International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Sep-24)

http://dx.doi.org/10.12785/ijcds/160191

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] and Ma. Tanya A. Tupac [1]

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

Received 12 Mar. 2024, Revised 24 May 2024, Accepted 26 May 2024, Published 7 Sep. 2024

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 rapid advancement of information technology (IT) has undeniably transformed various sectors, including academics, government, and private enterprises. However, this progress also presents significant challenges, notably in information security. Cyberattacks targeting organizations have escalated, exposing them to increased risks Wiley, McCormac, and Calic [1]. A primary vulnerability in organizational landscapes arises from human error, often due to noncompliance or insufficient awareness, which has become a prominent cause of security breaches, surpassing even malicious intentions [2, 3]. Despite the extensive implementation of technical solutions, these alone are inadequate to mitigate such vulnerabilities effectively. The human element often represents the weakest link in information security, emphasizing the necessity for enhanced engagement and awareness [4, 5]. Surprisingly, organizations frequently overlook the crucial role of human factors in their security strategies. Alarmingly, human error is implicated in approximately 95% of security breaches, highlighting the urgent need for proactive and preventive measures [6]. 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 [7]. 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. This study delves into the intersection of personality traits and information security awareness, a crucial yet underexplored dimension. Leveraging the Big Five Inventory (BFI) model, we examine how distinct personality dimensions—openness, conscientiousness, extraversion, agreeableness, and neuroticism—correlate with information security behaviors among IT users [8]. Applying the Knowledge-Attitude-Behavior (KAB) paradigm further aids in understanding how personality traits influ-

E-mail address: january.febro@g.msuiit.edu.ph, miaamor.catindig@g.msuiit.edu.ph

ence individuals' attitudes, augment their knowledge, and ultimately affect their security behaviors. This exploration is vital for developing tailored interventions that enhance information security awareness and resilience. The primary contributions of this study are threefold:

1) **Empirical Analysis:** Through quantitative methods, we identify significant correlations between the Big Five personality traits and various components of information security awareness among undergraduate students.
2) **Theoretical Insights:** We enrich the existing literature by integrating personality psychology with information security practices, offering a nuanced understanding of how individual differences shape security behaviors.
3) **Practical Implications:** Our findings inform the development of targeted cybersecurity awareness programs that consider personality profiles, enhancing the effectiveness of these initiatives in promoting secure behaviors.

As we progress, the paper will present a conceptual framework in Section 2 and a literature review in Section 3. The methodology is detailed in Section 4, findings are discussed in Section 5, and the implications of these findings are explored in Section 6. Section 7 concludes with a summary of the study, its limitations, and directions for future research.

2. CONCEPTUAL FRAMEWORK

A. KAB Model

Introduced by Kruger and Kearney [9], the Knowledge-Attitude-Behavior (KAB) framework measures information security awareness, grounded in the interconnected components of affect, behavior, and cognition [10, 11]. This model elucidates how knowledge influences behaviors, mediated by attitudes—suggesting that enhanced knowledge fosters more positive attitudes, which in turn promote better security practices [3]. This framework is instrumental in explaining cybersecurity awareness and behaviors across diverse settings [3, 12, 13]. The KAB framework is a comprehensive tool for understanding the interplay between IT service usage, security knowledge, and security practices. It underscores the importance of: 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

Personality significantly influences individual behavior through distinct traits [14]. The Big Five Inventory (BFI) encapsulates key dimensions—openness, conscientiousness, extraversion, agreeableness, and neuroticism—that predict user behavior across various domains [8, 15]. For instance, high extraversion and openness are associated with increased risk-taking behaviors, while high agreeableness and conscientiousness typically reduce such risks. The application of personality assessment to predict user behavior in cybersecurity contexts has gained notable traction, providing insights into how traits influence information processing and vulnerability to security threats like phishing [15, 16].

