# Factors Influencing Employees' Information Security Behavior in the Telework Environment: An Empirical Study of the Philippines

Jess David A. Doria

*jess_david_doria@dlsl.edu.ph*
*De La Salle Lipa, 1962 J.P. Laurel National Highway, Mataas na Lupa Lipa City 4217, Philippines*

**Abstract**

The advent of teleworking has given rise to unique issues and opportunities within the field of cybersecurity, and employees may not have the acceptable level of awareness, knowledge, and behavior to effectively protect sensitive information and systems while working remotely. This research aims to conduct quantitative research anchored in the theory of planned behavior (TPB) and investigate the factors influencing Filipino teleworkers' intention to engage in secure behavior, primarily in the areas of password management, infrastructure security, email security management, organizational security policy, organizational support and training, and perceptions of security. This study employed multiple linear regression analysis to validate the hypotheses and identify the significant factors that will influence the teleworkers' information security behavior. Results show that not all predictors were perceived as relevant security factors by the respondents, which can potentially lead to security lapses. To enhance employees' information security behavior, this study proposed an integrated, three-pronged collaborative strategy involving both employees and the organization, with mutual accountability. This strategy targets critical areas such as infrastructure security management, organizational security policy, and organizational support and training. By prioritizing these aspects, organizations can effectively bolster security measures and cultivate a culture of heightened security awareness, thus mitigating potential risks.

Keywords: cybersecurity; security behavior; user education; remote work; teleworking; theory of planned behavior

## 1. Introduction

### *1.1. Background of the Study*

The Philippines has consistently been a target of cyberattacks over the past years, ranking 15th most vulnerable globally, according to a 2022 Kaspersky report. According to the National Privacy Commission's 2022 annual report, the archipelago experienced breaches that totaled 224, with human error and malicious attacks as the primary causes. Notwithstanding efforts, the nation receives weak cybersecurity rankings, securing the 61st spot out of 182 countries in the International Telecommunications Union's (2021) Global Cybersecurity Index and the 45th spot out of 164 countries in the National Cybersecurity Index (NCSI). According to Campbell (2023), the Philippines received low scores in global cybersecurity contributions, digital service protection, and safeguarding essential services.

With the COVID-19 pandemic, most companies have allowed some of their workforce to work away from the traditional office and provide flexibility to either work from home or other locations (Wachira, 2021). Almost half (49%) of the workforce in the Philippines is still working in either a hybrid or fully remote

environment, according to a survey by HR Asia conducted in June 2023. The aforementioned number highlights the continued significance of remote employment, even after the pandemic restrictions continue to loosen (Estrellado, 2023). Consequently, there has been a notable change in the preferences and expectations of individuals, with a greater emphasis placed on prioritizing opportunities for remote work rather than returning on-site (Atstaja et al., 2021). In JobStreet's Future of Recruitment Report from 2022, 46% and 28% of the 11,438 Filipino respondents preferred hybrid and remote work, respectively (Monzon, 2023).

Given the rapid transition towards increased remote work opportunities during the pandemic and even post-pandemic, there has been a significant surge in cyberattacks (Atstaja et al., 2021). Cyber-attackers have seen the pandemic as the perfect opportunity to step up their illegal activities by taking advantage of the increased vulnerability of employees who work remotely (Hijji & Alam, 2022). According to Verizon's 2023 Data Breach Investigation Report (DBIR), 83% of all the reported breaches involved external actors, and they took advantage of the general panic to deceive remote workers into giving out data, money, and even access to corporate systems (Galajda, 2023). This stems from a plethora of factors, one of which is the rapid adoption of digital technologies to cater to teleworking. Businesses must either speed up development or outsource tasks to have their systems online in order to continue business operations (Saeed, 2023). Such an undertaking might not be tied to the enhancement of their existing information security programs and policies, such as defining the teleworkers' responsibilities and boundaries while working remotely (Tela et al., 2019; Zhen et al., 2022). The prevalence of teleworking arrangements also enabled the employees' home offices to be an extension of the corporate infrastructure, thereby reducing the capability of organizations to fully secure or monitor the employees' work activities (Simonet & Teufel, 2022).

