The Big Five in Action: A Systematic Review of Personality, Cyber Awareness, and Behaviors

Saroja Roy Grandhi and Jeremiah D. Still

Old Dominion University, Norfolk VA 23529, USA
{ sgran029, jstill } @odu.edu

Abstract. With cybercrime on the rise, understanding the human factors that contribute to online vulnerability is essential for developing effective prevention and mitigation strategies. Understanding individual differences is crucial for developing effective cybersecurity interventions. Personality traits, specifically the Big Five (openness, conscientiousness, extraversion, agreeableness, and neuroticism), have been shown to influence a wide range of human behaviors, including those related to cybersecurity. This systematic review examines the relationship between these personality traits and cyber awareness/behaviors in end-users. A systematic search across five databases (PubMed, Web of Science, APA PsycInfo, ACM Digital Library, and ProQuest) was conducted, covering 2014 to 2024. Studies were included if they: 1.) measured Big Five Personality Traits, 2.) assessed the relationship between these traits and cyber awareness or cybersecurity behaviors, and 3.) involved end-users. Forty studies met the inclusion criteria. Conscientiousness consistently emerged as a key factor associated with positive cybersecurity behaviors. Agreeableness and openness were also positively related to secure cyber behaviors, while neuroticism and extraversion were linked to increased vulnerability. These findings underscore the potential value of individual difference knowledge, like personality traits, in designing human-centered computing systems. Future developers can enhance their user experience and security compliance by designing with these traits in mind.

Keywords: Personality Traits, Cyber Security, Human Factors.

1 Introduction

Cybersecurity continues to be a growing concern as the prevalence of cyber threats increases globally. Despite advancements in technological defenses, human factors remain one of the weakest links in ensuring robust cybersecurity. According to the 2023 FBI Internet Crime Report, there were 880,418 cybercrime complaints, resulting in financial losses exceeding $12.5 billion (Federal Bureau of Investigation, 2024). Much of the existing research in cybersecurity has emphasized enhancing computer network systems (Nobles, 2018), with a prevalent belief that advancements in information technology and software development are key to improving information security (Benson & McAlaney, 2020). Several researchers have mentioned that humans are considered the greatest vulnerability to security, which has also been confirmed by recent reports.

The 2024 Verizon Data Breach Investigations Report highlighted that the human element accounted for 68% of data breaches (Verizon, 2024). These alarming statistics emphasize the need to promote secure online behaviors and enhance individual cyber awareness to mitigate risks.

Human behaviors in digital environments can often deviate from rational security practices, leaving individuals susceptible to threats such as phishing attacks, password breaches, and identity theft. Scholars have increasingly recognized the importance of individual differences in cybersecurity behaviors (Shillair et al., 2015). Understanding the psychological factors underlying user behaviors is essential for understanding how to design effective interventions that encourage safer usage. Traditionally, personality traits have been employed to predict individuals' attitudes and behaviors across various contexts. In cyber environments, they are critical for predicting susceptibility to cyber threats and guiding the design of security interventions (Hadlington & Chivers, 2020). A commonly employed measure of personality is the Big Five personality traits model. We completed a systematic literature review examining the relationship between Big Five traits and cyber awareness in end-users.

1.1 The Big Five Personality Traits

Personality traits refer to enduring patterns of thoughts, emotions, and behaviors that distinguish individuals from each other (Funder, 2001). These traits are shaped by genetic predispositions, environmental influences, and personal experiences, resulting in unique personality profiles for each individual (McCrae & John, 1992). How individuals perceive and respond to situations, including their likelihood of engaging in risky or malicious behaviors, can be significantly influenced by their unique personality traits (Nurse et al., 2014). The Big Five Personality Traits are: 1.) openness, 2.) conscientiousness, 3.) extraversion, 4.) agreeableness, and 5.) neuroticism (Costa & McCrae, 1992). This measure of personality traits is widely accepted for predicting human behaviors, from social interactions to professional decision-making (Liani et al., 2021). Further, they have been extensively studied and validated across cultures, demonstrating an ability to be useful and robust (McCrae & Costa Jr., 1999; Soto & John, 2017). Table 1 provides a brief description of each trait based on their foundational work.

Table 1. Big Five Personality Traits Descriptions

Trait	Description
Openness	Involves imagination, creativity, and a preference for novelty and variety.
Conscientiousness	Characterized by self-discipline, organization, and a goal-oriented approach to tasks.
Extraversion	Associated with sociability, assertiveness, and the tendency to seek stimulation in social settings.
Agreeableness	Reflects a cooperative, trusting, and compassionate nature.

Neuroticism	Indicates emotional instability and a tendency to experience negative emotions, such as anxiety.

These traits have been shown to influence various cybersecurity behaviors, offering insight into why some individuals adopt secure online practices while others engage in risky behaviors. For instance, individuals who are highly conscientious are more likely to adopt proactive security measures as they have higher information security awareness. Those with high neuroticism showed less general trust, making them less vulnerable to online threats (Albladi & Weir, 2017). Several studies have supported the predictive utility of the Big Five in cybersecurity contexts, demonstrating associations between personality traits and behaviors. Examples include password management, phishing susceptibility, and compliance with security protocols (Gratian et al., 2018; Rahman et al., 2024; Alanazi et al., 2020).

Cyber Awareness. Cyber awareness refers to the knowledge and behaviors individuals exhibit to ensure their online safety, information security, and privacy protection (Thomson, 2021; Vestad, 2022). Research indicates that individual differences in personality traits may significantly influence levels of cyber awareness. For instance, individuals with high conscientiousness, openness, and agreeableness tend to exhibit greater proactive awareness and show enhanced knowledge of online risk (Raywood-Burke et al., 2023; Naga et al., 2024). Conversely, those with high agreeableness were linked with lower security awareness (Pratama, Firmansyah, & Rahma, 2022).

A lack of cyber awareness can have severe implications for individuals and organizations. Information security awareness (ISA), a widely accepted construct for cyber awareness, focuses on users' understanding of security policies and their commitment to adhering to them (Ande et al., 2019). ISA involves two key components: recognizing the importance of information security protocols and demonstrating a consistent commitment to best practices (McCue, 2023; Parsons et. al. 2014). The latter aspect of ISA ties directly to individual differences, which may influence the adoption of accepted practices and behaviors (Hadlington et al., 2020).