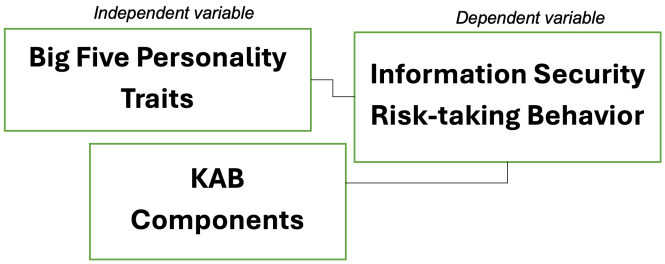

Figure 1. Conceptual Framework

Figure 1 presents our conceptual model that integrates the KAB and BFI frameworks, illustrating how individual knowledge and attitudes towards information security, shaped by personality traits, impact security behaviors. This study hypothesizes significant correlations between the Big Five personality traits and information security risk-taking behaviors within the KAB framework.

3. LITERATURE REVIEW

A. Information Security

Information security, often synonymous with cybersecurity, involves safeguarding personal and corporate data assets against unauthorized access and threats [5, 17]. This field is pivotal for maintaining the confidentiality, integrity, and availability of information, which is essential for the smooth operation of any organization. The literature often uses the terms "information security" and "cybersecurity" interchangeably, a practice we will continue in this study [5, 18]. Wilner [19] argues that "information security" more accurately describes the protection of data, a stance supported by the current academic discourse.

B. Information Security and Human Behavior

Integrating human behavior into information security practices has become increasingly recognized as crucial. Establishing an Information Security Policy (ISP) is vital, but its effectiveness significantly depends on the human factors at play within an organization [20]. Studies indicate that noncompliance with security measures, ranging from casual neglect to intentional sabotage, is a significant contributor to security breaches [21, 22]. The evolving research on technology acceptance and behavior science theories, such as the Big Five Inventory (BFI), underscores the importance of understanding and predicting security behaviors among employees [18, 23].

C. Personality Traits and Information Security

The relationship between personality traits and information security behaviors has garnered increasing attention in cybersecurity research. The Big Five personality traits—neuroticism, extraversion, openness, agreeableness, and conscientiousness—offer valuable insights into predicting and understanding the behavioral patterns that affect security practices. Each trait contributes uniquely to how individuals perceive and interact with cybersecurity protocols.

1) Neuroticism: Characterized by emotional instability and anxiety, neuroticism has been variably linked to information security behaviors. Russell et al. [24] observed an inverse correlation between neuroticism and secure cyber behaviors, indicating that individuals with higher levels of neuroticism might engage in less effective cybersecurity practices. This relationship suggests that neuroticism could impair the ability to consistently follow security protocols, possibly due to heightened stress and anxiety levels that distract from vigilant security practices.
2) Extraversion: Extraverts are known for their sociability and assertiveness, which could influence their attitudes towards cybersecurity. According to Pattinson et al. [25], extroverts may exhibit a more proactive approach to security due to their assertive communication and willingness to engage with security measures. However, their sociable nature might also expose them to greater risks, such as oversharing information on social media, potentially compromising security.
3) Openness: Openness involves a high level of curiosity and creativity, leading to enthusiasm for exploring new technologies and security measures. Morales-Vives et al. [26] found that intelligence, mediated by openness, significantly influences compliance with preventive security measures. Individuals high in openness are likely to embrace and understand the benefits of new security technologies, contributing positively to organizational security.
4) Agreeableness: Agreeable individuals are cooperative, kind, and trusting—traits that generally promote compliance with organizational policies. Shropshire, Warkentin, and Sharma [27] noted that agreeableness correlates positively with the intent to adopt security measures. However, the trusting nature of agreeable individuals may also make them vulnerable to social engineering attacks, as they are more likely to trust others and could be deceived by phishing attempts.
5) Conscientiousness: This trait is marked by a high degree of diligence, organization, and responsibility. Conscientious individuals are likely to adhere strictly to security protocols. Frauenstein and Flowerday [16] observed that conscientious individuals are less susceptible to social networking site (SNS) phishing attacks due to their methodical and cautious approach to processing information and disciplined adherence to security practices. By examining these personality traits, our study aims to provide deeper insights into how individual differences influence cybersecurity behavior. This nuanced understanding will aid in designing more effective information security strategies tailored to diverse personality profiles, enhancing overall organizational security.

