Journal of Arts, Humanities and Social Science (JAHSS)

ISSN: 3006-9491 (Online)

Volume 2 Issue 3, (2025)

https://doi.org/10.69739/jahss.v2i3.1132

https://journals.stecab.com/jahss

Published by
Stecab Publishing

Research Article

Assessing Information Security Awareness for a Tailored Intervention Program: A Study of Employees at Ifugao State University, Cordillera Administrative Region, Philippines

*[1]Faith Joy A. Pugong

About Article

Article History

Submission: September 21, 2025
Acceptance : October 27, 2025
Publication : November 03, 2025

Keywords

Descriptive Survey, Ifugao State University, Information Security Awareness, Knowledge-Attitude-Behavior Level

About Author

[1] Ifugao State University, Philippines

Contact @ Faith Joy A. Pugong
fateambojnon101@gmail.com

ABSTRACT

Cybersecurity, especially information security, is a shared responsibility. Given that information is vital for any organization, this study was conducted to evaluate information security awareness (ISA) among the employees at Ifugao State University (IFSU) across its six campuses. It employed a quantitative approach, primarily using the descriptive research method. By utilizing a semi-structured questionnaire from the Human Aspects of Information Security Questionnaire (HAIS-Q), data were collected from the five hundred (n=500) employees and analyzed using statistical methods such as ANOVA, post-hoc tests, and independent t-tests. The findings revealed that IFSU employees generally exhibit moderate awareness of information security, with significant age-related differences but no notable differences based on sex or type of employee. Interestingly, both younger and older employees demonstrated inconsistent behaviors despite possessing sufficient knowledge and attitudes. To improve the ISA among IFSU employees, a customized, tailored, age-sensitive intervention program has been proposed.

Citation Style:

Pugong, F. J. A. (2025). Assessing Information Security Awareness for a Tailored Intervention Program: A Study of Employees at Ifugao State University, Cordillera Administrative Region, Philippines. *Journal of Arts, Humanities and Social Science, 2*(3), 143-155. https://doi.org/10.69739/jahss.v2i3.1132

1. INTRODUCTION

Accessing the wide range of information has become convenient recently in the academic landscape due to the abundance of information on the internet, mobile applications, and cloud computing. However, this convenience also brings the constant risk of cybercriminals and hackers compromising this information. Developed countries like the Philippines are increasingly recognizing potential information security risks as they still lack sufficient protection levels (Dacanay *et al.*, 2024; Omorog & Medina, 2017).

Information, the lifeblood of an organization (SHARP, 2017), is linked as an intangible asset for its usage as a strategic resource and a material for decision-making in increasing the organization's value. Securing information encompasses protecting data, information, and equipment from unauthorized parties so that the information resources remain safe from all threats and risks (Paulsen & Byers, 2019). The rounded safety of the setting where the information is located will ensure the integrity, availability, and confidentiality of the organization's information, as it is susceptible to information system security threats, as claimed by (Khando *et al.*, 2021).

Humans are found to be one of the weakest links in attempts to secure systems and networks, as underscored by Haeussinger and Kranz (2017). As cited in their study, Evans *et al.* (2019) stated that the lack of users' information Security Awareness causes many security risks and challenges, highlighting the importance of the human side of information security as an equal to the technical aspect (The Inquirer, 2017). Hence, technological protection can be maximally strong, but information security is only as strong as its weakest link (Kont, 2023).

One of the recognized Universities in the Philippines and even globally, particularly in the Cordillera Administrative Region, is the Ifugao State University (IFSU). Recently, in December 2023, the IFSU official Facebook page was hacked, which took time to recover (IFSU-MIS, 2023). Regarding information security, no literature describes the ISA of students, faculty, and administrative personnel of the said university. Thus, this study will be conducted to assess the level of information security awareness among employees of Ifugao State University in the six (6) campuses, namely: IFSU-Aguinaldo, IFSU-Hapao, IFSU-Lagawe, IFSU-Lamut, IFSU-Potia, and IFSU-Tinoc. Specifically, it is to determine the knowledge, attitude, and behavior level of Ifugao State University employees towards information security in terms of a.) Password Management, b.) Email Use, c.) Internet Use, d.) Social Media Use, e.) Mobile Use, f.) Information Handling, g.) Incident Handling. It also aims to find out if there is a significant difference on the KAB level of Ifugao State University employees towards information security awareness when grouped according to: a.) age, b.) sex, c.) type of employee. Herein, the researcher will ascertain what intervention program can be proposed to enhance the Information Security Awareness of Ifugao State University employees.

The result of this study can guide the administrators and decision-makers of Ifugao State University to craft policies to improve the institution's information security awareness and strengthen information management. This also provides insights and information to the Ifugao State University employees about the necessity of complying with the information security laws and policies. Moreover, this study will serve as a reference for other researchers in assessing the ISA of other educational institutions or organizations.

2. LITERATURE REVIEW

Information system security threats, as mentioned in the study of Mahardika *et al.* (2020), are activities taken both from within and outside systems that maintain the balance of the information system. The heightened threats to information security arise from individuals, organizations, connections, and events not only related from outside of private and public organizations such as opponents or other individuals and groups but can also be used from within the institution visible from the several data reports incidents in the academic landscape (Rahman *et al.*, 2021).

The ThreatDown research (2024) reported a spike in cyberattacks, of which phishing, ransomware, and malware were distinguished as the top cases, grossing 92% in K-12 and 70% in higher education between 2022 and 2023. The result of investigation report associated 92% of attacks as financially motivated across the broader education industry, while 8% are espionage (Verizon's Data Breach, 2023). The series of cyberattacks from well-known higher education globally is switching evidence, hence safeguarding information security is an absolute concern of significant that must be taken seriously by all officials and employees of private and public institutions (U.S. Department of Education, 2024).

Recent studies have shown that most of these occurrences of security incidents pertain to human errors. Puspitaningrum *et al.* (2018) claimed that cyber-attacks were linked to human error related to information security as the result of employees' lack of awareness about information security in the form of opening unsafe websites, inappropriate opening attachments/ links, downloading files without scanning, using simple passwords, careless passwords sharing, losing devices or access to mobile devices, often connecting devices to public networks. Sommestad (2018) emphasized that all employees in an organization are aware of their role and responsibility towards securing the information they work with.

Check Point Cyber Security Report (2022) reported that the number of cyberattacks around the world increased by 38% due to the lack of employee cybersecurity awareness and precautionary behaviors. Employees' behaviors are difficult to control, with the end user often being undertrained or unaware of what security is all about (Pike, 2019). This stresses the need for organizations including HEI to integrate security awareness with organizations' objectives to increase management and employee involvement in averting security incidents by reducing the risk of bad behavior of employees and negative interaction with information resources through the implementation of information security culture, the level of risk to information resources is reduced (Asker & Tamtam, 2020). As highlighted by Pollini *et al.* (2021), understanding the nuances of employee awareness can help in the identification of human errors and further determination of the areas with the largest impact on overall system security. McCombes (2019) contended that a lack of employees' information security awareness through Information Security Policies and procedures was the major cause of the mishandling of sensitive information.