Cyber Behaviors. Individuals often express concern about cybersecurity, but few consistently take action to protect their information (Crossler et al., 2013). Differences in decision-making processes can often explain this disparity between concern and action—intentions involve deliberate thought, while impulsive decisions may drive actual behaviors, often requiring minimal cognitive effort (Willison & Warkentin, 2013).

Personality traits are helpful as they are often more reliable than stated intentions (Shropshire et al., 2015). Understanding the relationship between personality traits and cyber behaviors has significant practical implications. Cyber behaviors encompass a range of activities, including secure password management, cautious email handling, and prudent social media usage. Studies have shown that conscientiousness positively correlates with secure behaviors, such as creating strong passwords and regularly updating software, whereas neuroticism has been linked to maladaptive behaviors, including risky internet use (Anawar et al., 2019; Leng et al., 2020). These findings

underscore the need for a more intricate understanding of individual differences in cybersecurity behaviors.

1.2 Addressing a Theoretical Gap

Numerous studies have examined individual traits in isolation. However, researchers have rarely provided a comprehensive overview of how the Big Five model influences cybersecurity outcomes (e.g., Bishop et al., 2020; Canham et al., 2024). Uniquely, we are addressing the theoretical gap that specifically examines the relationship between the Big Five personality traits and cyber awareness. Our systematic review provides a more comprehensive understanding of the relationship and research landscape. This research seeks to inform the future design of tailored interfaces and interventions that consider individual personality profiles, ultimately promoting safer online behaviors.

2 Methods

To ensure transparency and thoroughness, this systematic review adhered to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Page et al., 2021). PRISMA provides standardized protocols and checklists designed to enhance the preparation and reporting of systematic reviews. The key elements of the systematic review process considered in line with PRISMA guidelines are outline in Table 2.

Table 2. PRISMA guidelines and their application

Checklist Item	Application
Eligibility criteria	Inclusion and exclusion criteria were established prior to data collection. These criteria are detailed in Section 2.2, with studies grouped based on their alignment with the research objectives. Gray literature was included to ensure comprehensiveness.
Information sources	Databases searched included PubMed, Web of Science, APA PsycInfo, ACM Digital Library, and ProQuest. Searches were conducted on 15th September 2024, ensuring recent and diverse studies.
Search strategy	Full search strategies, including keywords and filters are provided in Table 3.
Selection process	Titles and abstracts were screened independently by two reviewers for thematic relevance, followed by full-text screening based on inclusion and exclusion criteria. Discrepancies were resolved through discussion. Covidence was used for removing duplicates.
Data collection process	Data extraction was conducted by two reviewers who independently transcribed key information into an Excel sheet without the use of any automation tools. All required data were available in the reviewed records, including from gray literature sources.

Data items	Outcomes included study focus, personality measures used, cyber awareness and behaviors measured, and findings. Additional variables included study design, sample demographics, delivery method and location. Details narratives were extracted for the non – empirical studies with missing information.
Study risk of bias assessment	Risk of bias was not explicitly assessed due to methodological differences across studies. Section 2.3 provides further information.
Effect measures	Effect measures, such as correlations and descriptive comparisons, were not explicitly calculated as this review focused on narrative synthesis. Statistical analysis was beyond the scope of this study.
Synthesis methods	Narrative synthesis was employed to integrate findings across studies.
Reporting bias assessment	Reporting bias was not assessed as statistical analysis of findings was not conducted. The absence of reporting bias measures did not impact the review outcomes.
Certainty assessment	Certainty in the evidence was supported by including peer-reviewed studies and published thesis/dissertation approved by institutional committee.

2.1 Information Sources and Search Strategy

A comprehensive search was conducted in September 2024 across five major electronic databases: PubMed, Web of Science, APA PsycInfo, ACM Digital Library, and ProQuest. The search focused on studies published between 2014 and 2024, capturing recent research on the relationship between Big Five personality traits and cybersecurity behaviors or awareness.

Search queries were developed based on three core concepts: cybersecurity, personality traits, and awareness or behaviors. Boolean operators (AND, OR) were applied where applicable to broaden the scope of retrieval. The primary search strings included:

1. "cyber*" OR "cyber security" OR "information security" OR "digital security" OR "computer security" OR "social engineering" OR "IT security"
2. AND "awareness" OR "behavior" OR "behaviour" OR "attitudes"
3. AND "personality" OR "Big Five" OR "Conscientiousness" OR "Openness" OR "Extraversion" OR "Agreeableness" OR "Neuroticism"

Table 3 presents the detailed search strategies and the corresponding number of results for each database. Grey literature, including dissertations, theses, and conference proceedings, was included. This offers a more complete overview of the available literature but does include non-peer-reviewed publications. The initial search yielded 433 records. Covidence was used to organize the records and remove duplicates(Covidence, 2024).

Table 3. Search queries and results

Database	Search Query	Results
PubMed	(cyber*[Title/Abstract] OR "cyber security"[Title/Abstract] OR "information security"[Title/Abstract] OR "digital security"[Title/Abstract] AND (awareness*[Title/Abstract] OR "Behavior"[Title/Abstract] AND (personality*[Title/Abstract] OR "Big Five"[Title/Abstract] OR "Conscientiousness"[Title/Abstract] OR "Openness"[Title/Abstract] OR "Extraversion"[Title/Abstract] OR "Agreeableness"[Title/Abstract] OR "Neuroticism"[Title/Abstract])	81
ACM Digital Library	[[Abstract: "cyber"] OR [Abstract: "cyber security"] OR [Abstract: "information security"] OR [Abstract: "digital security"] AND [[Abstract: "awareness"] OR [Abstract: "behavior"] AND [[Abstract: "personality"] OR [Abstract: "big five"] OR [Abstract: "big five traits"] OR [Abstract: "conscientiousness"] OR [Abstract: "openness"] OR [Abstract: "extraversion"] OR [Abstract: "agreeableness"] OR [Abstract: "neuroticism"]]	53
Web of Science	AB=(("cyber" OR "cyber security" OR "information security" OR "digital security") AND ("awareness" OR "behaviors") AND ("personality" OR "big five" OR "conscientiousness" OR "openness" OR "extraversion" OR "agreeableness" OR "neuroticism"))	79
ProQuest	abstract((("cyber" OR "cyber security" OR "information security" OR "digital security") AND ("awareness" OR "behavior") AND ("personality" OR "big five" OR "conscientiousness" OR "openness" OR "extraversion" OR "agreeableness" OR "neuroticism")))	167
PsycInfo	AB ((((("cyber" OR "cyber security" OR "information security" OR "digital security") AND ("awareness" OR "behavior") AND ("personality" OR "big five" OR "conscientiousness" OR "openness" OR "extraversion" OR "agreeableness" OR "neuroticism"))))	53