D. Unique Aspects of Information Security Risk-taking

Several unique factors influence information security risk-taking behavior:

1) *Digital Environment*:The rapid evolution of cyber threats requires dynamic and adaptable security strategies to mitigate risks effectively [28].
2) *Anonymity and Psychological Distance*: The often anonymous nature of cyber threats can diminish the perceived immediacy and severity of these risks, affecting individual behavior in security practices [29].
3) *Cognitive Biases*: Common cognitive biases, such as the illusion of invulnerability, can lead individuals to underestimate their likelihood of being targeted by cyberattacks [30].
4) *Adaptability to Changing Threats:* The continual evolution of cyber threats necessitates that information security measures be flexible and responsive to new challenges [31].

The literature review thus provides a comprehensive framework for understanding the multifaceted relationship between human behavior, personality traits, and effective information security practices. This review sets the stage for this study's contribution, which aims to bridge the gaps identified in previous research, offering insights into developing more nuanced and effective security strategies tailored to individual behavioral profiles.

E. Developments in Information Security Awareness Research

Recent studies on information security awareness have shed light on the critical roles of attitude, knowledge, and individual and intervention factors in shaping information security behaviors. For instance, Susanto and Maulana

[32] emphasized the dominance of attitude over knowledge in predicting secure behaviors among local government employees, pointing out the effectiveness of training interventions. This aligns with Setiawan and Rizal's [33] findings that post-pandemic, there is a heightened need for targeted educational reforms to boost information security awareness among college students [33]. However, these studies, including Fatoki, Shen, and Mora-Monge [34], focus less on exploring the underlying psychological mechanisms, like optimism bias, that significantly impact security behavior [34]. Additionally, Butavicius, Taib, and Han [35] and Witsenboer, Sijtsma, and Scheele [36] offered valuable insights into phishing detection and cyber security behaviors among students, respectively, but their research often lacks a longitudinal perspective necessary to observe changes in time [35, 36]. Further contributing to this field, AlGhamdi, Win, and Vlahu-Gjorgievska [37] and Solomon et al. [38] provided models to assess and enhance compliance with information security controls and contextual security awareness, respectively, focusing on culturally and contextually sensitive frameworks [37, 38]. Chen and Yuan [30] and [26] explored how ignorance, cognitive biases, and intelligence integration with personality traits influence security behaviors and compliance with preventive measures [26, 30]. Our study extends these discussions using a quantitative modeling approach through Spearman correlation analysis and logistic regression. This enables us to:

- **Predict and Analyze:** By using logistic regression, we can predict information security behaviors based on personality traits and measure the impact of each trait with high accuracy. This nuanced understanding allows for targeted interventions directly informed by empirical data.
- **Capture Temporal Dynamics:** Our modeling approach considers the dynamic interplay between personality traits and security behaviors over time, addressing a significant gap in current research that often overlooks these temporal dynamics.
- **Integrate Personality with Behavior:** Our study offers an integration of personality traits, providing a more comprehensive view of their impact on information security behaviors. We also explore how these traits interact with knowledge and attitude to form a robust information security behavior model, as Susanto and Maulana [32] suggested.

By addressing these aspects, our research enriches the theoretical framework and provides practical insights for developing more effective, personalized information security strategies. This ensures that interventions are not only empirically grounded but also finely tuned to meet the nuanced needs of individuals, thereby enhancing the effectiveness of cybersecurity measures.