From this view, an employee's Information Security Awareness (ISA) exerts a significant impact on information security behaviors and employees' security policy compliance (Li *et al.*, 2019). As described by Pike (2019), ISA refers to the level of knowledge and understanding of security issues within an organization, along with an awareness of threats and security countermeasures and precautions, ensuring that all employees in an organization are aware of their role and responsibility towards securing the information they work with.

The National Institute of Standards and Technology, as mentioned in the study of Nugraha and his associates (2022), ISA is a condition where the focus is on information security problems. As mentioned in the study of AlMindeel and Martins (2021), it has an impact on changing individuals' perceptions, values, attitudes, behavior, norms, work habits, and organizational culture and structures concerning secure information practices. O'Flaherty (2021) interpreted it as a bulwark of an organization in the face of current information security threats. With these, ISA has become a top priority for senior management in the workplace (Azad *et al.*, 2019), in research and practice (Vaidya, 2022).

It also encompasses an awareness and understanding of security issues, which is a significant determinant of compliant behavior with security measures (Haeussinger & Kranz, 2017). The role of individual behavior in mitigating cyber threats has been given attention (Acuña, 2016). Understanding how individuals differ in their awareness, knowledge, and cybersecurity behaviors when exposed to multiple cyber threats is still quite limited (Zwilling *et al.*, 2020). Ismail *et al.* (2022) pinpointed the presence of the gap between the advancement of technology and how much the employees' awareness of the institutions, private and public, is challenged in preserving their assets. Pike (2019) elaborated that, as security awareness among end users is often overlooked and limited action is posited to increase the security awareness of end users in an information security program.

In the Philippines, Information Security Awareness (ISA) is a growing concern as it involves the protection of online data due to web collaboration (Quisumbing, 2019). Despite the existing cybersecurity laws (RA 8792- Electronic Commerce Act and RA 10173 Data Privacy Act), the Philippines' cybersecurity and data privacy awareness are very low (Philippine Institute for Development Studies, 2021). To higher educational institutions, this would face some risks such as losing intellectual property, and personal information relating to students, staff, or faculty (Senthilkumar & Easwaramoorthly, 2017). Effective information security awareness encompasses an understanding of security procedures and personal responsibilities (Information Systems Audit and Control Association, 2023), which is essential to operational security (Assenza *et al.*, 2020). Therefore, research needed a deliberate measurement of the employee's level of awareness of information security (ENISA, 2019).

De Maggio *et al.* (2019) presented the topic and found a deep connection with 'cultural' perceptions and individual 'conscience' rather than mere 'knowledge' viewing it as an ingrained habit underscores its significant impact on daily activities, they further connected it to aspects such as security measures, training, asset protection, prevention and awareness of vulnerabilities are rarely considered. Eydgahi and Rajab (2019) pointed out that only a small part is related to information security awareness in operational organizations. Earlier studies have used network knowledge, attitude, and practices as a useful measure to determine the effectiveness of problems and activities, verifying it as a communication model to identify the efficiency of programs, especially the effects of the approved public program (Ahmad *et al.*, 2023). This concept is advanced by Krugger, as mentioned in the study of Bognár and Bottyán (2024), introducing a methodical tool for information security awareness assessment which emphasizes the development of a question, manager consultations for importance weightings, practical data integration, and tool automation. The imperative to accurately assess ISA is clear, advocating for the use of detailed, reliable, and context-aware tools that majorly rely on the identified three critical components using the knowledge-attitude-behavior (KAB) in utilizing methods like questionnaires, interviews, and behavior tests (Fertig & Schütz, 2020). This is inclined to the proposed systematic measurement of Rohan *et al.* (2023) on information security and seven focus areas consisting of password management, email use, internet use, social media use, mobile use, information handling, and incident reporting, while three dimensions knowledge consist of knowledge, attitude, and behavior. Research focused on mitigating identity theft risks among youth underscored the importance of effective cybersecurity awareness education (Corradini *et al.*, 2020).

Li *et al.* (2019) boldly revealed the significant impact on information security behaviors and employees' security policy compliance, increasing the need to measure the level of employees' awareness of information security in academic settings. Breaches in schools, colleges, and universities are under constant attack by modern threat actors such as password management, email use, internet use, social media use, mobile use, information handling, and incident reporting, as proposed by Parsons *et al.* (2017).

One of the challenging tasks for most computer users is password management, which has led users to many malpractices that open the door for most information security breaches over time (Fernando *et al.*, 2023). This online account maintenance comes with password management, which consists of strong password creation, mitigation of password reuse, periodic renewal, sharing, and instant availability (Luevanos *et al.*, 2017). Pearman *et al.* (2019) accentuated that an average internet user has to maintain 12 to 26 password-protected accounts, and an average undergraduate has to maintain 8 academic password-protected accounts separately, while the majority of them forget newly created passwords within the first 12 hours. Take the ransomware attack on Howard University, which was blamed on password mishandling in 2021, prompting the faculty and staff to reset their passwords, comply with complex password requirements, and upgrade cloud-based security as protection against further phishing attacks (Ngo, 2021).

A recent experiment found that over a fifth of university faculty and staff clicked on at least one of three simulated phishing emails from either known or unknown senders (Li *et al.*, 2020). Several campus members of the University of Arkansas acknowledged having fallen victim to these attacks, causing their accounts to be compromised (University of Arkansas, 2023). The Philippines, being the 5th among the Southeast Asian countries with the most phishing attacks (IPV Network, 2023), is also vulnerable to phishing and malware attacks with the garnered records of hacked Philippine Health Insurance and Department of Health website, the data breaches by Medusa ransomware exposing records of applicants and employees under multiple state agencies such as Philippine National Police, National Bureau of Investigation, Bureau of Internal Revenue, and the Special Action Force (CYFIRMA, 2023).

Meanwhile, the University of Michigan severed its ties to its internet provider and cut off access to some systems after experiencing a cyberattack linked to internet usage after a careful evaluation of significant security concerns (Greig, 2023). Sarker (2021) emphasized that the disguised cyber threats along the internet use from traditional national security threats, from random downloads of files, access to doubtful websites, and input of information online have caused national security in its traditional sense to be challenged and inefficient in cyberspace. Aside from internet use, mobile devices are becoming a method to provide an efficient and convenient way to access, find, and share information; however, the availability of this information has caused an increase in cyberattacks (Dawson *et al.*, 2016). According to Morgan (2016), mobile apps are often the cause of unintentional data leakage. This is due to a lack of physical security of mobile devices, information sharing via Wi-Fi, and shoulder surfing, providing the opportunity for malicious cyber attackers to hack into various popular mobile devices through malware, adware, and riskware (Shishkova, 2021). The unsecured school-connected devices in Cleveland City Schools in Tennessee caused the ransomware attack affecting the student, faculty, and family data (News Channel 9, 2023).

Another factor networked to information security in information handling referred to the process of data management, including labeling, storage, transfer, deletion, and destruction, while ensuring the protection of proprietary information and compliance with classification schemes (Fenelly & Perry, 2020). Stanford University Department of Public Safety was attacked by an Akira ransomware group that claimed 430GB of private information and confidential university documents (Stanford University, 2024). Likewise, Universities of California, Los Angeles, Missouri, Rutgers, Stanford University's School of Medicine, and New York's Yeshiva University were part of MOVEit file transfer breach through a third-party vendor used in enrollment operations as the students' and employees' social security numbers and financial information were stolen, with some ported online demanding ransom in exchange (Coffey, 2023). Two hundred thirty thousand (230,000) personal records of sensitive, personal information relating to students, alumni, and employees were stolen from the University of Michigan in August (University of Michigan, 2023).