2.2 Inclusion and Exclusion Criteria

The inclusion and exclusion criteria were systematically defined using the PICO (Population, Intervention/Exposure, Comparator, and Outcome) model to ensure that only studies relevant to the research objectives were considered. (See Table 4)

Table 4. Inclusion and exclusion criteria in PICO model

Criteria	Inclusion	Exclusion
Population	Studies on end-users (students, employees, public) interacting with digital systems.	Studies on organizational/technical infrastructures without individual behavior assessment.
Intervention /Exposure	Research on cyber awareness and cybersecurity behaviors, focusing on threats (e.g.,	Studies using other personality models (e.g., HEXACO, Dark

	phishing, malware) and secure practices (e.g., password management, data sharing). Studies examining Big Five personality traits in this context.	Triad) or addressing cybersecurity solely from a technical perspective without behavioral assessment.
Comparator	Studies with measurable outcomes linking personality traits to cyber awareness or behaviors.	Studies without measurable outcomes or without a clear link between personality traits and cybersecurity behaviors.
Outcome	Relationship between Big Five traits and cyber awareness/cybersecurity behaviors (e.g., phishing detection, secure password management, security compliance).	Studies reporting only technical outcomes without behavioral or personality reference.
Study Characteristics	Peer-reviewed empirical studies, approved theses/dissertations using validated instruments, and studies published in English (2014–2024).	Non-peer-reviewed studies, grey literature, non-validated measurement tools, or studies published before 2014.

2.3 Study Selection and Data Extraction

The study selection process was carried out in two phases: title and abstract screening, followed by full-text review. Initially, 433 records were identified through the database search. After removing 132 duplicates, 301 unique records were retained for screening. Two reviewers independently screened the titles and abstracts of these records to determine their relevance based on the inclusion and exclusion criteria. Following the initial screening, 66 full-text articles were assessed for eligibility, out of which 40 studies met the inclusion criteria and were included in the final synthesis. A detailed overview of the study selection process is provided in the PRISMA flow diagram (Figure 1).

Data extraction was carried out using a standardized form developed specifically for this review. Both reviewers extracted key information from each included study, which encompassed details such as author(s), year of publication, country, sample size, and study design. Demographic characteristics of participants, including age and gender distribution, were recorded under population characteristics. Instruments used to measure the Big Five personality traits (e.g., NEO-PI-R, BFI) were documented, along with the specific cybersecurity outcomes assessed, such as phishing detection, password management, and compliance with security protocols. Key findings from each study, including statistical significance and effect sizes where applicable, were also extracted. Any discrepancies in the extracted data were resolved through consensus discussions between the reviewers. A risk of bias assessment was not conducted because as we found no suitable tool to evaluate the diverse range of study designs (qualitative, quantitative, descriptive) and study types included in this systematic review. The collated data were systematically tabulated and served as the foundation for the narrative synthesis presented in the results section.

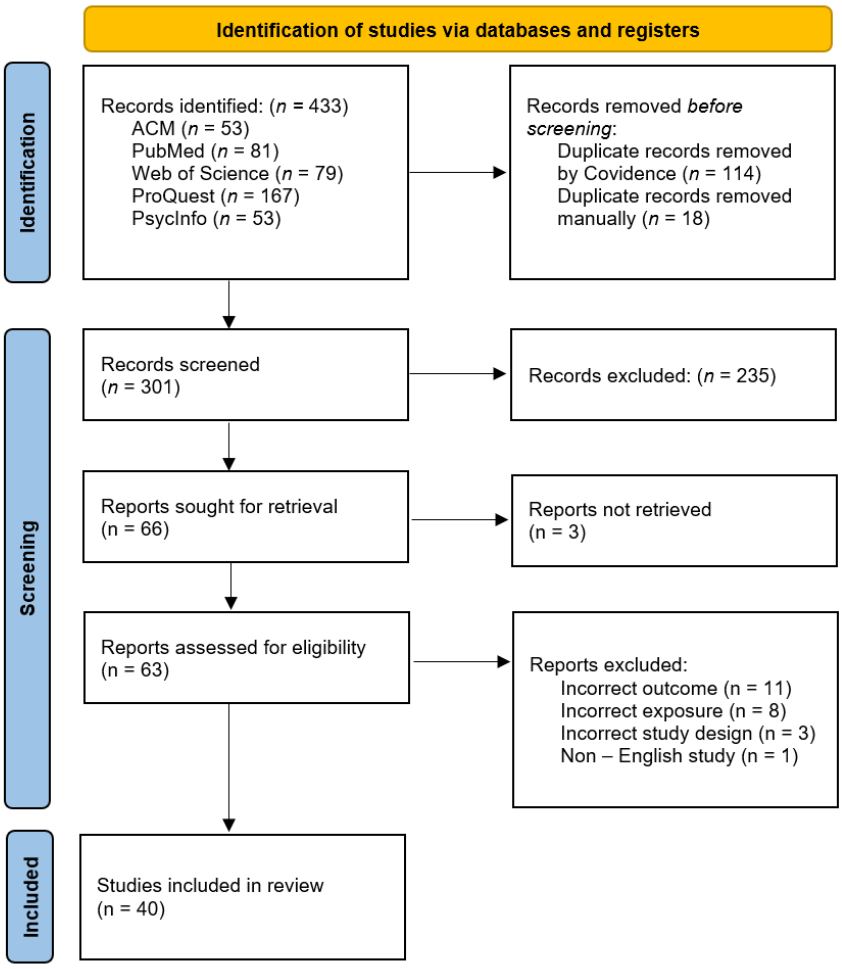

Fig. 1. Study selection process flow chart

3 Results

The selected studies represented diverse methodologies and populations. Geographic distribution of studies included samples from North America (United States (n = 16), Canada (n = 1)), Europe (n = 6), Africa (n = 2), Middle Eastern countries (n = 6), Australia (n=3), and Asia (n = 6), with two studies of them conducted across multiple regions (Tolah et al., 2021; Halevi et al., 2016). Four studies have not specified the region (Cho et al., 2016; López-Aguilar & Solanas, 2021; Raywood-Burke et al., 2021; van der Schyff & Flowerday, 2021). The populations studied consisted predominantly of employees/working professionals (n = 19), general adults (n = 9), and students (n = 16).

