International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

Investigating the Relationship Between Personality Traits and Information Security Awareness

January F. Naga[1], Mia Amor C. Tinam-isan[1], Melody Mae O. Maluya[1], Kaye Antonnette D. Panal [1], Ma. Tanya A. Tupac [1]

[1] Department of Information Technology, MSU-Iligan Institute of Technology, Iligan City, Philippines

E-mail address: january.febro@g.msuiit.edu.ph, miaamor.catindig@g.msuiit.edu.ph, melodymae.maluya@g.msuiit.edu.ph, kayeantonnette.panal@msuiit.edu.ph, matanya.tupac@g.msuiit.edu.ph

Received ## Mon. 20##, Revised ## Mon. 20##, Accepted ## Mon. 20##, Published ## Mon. 20##

Abstract: This study delves into the crucial intersection of personality traits and information security behaviors in an era of increasing technological reliance. Using a quantitative approach, we explore the correlation between the Big Five Personality Traits (BFI) and the Knowledge-Attitude-Behavior (KAB) components related to information security awareness. Our study, which involved 311 undergraduate students chosen through stratified random sampling, uses Spearman correlation analysis and logistic regression modeling to examine correlations between personality traits from the BFI and information security risk status. The findings reveal significant correlations, particularly highlighting the roles of neuroticism (33.33%), lack of direction (16.67%), extraversion (16.67%), and antagonism (16.67%) in increasing susceptibility to security risks. The logistic regression model demonstrates 85.7% accuracy, indicating its effectiveness in correlating personality traits with information security behaviors. The study underscores the importance of considering individual personality profiles in cybersecurity strategies. By understanding the interplay between personality traits and security behaviors, organizations can effectively develop targeted interventions to enhance information security awareness and resilience. These findings provide a nuanced understanding of the psychological factors shaping cybersecurity attitudes and behaviors. Also, these findings have significant implications for crafting targeted cybersecurity awareness programs, suggesting that integrating personality traits into these initiatives could promote cyber-secure behavior more effectively. This research adds valuable insights to information security, emphasizing the need for a more personalized approach to awareness strategies and future research to explore this relationship further.

Keywords: BFI characteristics; Cybersecurity; Information Security; Personality Factor

1. Introduction

The accelerated advancement of Information Technology has resulted in significant transformations across various sectors, including academics, government, and private organizations [1]. However, despite its benefits, technological advancement has also brought about an increase in information security risks. Cyberattacks targeting organizations are rising, resulting in numerous security incidents [2]. Within organizational landscapes, human error stemming from noncompliance or lack of awareness has emerged as a leading cause of security breaches, surpassing deliberately malicious intentions [3, 4]. Relying solely on technical solutions is insufficient in addressing these vulnerabilities [5]. Humans are often the weakest link in information security, making their engagement and awareness crucial [6, 7]. However, organizations occasionally overlook this critical aspect.

Alarmingly, human error is responsible for 95% of security vulnerabilities within organizations, underscoring the necessity for proactive preventive measures [8]. Security breaches, encompassing virus infections, identity theft, and hacking, stem directly from users' inattentiveness, inadequate awareness, and failure to take appropriate measures. The literature highlights that many users falsely believe they are safe from cybercriminals due to their perceived lack of prominence or affluence, which can compromise their security [9]. The prevalence of cybercriminal activities could be mitigated through heightened knowledge, improved attitudes, and proactive conduct among users in various sectors, including government entities, educational establishments, and even households.

Personality, a constellation of distinctive traits and qualities, profoundly shapes an individual's character [10].

E-mail:author's email

The “Big Five Inventory” (BFI) model encapsulates five fundamental personality dimensions: “openness, conscientiousness, extraversion, agreeableness, and neuroticism” [11]. Leveraging personality as a factor to comprehend and predict user behavior has gained substantial traction across various domains [12-16]. For example, Frauenstein and Flowerday [17] investigate how personality traits influence information processing and susceptibility to phishing attacks on social networks.

Understanding the human element is as critical as technological safeguards in the rapidly evolving information security landscape. This study examines an overlooked but essential facet of information security - the impact of personality factors on security behaviors in an organization. Utilizing the Knowledge, Attitude, and Behavior (KAB) paradigm, this study examines how these characteristics impact individuals' attitudes, enhance their knowledge, and affect their actions in information security. This investigation is crucial because it provides a detailed understanding of the human elements that form the basis of security protocols and risk management techniques. This understanding can potentially lead to creating more efficient and customized cybersecurity interventions suitable for various organizational settings.

In the following sections of this paper, we initiate the presentation of the conceptual framework in Section 2. Section 3 provides a concise overview of the literature review and elucidates our approach in Section 4. Section 5 delves into the elaboration of the findings, Section 6 centers on the discussion, and Section 7 encompasses the implications, limitations, and future directions segments, encapsulating the study's implications and outlining potential avenues for future research. Finally, Section 8 serves as the conclusion.

2. Conceptual Framework

A. KAB Model

The Knowledge-Attitude-Behavior (KAB) framework was introduced by Kruger and Kearney [18] to measure information security awareness. This model is based on the social psychological model's interconnected components of affect, behavior, and cognition [19, 20] which align with attitude, behavior, and knowledge, respectively. The KAB framework is widely used to explain cybersecurity awareness and behaviors [1, 4, 21]. According to the KAB model, while knowledge can impact behaviors, attitude often mediates between the two factors. In other words, increased knowledge leads to better attitudes, improving information security behaviors [4].

The KAB model provides a comprehensive framework for understanding how IT Service Usage, Security Knowledge, and Security Practices interrelate and influence individuals' information security awareness and behavior. It highlights that enhancing knowledge, fostering positive attitudes, and promoting secure behaviors are essential in effectively mitigating security risks and vulnerabilities.

Security Knowledge: The KAB model posits that knowledge forms the basis for behavioral change. In this context, the "Security Knowledge" concept aligns with the KAB model's “knowledge” component.

IT Service Usage: The "attitude" component of the KAB model pertains to an individual's beliefs, perceptions, and attitudes towards a particular behavior. In the context of IT Service Usage, if end-users cultivate a positive outlook on integrating secure online practices and acknowledge potential risks associated with various services, such as online banking or social networking, they are more likely to demonstrate prudent and safe behavior.

Security Practices: The "security practices" correspond to the “behavior” component of the KAB model. This includes how end-users interact with IT systems, software security, email security, data management, and network management. The text emphasizes the importance of these practices, highlighting how learning about and implementing them can mitigate risks posed by cybercriminal activities. Good data and network management align with responsible behaviors that contribute to the security of IT systems, which is in line with the behavior component of the KAB model.

B. Personality Traits

Risk-taking tendency reflects an individual's inclination to embrace or avoid risks based on their attitude toward uncertain outcomes [22]. Although risk perception may fluctuate based on circumstances, an individual's underlying disposition towards perceived risk remains consistent [23]. An individual's personality traits can also affect their tendency to take risks. Research shows that high scores on extraversion and openness, combined with low agreeableness, conscientiousness, and neuroticism, are linked to more significant risk-taking behaviors [22]. The BFI model has been widely used to understand and predict various factors in diverse and complex contexts [24]. The model is the leading theoretical framework for assessing and understanding personality [25]. It comprises five factors: “neuroticism,” “extraversion,” “openness,” “agreeableness,” and “conscientiousness” [11].