Similarly, the data breach at the University of the East in 2019, wherein unauthorized logs on the server of one of their employees were discovered, data was copied, and used for blackmailing the Dean of the University of the East College of Computer Studies and Systems (National Privacy Commission, 2020). Romblon State University fell victim to a data breach perpetrated by DeathNote Hacker Philippines to expose alleged misconduct by faculty members, of which they managed to steal the personal information of both students and faculty members (Philippine News Agency, 2024). This incident probes the importance of early detection and reporting of cyberattacks (Morgan, 2016).

Incident reporting is essential for today's organizations to understand that when incidents do occur, they must be prepared to respond and then learn from them (Incident Report, 2024). In addition to an increasing number of incidents, many organizations are now dealing with security regulations, higher customer expectations, and new reporting requirements correlated to data privacy and infrastructure resilience despite the limited cybersecurity skills (De Zan, 2019). An initial probe led by the PUP-Information and Communications Technology Office (ICTO) into the hacking of the PUP Student Information System (SIS) showed that no "sensitive" users' information was "compromised" despite some of its students' data being leaked. FEU said it tapped an external cybersecurity provider to assist them with the investigation. Both universities said it has informed the National Privacy Commission (NPC) of the breach in their student portals. In a statement, the PUP-ICTO said they have already determined the extent of the data breach and are now strengthening the information systems' security features. San Beda University also experienced a breach in its student portal when an alleged hacker gained access to its students' data and released it on the social media app Twitter (Manila Bulletin, 2020). Learning from incidents is a vital strategy that can help improve risk awareness, protective measures, and organizational response capability (Connolly and Wall, 2019). Washington Technology Solution (2024) painted a critical role played by an information security awareness program in the overall security posture of the state.

Khando *et al.* (2021) stated Information Security Management System encompasses processes and activities defined by the International Organization for Standardization. Ralph Johnson, State Chief Information Security Officer, as mentioned in their study, highlighted that standardization equips employees with the necessary knowledge and tools to safeguard themselves and the state from digital threats, improving personal security practices beyond the workplace (Vaidya, 2022). He further added that the awareness trains individuals to identify phishing attempts, suspicious activities, and other threats, thereby mitigating the risk of data breaches and cyberattacks. It was supported by the study of Omorog (2020), concluding that Filipinos are susceptible to cyberattacks, because of being derivative-practicing online measures with a limited understanding of the purpose, the proper education through training and awareness is an effective approach to remedy the situation. Strengthening information security awareness is not only an assessment of the level of mindfulness but also the evaluation of the efficiency of safety measures to reduce user errors (Datta & Nwankpa, 2023) and bolster security practices in the academic field (Mai & Tick, 2021).

In the Philippine landscape, the Commission on Higher Education (CHED) and the National Privacy Commission mandate the compliance of Higher Education Institutions with the Data Privacy Act of 2012, known as the Republic Act No. 10173 (Glaspie, 2018). Yet, the study of CHED's Information Systems Strategic Plan revealed that the Information Security policies of the organization are still partially compliant (Cheng, 2021). This is also the result of a case study on the level of compliance with the provisions of Republic Act No. 10173 and the NPC's five pillars of Data Privacy Accountability in Bukidnon State University (Flores & Ching 2018). Further study by the CELIS Institute (2018) exposed some factors, such as lack of awareness, budget, and time constraints, as barriers to the Data Privacy Act. This result is inclined with the discoveries of the Philippines' cybersecurity, affirming that data privacy awareness is very low (Philippine Institute for Development Studies, 2021).

In an interview by the Philippine Daily Inquirer (2023), Vitaly Kamluk- head of the Apac Unit of Kaspersky's Global Research & Analysis Team, emphasizes the fact that Filipino users may fall more easily for such attacks means that their security awareness and maturity are probably not at the right level compared to other countries. This was also stressed by Privacy Commissioner John Henry Naga after the multiple phishing attacks occurred in early 2023, to enhance client education and awareness to prevent similar attacks in the future. According to the Department of Information and Communication Technology (2019), only 44% of Filipinos have heard of cybersecurity and data privacy. This shows that even though the government and educational institutions are trying their best to implement Information Security Awareness among HEIs, there are still several factors that hinder compliance with DPA. Meanwhile, a study on Information Security Awareness conducted by Quisumbing (2019) at the Philippine State University revealed that the students of the University have an adequate level of ISA. However, the awareness level about rules and knowledge-required issues is still low, so the development of an ISA Training program to be conducted is recommended (Hakkala *et al.*, 2018). This is a somewhat similar recommendation that was concluded in the study of the Cagayan State University Academic Community by Escobar (2022), whereby the students need more improve on cybersecurity knowledge through cybersecurity policy. On the other hand, the faculty members and administrative staff must maintain cybersecurity knowledge through continuing professional development on cybercrimes. This proves that HEIs have the responsibility to equip their students and personnel with ISA, enabling them to adapt to the continually evolving cyber threat landscape, including the rise of artificial intelligence; thus, the implementation of ISA among HEIs is the responsibility of institutions to their clients. This characterization encompasses procedural aspects and is suitable for this review, as the researcher explores ISA from an awareness-raising perspective.

3. METHODOLOGY

This study utilized the descriptive method of research. Such a method is appropriate in this study as it highlights the apprehensions, showcasing the prevailing knowledge, attitude, and behavioral patterns of the Ifugao State University employees about information security. Moreover, a quantitative technique was also used in this study. It was linked to the means of data identifying different levels of knowledge, attitude, and behavior with their relevant variable. Also, for determining the significant difference of the KAB level of Ifugao State University employees towards information security awareness when grouped according to age, sex, and type of employee. The data collected through this research method resulted in the determination of the intervention programs to further enhance the training and assessment.

This research was conducted at the Ifugao State University, Cordillera Administrative Region, Philippines. Thus, all of the six (6) campuses namely: IFSU-Aguinaldo, IFSU-Hapao, IFSU-Lagawe, IFSU-Lamut, IFSU-Potia, and IFSU-Tinoc were included as research locale of the study.

The researcher used Slovin’s formula to obtain the study’s sample size for every campus. All in all, five hundred (500) individuals were chosen using random sampling as respondents for this study. The respondents were given equal opportunities to complete the questionnaire as representatives of each campus, irrespective of their sex, age, or type of employee (non-teaching or teaching).