The widespread adoption of teleworking, coupled with the increased diffusion of digital technologies, has presented new challenges and weaknesses with regards to the protection of data security and privacy (Saeed, 2023). Employees may not have the required level of awareness, knowledge, and behavior to effectively protect sensitive information and systems while working remotely (Simonet & Teufel, 2022). The reason for choosing this research is based on the significant influence of the pandemic on business practices and the increased exposure to security and privacy risks. The advent of remote work has given rise to unique issues and opportunities within the field of cybersecurity (Tela et al., 2019), so understanding the aspects influencing security behavior as one of the main reasons for security breaches when teleworking is the primary motivation for this study. Adopting secure workplace practices is necessary to maintain secure technological usage among employees. When employees are aware of possible security breaches, they utilize computer devices with greater caution, which may lead to a more sustainable usage of technology in the workplace (Saeed, 2023). As such, understanding what factors motivate teleworkers to plan their security behaviors consciously and being aware of security threats is essential for assisting organizations in resolving behavioral issues in information security (Zhen et al., 2022).

### *1.2. Literature Review*

In the evolving landscape of remote work, the need for a comprehensive understanding of the factors influencing employees' information security behavior has become paramount (Simonet & Teufel, 2022). This section aims to explore existing research and scholarly contributions that delve into the intricate dynamics shaping information security practices in the telework environment. A lack of an accurate conceptual definition might undermine the original implications of the theories presented and cause misinterpretations (Zhen et. al., 2022). Thus, the components of this research model are discussed in the following paragraphs.

*1.2.1. Password Management*

Promoting secure usage practices is one of the core elements of protecting organizational assets; one of which is effective password management (Saeed, 2023). With the prevalence of online applications, maintaining passwords has become a challenging task for most computer users, and this has led to a number of human errors that have paved the way for the majority of information security breaches over time (Fernando et al., 2023). Almehmadi and Alsolami (2019) found that the majority of users do not secure their passwords or even require the use of strong passwords, thereby making the work of hackers simpler. The lack of awareness regarding password management increases the probability of cyber-attacks, unauthorized access, and exploitation of devices and services (Bansal, 2023).

*1.2.2. Infrastructure Security Management*

Another factor that needs to be considered in building a robust information security program is the convergence of novel technologies and management trends, which demands a greater emphasis on cybersecurity as the digital landscape evolves (Mandal et al., 2023). This pressing concern has raised the need for a comprehensive approach to safeguarding sensitive data and systems (Khan, 2023), resulting in the development of a wide range of software products that offer a suite of protection technologies. (Chandel et. al., 2019). Implementing a secure infrastructure minimizes the likelihood of system vulnerabilities (Saeed, 2023). However, the significance of the human factor is becoming increasingly apparent, and it is well established that technical solutions alone cannot adequately prevent security breaches (Wiley et al., 2020). Research suggests that it is challenging to implement security controls if employees lack adequate education in effective information technology security practices (Kljunikov, 2019).

*1.2.3. Email Security Management*

As organizations continue to embrace the concept of teleworking, email has become a significant component and is considered to be one of the most commonly used media to communicate, and Altulaihan (2023) discussed how emails have also become a tool for perpetration and other cybercrime operations such as phishing, spoofing, and even disinformation. This necessitates the integration of email security in both personal and business email accounts, and organizations should also adopt a number of steps to improve email security (Chintala et al., 2022). Teleworkers, according to Milhailovic et al. (2021), do not identify the threat of phishing email, the likelihood of infecting their devices with malware, cybercriminals' possible access to private data, and so on. Asker and Tamtam (2023) also claimed that remote users may lack the required understanding about email risks.

*1.2.4. Organizational Security Policy*

Organizational cybersecurity requirements differ depending on their line of business; hence, organizational cybersecurity policies should be tailored to the nature of business and their corresponding security requirements (Saeed, 2023). However, some businesses fail to adopt a telework security plan that outlines teleworkers' standards, boundaries, and duties for preventing and responding to security events, placing enterprises at risk from threats to network security (Simonet & Teufel, 2022). Asfoor et al. (2022) also highlighted that some firms develop policies that are generic and not aligned with organizational requirements. In line with this, it is assumed that sufficient knowledge about an organization’s security

policy influences the information security behavior of a teleworker. Employees fail to comply due to complicated information security standards, thereby contributing to their stress and anxiety toward security.