4. METHODS

A. Study Demographics and Sampling Method

The research was conducted during the academic year 2020-2021 at Mindanao State University - Iligan Institute of Technology (MSU-IIT), which has a student population of 7,718 undergraduate students. Our participant pool included students from all year levels across seven distinct colleges within the university, ensuring a comprehensive representation of the student body. Stratified random sampling was employed to ensure that each subgroup within the university was adequately represented. This method divided the total population into smaller, more homogeneous groups based on their college affiliation. Participants were randomly selected from each subgroup proportionally to their subgroup's size relative to the total population. This technique helps reduce sampling bias and improves the sample's representativeness. For the purpose of this study, we aimed to achieve a 95% confidence level with a 5% margin of error, appropriate for the population size of 7,718 students. A total of 311 students participated in the survey, which falls within the 10% to 30% range recommended for reliable and valid sampling when the sample elements exceed 20 [39]. This sample size was determined to provide sufficient data for meaningful statistical analysis, aligning with established sampling methodologies. 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.

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

B. Data Collection

Data were collected through an online survey utilizing Google Forms, which included sections to assess participants' Big Five Inventory (BFI) characteristics, security

knowledge, IT service usage, and security practices. The survey was mandatory, and all questions required an answer to ensure completeness. Respondents were instructed to log in using their My.IIT email addresses. This is to ensure that only individuals within the organization are included.

C. Instruments and Measurement Tool

1) **Survey Design and Structure** The study employed a comprehensive self-completion questionnaire to assess the interplay between participants' Big Five Inventory (BFI) characteristics and their information security behaviors. To ensure the integrity of the data, the survey incorporated controlled questions designed as attention checks to validate the authenticity of responses. Participants failing these checks were systematically excluded from further analysis, thereby enhancing the reliability of the data collected.
2) **Anonymity and Ethical Considerations:** Complete anonymity was granted to all respondents to mitigate potential bias and encourage honest responses, particularly when addressing potentially sensitive topics related to security practices. Although participation in the survey was voluntary, once engaged, respondents were required to answer all questions to ensure comprehensive data collection. The survey's introductory page clearly outlined the study's objectives, scope, researcher contact information, and an informed consent form, adhering to ethical research standards.
3) **Survey Sections and Scales:** The questionnaire was divided into five main sections, each designed to capture different dimensions of the participants' profiles and behaviors:
   - **Section A:** Demographic Information - This section collected basic demographic data to facilitate subgroup analyses and to control demographic variables in the analysis.
   - **Section B:** BFI Characteristics - Participants' personality traits were measured using a 5-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree). This scale helped quantify the degree to which participants identified with each Big Five personality trait.
   - **Section C:** Security Knowledge - This section assessed participants' awareness and understanding of information security concepts using a 5-point Likert scale from 1 (very low) to 5 (very high). This scale evaluated the depth of knowledge that participants held about information security practices.
   - **Section D:** IT Service Usage - IT service usage was measured on a 5-point frequency scale from 1 (never) to 5 (always), gauging how frequently participants engaged with various IT services, which are potential vectors for security threats.
   - **Section E:** Security Practices - Participants' actual security behaviors were evaluated using a 5-point frequency scale, ranging from 1 (never) to 5 (always), to understand their practical engagement with security measures.
4) **Reliability and Validity of the Instrument:** The validity and reliability of the survey instrument were rigorously tested. An adaptation of the reliability assessment methodology by Alohali et al. [40], focusing on the internal consistency of the survey sections. The Cronbach's alpha values for each section exceeded the accepted threshold of 0.7, indicating a high level of internal consistency. Table 2 in the study documentation presents these results, affirming the survey's capability to yield reliable and consistent data across various constructs measured.