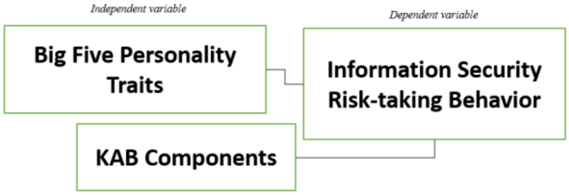

Independent variable
Dependent variable
Big Five Personality Traits
Information Security Risk-taking Behavior
KAB Components

Figure 1. Conceptual Framework

To put it briefly, the KAB Framework deals with how knowledge, attitudes, and behaviors interact. This study can help us comprehend how individual's knowledge and attitudes toward information security can affect their actual information security behaviors. In contrast, the BFI framework offers a way to evaluate and classify personality traits based on five dimensions: openness, conscientiousness, extraversion, agreeableness, and neuroticism. This framework can provide insights into how certain personality traits may contribute to specific behaviors related to information security risk-taking. Combining these two frameworks, our conceptual model in Figure 1 considers cognitive aspects (knowledge, attitudes) and individual characteristics (personality traits) that might influence information security behaviors.

In this study, we hypothesize that:

There is a significant positive/negative correlation between information security risk-taking behavior and the Big Five Personality Traits (BFI), considering the Knowledge, Attitude, and Behavior (KAB) framework in information security.

3. Literature Review

A. Information Security

"Information security" is the administration and safeguarding of personal or corporate information and data assets [7, 26], synonymous with cybersecurity. In the scholarly discourse, the phrases "information security" and "cybersecurity" are often used interchangeably [7, 27], and this approach is maintained in the current study. Wilner [28] advocates for the term "information security" as a more precise descriptor for data protection. Recognizing how individual differences among employees influence their information security (or cybersecurity) practices is crucial for organizations, as indicated by Fatokun et al. [29]. This area remains pivotal, highlighted by a scarcity of research focusing on individual differences [27, 30, 31].

Safeguarding valuable information assets is critical for organizational operations. Information security aims to protect these assets by ensuring confidentiality, integrity, and availability. This involves comprehensive frameworks encompassing systems, operations, and internal procedures. John McCumber's MC model [32] highlights the interconnectedness of computer security and communication across various information environments, focusing on information status, critical information characteristics, and security measurement and emphasizing information protection during transmission, storage, and processing.

The rapid advancements in information and communication technology have brought complexity to information security [33]. The challenge lies in technological factors and human factors, which are crucial in upholding security practices. Reports indicate that around 90% of organizations encounter at least one information security incident annually, underscoring the significance of addressing individual behavior and concerns in security strategies [33].

Individuals within the organization are responsible for a significant portion of information systems security breaches, with research showing that more than half of these incidents are internally sourced [34]. Traditional organizational approaches to managing information security have focused on technological vulnerabilities, often overlooking the importance of people, policies, processes, and culture. This leaves organizations vulnerable to internal breaches.

B. Information Security and Human Behavior

The behavioral aspect of information security is increasingly recognized as crucial. Establishing an Information Security Policy (ISP) as part of the information security culture is vital, but its effectiveness hinges on human factors [35]. Information security in organizations is about implementing technological safeguards and managing the human element. Noncompliance with information security measures significantly contributes to security breaches [36].

Individual non-compliance varies from casual neglect of security protocols to severe, malicious acts against the organization [24, 37]. Research on technology acceptance and use in the context of information security has evolved to include behavioral science theories, such as the BFI, to better understand and predict employees' information security behaviors [27, 38].

C. Personality Traits and Information Security

There has been a surge in applying behavioral science principles to information security issues, particularly in the last two decades. This emerging field aims to understand the link between personality traits and information security behaviors, as noted in studies like Gratian et al. [30] and Shropshire et al. [24]. While this area is still in its infancy, it holds significant potential for enhancing our understanding of security breaches from a human perspective.

Personality traits evolve over a lifetime [39] and are inherent in all humans and influence behaviors across different cultural contexts [40]. The BFI provide a critical lens for understanding and predicting cybersecurity behaviors. Studies have found that personality traits are crucial in predicting and understanding cybersecurity behaviors [10]. Even though people may intend to comply with safe practices, their actual behaviors may differ from their intentions. The "Big Five" personality factors have been researched about cybersecurity behavior, but there is no consensus on which factors are the most significant.

1) Neuroticism: Characterized by anxiety and emotional instability, has been linked to varied information security behaviors. For instance, Russell et al. [41] observed an inverse correlation between neuroticism and secure cyber behaviors, suggesting that higher levels of neuroticism may lead to less effective cybersecurity practices.

2) Extraversion: Extraverts' sociability and assertiveness might influence their cybersecurity attitudes [42].

3) Openness: People high in openness are typically curious and inventive, which might encourage the exploration of new technologies and security measures. Morales-Vives et al. [43] found that intelligence, mediated by openness, influences compliance with preventive measures.

4) Agreeableness: Agreeable, cooperative, and trusting individuals might be more compliant with organizational information security policies. Shropshire et al. [24] noted a positive relationship between agreeableness and the intent to adopt information security measures. However, their trusting nature could also make them susceptible to social engineering attacks.

5) Conscientiousness: Conscientious individuals who are organized and responsible individuals are likely to adhere strictly to information security protocols. Frauenstein and Flowerday [17] found that conscientious users exhibit lower susceptibility to SNS phishing due to reduced heuristic processing.

D. Unique Aspects of Information Security Risk-taking

Several factors differentiate information security risk-taking behavior. These include:

1) *Digital Environment:* Cyber risks continually change and are complex, making risk assessment and decision-making difficult. Fast information flow and frequent technology changes might overwhelm users and influence their risk-taking decisions online, unlike in traditional settings. Digital environments, where interactions and transactions occur in a networked and virtual world, present distinct problems and risks than physical settings. The immateriality of the digital environment might mask dangers' immediacy and potential impact, resulting in a different risk perception than physical threats. The digital environment is dynamic and complex, developing with new technology and attack approaches. Cybersecurity risk assessment and decision-making are more difficult than in construction or finance because threats appear and evolve quickly [44].

2) *Anonymity and Psychological Distance:* A significant difference in cybersecurity is the role of anonymity and psychological distance. Unlike the direct, physical risks encountered in sports or health-related behaviors, cybersecurity often deals with anonymous threats, which can feel less immediate and real. This is consistent with findings that suggest a higher perceived risk when negative consequences are likely to be immediate [45].

3) *Cognitive Biases:* Cognitive biases, such as the illusion of invulnerability, are particularly pronounced in information security. Users often underestimate the likelihood of being targeted by cyberattacks, a bias that might not be as evident in other fields. Information security risk-taking is influenced by the commonality of cognitive biases across many disciplines, affecting people's perceptions and reactions to risks. Overconfidence, for instance, impacts decision-making universally, leading individuals to underestimate potential risks in various situations, from daily life to financial decisions. This illusion of invulnerability is prevalent in information security, where individuals may feel safe from cyberattacks, leading to inadequate safety precautions and increased vulnerability to online threats [46].

4) *Adaptability to Changing Threats:* Information security is dynamic and requires constant adaptation to combat new threats. Cybercriminals constantly change attack methods and target new platforms, making information security a dynamic domain. The move from desktop to mobile platforms and the rise of social engineering and botnets show cyber dangers' adaptability. Safety precautions and interventions must be flexible, especially in cybersecurity, where user behaviors and cyber threats change constantly. S. This need for flexibility, highlighted in works like those by Vance et al. [47], is crucial in personal health or workplace safety decisions, emphasizing the importance of adaptability in risk management strategies.

5) *Complexity and Evolution of Threats:* The complexity and evolution of cyber threats are evident in the continual adaptation and sophistication of attack methods, as demonstrated in various domains like social media, cloud computing, smartphones, and critical infrastructure. These threats evolve in complexity and scope, leveraging technological advancements to exploit new vulnerabilities and increase the scale of attacks. For instance, attackers' use of social media exemplifies how technological proliferation can facilitate the rapid spread of malware to a large user base, exploiting both technical vulnerabilities and human factors [44].

6) *Online Social Influences:* Social dynamics, heavily influencing decisions in various fields, manifest uniquely in cybersecurity risk-taking through online influences and social engineering tactics. These dynamics can influence cybersecurity decisions, underscoring the importance of understanding the impact of social effects in developing cross-domain risk mitigation measures [48].