One study did not explicitly mention the study population (Cho et al., 2016), and one was a database-driven literature analysis (López-Aguilar & Solanas, 2021).

Methodologically, 30 studies employed online surveys, which emerged as the most used method for data collection. Online surveys were favored for their scalability and cost-effectiveness (e.g., Warrington, 2017). Other delivery methods included in-person surveys (n = 6) and one secondary data analysis (Mills, 2018). Few studies used other methods such as interviews (Tolah et al., 2021), synthetic data (Atta Ur Rahman et al., 2024), and online simulations (Bajwa et al., 2024; Canham et al., 2022, 2024) along with the online surveys. Al-Bustani et al. (2022) used email-based social engineering simulation using simulated phishing links, while Cho et al. (2016) used synthetic data generation using Stochastic Petri Nets (SPN). Study designs were varied across the studies.

The studies used a variety of validated personality measures, with the International Personality Item Pool (IPIP-50; Goldberg et al., 2006) (n = 10) and the Big Five Inventory (BFI-44; John et al., 1991) being the most frequently employed. Additionally, custom-developed scales were applied in 3 studies to measure the Big Five personality traits (Alanazi et al., 2020; Anawar et al., 2019; Schoenherr & Thomson, 2021). Shortened versions of the BFI and IPIP were also utilized in studies to assess personality traits rapidly (e.g., Albladi & Weir, 2017; Mahindra, 2023; Mills, 2018). These variations in personality measures reflect the methodological diversity across the reviewed studies.

3.1 Cyber Awareness and Behaviors Measured

Cybersecurity Awareness Topics. Cybersecurity awareness was a primary focus in several studies, employing diverse measures to evaluate knowledge and understanding of security threats. Information security awareness was one of the most widely measured aspects, featured in seven studies (Aharony et al., 2020; Naga et al., 2024; Hadlington et al., 2020; Letica, 2019; McCormac et al., 2017; McCue, 2023; van der Schyff & Flowerday, 2021). This measure assessed individuals' knowledge about cyber threats and their ability to recognize phishing attempts, social engineering tactics, and other risks. Proactive awareness was explored in four studies (Bishop et al., 2020; Gratian et al., 2018; Raywood-Burke et al., 2021; Upadhyay et al., 2022), reflecting participants' ability to anticipate and prevent security issues before they occur. Three studies specifically investigated security awareness, highlighting its foundational role in understanding cybersecurity threats and responses (Pratama et al., 2022; Tolah et al., 2021). Protection motivation was measured in one study, focusing on participants' understanding of security concepts and their drive to adopt secure practices, respectively (Vestad, 2022).

Cybersecurity Behaviors Topics. Cybersecurity behaviors were captured across multiple domains, emphasizing proactive and reactive security practices. Security compliance or related practices were evaluated in studies (n = 9) reflecting participants' adherence to established cybersecurity protocols and behaviors (Alanazi et al., 2020;

Dreibelbis, 2016; Naga et al., 2024; Halevi et al., 2016; Kennison & Chan-Tin, 2020; Pattinson et al., 2015; Shappie et al., 2020; Tolah et al., 2021; Weems et al., 2018). Phishing susceptibility or vulnerability emerged as the most studied topic in behaviors *(n* = 12*)* (Al-Bustani et al., 2023; Albladi & Weir, 2017; Anawar et al., 2019; Rahman et al., 2024; Canham et al., 2022, 2024; Frauenstein & Flowerday, 2020; Cho et al., 2016; López-Aguilar & Solanas, 2021; Mahindra, 2023; Martin, 2017; Weems et al., 2018). This highlights the critical role of recognizing and avoiding phishing attempts in cybersecurity behaviors.

Password practices, including creating and updating strong passwords, were explored (Bishop et al., 2020; Gratian et al., 2018; Raywood-Burke et al., 2021; Upadhyay et al., 2022). File protection behaviors were measured (Warrington, 2017), focusing on controlling access to sensitive information. Risky mobile behaviors, such as insecure app usage or accessing sensitive data over unprotected networks, were also analyzed (Lau, 2020; Mills, 2018). Two studies investigated victimization, including breaches and malware attacks, aimed to identify vulnerability patterns and behavioral lapses (Rodríguez-Enríquez et al., 2019; van de Weijer & Leukfeldt, 2017).

Other areas of focus included security behavior intentions measured using SeBIS (Security Behavior Intentions) scale (Bajwa et al., 2024; Bishop et al., 2020; Gratian et al., 2018; Raywood-Burke et al., 2021; Upadhyay et al., 2022), data sharing practices (Halevi et al., 2016; Schoenherr & Thomson, 2021), online prosocial behaviors (Leng et al., 2020), screen time (Rodríguez-Enríquez et al., 2019), and clicking behaviors (Canham et al., 2024). These studies collectively highlight the diversity and complexity of cybersecurity behaviors, underscoring the importance of individual practices and broader behavioral patterns in maintaining cybersecurity resilience.

3.2 Trait-Specific Results

Conscientiousness. Conscientiousness was positively associated with cybersecurity behaviors and awareness in 29 of the 40 reviewed studies (e.g., Abdulateef M Yaser Al-Bustani et al., 2023; Lau, 2020; Aharony et al., 2020; van de Weijer & Leukfeldt, 2017). These studies highlighted that individuals with high conscientiousness scores were significantly more likely to have higher security awareness and engage in secure behaviors, such as informed cybersecurity decisions (Bajwa et al., 2024), cyber hygiene (Schoenherr & Thomson, 2021), lesser screen time (Rodríguez-Enríquez et al., 2019), robust password management (Gratian et al., 2018), and compliance with organizational policies (Dreibelbis, 2016). However, two studies reported negative or negligible associations. For instance, Mills (2018) found that conscientiousness was significantly related to risky mobile device use, such as viewing pornography. Similarly, Martin (2017) observed that high conscientiousness showed lower phishing detection.