TABLE II. Summary of Components

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

D. Data Analysis Techniques

Spearman's correlation: Our study utilized Spearman correlation analysis, a non-parametric method, to explore the relationships between various ranked variables. This method was chosen because it does not require the assumption of normal distribution and is ideal for ordinal data, such as the 5-point Likert scale used in our survey. Spearman's correlation coefficient (or rs) quantifies the strength and direction of a monotonic relationship between two variables. Values range from -1 (perfect negative correlation) to +1 (perfect positive correlation), with 0 indicating no correlation [41]. We conducted the Spearman correlation analysis using Orange software, which facilitated evaluating the relationships within the data. This analysis helped to identify whether variables related to personality traits and information security behaviors had positive, negative, or no correlations, and the strength of these correlations was categorized as weak (rs within 0.1 - 0.3), moderate (rs within 0.3 - 0.5), or strong (rs within 0.5 – 1.0). The assumptions for Spearman's correlation, such as the requirement for the data to be at least ordinal and the relationship between variables to be monotonic, were carefully considered and met in this study, ensuring the validity of the results.

Logistic Regression Modeling: Logistic regression was implemented to delve deeper into how BF characteristics predict the risk status of end-users regarding information security. This statistical technique allowed us to explore the probabilities associated with the various categories of the dependent variable (risk status) based on the independent variables (BFI characteristics). Before applying logistic regression, we conducted feature selection using

the Relief-Based Feature Selection (RBFS) method. RBFS is particularly effective in identifying the most relevant features by measuring the quality of attributes based on how well their values distinguish between instances that are near to each other [42]. This step enhanced our logistic regression model's predictive accuracy and computational efficiency. Figure 2 illustrates our modeling workflow.

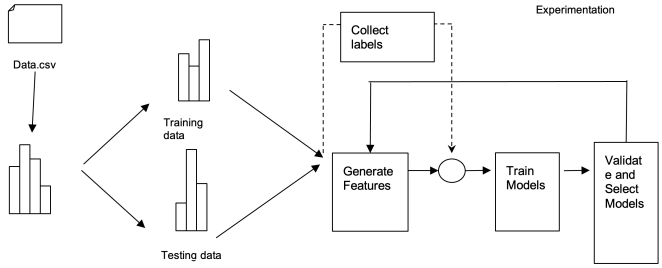

Figure 2. Modeling Workflow

We then transformed all categorical data into a numerical format to facilitate the logistic regression analysis, ensuring all input data fit the technique. The logistic regression process was structured around a 10-fold cross-validation method to maximize the reliability and generalizability of our findings. This approach minimized overfitting by testing the model across multiple subsets of the data, thus providing a robust assessment of its predictive power.

E. Tools and Software for Data Analysis

In our study, we employed Orange Data Mining Software and Python to handle our data analysis needs, each selected for their strengths in statistical analysis, visualization, and model building. Orange Data Mining Software, an open-source platform with a user-friendly graphical interface, was particularly useful for quick visualizations and preliminary analyses, employing widgets that simplified the process of exploring data relationships through Spearman correlation and other statistical methods. This allowed us to easily interpret and understand our data without deep coding. Python, known for its extensive libraries and community support, provided the depth required for more rigorous statistical tasks and model building. We utilized Python for detailed statistical analysis, logistic regression modeling, and data preparation tasks using libraries like SciPy, Statsmodels, and Pandas. This included implementing feature selection techniques such as Relief-Based Feature Selection (RBFS) and validating our models through 10-fold cross-validation to ensure their robustness and accuracy. Combining Orange's capacity for quick data handling and visualization with Python's advanced analytical capabilities allowed for a thorough exploration and evaluation of the data. This dual-tool approach was crucial for efficiently covering all phases of our analysis, from data preparation to complex model evaluation, ensuring comprehensive insights into the relationships between personality traits and information security behaviors.

5. RESULTS

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

1) *Security Knowledge* TThe 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 Resuts

Terms	Very Low	Low	Average	High	Very High
Knowledge of Information Security-Related Terms					
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 high-

light 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. Performance Frequency of 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 unknown resources	3.22	3.86	15.11	20.26	55.56
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

Security Practices	Never (%)	Rarely (%)	Sometimes (%)	Often (%)	Always (%)
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 6. 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. Correlation Coefficients for BFI Notation and Meaning

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
Conscientiousness vs. Lack of Direction	A3: Does a thorough job	-0.146
	A8*: Can be somewhat careless	+0.018
	A13: Is a reliable worker	-0.123
	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."