The researcher used a semi-structured questionnaire which is the Human Aspects of Information Security Questionnaire (HAIS-Q). HAIS-Q is a method to evaluate Information Security Awareness within an organization and commonly used with a broad variety of populations, the general public, and employees from government and financial institutions (Parsons *et al.*, 2017). They added that this method has been peer-reviewed several times and was regarded as valid. Its reliability ranges from .844 to .918 Cronbach’s alpha and for internal reliability for each of the seven areas is between .75 and .82, wherein it exceeded the Cronbach’s recommended alpha coefficient which is .70. However, in this study, the questionnaire consists of eighty-four (84) questions having positive and negative values to ensure that the respondent understands the meaning and purpose of the questions. Such 84 questions linked to the seven (7) different focus areas (password management, email use, internet use, social media use, mobile devices, information handling, incident handling) where ISA is generally deemed to come into play within an organization, along with three (3) sub-areas (knowledge, attitude and behavior). To avoid bias, the questionnaire was composed using a four-point Likert Scale. Each question was rated using the 4-point modified Likert scale: strongly disagree, disagree, agree, and strongly agree.

4. RESULTS AND DISCUSSION

4.1. The KAB Level of IFSU Employees about Information Security across Seven Indicators

The KAB Level of IFSU employees about information security awareness across the seven indicators is reflected in Table 1. The mean score was calculated and used to interpret the data. The overall mean scores for knowledge (66.69), attitude (67.84), and behavior (64.77) indicate that employees have a moderate understanding of information security. Across the three levels, the overall mean score of 66.43 (average and need improvement) further highlights inconsistencies between knowledge, attitude, and behavior, which could pose risks to the information security framework.

Table 1. The Knowledge, Attitude, and Behavior Level about Information Security Across the Seven Indicators

Indicator		Knowledge	Attitude	Behavior	Mean	Qualitative Interpretation
1	Password Management	70.4	70.89	66.51	69.27	Average and Need Improvement
2	Email Use	61.36	62.84	61.21	61.80	Average and Need Improvement
3	Internet Use	51.32	68.37	61.32	60.34	Average and Need Improvement
4	Social Media Use	71.67	72.6	64.48	69.58	Average and Need Improvement
5	Mobile Device	72.78	65.7	68.29	68.92	Average and Need Improvement
6	Information Handling	72.24	65.57	65.67	67.83	Average and Need Improvement
7	Incident Reporting	67.04	68.9	65.91	67.28	Average and Need Improvement
	Overall Mean	66.69	67.84	64.77	66.43	Average and Need Improvement

Legend:
80-100 = Good
60-79.99 = Average and Need Improvement
0-59.99 = Poor and Need Direct Action

Under knowledge level, the table shows that the respondents demonstrate highest knowledge level in Mobile Device Security (M=72.24) followed by Social Media Use (M=71.67). This means that they are aware of security risks associated in these areas. On the other hand, Internet Use (M=51.32) and Email Use (M=61.36) shows significantly lower scores. This implies a low level of awareness regarding safe browsing practices and email security threats.

The results of this study displayed a similarity to the study of Hadlington (2017) on the human factors in cybersecurity, examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity. His study found that individuals often have moderate cybersecurity mindfulness, particularly in password management and Internet use, and that many users engage in risky behaviors without strong protective measures. An associated review highlights that social media and mobile device use are areas where users have average security awareness, leading to vulnerabilities. University students showed average knowledge in areas like email use, password management, and incident reporting (Alqahtani & Kavakli-Thorne, 2020). The same with thru with the employees who showed moderate knowledge in password management, email use, and internet use, indicating room for improvement in cybersecurity knowledge (Fadlika *et al.*, 2023).

In terms of attitude, Password Management (M=70.89) and Social Media Use (M=72.60) received the highest scores. This implies that the employees have a high level of awareness, acknowledging the importance of strong passwords and careful social media use. However, Email Use (M=62.84) and Information Handling (M=65.57) scored lower, meaning that the respondents may not fully recognize the risks associated with mishandling emails and sensitive information.

A similar average result is found in the study of Umejiaku *et al.* (2023) uncovered that even when users know password rules, their attitude toward convenience often outweighs security concerns. Users admitted feeling that "strong passwords" were important, but their attitude showed a preference for ease and memorability over security (Wash and Rader, 2021). Attitudes toward email security were found to be casual — users believed phishing was a "distant threat," causing carelessness (Rauf *et al.*, 2023).

Further, while users' express concerns about privacy breaches, their attitude towards actual protective behavior was passive (Sundaram & Shetty, 2022). Despite awareness, the attitude toward mobile device security remained casual, treating phones more like personal items than security-sensitive devices (Alotaibi *et al.*, 2019). Employees' attitude toward data handling was that shortcuts were acceptable if tasks were urgent, risking policy non-compliance (Watchtel, 2023).

In the behavior level, Mobile Device Security (M=68.29) had the highest behavior score, implying that employees are more likely to implement security measures for mobile devices. However, Email Use (M=61.21) and Internet Use (M=61.32) recorded the lowest behavior average. These indicate poor adherence to safe email and web browsing practices.

In line with the aforementioned findings, the research by Giwah *et al.* (2020) revealed that the motivation of mobile device users to protect themselves, along with their confidence in their capabilities, significantly influenced whether they would implement security measures. The study highlighted that people are more inclined to take protective steps, such as activating device locks, updating software, and modifying app permissions, when it comes to the security of their mobile devices. Nevertheless, a survey conducted by Mimecast revealed that nearly 50% of employees in Western countries admitted to opening emails even though they considered them suspicious. This behavior persisted despite their awareness of potential cyber risks and participation in cybersecurity training, highlighting a gap between knowledge and practice (Mimecast Limited, 2020).

Additionally, this insight is supported by Spanning's 2018 Cybersecurity and Risk Awareness Survey, which found that while employees understand fundamental cybersecurity risks, they still partake in hazardous behaviors like downloading unauthorized applications and disregarding safe browsing practices. This indicates a gap between employees' understanding of cybersecurity best practices and their actual actions, jeopardizing organizational security (Spanning, 2018). Similar conclusions were drawn in the National Cybersecurity Alliance and CybSafe's report titled "Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2023." The report highlights that despite acknowledging cybersecurity awareness, digital anxiety and frustration continue to impede better cyber hygiene, and a persistent gap between knowledge and action, particularly in behaviors that protect privacy and sensitive information, remains evident (National Cybersecurity Alliance & CybSafe, 2023).

In summary, the study's findings indicate that employees' knowledge is mostly Average/Moderate across all studies because they only have a basic and/or general understanding of cybersecurity. Their attitude is positive but often passive or careless. They acknowledge the importance of information security, but don't always feel urgent about it due to convenience, ease, and memorability, so they are likely to compromise on risk practices. Consequently, needs for improvement in almost all areas, such as passwords, mobile use, email security, and reporting. This highlights a disconnection between knowledge, attitudes, and behavior. While employees are aware of security risks in areas like mobile devices and social media, it demonstrated gaps in both understanding and adherence to security practices such as email use and internet browsing.

4.2. KAB Level of IFSU Employees towards Information Security Awareness when grouped according to Age

The significant difference between the knowledge, attitude, and behavior of the respondents about information security when grouped by age was tested and analyzed using Analysis of Variance (ANOVA). Results were reflected in Table 2.