4. METHODS

A. Participants

The study was conducted during the academic year 2020-2021 among undergraduate students who were enrolled at Mindanao State University - Iligan Institute of Technology

(MSU-IIT). The total number of individuals in the study population was 7,718. The participant pool encompassed undergraduate students from diverse year levels within the seven distinct colleges at the institution. Stratified random sampling was utilized to represent all undergraduate students comprehensively. This technique involves segmenting the population into homogeneous subsets based on specific characteristics. We categorized undergraduate students into subgroups corresponding to their respective colleges. A random selection of participants was drawn from each subgroup, with the number determined based on the population size within that subgroup.

TABLE I. DEMOGRAPHIC PARTICIPANTS

	N	%
Sexual Orientation		
Female	236	75.9
Male	71	22.8
LGBTQ+	4	1.3
Age		
18	23	7.4
19	73	23.5
20	87	28.0
21	57	18.3
22	50	16.1
23	10	3.2
24	1	0.3
Year Level		
First Year	94	30.2
Second Year	96	30.9
Third Year	63	20.3
Fourth Year	58	18.6

Considering the sample size, a 95% confidence interval and a 5% margin of error were considered to establish an appropriate population of 7,718. The study involved the participation of 311 respondents across varying year levels and college affiliations. A sample size ranging from 10% to 30% is considered sufficient when well-chosen and when the sample elements exceed 20 (Mugenda & Mugenda, 2003). In line with this guidance, the chosen sample size for this study aligns with established principles of sampling methodology. The participants encompassed a diverse group comprising 236 females, 71 males, and 4 individuals identifying as LGBTQ. The age range of the participants was 18-24 years (M=21). Additional demographic information, including year level and college affiliation, is provided in Table 1.

B. Measures

The survey was conducted online via Google Forms. In addition to inquiries to assess participants' Big Five Inventory (BFI) characteristics, security knowledge, IT service usage, and security practices, the survey also included demographic questions regarding age, gender, college affiliation, and year level. The survey incorporated controlled questions designed as attention checks to identify respondents who might not provide truthful answers. Participants who answered any of the controlled questions incorrectly have been excluded from the study.

To participate in the survey, respondents were instructed to log in using their My.IIT email address through Google Forms, ensuring that only individuals within the organization were included. The research employed a self-completion questionnaire, affording respondents complete anonymity. This approach aimed to mitigate concerns related to potentially ethically ambiguous choices. While the questionnaire itself was not obligatory, all its questions were. The survey's objectives, scope, contact information, and informed consent were presented on the initial page.

The survey was used as a research instrument to investigate the relationship between the participants' BFI characteristics (independent variable) and their risk status as end-users (dependent variable). This risk status was derived from their security knowledge, IT service usage, and security practices. The five (5) main sections are as follows:

- Section A: Demographic
- Section B: BFI Characteristics were assessed using a 5-point Likert scale from 1 (strongly disagree) to 5 (strongly agree).
- Section C: Security Knowledge (The evaluation was conducted using a 5-point Likert scale ranging from very low to very high).
- Section D: IT Service Usage (The measurement is based on a 5-point Likert scale that ranges from 1, which means "never," to 5, which means "always.")
- Section E: Security Practices (The individuals were evaluated by using a 5-point Likert scale, which ranged from 1 “never” to 5 “always”.)

A reliability test was conducted to assess the validity and reliability of the survey instrument, which was adapted from Alohali et al. [49]. The outcomes of the reliability test are presented in Table 2, where each factor in the questionnaire comprises a minimum of 5 items. The Cronbach's alpha values for each variable exceed the acceptable threshold of 0.7. Following the rule of thumb, the survey instrument utilized in this study demonstrates both validity and reliability, as evidenced by its satisfactory internal consistency.

TABLE II. RELIABILITY TEST OF THE QUESTIONNAIRE

Component	No. of Items	Cronbach’s alpha
BFI	44	1.023
Security Knowledge	20	0.941
IT Usage Service	8	0.745
Security Practices	26	0.878

C. Analysis

The data analysis in this study employs Spearman correlation analysis to explore relationships between variables and subsequently employs logistic regression modeling to delve further into predictive insights.

1) Spearman's correlation: The application of correlation analysis is a well-established method for uncovering significant relationships within data [50]. These relationships aid in discerning the pertinence of attributes concerning the target class under consideration. We used Orange software for the correlation analysis to address the research inquiries. Spearman's correlation coefficient (ρ or rs) measures the strength and direction of the monotonic relationship between two ranked variables. A monotonic relationship falls into two categories: (1) when an increase in one variable is associated with an increase in the other variable, or (2) when an increase in one variable is associated with a decrease in the other variable. The Spearman's coefficient (rs) is a statistical measure that ranges from -1 to 1. A value of +1 indicates a perfect positive correlation between ranks, while a value of -1 indicates a perfect negative correlation between ranks. A value of 0, on the other hand, signifies no correlation between ranks. Spearman's Correlation Analysis can determine whether two variables have a positive, negative, or no correlation. A positive correlation means that as one variable increases, the other increases, and vice versa. Conversely, a negative correlation signifies that as one variable increases, the other decreases, and vice versa. The strength of the correlation can be categorized as weak (rs within 0.1 - 0.3), moderate (rs within 0.3 - 0.5), or strong (rs within 0.5 – 1.0). It is crucial to satisfy the assumptions when employing Spearman's coefficient. The first assumption states that the two correlated variables should be measured on an ordinal, interval, or ratio scale. This study measured the variables using ordinal scales such as 5-point Likert scales. The second assumption emphasizes a monotonic relationship between the two variables, which was considered in this study.

2) Logistic Regression: In our study, the use of logistic regression went beyond merely predicting risk status based on BFI characteristics; it was pivotal in deepening our understanding of how these characteristics relate to end-users susceptibility to information security risks. Figure 2 illustrates the architecture of our analysis model. Before the modeling process, we implemented feature selection, which is crucial for refining the input variables in the model. This step enhances computational efficiency and the overall performance of the analysis. An essential technique in our feature selection process was the Relief-Based Feature Selection (RBFS) [51]. RBFS excels in identifying interactions among features and assigning scores to each feature to facilitate the ranking and selecting the most relevant attributes for analysis. This method is adaptable to various data types, supporting classification and regression tasks. Relief-based algorithms (RBAs), to which RBFS belongs, are known for balancing different objectives and adapting to diverse data characteristics.

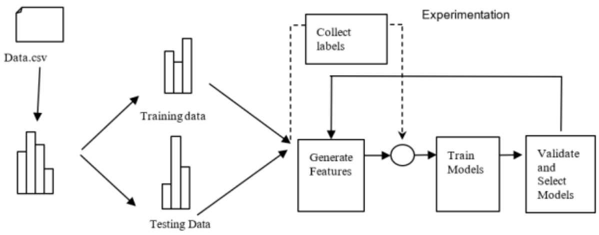


Figure 2. Conceptual Framework

This study primarily applied logistic regression to examine the relationship between personality traits and risk status. By analyzing this relationship, we gained insights into the patterns and factors that might contribute to end-users' vulnerability in information security contexts. We enhanced the robustness of our analysis through a 10-fold cross-validation method, which helped reduce bias and improve the validity of our findings by exposing the model to a broad spectrum of data scenarios.

Furthermore, we transformed the data into a numerical format to ensure compatibility with logistic regression analysis. This transformation was crucial for the model's practical interpretation and analysis of the data. Logistic regression emerged as a valuable tool in our study through this methodological approach, enabling us to explore the complex interplay between personality traits and information security risk behaviors. The insights derived from this analysis are instrumental in informing the development of targeted and effective cybersecurity strategies and interventions, tailored to the specific traits and behaviors of end-users.

5. Results

A. Understanding KAB Components and Information Security AwarenessSpearman's Correlation

1) Security Knowledge

The data analysis in this study employs Spearman correlation analysis to explore relationships between variables and subsequently employs logistic regression modeling to delve further into predictive insights.