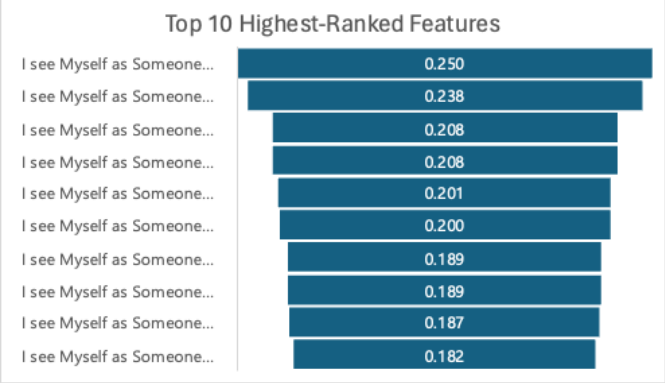

Figure 3. Top-10 Best Ranked Features

This study employed logistic regression to predict individuals' risk status based on Big Five Personality Traits, achieving 85.7The 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. Discussions

The survey result highlights significant disparities in understanding 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 and is instrumental in shaping secure behaviors, including adopting advanced security practices. The survey also reveals significant engagement with essential IT services such as email, social media, and search engines, integral to daily activities, thus underscoring the need for secure usage protocols. The observed variability in behaviors related to online streaming and banking services suggests a need for security practices tailored to these specific activities. This diversity in usage patterns highlights how habitual engagement with IT services shapes attitudes and behaviors within the Knowledge-Attitude-Behavior (KAB) framework, emphasizing the need for targeted educational and behavioral interventions. Participants' security practices, including 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 suggests reinforcing positive behaviors through increased knowledge can cultivate a robust information security culture. Moreover, the study explores the intricate correlation between Big Five Inventory (BFI) traits—such as openness, conscientiousness, extraversion, agreeableness, and neuroticism—and information security risk-taking behaviors. By employing the KAB model, we find significant correlations where traits like Agreeableness and Conscientiousness are associated with a decreased risk status. In contrast, characteristics such as Neuroticism and a tendency toward a lack of focus correlate with higher risk statuses. This nuanced understanding is crucial for developing more efficient and tailored information security methods. Drawing on prior research, our findings align with the significant roles of conscientiousness, agreeableness, and openness in shaping cybersecurity behaviors, as noted in studies by Shappie et al. [14] and Alohali et al. [40]. Using Spearman correlation analysis and logistic regression, our study not only confirms the impact of these traits on cybersecurity risk behaviors but also highlights the predictive power of these models, achieving an 85.7% classification accuracy in assessing the influence of traits like Neuroticism, Lack of Direction, Antagonism, Extraversion, and Introversion on cybersecu-

rity risks. The interaction between the Big Five Personality Traits and the Knowledge-Attitude-Behavior framework within the context of information security demonstrates how individual personality qualities fundamentally impact one's approach to information security, influencing knowledge, attitudes, and behaviors. For instance, traits such as openness and conscientiousness significantly enhance an individual's understanding and awareness, while agreeableness fosters positive perceptions and approaches to cybersecurity practices. Conversely, neuroticism, marked by anxiety and worry, can negatively affect attitudes, leading to apprehension or poor decision-making in cybersecurity contexts. The implications of this study are significant for the development of cybersecurity interventions. By highlighting the necessity of integrating personality traits into cybersecurity strategies, the research suggests that organizations can substantially enhance the effectiveness of their security measures. Tailored educational programs that consider long-term impacts, and the psychological profiles of users can bridge the gap between human psychology and cybersecurity decision-making. This approach allows for the customization of training programs that account for individual differences in stress response, attention to detail, and cooperation, thereby improving the practicality and efficacy of cybersecurity measures and creating a more secure and responsive cybersecurity environment.