Neuroticism. Neuroticism, characterized by emotional instability and heightened anxiety, was identified as a risk factor for cybersecurity behaviors and awareness in 10 of the 40 reviewed studies (e.g., Halevi et al., 2016; Cho et al., 2016; Kennison & Chan-Tin, 2020; Leng et al., 2020). Individuals with higher levels of neuroticism were

consistently more likely to exhibit impulsive decision-making and maladaptive responses to cybersecurity threats, such as engaging in risky behaviors (e.g., van de Weijer & Leukfeldt, 2017; Kennison & Chan-Tin, 2020). Higher neuroticism in individuals was also associated with lower information security awareness (Naga et al., 2024; McCormac et al., 2017). Notably, some studies found neuroticism to have a positive impact in specific contexts. For example, Atta Ur Rahman et al. (2024) observed that neuroticism was associated with avoidance behaviors in phishing scenarios. Neuroticism was positively related to systematic processing, offering some protection against phishing (Frauenstein & Flowerday, 2020). Neuroticism was negatively correlated with trust, but the lack of trust made neurotic individuals less vulnerable to social network threats (Albladi & Weir, 2017). Aharony et al. (2020) pointed out that neuroticism (emotional instability) was linked to higher threat perception and lower engagement in security measures.

Openness. Openness was positively associated with cybersecurity awareness and behaviors (n = 14)(e.g., Dreibelbis, 2016; Naga et al., 2024; Cho et al., 2016; Shappie et al., 2020). These studies emphasized that individuals high in openness were more likely to engage in adaptive cybersecurity practices, such as reviewing privacy settings (van der Schyff & Flowerday, 2021) and identifying novel threats promoting a security culture framework (Tolah et al., 2021). For example, Leng et al. (2020) found that openness in 1398 Chinese college students was significantly linked to higher online prosocial behaviors, while Halevi et al. (2017) highlighted openness as a predictor of higher self-efficacy promoting secured password use and data-sharing behaviors. Openness is also positively associated with proactive awareness of device security (Raywood-Burke et al., 2021) and information security awareness (McCormac et al., 2017).

Studies also reported negative associations between openness and cybersecurity outcomes (van de Weijer & Leukfeldt, 2017). These studies noted that high openness occasionally correlated with riskier behaviors, such as experimenting with security choices prone to phishing attacks (Atta Ur Rahman et al., 2024). Openness positively influenced heuristic processing, increasing susceptibility, and improved systematic processing for detecting phishing attempts (Frauenstein & Flowerday, 2020). The exploratory tendencies of open individuals, while beneficial in identifying new risks, sometimes conflicted with adherence to established security protocols.

Extraversion. Extraversion, characterized by sociability and assertiveness, demonstrated mixed associations with cybersecurity awareness and behaviors. Positive associations (n = 5) were linked to extroverts' collaborative tendencies, facilitating confidence in handling security tasks (Aharony et al., 2020) and autonomy in cybersecurity decisions (Bajwa et al., 2024). For instance, Upadhyay et al. (2022) observed that extroverts were more likely to have good password management and proactive awareness. Extraversion also predicted better device securement (Gratian et al., 2018) and online prosocial behaviors (Leng et al., 2020).

However, most studies highlighted vulnerabilities associated with extraversion (n = 7). Studies reported that extraverts' social engagement often increased their

susceptibility to manipulation-based attacks, such as phishing and social engineering leading to cybervictimization (e.g., Albladi & Weir, 2017; Anawar et al., 2019; Atta Ur Rahman et al., 2024; Rodríguez-Enríquez et al., 2019). Vestad (2022) demonstrated that extroverts, driven by their preference for quick interactions, were more prone to impulsive decisions, which impacted security motivation. Also, extraverted individuals showed poor security awareness (Pratama et al., 2022).

Agreeableness. Agreeableness demonstrated consistent positive associations with cybersecurity awareness and behaviors (n = 13) (e.g., Dreibelbis, 2016; McCormac et al., 2017; Pattinson et al., 2015; Shappie et al., 2020). These studies highlighted that agreeable individuals, characterized by their cooperative and trusting nature, were more likely to comply with security protocols and engage in efforts to mitigate cybersecurity risks (Tolah et al., 2021; Vestad, 2022). For example, Upadhyay et al. (2022) observed that agreeable individuals had secure password generation and software updating behaviors along with proactive awareness. Hadlington et al. (2020) and McCue (2023) analyzed agreeableness to be higher in individuals with higher security awareness.

However, few studies reported negative associations, noting that agreeableness could increase vulnerability to manipulation-based attacks (n = 5). Trusting behaviors, while beneficial for collaboration, occasionally lead to susceptibility to phishing and social engineering tactics (Atta Ur Rahman et al., 2024; Canham et al., 2022; Frauenstein & Flowerday, 2020; Cho et al., 2016).

3.3 Overview of Big-Five Personality Traits on Cyber Awareness/Behaviors

Six studies explicitly assessed the impact of personality traits on cybersecurity awareness and behaviors. Among these, four studies concluded that personality traits did not significantly influence cybersecurity outcomes such as secure behaviors and phishing susceptibility (Bishop et al., 2020; Canham et al., 2024; López-Aguilar & Solanas, 2021; Weems et al., 2018). Warrington (2017) identified a weak association of big-five personality traits collectively with file protection behaviors. Also, Alanazi et al. (2020) presented that personality traits had a moderate but significant impact on ISCB. These findings underscore that while trait-specific analyses reveal nuanced influences on cybersecurity behaviors, the cumulative impact of personality remains variable and context-dependent.

4 Discussion

4.1 Reflection on findings

The review highlights the critical role of the Big Five personality traits in shaping cybersecurity awareness and behaviors, providing nuanced insights into individual differences. The use of varied methods, including literature review, online surveys, in-person surveys, interviews, and simulations, highlights the methodological diversity, boosting

the generalizability of findings across different contexts. Furthermore, the vast geographic dispersion of research confirms the results' cross-cultural applicability.

Conscientiousness consistently emerged as the most robust predictor of positive cybersecurity outcomes. Individuals high in conscientiousness demonstrated strong adherence to proactive security practices, such as effective password management, regular software updates, and compliance with organizational protocols (e.g., Gratian et al., 2018; Tolah et al., 2021). This reinforces the established literature on the role of conscientiousness in fostering structured and risk-averse behaviors, making it a valuable trait for designing cybersecurity training and interventions.

Phishing susceptibility or vulnerability, the most studied behavioral topic (n = 12), underscored its importance as a critical area for cybersecurity practices. Neuroticism was frequently associated with heightened risk, often manifesting as impulsivity or emotional reactivity, which compromised decision-making in cybersecurity contexts (e.g., Halevi et al., 2016; Kennison & Chan-Tin, 2020). However, some studies highlighted its protective effects in specific scenarios, such as systematic processing in phishing detection, emphasizing the dual nature of neuroticism (Frauenstein & Flowerday, 2020).