The findings reported in Table 3 provide insights into the significance of information security awareness as demonstrated by participants' Security Knowledge. The findings provide a comprehensive view of respondents' familiarity with various information security-related terms. Notably, the variation in understanding levels among participants emphasizes the significance of bolstering awareness efforts. For example, terms such as "Adware," "Spyware," and "Phishing" demonstrate a clear trajectory from low to high knowledge levels, indicating the need for targeted education on these specific topics.

The participants' awareness of IT security measures underscores the diverse comprehension levels across the listed measures. Terms such as "Anti-Virus," "Anti-Spyware," and "Anti-Spam" show varying knowledge distributions, indicating the need for targeted efforts to enhance understanding.

Exploring participants' awareness of statements about the organization's IT support highlights the need for comprehensive information dissemination. While a considerable portion is aware of the existence of the IT department, the understanding of its supportive role in addressing IT issues is evenly distributed across different knowledge levels. Furthermore, the knowledge concerning students' access to free anti-virus software exposes a gap in awareness, emphasizing the necessity of promoting this resource more effectively.

The results of this study highlight the significance of tailoring information security awareness programs to effectively target and address the specific knowledge deficiencies that have been found. By improving the comprehension of end-users regarding terms associated with information security, actions taken for IT security, and the support provided by organizations, it becomes possible to develop strategies that empower users with the necessary knowledge to make informed choices and contribute to establishing a more secure digital environment.

TABLE III. SECURITY KNOWLEDGE RESULTS

Terms	**Very Low**	**Low**	**Average**	**High**	**Very High**
Knowledge of Information Security-Related Terms					
Virus	3.21	11.9	31.51	30.22	23.15
Adware	18	24.76	36.01	15.11	6.11
Spyware	15.43	23.79	35.05	19.29	6.43
Phishing	7.07	15.43	29.90	26.05	21.54
Hacker	4.18	13.50	23.47	29.58	29.26
Firewall	10.93	15.43	32.8	22.50	18.33
Identity Theft	6.11	9.97	21.86	33.12	28.94
Worm	17.36	23.15	31.51	18.97	9.0
Trojan Horse	14.15	20.90	30.55	21.54	12.86
Knowledge of IT Security Measures					
Anti-Virus	2.57	15.11	32.8	31.51	18
Anti-Spyware	14.15	32.15	32.48	15.76	5.47
Anti-Spam	10.61	25.72	34.41	20.58	8.68
Firewall	14.15	21.86	32.15	18.97	12.86
Software Updates	1.61	11.25	26.69	34.08	26.37
Secure Password Practice	1.61	10.93	23.79	29.58	34.08
Back Ups	2.57	12.54	23.79	31.19	29.9
Security Measures on Mobile Devices	1.61	13.50	28.62	28.62	27.65
Knowledge of Statements on the Organization's IT Support					
Awareness of the existence of the ICTC	2.89	8.04	21.86	26.05	41.16
Knowing that the ICTC is supportive in any IT problems	6.43	13.18	29.90	29.9	20.58
Knowing that students of the university can use the anti-virus software on their devices for free	27.33	24.44	28.94	9.0	10.29

2) IT ServiceUsage

The findings about IT Service Usage, as presented in Table 4, underscore the significance of individuals' engagement with various IT services. The distribution of respondents' interaction with these services sheds light on the behavior patterns that can directly affect their awareness and security practices.

The high frequency of email utilization, with a substantial majority indicating "Always," highlights the integral role of email as a communication tool in daily life. Similarly, the substantial engagement with social media and search engines, where a considerable proportion of respondents consistently indicate "Always," accentuates the pervasive presence of these platforms in users' routines, emphasizing the importance of ensuring their secure usage.

TABLE IV. IT SERVICE USAGE RESULT

IT Service	**Never (%)**	**Rarely (%)**	**Sometimes (%)**	**Often (%)**	**Always (%)**
Email	1.0	0.6	9.0	22.19	67.2
Social Media	0.3	1.0	6.75	13.18	78.78
Online Streaming	18.33	13.50	21.54	16.4	30.23
Search Engine	0.3	0.6	6.75	17.36	74.92
Online Banking	21.22	18.97	21.86	21.22	16.72
Back-Up Cloud Services	1.0	4.5	17.36	22.19	54.98
Online Gaming	19.61	16.08	16.72	13.5	34.08
Online Shopping	6.43	11.25	19.61	22.19	40.51

The varying engagement levels observed in online streaming indicate a diverse range of behaviors, with a noteworthy percentage of participants falling within the "Sometimes" category. This variability underscores the need to address security concerns related to online streaming, given the potential exposure to risks associated with content consumption.

The mixed pattern in online banking usage, spanning multiple usage categories, reveals a complex landscape of user behavior. While a significant portion engages in online banking regularly, a notable percentage indicates infrequent or no usage. This variability emphasizes strengthening security practices in online financial transactions to safeguard sensitive information. Furthermore, the pronounced pattern of engagement with backup cloud services, where a majority indicates "Always" or "Often," reflects the increasing reliance on cloud storage for data backup. This dependence highlights the importance of securing cloud-based data storage and access to prevent unauthorized access or data breaches. In contrast, the distribution of responses regarding online gaming spans various usage categories, with a significant portion indicating "Sometimes." This finding calls for raising awareness about potential security risks associated with online gaming activities.

Various engagement patterns with different IT services highlight the necessity of implementing a comprehensive information security awareness program. This program should effectively cater to the multiple usage habits observed and encourage responsible practices across all these services.

3) *Security Practices*

Table 5 presents the analysis outcomes concerning participants' Security Practices, shedding light on the role of information security awareness and risk-taking behavior. Assessing participants' performance frequency in password security practices unveils insights into their risk-taking behavior and security consciousness. A notable percentage of respondents indicate engaging in password sharing, while a majority recognize the importance of not saving passwords on browsers. Strikingly, a substantial proportion of participants demonstrate using different sets of passwords for multiple accounts, emphasizing a security-conscious approach. Similarly, respondents exhibit cautious behavior by refraining from using the same password for private online services as for university applications. This phenomenon corresponds with an increased knowledge of information security and a greater grasp of the potential vulnerabilities of utilizing identical passwords. Moreover, the findings reveal the acknowledgment of secure password practices, such as enabling antivirus/firewall and keeping antivirus software up to date.

Regarding email security practices, participants' responses reveal their attentiveness to potential risks. Many respondents disregard emails and link attachments from unknown resources and actively check unexpected emails for signs of potential harm. Likewise, respondents tend to delete suspicious emails, reinforcing their security-aware behavior. Furthermore, participants show a mix of reliance on antivirus-antispyware software for recognizing malicious emails, reflecting both security-consciousness and technological trust.

The analysis of data management practices underscores participants' efforts to safeguard sensitive information. A substantial percentage demonstrates proactive behavior by regularly performing data backups and using encryption for sensitive computer data. This reflects a heightened security awareness, with participants actively taking steps to mitigate data loss and unauthorized access risks.

The findings underscore the significant impact of information security awareness on the creation of individuals' risk-taking tendencies and their adherence to security protocols. By recognizing potential threats and proactively implementing security measures, individuals actively contribute to establishing a more secure digital environment and exhibit their dedication to promoting information security awareness.