Table 2. ANOVA Results for Significant Difference in Respondents' Knowledge, Attitude, and Behavior about Information Security When Grouped by Age

Age	N	Mean	SD	F	P-value	Remark
21-30	231	2.587	.2035	12.74	.000	Reject Ho
31-40	193	2.713	.2404			
41-50	64	2.676	.2178			
Above 50	12	2.646	.1297			

The table shows that the average score for the varied age brackets was as follows: 21-30 had a mean of 2.587 (SD=.2035), 31-40 had a mean score of 2.713 (SD=.2404), 41-50 had a mean score of 2.676 (SD=.2178), and above 50 had a mean score of 2.646 (SD=.1297). These scores reflect slight variation among the age brackets, with 31-40 having the highest mean score.

The result suggests that there is a significant difference in the respondents' knowledge, attitude, and behavior about information security when grouped by their ages (F=12.74, p=.000). This further denotes that the knowledge, attitude, and behavior about information security are influenced by age, reflecting generational differences.

To clarify which age group differs significantly from each other, Post hoc analysis using Turkey HSD test was conducted. The result is shown in Table 3.

Table 3. Post Hoc Analysis Result

Overall Mean			
Tukey B[a,b]			
Age	**N**	**Subset for alpha = 0.05**	
		1	**2**
above 50	12	2.5542	
21-30	231	2.5869	
41-50	64	2.6758	2.6758
31-40	193		2.7131

Means for groups in homogeneous subsets are displayed.
a. Uses Harmonic Mean Sample Size = 36.877.
b. The group sizes are unequal. The harmonic mean of the group sizes is used. Type I error levels are not guaranteed.

A harmonic mean sample of 36.877, because of unequal group size, revealed that the mean scores for the 21-30 and above 50 age brackets did not differ significantly from each other. Similarly, there is no significant difference between the mean scores of the 31-40 and 41-50 age groups. This implies that within these broader age ranges, knowledge, attitude, and behavior about information security are relatively consistent.

These findings corroborate the conclusion of Nguyen and Le (2024) in their study using the Knowledge-Attitude-Behavior Model. They found that due to work experiences and responsibilities, middle-aged employees frequently merge strong attitudes towards security with safe behaviors. Furthermore, users aged 30 to 49 were more adept in information security due to their professional experiences and technology proficiency, thus, this makes them responsive in training and conformant with policy (Sari *et al.*, 2023; Omar *et al.*, 2021). In comparison, younger respondents who are aged 21 to 30 demonstrate a high level of self-confidence yet low consistency in their behavior, while older respondents aged 50 and above exhibited more caution but experienced technical problems in employing best practices (Pacheco, 2024; Nicholson *et al.*, 2023; Alharthi & Alghamdi, 2022).

The Theory of Planned Behavior, that applied in the study of Alanazi and *et al.* (2022), explains further the said findings, which postulates that behavior is motivated by intention, shaped by attitude, subjective norms, and perceived behavioral control. The likelihood of professional responsibilities and experiences that lead to better information security behavior among middle-aged employees indicates that they possess stronger intentions and perceived control. On the other hand, the lack of experience-driven pressure or norm to conform to the security behavior is not yet discerned by the younger users. For older users who still encounter difficulty in digital technology, even though they are well-informed about information security practices, this reduces their behavioral control.

4.3. KAB Level of IFSU Employees towards Information Security Awareness when grouped according to Sex

Table 4 presents the result of an independent samples t-test conducted to examine whether there is a significant difference in respondents' knowledge, attitude, and behavior about information security when grouped by sex. From the table, it can be gleaned that there are 314 females and 186 males. The mean score for the female respondents was 2.6274, while for the male respondents, it was 2.6780. The t-test revealed a t-value of .982, with a p-value of .322.

Table 4. Independent Samples t-Test Results for Significant Difference in Respondents' KAB When Grouped by Sex

	Sex	N	Mean	T (df)	P-value	Remark
KAB	Female	314	2.6274	.982 (498)	.322	Accept Ho
	Male	186	2.6780			

Scrutiny of the data indicates that there is no statistically significant difference in KAB between male and female, as the p-value is above the commonly accepted significance level of 0.05. Thus, the null hypothesis, which suggests no significant difference in KAB between sex, is accepted. This means that sex does not influence their views on information security in this particular context.

The finding is supported by the study of Branley-Bell *et al.* (2022) regarding cybersecurity among the employees of the tech industry. They concluded that in terms of security behavior and awareness levels of cybersecurity, there is no significant difference between females and males. This was seconded in the result of Tran *et al.*'s (2024) investigation of the role of gender in information security attitudes among corporate employees, which reveals that gender did not play a significant role in security. Likewise, this coincides with the empirical study of Mbaka and Tuma (2024), stating that gender has no significant influence on evaluating security decisions, which means males and females enforce similarly towards information security practices and decision-making.

4.4. KAB Level of IFSU Employees towards Information Security Awareness when grouped according to Type of Employee

The result of independent sample t=test presented in Table 5 examines whether there is a significant difference in the respondents' KAB, when grouped by type of employee. There were 254 non-teaching with a mean of 2.7088 and 246 teaching with a mean of 2.5815.

Table 5. Independent Samples t-Test Results for Significant Difference in Respondents' KAB When Grouped by Type of Employee

	Type of Employee	N	Mean	T (df)	P-value	Remark
KAB	Non-Teaching	254	2.7088	2.776 (498)	.096	Accept Ho
	Teaching	246	2.5815			

Examination of the result revealed there is no significant difference (t=2.776, p=.096) between the tested data. This supports the claim that being non-teaching staff or teaching staff does not affect the knowledge, attitude, and behavior about information security. Such a claimed assent by the study in a public university in the Southeastern United States of Yerby and Floyd (2018). They found that although the respondents (faculty and staff) demonstrated high to moderate levels of awareness and security behavior, there was no significant difference in information security awareness between faculty and staff. The KAB model also supports the claim that, concerning information security awareness, job roles or descriptions (teaching or non-teaching) have no significant effects on one's security awareness (Nguyen & Le, 2024). As concurred by the socio-technical systems theory in the study of Zoto *et al.* (2019), it was established that regardless of job position or title in an organization, this does not significantly alter their information security awareness or practices. Rather, the combination of social and technical elements, such as human actors, policies, training, and technology tools, can influence organizational awareness and behavior.

Overall, the knowledge, attitude, and behavior level of the IFSU employees towards information security awareness falls below "average and needs improvement" as interpreted by Kruger's scale. This indicates that the respondents have moderate awareness, which implies that some concepts are understood, but they need to improve their behavior and/or attitude. It recommends training and reinforcement. As validated, partial knowledge of employees is often demonstrated without translating into consistent behavior (Zou *et al.*, 2024). This implies that employees fail to apply their knowledge effectively in their daily tasks because there is no continuous reinforcement and nudges (CultureAI, 2024). Thus, these data confirm that having comprehensive and continuous information security training as an intervention program may enhance the information security knowledge, attitude, and behavior of IFSU employees.

The said intervention program may apply to all IFSU employees across campuses regardless of sex (male and female) and type of employee (teaching and non-teaching). As revealed that sex and job role or title have no significant effects on information security awareness and behavior. It is also established by Jiow *et al.* (2021) that, regardless of gender and job title, they do not influence cybersecurity behavior. Rather, this is shaped by one's psychological disposition and organizational reinforcement (University of Chicago, 2023).