### *1.2.5. Organizational Support and Training*

In addition to policy development, fostering a knowledge-sharing culture among employees, in addition to training, can also strengthen organizational resilience against security risks (Saeed, 2023). Information security awareness has been established as a critical component in information security, with the promotion of awareness for information security being recognized as a crucial part in protecting an organization from potential threats (Grassegger & Nedbal, 2021). According to Adjei Nyarko and Fong (2023), while most firms have procedures in place to ensure good cyber security compliance for their teleworkers, more than half of their respondents are either unaware or lack the necessary training to comply. Security tactics directed at the general population should emphasize increasing information and understanding rather than instilling fear (Simonet & Teufel, 2022). Gundu (2019) highlighted that formulating security policies does not imply employees' immediate understanding and compliance, as some might either be unaware or lack the proper comprehension.

### *1.2.6. Perception of Security*

The introduction of teleworking and firms' priority toward digital transformation have introduced shifts in firms' and employees' perceptions towards security (Milhailovic et al., 2021). Sulaiman et al. (2022) argued that individuals' perceptions of cybersecurity and data privacy challenges are impacted by their prior experiences, and the low barriers they thought were influenced by their prior experiences. Zhen et al. (2022) also highlighted that as employees understand the implications of information security threats, their attitude toward information security changes. In the study of Turner et al. (2020), employees trust their employers' cybersecurity protocols, but they also feel they are susceptible and that the protocols are not as dependable as compared to on-site working arrangements.

### *1.2.7. Theory of Planned Behavior in Security Research*

Recent studies in information security have employed the theory of planned behavior as a theoretical lens through which researchers can understand the security behavior of users. According to Almansoori et. al. (2023), while there is no single theory that encompasses the entirety of a user's security behavior, TPB is one of the prominent theories that can aid researchers in determining the factors affecting the information security behavior of an individual. Gundu (2019) proposed and designed a cybersecurity motivation/reinforcement model anchored on both the Theory of Planned Behavior (TPB) and Deterrence Theory (DT), which helped with advancing the improvement of knowledge into positive cybersecurity practices among South African employees. Results revealed that despite having high awareness levels, employees' initial attitudes toward cybersecurity compliance were detrimental. However, there was a 24% rise in actual cybersecurity behaviors after the implementation of cybersecurity awareness campaigns and deterrent measures, showing a decrease in policy infractions. Kim and Mou (2020) also used TPB, employed structural equation modeling, and highlighted that the TPB constructs have a strong influence on the user's information security behavior. Grassegger and Nedbal (2021) also employed TPB to investigate organizational and individual characteristics that influence employee information security awareness and how this affects their ability to perceive social engineering attacks.

### *1.2.8. Global Information Security Behavior Studies*

Simonet & Teufel (2022) explored how organizational, social, and personal factors affect cybersecurity awareness and home cybersecurity behavior. Protection Motivation Theory (PMT), which underpins this Swiss study, states that risk and effectiveness affect an individual's willingness to take preventive action. Results showed that both organizational and social factors had a strong positive influence on cybersecurity awareness and behavior. Personal factors, on the other hand, did not have any significant influence. Zhen et al. (2022) used knowledge-attitude-behavior (KAB) and knowledge inertia theory to examine Chinese remote workers' information security behavior. Results showed that KAB variables and learning inertia affected teleworkers' information security awareness. Mihailovic et al. (2021) examined teleworking's cybersecurity effects in Montenegro during and after the COVID-19 outbreak. The authors measured an organization's readiness using Georgiadou, Mouzakitis, and Askounis's (2021) cyber security culture framework, emphasizing the human component. This paradigm included two levels, organizational and individual, each with multiple dimensions and domains with defined application areas and quantitative indicators. Teleworking has no meaningful effect on digital information security but does improve organizational efficiency perceptions. Teleworking has been increasingly popular during the epidemic, but it has also increased the potential of cyberattacks, thus organizations should adopt teleworking rules. Tanriverdi & Metin (2021) used Leach's model to study employees' information security behavior during pandemic-related remote work. The model considered intrinsic and external factors like user psychology, personal beliefs, decision-making abilities, and security procedures or policies. The study also highlighted the importance of upgrading the profession's information security knowledge approach and teleworkers' awareness and behavior.