Extraversion showed mixed effects, often linked to vulnerabilities such as increased susceptibility to manipulation-based threats like phishing and social engineering (e.g., Anawar et al., 2019; Rodríguez-Enríquez et al., 2019). While extroverts excelled in collaborative security tasks and proactive measures, their preference for quick and less cautious interactions posed challenges to cybersecurity resilience (Vestad, 2022). Agreeableness also demonstrated dual effects, positively influencing cooperative security practices but increasing vulnerability to trust-based attacks (e.g., Atta Ur Rahman et al., 2024; Frauenstein & Flowerday, 2020).

Openness contributed positively to cybersecurity awareness in contexts requiring adaptability and innovation, such as reviewing privacy settings and engaging with new technologies (van der Schyff & Flowerday, 2021). However, its exploratory tendencies occasionally led to riskier behaviors, such as susceptibility to phishing attacks (Atta Ur Rahman et al., 2024). These findings highlight the importance of balancing openness-driven innovation with adherence to established security protocols.

4.2 Limitations of the Evidence

This review identified several limitations in the evidence base. The heterogeneity in methodologies, such as varying definitions and measures of cybersecurity awareness and behaviors, created challenges for synthesizing findings. The reliance on self-reported data in most studies introduced potential biases, including social desirability and memory errors. Furthermore, the underrepresentation of older adults limits the generalizability of these findings, particularly in diverse cultural and demographic contexts.

4.3 Limitations of the Review Process

Language restrictions excluded studies published in non-English languages, potentially omitting valuable insights from non-English-speaking regions. While gray literature

was included, variations in the operationalization of cybersecurity concepts hindered direct comparisons. Furthermore, the absence of a meta-analysis limited the ability to quantify effect sizes and assess the strength of associations across studies. The studies primarily emphasized training and behavioral interventions, with limited focus on leveraging findings for system and software design.

4.4 Implications for Practice and Future Research

Practice. This study underscores the importance of leveraging personality traits to design more effective and personalized cybersecurity interventions, as well as promoting human-centered cybersecurity systems. For instance, understanding how personality factors correlate with phishing susceptibility can inform the design of targeted defenses against online attacks (Rahman et al., 2024). Automated systems that suggest suitable privacy settings based on users' personality profiles could save time and reduce errors while enhancing secure practices (Halevi et al., 2016). Moreover, cybersecurity behavioral models that account for attitudes and personality make-up can provide deeper insights into awareness and the implementation of best practices, supporting the development of systems that align with user-specific needs (Shappie et al., 2020). By integrating these insights, organizations can create tailored interventions and user-friendly systems to enhance overall cybersecurity resilience.

Future Research. Cybersecurity policies should integrate psychological and behavioral insights to address human vulnerabilities effectively. Tailored training modules that capitalize on personality strengths, such as extroverts' collaboration or conscientious individuals' discipline, and emphasize the design of human-centered cybersecurity systems, can significantly improve organizational security (Naga et al., 2024). Policymakers must also prioritize inclusivity, ensuring interventions are accessible to underrepresented groups, to address gaps in global cybersecurity preparedness.

5 Conclusion

This review underscores the significant influence of the Big Five personality traits on cybersecurity awareness and behaviors, particularly highlighting the roles of conscientiousness in promoting positive security practices and neuroticism in increasing susceptibility to threats. While extraversion, agreeableness, and openness exhibit complex and context-dependent effects, these findings collectively emphasize the need for personalized cybersecurity design innovations tailored to individual differences. Despite the valuable insights gained, limitations in the existing literature, including methodological heterogeneity, reliance on self-reported data, and underrepresentation of certain populations, necessitate further investigation. Future research should prioritize including diverse cultural and demographic groups, developing standardized measures for cybersecurity awareness and behaviors, and exploring personality-based design and interventions to enhance cybersecurity compliance.

References

Aharony, N., Bouhnik, D., Reich, N.: Readiness for information security of teachers as a function of their personality traits and their assessment of threats. Aslib Journal of Information Management. 72, 787–812 (2020). https://doi.org/10.1108/AJIM-12-2019-0371.

Alanazi, S., Anbar, M., Ebad, S., Karuppayah, S., Al-Ani, H.: Theory-Based Model and Prediction Analysis of Information Security Compliance Behavior in the Saudi Healthcare Sector. Symmetry. 12, 1544 (2020). https://doi.org/10.3390/sym12091544.

Albladi, S.M., Weir, G.R.S.: Personality traits and cyber-attack victimisation: Multiple mediation analysis. In: 2017 Internet of Things Business Models, Users, and Networks. pp. 1–6. IEEE, Copenhagen (2017). https://doi.org/10.1109/CTTE.2017.8260932.

Al-Bustani, A.M.Y., Almutairi, A.K., Alrashed, A., Abdul Wahab Muzaffar: Social Engineering via Personality Psychology - Bypassing Users Based on Their Personality Pattern To Raise Security Awareness. In: 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD). IEEE, Manama, Bahrain (2023). https://doi.org/10.1109/ITIKD56332.2023.10100048.

Anawar, S., Kunasegaran, D., Mas'ud, M., Zakaria, N.: Analysis of phishing susceptibility in a workplace: A big-five personality perspectives. Journal of Engineering Science and Technology. 14, 2865–2882 (2019).

Ande, R., Adebisi, B., Hammoudeh, M., Saleem, J.: Internet of Things: Evolution and technologies from a security perspective. Sustainable Cities and Society. 54, 101728 (2020). https://doi.org/10.1016/j.scs.2019.101728.

Bajwa, M.H.A., Richards, D., Formosa, P.: Predicting Ethical Orientation Based on Personality for Tailored Cyberethics Training. In: Baghaei, N., Ali, R., Win, K., and Oyibo, K. (eds.) Persuasive Technology. pp. 65–74. Springer, Cham, Wollongong, NSW, Australia (2024). https://doi.org/10.1007/978-3-031-58226-4_6.

Benson, V., McAlaney, J.: Cyber influence and cognitive threats. Academic press, London (2020).

Bishop, L.M., Morgan, P.L., Asquith, P.M., Raywood-Burke, G., Wedgbury, A., Jones, K.: Examining Human Individual Differences in Cyber Security and Possible Implications for Human-Machine Interface Design. In: HCI for Cybersecurity, Privacy and Trust. pp. 51–66. Springer, Cham, Copenhagen, Denmark (2020). https://doi.org/10.1007/978-3-030-50309-3_4.