A. Limitations and Future Research Directions

The study provides valuable insights into the relationship between personality traits and information security behaviors; however, several limitations must be considered. Firstly, using a predominantly student population may restrict the generalizability of the findings to other professional or age groups where information security behaviors could significantly differ. Moreover, reliance on self-reported measures could introduce biases, as participants may not accurately report their security practices or risk behaviors. For future research, several paths can be pursued to address these limitations and expand the understanding of this field. Including a broader demographic in future studies could enhance the external validity of the findings to provide insights applicable across different contexts. Implementing longitudinal studies would allow for the examination of how personality traits and information security behaviors evolve over time or in response to interventions to offer a more dynamic perspective on these interactions. Furthermore, integrating qualitative methods would enrich the dataset and provide deeper insights into the cognitive and emotional factors that drive security behaviors. This approach would allow for a more nuanced understanding of the interactions between personality traits and security practices. It could help identify new variables or relationships not evident through quantitative methods alone. Additionally, exploring cultural factors and assessing the effectiveness of tailored interventions could deepen our understanding of cybersecurity, leading to the development of more customized, effective strategies. Developing adaptive security measures that respond to individual personality traits could also lead to more effective, user-focused cybersecurity strategies. These directions promise to refine theoretical frameworks and offer practical insights for enhancing information security measures. this culture.

7. CONCLUSION

The study's findings emphasize the crucial role of individual personality traits in shaping effective information security strategies. Organizations can develop more personalized and impactful interventions by aligning information security measures with the psychological profiles of users. This research highlights how BFI traits influence information security behaviors, advocating for a personalized approach to enhance cybersecurity practices. Such targeted initiatives not only encourage responsible IT service usage but also contribute significantly to the promotion of robust cybersecurity environments.

Acknowledgment

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

References

[1] A. Wiley, A. McCormac, and D. Calic. More than the individual: Examining the relationship between culture and information security awareness. *Computers & Security*, 88:101640, 2020.

[2] A. McCormac, T. Zwaans, K. Parsons, D. Calic, M. Butavicius, and M. Pattinson. Individual differences and information security awareness. *Computers in Human Behavior*, 69:151–156, 2017.

[3] 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*, 42:165–176, 2014.

[4] 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*, 9(3):e14234, 2023.

[5] R. von Solms and J. van Niekerk. From information security to cyber security. *Computers & Security*, 38:97–102, 2013.

[6] IBM. IBM 2015 Cybersecurity Intelligence Index, 2015.

[7] H. de Bruijn and M. Janssen. Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1):1–7, 2017.

[8] O. P. John and S. Srivastava. The big five trait taxonomy: History, measurement, and theoretical perspectives. In *Handbook of personality: Theory and research*, pages 102–138. Guilford Press, New York, NY, US, 2nd edition, 1999.

[9] H. A. Kruger and W. D. Kearney. A prototype for assessing information security awareness. *Computers & Security*, 25(4):289–296, 2006.

[10] 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*, 6(2):96–103, 1989.

[11] N. J. MacKinnon and J. Hoey. Operationalizing the relation between affect and cognition with the somatic transform. *Emotion Review*, 13(3):245–256, 2021.

[12] P. Nunes, M. Antunes, and C. Silva. Evaluating cybersecurity attitudes and behaviors in portuguese healthcare institutions. *Procedia Computer Science*, 181:173–181, 2021.

[13] 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*, 62(1):82–97, 2022.

[14] A. T. Shappie, C. A. Dawson, and S. M. Debb. Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media*, 9(4):475–480, 2020.

[15] 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*, 139:107603, 2023.

[16] E. D. Frauenstein and S. Flowerday. Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, 94:101862, 2020.