TABLE V. SECURITY PRACTICES

Security Practices	**Never (%)**	**Rarely (%)**	**Sometimes (%)**	**Often (%)**	**Always (%)**
Performance Frequency of Password Security Practices					
I don’t engage in password sharing	5.47	7.4	8.68	17.36	61.09
Password storage	29.9	17.04	21.22	14.79	17.04
Log off from online system	2.89	13.18	19.94	27.33	36.66
I don’t save my password on browser	7.4	18.65	19.94	16.08	37.94
Different set of passwords for multiple accounts	13.83	18	22.83	20.26	25.08
For private online services, I don’t use the same password as for university applications	8.68	14.15	13.5	16.4	47.27
It’s easy to remember new passwords	19.61	18.87	26.04	15.76	19.61
I get used and I think it's fine to type in my password every time I unlock my screen or I got logged out from my account	9.0	8.04	26.37	20.9	35.69
Performance Frequency of Software Security Practices					
I always enable the antivirus/firewall	6.11	14.15	24.76	25.4	29.58
Keep the antivirus software up-to-date	6.11	14.47	24.44	24.44	30.55
Install/use of authentic software and never got involved in using pirated or counterfeit software	6.43	16.08	29.9	24.76	22.83
Performance Frequency of Email Security Practice					
I disregard emails/link attachments from	3.22	3.86	15.11	20.26	55.56

unknown resources					
If I receive an unexpected email, I always check if it shows signs of being potentially harmful	3.22	5.79	13.5	25.08	52.41
Delete suspicious emails	2.25	8.68	14.14	20.26	54.66
Ignoring chain emails	1.93	2.25	8.68	18.65	68.49
I'm sure that my antivirus-antispyware software recognizes malicious emails	2.57	10.61	24.12	26.37	36.33
Performance Frequency of Network Management Practice					
Connect to public access networks/Wi-Fi	8.04	19.29	25.4	20.26	27
Disable wireless technologies when not in use	7.72	12.86	19.29	22.19	37.94
Use a VPN	26.69	20.9	27.65	14.15	10.61
Performance Frequency of Data Management Practice					
Destroy all data before hardware proposals	14.15	17.36	29.58	21.54	17.36
Avoid downloading files from suspicious/unknown /unreliable websites	4.18	14.15	22.51	21.22	37.94
Performing regular data backup	5.79	20.58	28.94	23.15	21.54
Scanning a USB drive before usage	2.25	16.72	18.64	22.19	40.19
Encryption for sensitive information on computer	11.25	19.94	24.76	23.15	20.90
Use encrypted for file transfer	12.22	20.26	26.69	24.12	16.72
I secure access to my private smartphone by using a print	1.29	3.54	10.29	18.65	66.24

B) *Identifying significant correlations between Information Security Risk-Taking Behavior and specific BFI traits*

This study employed the Big Five Inventory (BFI) characteristics as the independent variable, while the dependent variable was the risk status, which was determined based on the components of Knowledge, Attitude, and Behavior (KAB), including security knowledge, IT service utilization, and security practices. A Spearman correlation analysis was performed to examine the association between the Big Five Inventory (BFI) traits and the risk status of the end-user.

The analysis of the correlation between the BFI traits of the participants and their risk status has resulted in significant and enlightening discoveries, detailed in Table 5. The BFI characteristics were analyzed against the end-user's risk status, a composite measure derived from security knowledge, IT service usage, and security practices.

Noteworthy observations emerge from the correlation analysis. "Agreeableness vs. Antagonism" shows a stronger negative correlation with the end-user's risk status among the BFI dimensions. Specifically, traits such as finding fault with others (A2*), starting quarrels with others (A12*), and sometimes being rude to others (A37*) demonstrate notable negative correlations with risk status. This suggests that individuals exhibiting these characteristics tend to have a lower risk status due to their proclivity for cooperation and helpfulness. Experiencing depression (A4), displaying a tendency to be somewhat careless (A8), exhibiting high energy (A11), leaning towards quietness (A21), and being easily distracted (A43), demonstrate a positive correlation with the end-users risk status. This observation suggests that possessing traits associated with being depressed, somewhat careless, full of energy, quiet, and easily distracted corresponds to an elevated susceptibility to security risks.
Moreover, "Conscientiousness vs. Lack of Direction" traits significantly correlate with risk status. For instance, attributes such as doing a thorough job (A3), being a reliable worker (A13), and making plans and following through with them (A38) exhibit negative correlations with risk status. These findings indicate that conscientious individuals might also demonstrate responsible and cautious behavior, potentially leading to a lower risk status.

TABLE VI. BFI TRAITS CORRELATION AND END-USERS RISK STATUS

BFI	Notation and Meaning	Correlation Coefficient
Extraversion vs. Introversion*	A1: Is talkative	-0.059
	A6*: Is reserved	-0.039
	A11: Is full of energy	+0.049
	A16: Generates a lot of enthusiasm	-0.070
	A21*: Tends to be quiet	+0.004
	A26: Has an assertive personality	-0.189
	A31*: Is sometimes shy, inhibited	-0.129
	A36: Is outgoing, sociable	-0.053
Agreeableness vs. Antagonism*	A2*: Tends to find fault with others	-0.025
	A7: Is helpful and unselfish with others	-0.065
	A12*:Starts quarrels with others	-0.026
	A17: Has a forgiving nature	-0.074
	A22: Is generally trusting	-0.113
	A27*: Can be cold and aloof	-0.132
	A32: Is considerate and kind to almost everyone	-0.110
	A37*: Is sometimes rude to others	-0.007
	A42: Likes to cooperate with others	-0.122
Conscientiou	A3: Does a thorough job	-0.146
	A8*: Can be somewhat careless	+0.018
	A13: Is a reliable worker	-0.123

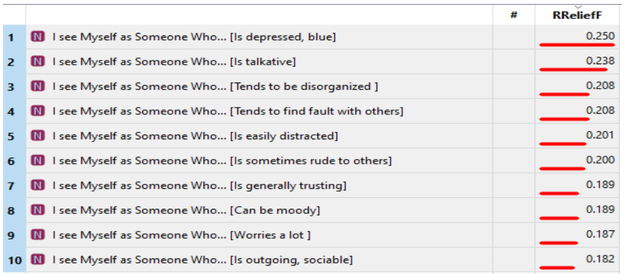
sness vs. Lack of Direction*	A18*: Tends to be disorganized	-0.019
	A23*: Tends to be lazy	-0.094
	A28: Perseveres until the task is finished	-0.162
	A33: Does things efficiently	-0.153
	A38: Makes plans and follows through with them	-0.170
	A43*: Is easily distracted	+0.009
Neuroticism vs. Emotional Stability*	A4: Is depressed, blue	+0.053
	A9*: Is relaxed, handles stress well	-0.027
	A14: Can be tense	-0.043
	A19: Worries a lot	-0.052
	A24*: Is emotionally stable, not easily upset	-0.172
	A29: Can be moody	-0.100
	A34*: Remains calm in tense situations	-0.148
	A39: Gets nervous easily	-0.036
Openness vs. Closedness to Experience*	A5: Is original, comes up with new ideas	-0.061
	A10: Is curious about many different things	-0.042
	A15: Is ingenious, a deep thinker	-0.106
	A20: Has an active imagination	-0.174
	A25: Is inventive	-0.118
	A30: Values artistic, aesthetic experiences	-0.099
	A35*: Prefers work that is routine	-0.098
	A40: Likes to reflect, play with ideas	-0.069
	A41*: Has few artistic interests	-0.071
	A44: Is sophisticated in art, music, or literature	-0.092

In contrast, some BFI characteristics exhibit weaker correlations with risk status. For instance, traits related to "Extraversion vs. Introversion," "Neuroticism vs. Emotional Stability," and "Openness vs. Closedness to Experience" display varied correlations that are generally closer to neutral. This suggests that the impact of these traits on the end-user's risk status might be less pronounced.

C) *Identifying Relevant Features*

The adopted model was employed to discern the most influential attributes among the BFI characteristics in relation to the target variable - Risk Status. The dataset comprises 45 columns, with one (1) target variable, Risk Status, and forty-four (44) features representing the BFI characteristics.

Figure 3 visualizes the ten most significant BFI characteristics based on their correlation with end-users security risk status. Leading the relevance ranking is the characteristic "Is depressed, blue," followed by "Is talkative" as the second most influential feature. The third-ranking feature by relevance is "Tends to be disorganized."