Canham, M., Dawkins, S., Jacobs, J.: Not All Victims Are Created Equal: Investigating Differential Phishing Susceptibility. In: Augmented Cognition. pp. 3–21. Springer, Cham, Washington DC, USA (2024). https://doi.org/10.1007/978-3-031-61569-6_1.

Canham, M., Posey, C., Constantino, M.: Phish Derby: Shoring the Human Shield Through Gamified Phishing Attacks. Frontiers in Education. 6, (2022). https://doi.org/10.3389/feduc.2021.807277.

Cho, J.-H., Cam, H., Oltramari, A.: Effect of personality traits on trust and risk to phishing vulnerability: Modeling and analysis. In: 2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA). pp. 7–13. IEEE, San Diego, CA (2016). https://doi.org/10.1109/COGSIMA.2016.7497779.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Computers & Security. 32, 90–101 (2013). https://doi.org/10.1016/j.cose.2012.09.010.

Dreibelbis, R.C.: It's More Than Just Changing Your Password: Exploring the Nature and Antecedents of Cyber-Security Behaviors, http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/more-than-just-changing-your-password-exploring/docview/1776708700/se-2?accountid=12967, (2016).

Federal Bureau of Investigation: Internet Crime Report 2023. Federal Bureau of Investigation (2024).

Frauenstein, E.D., Flowerday, S.: Susceptibility to phishing on social network sites: A personality information processing model. Computers & Security. 94, 101862 (2020). https://doi.org/10.1016/j.cose.2020.101862.

Funder, D.C.: Personality. Annual Review of Psychology. 52, 197–221 (2001). https://doi.org/10.1146/annurev.psych.52.1.197.

Goldberg, L.R., Johnson, J.A., Eber, H.W., Hogan, R., Ashton, M.C., Cloninger, C.R., Gough, H.G.: The international personality item pool and the future of public-domain personality measures. Journal of Research in Personality. 40, 84–96 (2006). https://doi.org/10.1016/j.jrp.2005.08.007.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A.: Correlating human traits and cyber security behavior intentions. Computers & Security. 73, 345–358 (2018).

Hadlington, L., Binder, J., Stanulewicz, N.: Fear of missing out predicts employee information security awareness above personality traits, age, and gender. Cyberpsychology, Behavior, and Social Networking. 23, 459–464 (2020). https://doi.org/10.1089/cyber.2019.0703.

Hadlington, L., Chivers, S.: Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. Policing: A Journal of Policy and Practice. 14, 479–492 (2020). https://doi.org/10.1093/police/pay027.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., Aloul, F., Chen, J.: Cultural and psychological factors in cyber-security. In: 18th International Conference on Information Integration and Web-Based Applications and Services. pp. 318–324. Association for Computing Machinery, Singapore (2016). https://doi.org/10.1145/3011141.3011165.

John, O.P., Donahue, E.M., Kentle, R.L.: Big Five Inventory (BFI). APA PsycTests (1991).

Kennison, S.M., Chan-Tin, E.: Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors. Frontiers in Psychology. 11, 546546 (2020). https://doi.org/10.3389/fpsyg.2020.546546.

Lau, N.: The Influence of Cognitive Factors and Personality Traits on Mobile Device User's Information Security Behavior, http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/influence-cognitive-factors-personality-traits-on/docview/2408266418/se-2?accountid=12967, (2020).

Leng, J., Guo, Q., Ma, B., Zhang, S., Sun, P.: Bridging Personality and Online Prosocial Behavior: The Roles of Empathy, Moral Identity, and Social Self-Efficacy. Frontiers in Psychology. 11, 575053 (2020). https://doi.org/10.3389/fpsyg.2020.575053.

Letica, I.B.: Some Correlates of Risky User Behavior and ICT Security Awareness of Secondary School Students. International Journal of Electrical and Computer Engineering Systems. 10, 85–89 (2019).

Liani, L., Baidun, A., Rahmah, M.: The Influence of Big Five Personality Trait and Self Control on Cyberloafing. In: 2021 9th International Conference on Cyber and IT Service Management (CITSM). pp. 1–5. IEEE, Bengkulu, Indonesia (2021). https://doi.org/10.1109/CITSM52892.2021.9588899.

López-Aguilar, P., Solanas, A.: Human Susceptibility to Phishing Attacks Based on Personality Traits: The Role of Neuroticism. In: 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). pp. 1363–1368. IEEE, Madrid, Spain (2021). https://doi.org/10.1109/COMPSAC51774.2021.00192.

Mahindra, V.: Personality Traits and Resistance to Online Trust Exploitation, http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/personality-traits-resistance-online-trust/docview/2890697385/se-2?accountid=12967, (2023).

Martin, J.: Something Looks Phishy Here: Applications of Signal Detection Theory to Cyber-Security Behaviors in the Workplace,

http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/something-looks-phishy-here-applications-signal/docview/1920109049/se-2?accountid=12967, (2017).

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M.: Individual differences and Information Security Awareness. Computers in Human Behavior. 69, 151–156 (2017). https://doi.org/10.1016/j.chb.2016.11.065.

McCrae, R.R., Costa Jr., P.T.: A Five-Factor theory of personality. In: Handbook of personality: Theory and research, 2nd ed. pp. 139–153. Guilford Press, New York, NY, US (1999).

McCrae, R.R., John, O.P.: An Introduction to the Five-Factor Model and Its Applications. Journal of Personality. 60, 175–215 (1992). https://doi.org/10.1111/j.1467-6494.1992.tb00970.x.

McCue, G.: Generational Information Security Awareness and the Role of Big Five Personality Traits, http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/generational-information-security-awareness-role/docview/2851785428/se-2?accountid=12967, (2023).

Mills, V.L.: Big Five Factors of Personality Traits, Age, and Employees' Risky Mobile Device Behavior, http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/big-five-factors-personality-traits-age-employees/docview/2039580797/se-2?accountid=12967, (2018).

Naga, J.F., Tinam-isan, M.A.C., Mae O. Maluya, M., Antonnette D. Panal, K., Tanya A. Tupac, Ma.: Investigating the Relationship Between Personality Traits and Information Security Awareness. International Journal of Computing and Digital Systems. 15, 1233–1246 (2024). https://doi.org/10.12785/ijcds/160191.

Nobles, C.: Botching Human Factors in Cybersecurity in Business Organizations. Holistica – Journal of Business and Public Administration. 9, 71–88 (2018). https://doi.org/10.2478/hjbpa-2018-0024.