However, the age range can be considered in tailoring the intervention, as shown that younger (21-30) and older (above 50) employees demonstrate low awareness, unlike the middle-aged (31-50) employees who exhibited better information security awareness and behavior. This reflects the study of Asiamah *et al.* (2024) and Busse *et al.* (2023), in which younger employees are subject to risky behavior due to their high self-efficacy, while older employees have low digital technology proficiency. Compared to middle-aged employees, they have an in-depth understanding and consistent behavior towards information security (Omar *et al.*, 2021). Furthermore, a difference in age group is vital in customizing information security interventions (Alshaikh, 2020). Therefore, to enhance the effectiveness and efficiency of an intervention program, it is not only applied universally but may also be tailored to an age group.

5. CONCLUSION

In light of the findings of the study, this research concluded that Ifugao State University employees are aware of security risks on mobile devices and social media, but lack sufficient knowledge of safe browsing and email security. They value strong passwords and social media safety, yet underestimate the threats posed by email, information handling, and online use. While their attitudes toward internet security are generally positive, their limited knowledge and inconsistent practices create vulnerabilities. This gap between knowledge, attitude, and behavior highlights that awareness alone does not ensure secure practices.

Moreover, age influences the KAB of IFSU employees on information security, with those aged 31–40 showing higher levels across all areas. Employees aged 21–30 and 50+ have adequate knowledge and attitude, but inconsistent behavior. In contrast, sex and employee type show no significant differences, indicating that information security awareness is generally consistent across gender and roles but varies by age.

It also recommends to address the gap between knowledge and behavior, the University may consider implementing a comprehensive cybersecurity awareness program across all campuses. Unlike traditional knowledge-based training, this program may adopt a knowledge-attitude-behavior (KAB) approach, incorporating real-world applications, simulations, and hands-on activities. To reinforce learning and accountability, a guideline or policy may be crafted for the conduct of regular training, emphasizing key points and encouraging proactive engagement. This initiative will not only strengthen the university's overall information security posture but also cultivate a stronger, more sustainable cybersecurity culture.

The University may carry out programs and strategies that are tailored to the age-specific needs of employees. For those aged 21–30, training can emphasize building consistent security behaviors through practical scenarios while reinforcing positive digital practices to address their high self-efficacy. Employees aged 31–40 may benefit from training that leverages their prior knowledge and cultivates leadership roles, enabling them to serve as peer leaders or mentors in promoting information security awareness. For employees aged 50 and above, training should focus on technical support and ICT proficiency to strengthen their ability to understand and apply information security practices effectively.

Further, to improve the information security awareness of the employees, the University may consider adopting the proposed intervention program. Also, researchers may consider exploring more topics and other areas related to this topic. A study after five years may also be considered to assess the effectiveness of intervention strategies adopted by the University concerning information security and cybersecurity.

REFERENCES

Ahmad, M., Shari, A. M. J., Razali, R. R., & Sujak, A. F. A. (2023). Knowledge, attitude, and practices towards internet safety and security among Generation Z in Malaysia: A conceptual paper. In S. K. Bhar & H. Rahmat (Eds.), *Proceedings of the International Conference on Communication, Language, Education and Social Sciences (CLESS 2022)* (pp. 4–10). Atlantis Press. https://doi.org/10.2991/978-2-494069-61-9_2

Alanazi, M., Freeman, M., & Tootell, H. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior, 136*, 107376. https://doi.org/10.1016/j.chb.2022.107376

Alharthi, S., & Alghamdi, A. (2022). Exploring the factors that influence the cybersecurity behaviors of young adults. *Computers in Human Behavior, 136*, 107376. https://doi.

org/10.1016/j.chb.2022.107376

AlMindeel, R., & Martins, J. T. (2021). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *Information Technology & People, 34*(2), 770-788.

Alotaibi, S., Alruban, A., Furnell, S., & Clarke, N. (2019). A novel behaviour profiling approach to continuous authentication for mobile applications. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP 2019)* (pp. 246–251). https://doi.org/10.5220/0007313302460251

Alqahtani, H., & Kavakli-Thorne, M. (2020). Exploring factors affecting user's cybersecurity behaviour by using mobile augmented reality app (CybAR). In *Proceedings of the 2020 12th International Conference on Computer and Automation Engineering (ICCAE 2020)* (pp. 129–135). Association for Computing Machinery. https://doi.org/10.1145/3384613.3384629

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security, 98*, 102003. https://doi.org/10.1016/j.cose.2020.102003

Asiamah, N., Bempong, J. A., & Sghaier, M. (2024). Internet self-efficacy moderates the association of information technology ability with successful ageing among older employees in three African samples. *European Journal of Ageing, 21*, Article 31. https://doi.org/10.1007/s10433-024-00827-9

Asker, H., & Tamtam, A. G. (2020). An investigation of the information security awareness and practices among third level education staff: Case study in Nalut, Libya. *European Scientific Journal, 16*(15), 20-32.

Assenza, G., Chittaro, A., De Maggio, M. C., Mastrapasqua, M., & Setola, R. (2020). A review of methods for evaluating security awareness initiatives. *European Journal for Security Research, 5*(2), 259-287.

Safa, N. S., Maple, C., Furnell, S., Azad, M. A., Perera, C., Dabbagh, M., & Sookhak, M. (2019). Deterrence and prevention-based model to mitigate information security insider threats in organisations. *Future Generation Computer Systems, 97*, 587-597.

Bognár, L., & Bottyán, L. (2024). Evaluating online security behavior: Development and validation of a personal cybersecurity awareness scale for university students. *Education Sciences, 14*(6), 588.

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies, 2022*(1), Article 2693080. https://doi.org/10.1155/2022/2693080

Busse, J., Busse, R., & Schumann, M. (2023). *Does technology matter? How digital self-efficacy affects the relationship between ICT exposure and job dissatisfaction* [Manuscript]. University of Göttingen. https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/0c9a24b0-3d43-42ff-b955-9c7471db1b1a/content

CELIS Institute. (2018, July 19). *Data protection privacy policy*

Check Point Cyber Security Report. (2022, May 21). *Check Point Cyber Security Report: Global cyber pandemic's magnitude revealed.* Security Insight.

Cheng, D. (2021). *Applicability of information governance for data privacy compliance in the education sector.* DLSU Research Congress 2021. https://www.dlsu.edu.ph

Coffey, L. (2023). *MOVEit signals growing cybersecurity threats for higher ed. Insiders Report.* https://www.insidehighered.com

Connolly, L. Y., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security, 87*, 101568.

Corradini, I., & Nardelli, E. (2020). Developing digital awareness at school: A fundamental step for cybersecurity education. In *Advances in Human Factors in Cybersecurity.* Springer International Publishing.

CultureAI. (2024). *Time to adapt: The state of human risk management in 2024.*

CYFIRMA. (2023, October 9). *Philippines threat overview.* https://www.cyfirma.com

Dacanay, D. J. B., Quinto, M. S., Parayno, J. F., & Fajutagana, J. (2024). *A comparative study of the Philippines in a global cybersecurity context and its implications on local cybersecurity practices.* ResearchGate. https://www.researchgate.net/publication/380268096

Datta, P. M., & Nwankpa, J. K. (2023). *Remote workers are more aware of cybersecurity risks than in-office employees: New study.* ProQuest. https://www.proquest.com

Dawson, M., Wright, J., & Omar, M. (2015). Mobile devices: The case for cyber security hardened systems. In *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (pp. 8-29). IGI Global Scientific Publishing.