[17] 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*, 39:447–459, 2013.

[18] C. Warrington, J. Syed, and R. Tappin. Personality and employees' information security behavior among generational cohorts. *Computer and Information Science*, 14:26, 2021.

[19] A. S. Wilner. Cybersecurity and its discontents: Artificial intelligence, the internet of things, and digital misinformation. *International Journal*, 73(2):308–316, 2018.

[20] A. AlHogail. Design and validation of information security culture framework. *Computers in Human Behavior*, 49:567–575, 2015.

[21] 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. *Security & Social Order Strategic Studies*, 7(4):41–58, 2019.

[22] 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*, 26(1):461–473, 2020.

[23] 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*, 04(04):203–212, 2013.

[24] 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*, 1(3-4):163–174, 2017.

[25] 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*, 20(1):18–28, 2012.

[26] 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*, 9(2), 2023.

[27] J. Shropshire, M. Warkentin, and S. Sharma. Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49:177–191, 2015.

[28] J. Jang-Jaccard and S. Nepal. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5):973–993, 2014.

[29] 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*, 75:547–559, 2017.

[30] H. Chen and Y. Yuan. The impact of ignorance and bias on information security protection motivation: a case of e-waste handling. *Internet Research*, 33(6):2244–2275, 2023.

[31] Anthony Vance, Mikko Siponen, and Seppo Pahnila. Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3):190–198, 2012.

[32] T. D. Susanto and M. D. Maulana. Evaluating the influence of attitude versus knowledge and individual factor versus intervention factor on information security awareness in local government. *Procedia Computer Science*, 234:1428–1434, 2024.

[33] B. Setiawan and M. A. Rizal. Measurement of information security and privacy awareness in college students after the covid-19 pandemic. *Procedia Computer Science*, 234:1396–1403, 2024.

[34] J. G. Fatoki, Z. Shen, and C. A. Mora-Monge. Optimism amid risk: How non-it employees' beliefs affect cybersecurity behavior. *Computers & Security*, 141:103812, 2024.

[35] M. Butavicius, R. Taib, and S. J. Han. Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, 123:102937, 2022.

[36] J. W. A. Witsenboer, K. Sijtsma, and F. Scheele. Measuring cyber secure behavior of elementary and high school students in the netherlands. *Computers & Education*, 186:104536, 2022.

[37] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska. Employees' intentions toward complying with information security controls in saudi arabia's public organisations. *Government Information Quarterly*, 39(4):101721, 2022.

[38] A. Solomon, M. Michaelshvili, R. Bitton, B. Shapira, L. Rokach, R. Puzis, and A. Shabtai. Contextual security awareness: A context-based approach for assessing the security awareness of users. *Knowledge-Based Systems*, 246:108709, 2022.

[39] O. M. Mugenda and A. G. Mugenda. *Research methods: Quantitative & qualitative apporaches*. Number 2. Acts press Nairobi, 2003.

[40] M. Alohali, N. Clarke, F. Li, and S. Furnell. Identifying and predict-

ing the factors affecting end-users' risk-taking behavior. *Information & Computer Security*, 26(3):306–326, 2018.

[41] 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*, 15(12):2907, 2018.

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

Biographies

January Febro Naga is a Mindanao State University - Iligan Institute of Technology (MSU-IIT) faculty member. Her research interest encompasses information systems, social computing, cybersecurity, and health informatics.

Mia Amor C. Tinam-isan a faculty in MSU-IIT, where she has served in the Information Technology Department within the College of Computer Studies. Mia has contributed to the academic community by teaching courses such as Database Systems, Software Engineering, and Data Security. Her research expertise spans domains in Information and Communication Technology for Development (ICT4D)

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 an alumna of MSU-IIT. Tanya has a strong passion for technology, which positions her to progress significantly in IT, demonstrating the core principles of a comprehensive education.

Kaye Antonnette D. Panal is an Information Technology graduate. Her dedication is to harness technology for social impact.