework. *Information Security for South Africa*, 1–9.
[11] Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: a survey. *Future Internet*, *11*(4), 89.
[12] Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. *2014 Workshop on Socio-Technical Aspects in Security and Trust, Vienna, Austria*, 24–30.
[13] Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421.