## *1.3. Research Framework*

Understanding human behavior has become a significant factor for organizations implementing cybersecurity policies and procedures with the aim of securing their domain against vulnerabilities and incidents (Almansoori et al., 2023). Security behavior can be defined and evaluated using two constructs: actual behavior and behavior intention (Tanriverdi & Metin, 2021). To provide a holistic context of the security behavior of users, previous research studies used different theories, one of the most widely used being the Theory of Planned Behavior (TPB) (Gundu, 2019; Tanrivedi & Metin, 2021) as shown in Fig 1.

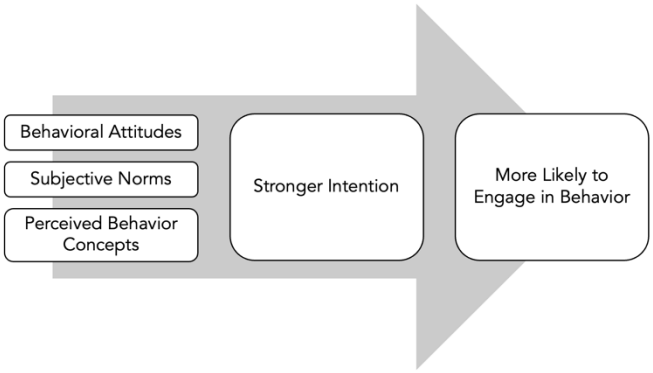


Fig 1. Theory of Planned Behavior

TPB states that an individual will have a stronger intention and a higher likelihood of engaging in the desired behavior if they perceive the activity to be engaging and beneficial, receive support from their social group, and believe they have the knowledge and capacity to do so (Saeed, 2023). According to this theory, behavioral attitudes, subjective norms, and perceived behavior concepts are the three motivational factors that influence intention, which is what drives a behavior.

This paper is anchored on Saeed's 2023 research entitled "Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia". In the context of his study, different factors such as password management, infrastructure security, and email security management, coupled with the organizational security policy, training, and support, and their perceptions towards security, can result in a stronger intention towards secure behavior, which would increase their likelihood of observing secure behavior when interacting with the digital infrastructure. The identified factors were treated as independent variables and aligned according to their corresponding TPB constructs. Saeed's study aimed to determine the level of influence of these factors on the teleworker's intention to engage in secure behavior. Results have shown that not all of the constructs were considered to be relevant security factors by the Saudi Arabian respondents. In addition to Saeed's research serving as the foundation for the independent variables in the conceptual framework, information security behavior as the dependent variable was informed by a complementary study. Zhen et. al. (2022) explored the factors influencing the information security awareness of full-time employees in China who are working in a teleworking environment. The dependent variable, which is information security awareness, reflected the employees' understanding and consciousness of information security practices while teleworking.