		#	RReliefF
1	N I see Myself as Someone Who... [Is depressed, blue]		0.250
2	N I see Myself as Someone Who... [Is talkative]		0.238
3	N I see Myself as Someone Who... [Tends to be disorganized]		0.208
4	N I see Myself as Someone Who... [Tends to find fault with others]		0.208
5	N I see Myself as Someone Who... [Is easily distracted]		0.201
6	N I see Myself as Someone Who... [Is sometimes rude to others]		0.200
7	N I see Myself as Someone Who... [Is generally trusting]		0.189
8	N I see Myself as Someone Who... [Can be moody]		0.189
9	N I see Myself as Someone Who... [Worries a lot]		0.187
10	N I see Myself as Someone Who... [Is outgoing, sociable]		0.182

Figure 3. Top-10 Best Ranked Features

This study employed logistic regression to predict individuals' risk status based on their Big Five Personality Traits, achieving 85.7% classification accuracy. The performance of this predictive algorithm was assessed using a confusion matrix, which provided insights into the accuracy of classifications and instances of misclassifications.

The analysis identified Neuroticism as a key trait linked to an “At Risk” status. Neuroticism encompasses a range of negative emotions such as anger, anxiety, self-consciousness, irritability, emotional instability, and depression. In contrast, Conscientiousness, characterized by thoughtfulness, good impulse control, and goal-directed behaviors, was significantly associated with a “Not At Risk” status.

Further, we compared the results of the correlation test, feature selection, and logistic regression to identify specific BFI characteristics with high relevance to being “At Risk.” These include:

1. Neuroticism (33.33%): As mentioned, this trait involves a predisposition to negative emotional states.
2. Lack of Direction (16.67%): This is indicative of a lower conscientiousness level, with traits such as being careless and easily distracted, which increase vulnerability to security risks.
3. Antagonism (16.67%): The low end of Agreeableness, Antagonism is characterized by immorality, disagreeableness, and socially unpleasant behaviors like manipulation and lack of empathy.
4. Extraversion and Introversion (16.67% each): Extraversion involves traits like talkativeness and emotional expressiveness, while Introversion is associated with a preference for solitude and lower energy in social situations.

These traits collectively contribute to the model’s ability to elucidate risk status within our study's framework. This nuanced understanding of personality traits and their relation to cybersecurity risks is crucial for developing targeted interventions and enhancing overall cybersecurity resilience. The model demonstrated notable accuracy, substantiating the hypothesis that these personality traits are reliable indicators of information security behaviors. This finding is particularly significant as it highlights BFI’s potent predictive capacity within the cybersecurity domain. It underscores a meaningful connection between individual personality profiles and their propensity for various cybersecurity risks. The model's ability to link these personality traits with security behaviors reinforces the importance of considering psychological factors in cybersecurity strategies and risk assessments.

6. Discussion

The survey result highlights significant disparities in the understanding of specific cybersecurity terms and concepts. This variation underscores the essential need for foundational education in information security, particularly for terms showing a trajectory from low to high knowledge levels, such as "Adware," "Spyware," and "Phishing." In contrast, higher understanding levels for "Software Updates" and "Secure Password Practices" reflect their perceived importance in safeguarding digital assets. This disparity in knowledge levels, as analyzed within the KAB framework, directly impacts individuals' attitudes toward cybersecurity. A deeper grasp of threats and protective measures fosters a proactive attitude, which is instrumental in shaping secure behaviors, including the adoption of advanced security practices.

The survey also highlights the significant involvement with IT services. These include email, social media, and search engines, essential for everyday activities. Therefore, they need secure usage protocols. The variability observed in the use of online streaming and banking services indicates diverse behavioral patterns, calling for security practices tailored to these specific activities. This aspect highlights how habitual use of certain IT services molds attitudes and behaviors within the KAB framework, emphasizing the need for targeted educational and behavioral interventions.

The security practices among participants indicate a security-conscious approach. Practices like using different passwords, cautious email behaviors, regular data backups, and encrypting sensitive data reflect a positive shift in attitudes and enhanced knowledge – core components of the KAB model. This finding suggests reinforcing positive behaviors through increased knowledge could cultivate a robust information security culture.

The study reveals the intricate correlation between BFI qualities - openness, conscientiousness, extraversion, agreeableness, and neuroticism - and information security risk-taking behaviors. By employing the KAB components, the risk status level can be determined—this analysis finds significant correlations between specific traits, such as Agreeableness and Conscientiousness, and a decreased risk status. In contrast, characteristics such as Neuroticism and a tendency towards a lack of focus correlate with higher risk status. This understanding is crucial for developing more efficient and tailored information security methods.

Drawing on the findings of Shappie et al. [10] and Alohali et al. [49], our study aligns with the significant roles of Conscientiousness, Agreeableness, and Openness in shaping cybersecurity behaviors. Shappie et al. [10] utilized linear and hierarchical regression analyses, while Alohali et al. [49] employed a bi-variate Pearson correlation and a neural network-based classification approach. Our study employs Spearman correlation analysis and logistic regression to explore the impact of various BFI traits on cybersecurity risk behaviors. With an 85.7% classification accuracy, the logistic regression model underlines the influence of traits such as Neuroticism, Lack of Direction, Antagonism, Extraversion, and Introversion on cybersecurity risk behaviors. This finding aligns with other studies exploring how personality traits influence cybersecurity behaviors. It provides valuable insights for organizations, guiding them in developing tailored training programs and policies.

The study offers insight into the interaction between the Big Five Personality Traits (BFI) and the Knowledge-Attitude-Behavior (KAB) framework within the context of information security (Figure 5). This model examines how individual personality qualities impact one's information security approach, specifically influencing knowledge, attitudes, and behaviors. The BFI traits fundamentally shape the information security KAB components, each exerting a distinct impact on how individuals comprehend, perceive, and act.

For the knowledge component, openness, marked by curiosity and a penchant for new ideas, significantly enhances an individual's understanding and awareness of information security. Similarly, conscientiousness, characterized by thoroughness and attention to detail, contributes substantially to acquiring in-depth security knowledge. Regarding attitudes towards cybersecurity practices, agreeableness, which includes cooperativeness and trust, fosters positive perceptions and approaches. In contrast, neuroticism, with its inherent anxiety and worry, can negatively skew attitudes, leading to apprehension or misjudgments in decision-making.

Behaviorally, conscientious individuals, known for their disciplined and responsible approach, tend to adopt safer cybersecurity practices. On the other hand, those with higher neuroticism might exhibit riskier behaviors due to distorted perceptions. Furthermore, extroverts, with their sociability and assertiveness, generally develop positive attitudes towards cybersecurity, though their sociable nature can also increase their susceptibility to social engineering attacks. This creates a nuanced relationship with their cybersecurity risk status.

This demonstrates that a person high in conscientiousness, openness, and agreeableness is likely to possess sound knowledge, a positive attitude, and practice safe cybersecurity behaviors. Conversely, an individual with high neuroticism and low openness might have limited knowledge, a negative attitude, and a propensity for riskier behaviors. Thus highlights the complex interplay between personality traits and information security, demonstrating how these traits shape all aspects of cybersecurity engagement, from knowledge, attitude and the actual behavior exhibited. This understanding is critical in predicting and modifying behaviors related to information security, offering insights into the development of targeted strategies and interventions.

Future research should integrate psychological theories to explain why certain personality traits lead to specific attitudes or behaviors in cybersecurity. Additionally, considering cultural and contextual factors might reveal how these relationships vary across different environments.

Essentially, the KAB model, when combined with the Big Five Personality Traits, demonstrates that an individual's knowledge, attitude, and behavior in information security are significantly impacted by their innate personality characteristics. This understanding is key for predicting and changing behaviors in various contexts, including cybersecurity. The study's recommendations for targeted educational programs and exploring long-term impacts open the way for more practical information security strategies. This bridges the gap between human psychology and cybersecurity decision-making.