Nurse, J.R.C., Buckley, O., Legg, P.A., Goldsmith, M., Creese, S., Wright, G.R.T., Whitty, M.: Understanding Insider Threat: A Framework for Characterising Attacks. In: 2014 IEEE Security and Privacy Workshops. pp. 214–228. IEEE, San Jose, CA (2014). https://doi.org/10.1109/SPW.2014.38.

Page, M.J., McKenzie, J.E., Bossuyt, P.M., Boutron, I., Hoffmann, T.C., Mulrow, C.D., Shamseer, L., Tetzlaff, J.M., Akl, E.A., Brennan, S.E., Chou, R., Glanville, J., Grimshaw, J.M., Hróbjartsson, A., Lalu, M.M., Li, T., Loder, E.W., Mayo-Wilson, E., McDonald, S., McGuinness, L.A., Stewart, L.A., Thomas, J., Tricco, A.C., Welch, V.A., Whiting, P., Moher, D.: The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. 88, n71 (2021). https://doi.org/10.1016/j.ijsu.2021.105906.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. Computers & Security. 66, 40–51 (2017). https://doi.org/10.1016/j.cose.2017.01.004.

Pattinson, M., Butavicius, M., Parsons, K., Mccormac, A., Calic, D.: Factors that Influence Information Security Behavior: An Australian Web-Based Study. In: Human Aspects of Information Security, Privacy, and Trust. pp. 231–241. Springer, Cham, Los ANgeles, CA, USA (2015). https://doi.org/10.1007/978-3-319-20376-8_21.

Pratama, A.R., Firmansyah, F.M., Rahma, F.: Security awareness of single sign-on account in the academic community: the roles of demographics, privacy concerns, and Big-Five personality. PeerJ Computer Science. 8, e918 (2022). https://doi.org/10.7717/peerj-cs.918.

Rahman, A.U., Al-Obeidat, F., Tubaishat, A., Shah, B., Anwar, S., Halim, Z.: Discovering the Correlation Between Phishing Susceptibility Causing Data Biases and Big Five Personality Traits Using C-GAN. IEEE Transactions on Computational Social Systems. 11, 4800–4808 (2024). https://doi.org/10.1109/TCSS.2022.3201153.

Raywood-Burke, G., Bishop, L.M., Asquith, P.M., Morgan, P.L.: Human Individual Difference Predictors in Cyber-Security: Exploring an Alternative Scale Method and Data Resolution to Modelling Cyber Secure Behavior. In: HCI for Cybersecurity, Privacy and Trust. pp. 226–240. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-77392-2_15.

Rodríguez-Enríquez, M., Bennasar-Veny, M., Leiva, A., Garaigordobil, M., Yañez, A.M.: Cybervictimization among secondary students: social networking time, personality traits and parental education. BMC Public Health. 19, 1499 (2019). https://doi.org/10.1186/s12889-019-7876-9.

Schoenherr, J.R., Thomson, R.: The Cybersecurity (CSEC) Questionnaire: Individual Differences in Unintentional Insider Threat Behaviours. In: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). pp. 1–8. IEEE, Dublin, Ireland (2021). https://doi.org/10.1109/CyberSA52016.2021.9478213.

Shah, R., Cemiloglu, D., Yucel, C., Ali, R., Katos, V.: Is cyber hygiene a remedy to IPTV infringement? A study of online streaming behaviours and cyber security practices. International Journal of Information Security. 23, 1913–1926 (2024). https://doi.org/10.1007/s10207-024-00824-0.

Shappie, A.T., Dawson, C.A., Debb, S.M.: Personality as a predictor of cybersecurity behavior. Psychology of Popular Media. 9, 475–480 (2020). https://doi.org/10.1037/ppm0000247.

Shillair, R., Cotten, S.R., Tsai, H.-Y.S., Alhabash, S., LaRose, R., Rifon, N.J.: Online safety begins with you and me: Convincing Internet users to protect themselves. Computers in Human Behavior. 48, 199–207 (2015). https://doi.org/10.1016/j.chb.2015.01.046.

Shropshire, J., Warkentin, M., Sharma, S.: Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security. 49, 177–191 (2015). https://doi.org/10.1016/j.cose.2015.01.002.

Soto, C.J., John, O.P.: Big Five Inventory-2, https://doi.apa.org/doi/10.1037/t64008-000, (2017). https://doi.org/10.1037/t64008-000.

Tolah, A., Furnell, S.M., Papadaki, M.: An empirical analysis of the information security culture key factors framework. Computers & Security. 108, (2021). https://doi.org/10.1016/j.cose.2021.102354.

Upadhyay, R.K., Singh, A., Singh, B.M.: Human side of cybersecurity: an empirical study. International Journal of Business Information Systems. 41, 408–422 (2022). https://doi.org/10.1504/ijbis.2022.126996.

van de Weijer, S.G.A., Leukfeldt, E.R.: Big five personality traits of cybercrime victims. Cyberpsychology, Behavior, and Social Networking. 20, 407–412 (2017). https://doi.org/10.1089/cyber.2017.0028.

van der Schyff, K., Flowerday, S.: Mediating effects of information security awareness. Computers & Security. 106, (2021). https://doi.org/10.1016/j.cose.2021.102313.

Veritas Health Innovation: Covidence systematic review software, www.covidence.org, (2024).

Verizon: 2024 Data Breach Investigations Report. Verizon Business (2025).

Vestad, A.: Personality Traits and Security Motivation. Studies in health technology and informatics. 299, 183–188 (2022). https://doi.org/10.3233/SHTI220980.

Warrington, C.: A study of personality traits to explain employees' information security behavior among generational cohorts, http://proxy.lib.odu.edu/login?url=https://www.proquest.com/dissertations-theses/study-personality-traits-explain-employees/docview/1883835487/se-2?accountid=12967, (2017).

Weems, C.F., Ahmed, I., Richard, G.G., Russell, J.D., Neill, E.L.: Susceptibility and resilience to cyber threat: Findings from a scenario decision program to measure secure and insecure computing behavior. PLoS One. 13, (2018). https://doi.org/10.1371/journal.pone.0207408.

Willison, R., Warkentin, M.: Beyond Deterrence: An Expanded View of Employee Computer Abuse. Management Information Systems Quarterly. 37, 1–20 (2013). https://doi.org/10.25300/MISQ/2013/37.1.01.