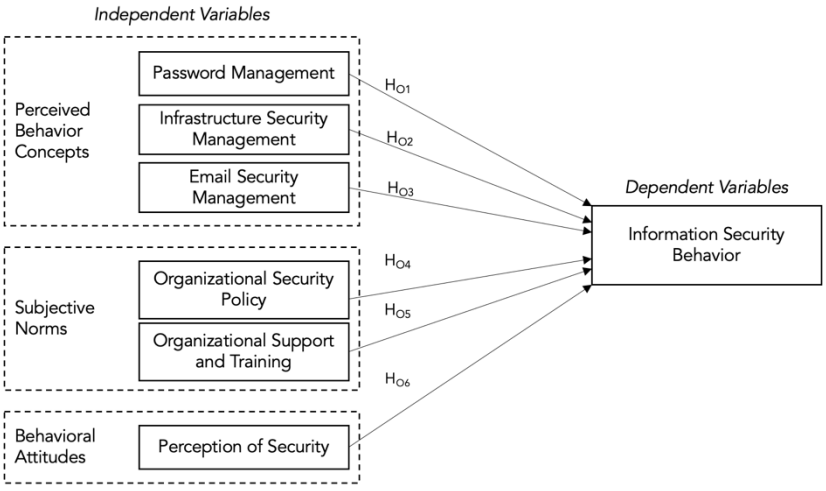


Fig 2. Operational Framework

The operational framework of this research, as shown in Fig 2, delineates the relationships between independent and dependent variables, establishing practical guidance for evaluating the factors that influence the behavior of Filipino teleworkers towards information security. The security factors, represented as independent variables, are aligned with their respective elements of the Theory of Planned Behavior (TPB). Perceived Behavior Concepts were measured in terms of password management, infrastructure security management, and email security management. Further, Subjective Norms were evaluated in terms of

organizational security policy and organization support and training. And lastly, Behavioral Attitudes were assessed in terms of perception of security.

### *1.4. Significance of the Study*

Cybersecurity in the Philippines has been the subject of numerous studies, but information security behavior in the area of teleworking has not received the same level of attention. This study assisted the researcher in ascertaining how Filipino teleworkers view the aforementioned constructs and offered solid pieces of evidence to demonstrate their level of information security behavior. Exhibiting a relationship with the theory of planned behavior and the identified study constructs on security provided a better understanding of how information security behavior is being influenced. With teleworking becoming part of the new normal, cybersecurity becomes paramount as organizations formulate security protocols to maintain the confidentiality, integrity, and availability of their assets (Haque, 2023). This study aimed to contribute to the existing body of knowledge, drawing out the factors distinct to teleworking and uncovering how organizations can address the risks related to such settings. Findings from this research can also assist organizations in formulating effective information security programs, policies, and guidelines for their teleworkers, contributing to a robust information security and risk management practice.

In addition to guiding corporate practices, the findings of the research have the potential to significantly impact the development of cybersecurity strategies and policies at the national level. The findings of this study could help policymakers create frameworks that handle the distinctive challenges presented by teleworking as the Philippines transitions to digital transformation motivated by teleworking trends. The study's local emphasis guarantees that the findings are relevant to the Philippines' particular socio-cultural setting, laying the groundwork for context-specific approaches and guidelines. This research contributes to the broader discussion on cybersecurity resilience and policy creation in the modern digital era by diving into the complexities of information security behavior in the telework setting.

### *1.5. Hypotheses*

The rapid popularity of teleworking raises ongoing concerns regarding the sufficiency of its technological foundations, workforce competencies, and remote office cybersecurity elements (Milhailovic et al., 2021). While there have been previous investigation initiatives, as stated in the preceding sections, no study has examined teleworkers' information security behavior in the context of the Philippines. The business sector's rapid digital transformation necessitates that personnel demonstrate secure behavior in order to protect the technological infrastructure of the organization. Consequently, the researcher employed TPB as a theoretical lens to comprehend the information security behavior of teleworkers in the Philippines. Listed below are the hypotheses for this research.

- Ho1: Password management does not significantly influence information security behavior.
- Ho2: Infrastructure security management does not significantly influence information security behavior.
- Ho3: Email security management does not significantly influence information security behavior.
- Ho4: Organizational security policy does not significantly influence information security behavior.
- Ho5: Organizational support and training do not significantly influence information security behavior.
- Ho6: Perception of security does not significantly influence information security behavior.