7. Conclusion

This research offers significant insights into the intersection of personality traits and information security behavior, emphasizing the need for targeted awareness initiatives and the promotion of responsible IT service usage to enhance cybersecurity practices. The study highlights the impact of personality traits, particularly those within the BFI, on security behavior, suggesting the necessity of user-centric and personalized approaches in cybersecurity awareness. However, the research has limitations, including potential external influences on risk-taking behavior and the simplicity of the model, which might not capture all interactions or effects. Specific demographics and environments could influence the generalizability of the findings, and the reliance on self-reported data might introduce biases. Despite these limitations, the study opens up several avenues for future research. Refining awareness initiatives to align with individual personality traits, conducting longitudinal studies to understand the evolution of these traits, exploring cultural factors, and assessing the effectiveness of tailored interventions could deepen our understanding of cybersecurity. Developing adaptive security measures that respond to individual personality traits could lead to more effective, user-focused cybersecurity strategies. The research underscores the importance of integrating a culture of information security within organizations to mitigate risks to information assets effectively, highlighting the role of individualized treatments aligned with personality traits as part of this culture.

Acknowledgment

This study is funded by MSU-Iligan Institute of Technology (S.O. 00108-2022).

References

[1] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82-97, 2022/01/02 2022, doi: 10.1080/08874417.2020.1712269.

[2] A. Wiley, A. McCormac, and D. Calic, "More than the individual: Examining the relationship between culture and Information Security Awareness," *Computers & Security*, vol. 88, p. 101640, 2020/01/01/ 2020, doi: https://doi.org/10.1016/j.cose.2019.101640.

[3] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson, "Individual differences and Information Security Awareness," *Computers in Human Behavior*, vol. 69, pp. 151-156, 2017/04/01/ 2017, doi: https://doi.org/10.1016/j.chb.2016.11.065.

[4] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Computers & Security*, vol. 42, pp. 165-176, 2014/05/01/ 2014, doi: https://doi.org/10.1016/j.cose.2013.12.003.

[5] S. Furnell and N. Clarke, "Power to the people? The evolving recognition of human aspects of security," *Computers & Security*, vol. 31, no. 8, pp. 983-988, 2012/11/01/ 2012, doi: https://doi.org/10.1016/j.cose.2012.08.004.

[6] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," *Heliyon*, vol. 9, no. 3, p. e14234, 2023, doi: 10.1016/j.heliyon.2023.e14234.

[7] R. von Solms and J. van Niekerk, "From information security to cyber security," *Computers & Security*, vol. 38, pp. 97-102, 2013/10/01/ 2013, doi: https://doi.org/10.1016/j.cose.2013.04.004.

[8] IBM, "IBM 2015 Cybersecurity Intelligence Index." [Online]. Available: https://www.ospi.es/export/sites/ospi/documents/IBM_2015_CyberSecurity_Intelligence_Index.pdf

[9] H. de Bruijn and M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," *Government Information Quarterly*, vol. 34, no. 1, pp. 1-7, 2017/01/01/ 2017, doi: https://doi.org/10.1016/j.giq.2017.02.007.

[10] A. T. Shappie, C. A. Dawson, and S. M. Debb, " Personality as a predictor of cybersecurity behavior," *Psychology of Popular Media*, vol. 9, no. 4, pp. 475-480, 2020, doi: https://psycnet.apa.org/doi/10.1037/ppm0000247.

[11] O. P. John and S. Srivastava, "The Big Five Trait taxonomy: History, measurement, and theoretical perspectives," in *Handbook of personality: Theory and research, 2nd ed.* New York, NY, US: Guilford Press, 1999, pp. 102-138.

[12] I. Arpaci, K. Karatas, I. Kusci, and M. Al-Emran, "Understanding the social sustainability of the Metaverse by integrating UTAUT2 and big five personality traits: A hybrid SEM-ANN approach," *Technology in Society*, vol. 71, p.

102120, 2022/11/01/ 2022, doi: https://doi.org/10.1016/j.techsoc.2022.102120.

[13] M. Akbari, M. Seydavi, S. Jamshidi, C. Marino, and M. M. Spada, "The Big-five personality traits and their link to problematic and compensatory Facebook use: A systematic review and meta-analysis," *Addictive Behaviors*, vol. 139, p. 107603, 2023/04/01/ 2023, doi: https://doi.org/10.1016/j.addbeh.2022.107603.

[14] J. A. Espinoza, T. A. O'Neill, and M. B. L. Donia, "Big Five factor and facet personality determinants of conflict management styles," *Personality and Individual Differences*, vol. 203, p. 112029, 2023/03/01/ 2023, doi: https://doi.org/10.1016/j.paid.2022.112029.

[15] S. M. Kennison and E. Chan-Tin, "Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors," *Frontiers in Psychology*, vol. 11, 2020, doi: 10.3389/fpsyg.2020.546546.

[16] A. Shaw and J. Choi, "Big Five personality traits predicting active procrastination at work: When self- and supervisor-ratings tell different stories," *Journal of Research in Personality*, vol. 99, p. 104261, 2022/08/01/ 2022, doi: https://doi.org/10.1016/j.jrp.2022.104261.

[17] E. D. Frauenstein and S. Flowerday, "Susceptibility to phishing on social network sites: A personality information processing model," *Computers & Security*, vol. 94, p. 101862, 2020/07/01/ 2020, doi: https://doi.org/10.1016/j.cose.2020.101862.

[18] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Computers & Security*, vol. 25, no. 4, pp. 289-296, 2006/06/01/ 2006, doi: https://doi.org/10.1016/j.cose.2006.02.008.

[19] G. H. Eifert and L. Craill, "The Relationship between Affect, Behaviour, and Cognition in Behavioural and Cognitive Treatments of Depression and Phobic Anxiety," *Behaviour Change*, vol. 6, no. 2, pp. 96-103, 1989, doi: 10.1017/S0813483900007634.

[20] N. J. MacKinnon and J. Hoey, "Operationalizing the Relation Between Affect and Cognition With the Somatic Transform," *Emotion Review*, vol. 13, no. 3, pp. 245-256, 2021, doi: 10.1177/17540739211014946.

[21] P. Nunes, M. Antunes, and C. Silva, "Evaluating cybersecurity attitudes and behaviors in Portuguese healthcare institutions," *Procedia Computer Science*, vol. 181, pp. 173-181, 2021/01/01/ 2021, doi: https://doi.org/10.1016/j.procs.2021.01.118.

[22] N. Nicholson, E. Soane, M. Fenton ‐ O'Creevy, and P. Willman, "Personality and domain ‐ specific risk taking," *Journal of Risk Research*, vol. 8, no. 2, pp. 157-176, 2005/03/01 2005, doi: 10.1080/1366987032000123856.

[23] E. U. Weber and R. A. Milliman, "Perceived Risk Attitudes: Relating Risk Perception to Risky Choice," *Management Science*, vol. 43, no. 2, pp. 123-144, 1997, doi: 10.1287/mnsc.43.2.123.

[24] J. Shropshire, M. Warkentin, and S. Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Computers & Security*, vol. 49, pp. 177-191, 2015/03/01/ 2015, doi: https://doi.org/10.1016/j.cose.2015.01.002.

[25] J. Shropshire, M. Warkentin, A. Johnston, and M. Schmidt, "Personality and IT security: An application of the five-factor model," *AMCIS 2006 Proceedings*, p. 415, 2006. [Online]. Available: https://aisel.aisnet.org/amcis2006/415.

[26] L. Cheng, Y. Li, W. Li, E. Holm, and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Computers & Security*, vol. 39, pp. 447-459, 2013/11/01/ 2013, doi: https://doi.org/10.1016/j.cose.2013.09.009.