De Maggio, M. C., Mastrapasqua, M., Tesei, M., Chittaro, A., & Setola, R. (2019). How to improve the security awareness in complex organizations. In *International Conference on Applied Human Factors and Ergonomics.* Springer. https://www.researchgate.net

Department of Information and Communication Technology. (2019, September 14). *National ICT Household Survey Summary Report.* https://dict.gov.ph

De Zan, T. (2019). *Mind the gap: The cyber security skills shortage and public policy interventions.* https://www.ctga.ox.ac.uk

ENISA. (2019, May 7). *ENISA threat landscape report 2018: 15 top cyber-threats and trends.* Heraklion: European Network and Information Security Agency (ENISA).

Escobar, D. T. C. (2022). Cybersecurity Knowledge of The Cagayan State University Academic Community: Basis for Cybersecurity Policy. *Journal of Positive School Psychology, 6*(5).

Eydgahi, A., & Rajab, M. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security, 80.*

Fadlika, R., Ruldeviyani, Y., Butarbutar, Z. T., Istiqomah, R. A., & Fariz, A. A. (2023). Employee information security awareness in the power generation sector of PT ABC. *International Journal of Advanced Computer Science and Applications, 14*(4), 594–601.

Fenelly, L., & Perry, M. (2020). *Handbook of loss prevention and crime prevention* (6th ed.). ScienceDirect.

Fernando, W. P. K., Dissanayake, D. A. N. P., Dushmantha, S. G. V. D., Liyanage, D. L. C. P., & Karunatilake, C. (2023). Challenges and opportunities in password management: a review of current solutions. *Sri Lanka Journal of Social Sciences and Humanities, 3*(2).

Fertig, T., & Schütz, A. (2020). About the measuring of information security awareness: A systematic literature review. In *Proceedings of the 53rd Hawaii International Conference on System Sciences.*

Flores, R., & Ching, M. (2018). Philippine SUCs compliance performance on RA 10173: A case study on Bukidnon State University. *ACM International Conference Proceeding Series.* https://www.dlsu.edu.ph

Giwah, A. D., Wang, L., Levy, Y., & Hur, I. (2020). Empirical assessment of mobile device users' information security behavior towards data breach: Leveraging protection motivation theory. *Journal of Intellectual Capital, 21*(2), 215–233. https://doi.org/10.1108/JIC-03-2019-0063

Glaspie, H. (2018). *Assessment of information security culture in higher education* (Electronic thesis No. 6009). University of Central Florida. https://stars.library.ucf.edu

Greig, J. (2023). *University of Michigan severs ties to Internet after cyberattack.* The Record.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346. https://doi.org/ 10.1016/j.heliyon.2017.e00346

Haeussinger, F., & Kranz, J. (2017). Antecedents of employees' information security awareness: Review, synthesis, and directions for future research. *Association for Information Systems Electronic Library.*

Hakkala, A., Isoaho, J., & Virtanen, S. (2018). *Cyber security competence in working life.* https://www.culture.ai/resources/reports/time-to-adapt-the-state-of-human-risk-management-in-2024

IFSU-MIS. (2023, December 29). *Information management.* https://mis.ifsu.edu.ph

Incident Report. (2024, June 8). *What is incident reporting*? https://www.incidentreport.net

Information Systems Audit and Control Association. (2023, October 2). *ISACA's state of cybersecurity 2023 report.*

IPV Network. (2023, August 28). *Riding the digital wave: Cybersecurity realities in the Philippines.*

Al-Shanfari, I., Yassin, W., Tabook, N., Ismail, R., & Ismail, A. (2022). Determinants of information security awareness and behaviour strategies in public sector organizations among employees. *International Journal of Advanced Computer Science and Applications, 13*(8).

Jiow, H. J., Mwagwabi, F., & Low-Lim, A. (2021). Effectiveness of protection motivation theory based: Password hygiene training programme for youth media literacy education. *Journal of Media Literacy Education, 13*(1), 67–78. https://doi.org/10.23860/JMLE-2021-13-1-6

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & security, 106*, 102267.

Kont, K. (2023). Information security awareness of librarians in the Baltic countries: A comparative analysis. *Baltic Journal of Modern Computing, 11*(3), 450–474. https://www.researchgate.net

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13–24.

Li, W., Lee, J., Purl, J., Greitzer, F. L., Yousefi, B., & Laskey, K. B. (2020). Experimental investigation of demographic factors related to phishing susceptibility. *53rd Hawaii International Conference on System Sciences.*

Luevanos, C., Elizarraras, J., Hirschi, K., & Yeh, J. (2017). Analysis on the security and use of password managers. *18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT).*

Mai, P., & Tick, A. (2021). Cyber security awareness and behavior of youth in smartphone usage: A comparative study between university students in Hungary and Vietnam. *Acta Polytechnica Hungarica, 18*, 67–89. https://doi.org/10.12700/APH.18.8.2021.8.4 https://acta.uni-obuda.hu/ Mai_Tick_115.pdf

Manila Bulletin. (2020, June 19). *PUP, FEU probe hacking of* *student portal.*

Mbaka, W., & Tuma, K. (2024). Role of Gender in the Evaluation of Security Decisions. *IEEE Security & Privacy, 22*(2), 38-48. https://networkinstitute.org/2024/01/26/research-spotlight-gender-and-cybersecurity-decisions/

McCombes, S. (2019). *Descriptive research.* Scribbr.

Mimecast Limited. (2020, October 27). Mimecast research: Half of workers admit to opening emails they considered suspicious. *GlobeNewswire.* https://www.globenewswire.com/en/news-release/2020/10/27/2114887/0/en/Mimecast-Research-Half-of-Workers-Admit-to-Opening-Emails-They-Considered-Suspicious.html

Morgan, S. (2016). *Cybersecurity business report.* CSO.

National Cybersecurity Alliance & CybSafe. (2023). *Oh behave! The annual cybersecurity attitudes and behaviors report 2023.* https://staysafeonline.org/online-safety-privacy-basics/oh-behave/

National Privacy Commission. (2020, October 22). CID BN 19 *067 in re University of the East resolution 2020.*

News Channel 9. (2023, August 16). *Cleveland City Schools hit by ransomware attack Tuesday, personal data not affected.*

Ngo, M. (2021). Howard University hit by a ransomware attack. *The New York Times.*

Nguyen, B. H., & Le, H. N. Q. (2024). Investigation on information security awareness based on KAB model: the moderating role of age and education level. *Information & Computer Security, 32*(5), 598-612. https://doi.org/10.1108/ICS-09-2023-0152

Nguyen, T. D., & Le, D. H. (2024). Information security awareness in Vietnamese organizations: A KAB model approach. *Information & Computer Security, 32*(1), 89–110. https://doi.org/10.1108/ICS-09-2023-0152

Nicholson, J., Coventry, L., & Briggs, P. (2023). Cybersecurity personas for older adults. In *Proceedings of the GoodIT '23: ACM International Conference on Information Technology for Social Good* (pp. 1–7). Northumbria University. https://researchportal.northumbria.ac.uk/files/112884337/goodit23_55.pdf