## 2. Methods

### *2.1. Research Design*

This cross-sectional study used a descriptive, causal research design in determining the objectives of the study and collected quantitative data by administering an online questionnaire,. It adopted a causal research design to explore relationships among variables, focusing on security factors' influence on teleworkers' security behavior (Karjalainen et al., 2019; Goh et al., 2022). Integrating both descriptive and causal elements enhanced the study's capacity to understand how security factors affect teleworkers' information security behavior. This study focused on information security behavior among Filipino teleworkers within the organizational context of the Philippines. It targeted employees engaged in non-security roles, particularly in full-remote and hybrid work, and currently employed in firms located in developed regions like the NCR and CALABARZON. The snowball sampling technique was employed to gather a diverse pool of respondents beyond the researcher's initial network. The research utilized an instrument adapted from Saeed's study, administered through Google Forms, and employed Likert scales for responses. Data analysis was conducted using multiple regression to test the influence of the chosen predictors on information security behavior concurrently. Ethical considerations included informed consent, confidentiality, and transparent research practices.

### *2.2. Respondents of the Study*

This study focused on Filipinos who currently engage in non-security-related roles and under teleworking arrangements, specifically in full-remote and hybrid work settings, spanning various companies in the private sector that have adopted this form of working arrangement. According to Generalao (2021), highly "teleworkable" firms are mostly situated in developed regions like the National Capital Region (NCR) and Region 4A (CALABARZON), with a weighted average of 33.89% and 25.97%, respectively. Consequently, this study specifically focused on private companies situated in the aforementioned regions. The employer's main headquarters may be situated anywhere on the globe, without any restrictions, regardless of its affiliation with a global or local firm. This holds true as long as the company has established operations and is officially registered in the Philippines. Meanwhile, the respondents faced no restrictions on their place of residence or the location from which they conducted their remote work. However, their job function must not be directly aligned with information security and must require the use of computing devices. This study required 146 respondents to obtain a 95% confidence level.

### *2.3. Sampling Design*

The researcher employed the snowball sampling technique (Parker et al., 2019; Zickar et al., 2023), wherein the researcher requested their initial network of respondents to have the questionnaire filled out by their contacts who meet the eligibility criteria. This method is chosen for its potential to create a ripple effect, expanding the pool of respondents beyond the researcher's immediate network. As early participants completed the survey, they were advised to further recommend and distribute the questionnaire among their own professional connections, fostering a chain reaction of survey participation. This iterative process not only increased the sample size but also promoted diversity in the study's respondent base, capturing insights from a broader range of organizational settings and perspectives in the context of the Philippines.

### *2.4. Research Tools and Instruments*

The study used the instrument adapted from the study of Saeed (2023) and was administered through Google Forms. Table 1 enumerates the research factors and their corresponding numbers of questions. The researcher used the questionnaire from Saeed's study (2023), which employed existing available questionnaires, was tailored to be aligned with the research variables, and peer reviewed by subject matter experts for content validity. The questions for information security behavior, which is the dependent variable, are lifted from the study of Zhen et. al., (2022), which focused on the factors influencing the information security awareness of employees working remotely in China.

Table 1. Breakdown of research factors

| Type of Variable | TPB Constructs | Research Factors | Number of Questions |
|---|---|---|---|
| Independent Variable | Perceived Behavioral Concepts | Password Management | 6 |
| | | Infrastructure Security Management | 8 |
| | | Email Security Management | 4 |
| | Subjective Norms | Organizational Security Policy | 5 |
| | | Organizational Support and Training | 3 |
| | Behavioral Attitudes | Perception of Security | 6 |
| Dependent Variable | - | Information Security Behavior | 4 |

To ensure that the respondents are qualified to participate in the study, the survey questionnaire included a participant eligibility questionnaire. The questions were designed to identify respondents who meet specific criteria, ensuring the relevance and accuracy of the collected data for the research objectives. If any of the questions were not satisfied, the respondent was prompted to terminate the questionnaire. The respondent's demographic profile, such as age, gender, and type of industry, was presented as classifiers and did not influence both independent and dependent variables, as it only aided the researcher in classifying the respondents.

Due to the change of locale, the researcher retested the instrument for reliability prior to the actual data gathering. The reliability test examined the consistency of people's responses to different questions on a multiple-item scale. The researcher gathered 30 respondents outside the locale of the study, which is outside NCR and CALABARZON but still within the Philippines. Cronbach's alpha was used to assess consistency in the reliability test.