[27] C. Warrington, J. Syed, and R. Tappin, "Personality and Employees' Information Security Behavior among Generational Cohorts," *Computer and Information Science*, vol. 14, p. 26, 01/01 2021, doi: 10.5539/cis.v14n1p26.

[28] A. S. Wilner, "Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation," *International Journal*, vol. 73, no. 2, pp. 308-316, 2018, doi: 10.1177/0020702018782496.

[29] F. B. Fatokun, S. Hamid, A. Norman, and J. O. Fatokun, "The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities," *Journal of Physics: Conference Series*, vol. 1339, no. 1, p. 012098, 2019/12/01 2019, doi: 10.1088/1742-6596/1339/1/012098.

[30] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Computers & Security*, vol. 73, pp. 345-358, 2018/03/01/ 2018, doi: https://doi.org/10.1016/j.cose.2017.11.015.

[31] M. Whitty, J. Doodson, S. Creese, and D. Hodges, "Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords," *Cyberpsychology, Behavior, and Social Networking*, vol. 18, no. 1, pp. 3-7, 2015, doi: 10.1089/cyber.2014.0179.

[32] J. McCumber, *Assessing and Managing Security Risk in IT Systems: A Structured Methodology*, New York: Auerbach Publications, 2004, p. 288. [Online]. Available: https://doi.org/10.1201/9780203490426.

[33] A. Erceg, "Information security," *Tehnički glasnik*, vol. 13, no. 2, pp. 123-128, 2019, doi: 10.31803/tg-20180717222848.

[34] J. L. Spears and H. Barki, "User Participation in Information Systems Security Risk Management," *MIS Quarterly*, vol. 34, no. 3, pp. 503-522, 2010, doi: 10.2307/25750689.

[35] A. AlHogail, "Design and validation of information security culture framework," *Computers in Human Behavior*, vol. 49, pp. 567-575, 2015/08/01/ 2015, doi: https://doi.org/10.1016/j.chb.2015.03.054.

[36] H. R. Peikari and B. Banazdeh, "The relationship between information security awareness and the intention to violate information security with the mediating role of individual norms and self-control," (in fa), *Security & Social Order Strategic Studies*, vol. 7, no. 4, pp. 41-58, 2019, doi: 10.22108/ssoss.2019.108446.1174.

[37] S. R. Kessler, S. Pindek, G. Kleinman, S. A. Andel, and P. E. Spector, "Information security climate and the assessment of information security risk among healthcare employees," *Health Informatics Journal*, vol. 26, no. 1, pp. 461-473, 2020, doi: 10.1177/1460458219832048.

[38] J. Uffen, N. Kaemmerer, and M. H. Breitner, "Personality Traits and Cognitive Determinants—An Empirical Investigation of the Use of Smartphone Security Measures," *Journal of Information Security*, vol. 04, no. 04, pp. 203-212, 2013, doi: 10.4236/jis.2013.44023.

[39] B. W. Roberts and D. Mroczek, "Personality Trait Change in Adulthood," *Current Directions in Psychological Science*, vol. 17, no. 1, pp. 31-35, 2008, doi: 10.1111/j.1467-8721.2008.00543.x.

[40] R. R. McCrae and P. T. Costa, Jr., "Personality trait structure as a human universal," *American Psychologist*, vol. 52, no. 5, pp. 509-516, 1997, doi: https://psycnet.apa.org/doi/10.1037/0003-066X.52.5.509.

[41] J. D. Russell, C. F. Weems, I. Ahmed, and G. G. Richard Iii, "Self-reported secure and insecure cyber behaviour: factor structure and associations with personality factors," *Journal of Cyber Security Technology*, vol. 1, no. 3-4, pp. 163-174, 2017/10/01 2017, doi: 10.1080/23742917.2017.1345271.

[42] M. Pattinson, C. Jerram, K. Parsons, A. McCormac, and M. Butavicius, "Why do some people manage phishing e‐mails better than others?," *Information Management & Computer Security*, vol. 20, no. 1, pp. 18-28, 2012, doi: 10.1108/09685221211219173.

[43] F. Morales-Vives, P. J. Ferrando, A. Vigil-Colet, and A. Hernández-Dorado, "Which profile of people tends to ignore preventive measures against COVID-19? The role of intelligence and the big five personality traits," *Heliyon*, vol. 9, no. 2, 2023, doi: 10.1016/j.heliyon.2023.e13277.

[44] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973-993, 2014/08/01/ 2014, doi: https://doi.org/10.1016/j.jcss.2014.02.005.

[45] P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Computers in Human Behavior*, vol. 75, pp. 547-559, 2017/10/01/ 2017, doi: https://doi.org/10.1016/j.chb.2017.05.038.

[46] H. Chen and Y. Yuan, "The impact of ignorance and bias on information security protection motivation: a case of e-waste handling," *Internet Research*, vol. 33, no. 6, pp. 2244-2275, 2023, doi: 10.1108/INTR-04-2022-0238.

[47] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Information & Management*, vol. 49, no. 3, pp. 190-198, 2012/05/01/ 2012, doi: https://doi.org/10.1016/j.im.2012.04.002.

[48] S. Egelman, L. F. Cranor, and J. Hong, "You've been warned: an empirical study of the effectiveness of web browser phishing warnings," presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Florence, Italy, 2008. [Online]. Available: https://doi.org/10.1145/1357054.1357219.

[49] M. Alohali, N. Clarke, F. Li, and S. Furnell, "Identifying and predicting the factors affecting end-users' risk-taking behavior," *Information & Computer Security*, vol. 26, no. 3, pp. 306-326, 2018, doi: 10.1108/ICS-03-2018-0037.

[50] S. Kumar and I. Chong, "Correlation Analysis to Identify the Effective Data in Machine Learning: Prediction of Depressive Disorder and Emotion States," *International Journal of Environmental Research and Public Health*, vol. 15, no. 12, p. 2907, 2018. [Online]. Available: https://www.mdpi.com/1660-4601/15/12/2907.

[51] K. Kira and L. A. Rendell, "The feature selection problem: traditional methods and a new algorithm," presented at the Proceedings of the tenth national conference on Artificial intelligence, San Jose, California, 1992.

January Febro Naga is a doctoral candidate in Information Technology at De La Salle University-Manila. In addition to her rigorous academic pursuits, January is a faculty member at the Mindanao State University - Iligan Institute of Technology (MSU-IIT). Her research interest encompasses a unique intersection of information systems, social computing, cybersecurity, and health informatics.

Mia Amor C. Tinam-isan is an educator affiliated with the MSU-IIT, where she has served in the Information Technology Department within the College of Computer Studies for the past six years. With a desire for fostering knowledge and innovation, Mia has contributed to the academic community by teaching courses such as Database Systems, Software Engineering, and Data Security. Her research expertise spans critical domains in Information and Communication Technology for Development (ICT4D), Cybersecurity, and Data Mining. Mia Amor C. Tinam-isan has demonstrated her commitment to advancing technology and knowledge within and beyond her institution.

Melody O. Maluya is currently pursuing a Master's Degree in Computer Applications at the MSU-IIT. With aspirations to make significant contributions to the field, Melody continually seeks opportunities to enhance her expertise and make a meaningful impact.

Tanya Ardoña is a proud alumna of MSU-IIT, where she graduated Cum Laude with a Bachelor of Science degree in Information Technology, Class of 2022. A perfect blend of intellect and athleticism, Tanya excelled academically and showcased her prowess in sports, earning her the esteemed Athletics Awardee title. Tanya was recognized as a TES Scholar during her time at MSU-IIT as a testament to her dedication and hard work. Tanya possesses a strong passion for technology, which positions her to achieve significant progress in the IT field, demonstrating the core principles of a comprehensive education.

Kaye Antonnette D. Panal is a distinguished Information Technology graduate recognized for her academic achievements and dedication to harnessing technology for social impact. Kaye consistently showcased her aptitude for innovative problem-solving and software development during her academic journey.