Nugraha, A. C., Hidayanto, A. N., Indriany, H. S., Kurniati, H., Firdaus, B. M., & Bastara, A. (2022). Cybersecurity project implementation for resources protection: A case study of the National Narcotics Board. *IOP Conference Series: Materials Science and Engineering.*

Omar, S. Z., Kovalan, K., & Bolong, J. (2021). Effect of age on information security awareness level among young internet users in Malaysia. *International Journal of Academic Research in Business and Social Sciences, 11*(19), 245–255. https://doi.org/10.6007/IJARBSS/v11-i19/11733

Omorog, C. D., & Medina, R. P. (2017). *Internet security awareness of Filipinos: A survey paper.* arXiv. https://arxiv.org/abs/2012.03669

O'Flaherty, K. (2021). Breaking down five 2018 breaches and what they mean for security in 2019. *Forbes.*

Pacheco, E. (2024). *Older adults' safety and security online: A post-pandemic exploration of attitudes and behaviors.* PhilArchive. https://philarchive.org/archive/PACOAS

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): two further validation studies. *Computers & Security, 66*, 40-51.

Paulsen, C., & Byers, R. (2019). *Glossary of key information security terms* (NIST Special Publication 800-114). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114.pdf

Pearman, S., Zhang, S., Bauer, L., Christin, N., & Cranor, L. (2019). *Why people (don't) use password managers effectively. USENIX Proceedings of the Fifteenth Symposium on Usable Privacy and Security.* Boise State UniversityScholarWorks. https://scholarworks.boisestate.edu/cs_fac_pubs/148/

Philippine Daily Inquirer. (2023, November 3). *Cybersecurity awareness in PH needs improvement.*

Philippine Institute for Development Studies. (2021, August 16). *Did you know that awareness of cybersecurity and data privacy in PH is low?.*

Philippine News Agency. (2024, April 30). *Romblon State University assesses data breach after website hacking.*

Pike, A. (2019). *An evaluation of the information security awareness of university students.* [Unpublished master's thesis].

Pollini, A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). *Leveraging human factors in cybersecurity: An integrated methodological approach. Cognition, Technology and Work.* Springer Nature.

Puspitaningrum, E. A., Devani, F. T., Putri, V. Q., & Hidayanto, A. N. (2018). Measurement of employee information security awareness: Case study at the Directorate General of Resources Management and Postal and Information Technology Equipment Ministry of Communications and Information Technology. *Advances in Science, Technology, and Engineering Systems Journal, 5.* https://www.researchgate.net

Quisumbing, L. (2019). *Preemptive evaluation through information security awareness: Perception of information technology students in a Philippine State University.*

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human factors in cybersecurity: A scoping review. In The *12th International Conference on Advances in Information Technology.*

Rauf, U., Mohsen, F., & Wei, Z. (2023). A taxonomic classification of insider threats: Existing techniques, future directions & recommendations. *Journal of Cyber Security and Mobility, 12*(2), 221–252. https://doi.org/ 10.13052/jcsm2245-1439.1225

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon, 9*(3).

Sari, P. K., Handayani, P. W., & Hidayanto, A. N. (2023). Demographic comparison of information security behavior toward health information system protection: Survey study. *JMIR Formative Research, 7*, e49439. https://doi.org/10.2196/49439

Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. *Internet of Things, 14*, 100393.

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cyber security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering*, 263, 042043.

SHARP. (2017, January 9). *Information security brochure* (18644).

Shishkova, T. (2021). *IT threat evolution in Q3 2021: Mobile statistics.* Securelist.

Sommestad, T. (2018). Work-related groups and information security policy compliance. *Information & Computer Security, 26.*

Spanning. (2018). *Cybersecurity and risk awareness - Spanning report.* https://spanning.com/resources/reports/trends-us-worker-cyber-risk-aversion-threat-preparedness/

Stanford University. (2024, March 11). *Update on Department of Public Safety data security incident.*

Sundaram, R., & Shetty, S. (2022). Privacy concerns and protection behavior during the Covid-19 pandemic. *Problems and Perspectives in Management, 20*(2), 57–70. http://dx.doi.org/10.21511/ppm.20(2).2022.06

The Inquirer. (2017, November 11). *Massive data breach has cost Equifax nearly $90 million.*

ThreatDown. (2024, January 24). 2024 state of ransomware in education: 92% spike in K-12 attacks. *ThreatDown Newsletter.*

Tran, D. V., Nguyen, P. V., Vrontis, D., Nguyen, S. T. N., & Dinh, P. U. (2024). Unraveling influential factors shaping employee cybersecurity behaviors: An empirical investigation of public servants in Vietnam. *Journal of Asia Business Studies, 18*(6), 1445–1464. https://doi.org/10.1108/JABS-01-2024-0058

U.S. Department of Education. (2024, June 3). *Data security: K-12 and higher education.*

Umejiaku, A. P., Dhakal, P., & Sheng, V. S. (2023). Balancing password security and user convenience: Exploring the potential of prompt models for password generation. *Electronics, 12*(10), 2159. https://doi.org/ 10.3390/electronics12102159

University of Arkansas. (2023, November 30). *Phishing emails targeting university accounts.*

University of Chicago. (2023). *Digital studies M.A. and B.A./M.A. (DIGS) student manual 2023–2024.* https://humanities.uchicago.edu/sites/default/files/DIGS%202023-2024%20Handbook_0.pdf

University of Michigan. (2023, August 23). *August 2023 data incident.*

Vaidya, R. (2022). *Cyber security breaches survey 2019.* Department for Digital, Culture, Media and Sport.

Verizon's Data Breach. (2023, January 30). *Data breach investigation report.*

Wachtel, C. (2023). *Industry study 2023: Employees ignore data handling guidelines.* XPLM. https://www.xplm.com/news/press/industry-study-2023-employees-ignore-data-handling-guidelines/

Wash, R., & Rader, E. (2021). Prioritizing security over usability: Strategies for how people choose passwords. *Journal of Cybersecurity, 7*(1), tyab012. https://doi.org/10.1093/cybsec/tyab012

Washington Technology Solutions. (2024, January). *Information security awareness.* Office of Cybersecurity, State of Washington. https://watech.wa.gov/information-security-awareness-january-2024

Yerby, J., & Floyd, K. (2018). Faculty and staff information security awareness and behaviors. *Journal of The Colloquium for Information Systems Security Education, 6*(1), 23. https://cisse.info/journal/index.php/cisse/ article/view/90

Zoto, E., Kianpour, M., Kowalski, S. J., & Lopez-Rojas, E. A. (2019). A socio-technical systems approach to design and support systems thinking in cybersecurity and risk management education. *Complex Systems Informatics and Modeling Quarterly, 18*, 65–75. https://doi.org/ 10.7250/csimq.2019-18.04

Zou, Y., Le, K., Mayer, P., Acquisti, A., Aviv, A. J., & Schaub, F. (2024). Encouraging users to change breached passwords using the protection motivation theory. *ACM Transactions on Computer-Human Interaction, 31*(5), Article 63. https://doi.org/10.1145/3689432

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62*(1), 82-97.