Table 2. Reliability test results

| Variable | Number of Items | Cronbach Alpha (α) | Interpretation |
|---|---|---|---|
| Password Management | 6 | 0.855 | Highly Reliable |
| Infrastructure Security Management | 8 | 0.914 | Highly Reliable |
| Email Security Management | 4 | 0.870 | Highly Reliable |
| Perceived Behavior Concepts | 18 | 0.914 | Highly Reliable |
| Organizational Security Policy | 5 | 0.818 | Highly Reliable |
| Organizational Support and Training | 3 | 0.887 | Highly Reliable |
| Subjective Norms | 8 | 0.877 | Highly Reliable |
| Perception of Security | 6 | 0.823 | Highly Reliable |
| Behavioral Attitudes | 6 | 0.823 | Highly Reliable |
| Information Security Behavior | 4 | 0.929 | Highly Reliable |

As shown in Table 2, the Cronbach's alpha coefficients for all variables exceed 0.70, indicating a high level of internal consistency within the research instrument. This suggests that each variable assessed in the study demonstrates sufficient reliability, and all questions utilized in this research are deemed suitable for future investigations. The robust reliability of the research instrument enhances the credibility and validity of the study findings, providing assurance that the data collected accurately represents the variables under study.

### *2.5. Data Analysis and Interpretation*

All measures used a 4-point Likert scale, and the data gathered were analyzed statistically in order to interpret the mean scores of both the independent and dependent variables as presented in Table 3.

Table 3. Qualitative Interpretation of 4-Point Likert Scale Measurements (Pimentel, 2019)

| Likert Scale | Mean Range | Adjectival Rating | Verbal Interpretation |
|---|---|---|---|
| 4 | 3.28 – 4.00 | Strongly Agree | Very High Level |
| 3 | 2.52 – 3.27 | Agree | High Level |
| 2 | 1.76 – 2.51 | Disagree | Low Level |
| 1 | 1.00 – 1.75 | Strongly Disagree | Very Low Level |

The researcher used multiple linear regression to validate the hypotheses and identify the significant factors that influenced the teleworkers' information security behavior. Multiple linear regression was selected as the analytical framework to understand how changes in the independent variables are associated with changes in the dependent variable. The coefficients, standard errors, p-values, and confidence intervals of the predictor variables were examined to determine their individual significance in explaining the variance in the dependent variable. The interpretation of results involved identifying significant predictors and understanding their impact on information security behavior, considering both the direction and magnitude of their effects. The p-values of all the predictors were utilized as the basis for approving or rejecting the hypotheses.

### *2.6. Ethical Considerations*

The study follows the ethical standards outlined for research involving human data subjects. Informed consent was sought from all participants, emphasizing voluntary engagement and the right to withdraw without consequences. Confidentiality measures were strictly upheld, with all collected data anonymized and stored securely. The study is committed to transparent research practices, providing clear information about the research objectives, potential risks, and the responsible use of findings. The researcher understood that the security programs developed by organizations are highly confidential; thus, the study refrained from soliciting or collecting additional information beyond the scope and purpose of this research.

## 3. Results and Discussion

The instrument gathered a total of 210 respondents, but due to the participant eligibility questions, only 146 responses were considered valid and relevant to the study. The data collected was analyzed using Statistical Package for the Social Sciences (SPSS). The analysis included both descriptive and multiple linear regression to find out what factors influence Filipino teleworkers' information security behavior.

### *3.1. Demographic Information*

The descriptives for this study revealed several key demographic characteristics of the sample population. Regarding gender distribution, the majority of respondents identified as male (52.1%), while females accounted for 47.9% of the sample. There are slight variations observed for the age range of participants, with the majority falling within the 26–33 age range (40.4%), followed by those aged 34–41 (22.6%), and teleworkers aged 50 and up being the least represented. Furthermore, participants represented a diverse range of industries, with the largest proportions working in computer and information technology (19.2%) and healthcare and insurance (14.4%).

### *3.2. Descriptive Statistics*

Results revealed that for perceived behavior concepts, only infrastructure security management falls under Very High Level, with a composite mean score of 3.30. The very high level of infrastructure security management can be attributed to teleworkers' awareness that anti-virus software is installed on their work laptops/computers and is regularly updated. As for subjective norms, both variables have a Very High Level of interpretation, with organizational support and training garnering the highest composite mean score of 3.41, followed by organizational security policy at 3.36. The very high level of organizational support and training can be attributed to the ease of access in terms of helpdesk support when teleworkers experience IT-related issues. Whereas the very high level of organizational security policy can be linked to the teleworkers' awareness of the existence of an information security policy in their respective organization. Perception of security, under behavioral attitudes, also falls under Very High Level, with a composite mean score of 3.31. It can be attributed to teleworkers' recognition of the importance of paying attention to computer security. And lastly, information security behavior, as the dependent variable, falls under Very High Level, with a composite mean score of 3.31. It can be attributed to teleworkers' overall awareness of the potential security threats within their working environment and their negative consequences in the event of a security incident or data breach.

Table 4. Descriptive statistics of research variables

| Research Factors | Composite Mean | Std. Deviation | Interpretation |
|---|---|---|---|
| Password Management | 3.2146 | 0.5156 | High |
| Infrastructure Security Management | 3.2979 | 0.5410 | Very High |
| Email Security Management | 3.2603 | 0.5708 | High |
| Organizational Security Policy | 3.3589 | 0.5443 | Very High |
| Organizational Support and Training | 3.4064 | 0.5995 | Very High |
| Perception of Security | 3.3071 | 0.5604 | Very High |
| Information Security Behavior | 3.3065 | 0.6171 | Very High |

### *3.3. Regression Analysis*

The coefficient of determination is an indicator of how well the independent variable in the model can explain the variation of the dependent variable (Alqahtani, 2022). Based on Table 5, a coefficient of correlation (R) of 0.865 signifies that there is strong positive linear relationship between the dependent variable and one or more of the independent variables. The coefficient of determination (R2) of 0.748 suggests that the variance in the independent variables taken as a whole, accounts for about 74.8% of the variance in the dependent variable.

The results indicate that the set of independent variables together have a significant influence on the dependent variable, explaining a substantial portion of its variability in a linear manner.

Table 5. Coefficient of correlation and determination

| Model | R | $R^2$ | Adjusted $R^2$ | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.865 | 0.748 | 0.738 | 0.31611 |

a. Predictors: (Constant), Password Management, Infrastructure Security Management, Email Security Management, Organizational Security Policy, Organizational Support and Training, `Perception of Security

The F-test shown in Table 6 below determines if all of the independent variables have a simultaneous influence on the dependent variable.

Table 6. ANOVA results

| | Model | Sum of Squares | df | Mean Square | F | Sig (p-value) |
|---|---|---|---|---|---|---|
| 1 | Regression | 41.331 | 6 | 6.889 | 0.31611 | 0.000 |
| | Residual | 13.890 | 139 | .100 | | |
| | Total | 55.221 | 145 | | | |

A high F-value of 68.935 suggests that the regression model is statistically significant, indicating that at least one of the independent variables has a significant effect on the dependent variable. Meanwhile, the p-value of 0.000 suggests that the model is significant and that the predictors have a significant influence on information security behavior when used together.

Multiple linear regression analysis was used in this research to analyze the relationship between the independent variables (password management, infrastructure security management, email security management, organizational security policy, organizational support and training, and perception of security) and the dependent variable (information security behavior) (Calonico et. al., 2019). The results of the multiple regression test of the model, shown in Table 7, explained 74.8% of the variance. This proved that the six (6) predictors in the standard model are significantly predictive of information security behavior with ANOVA statistics [F (6, 139) = 68.935, p = 0.000].

Table 7. Multiple linear regression table

| Model | Unstandardized Coefficients | | Standardized Coefficients | t | p-value |
|---|---|---|---|---|---|
| | B | Std. Error | Beta | | |
| (Constant) | -0.441 | 0.196 | | -2.250 | 0.026 |
| Password Management | 0.041 | 0.071 | 0.034 | 0.580 | 0.563 |
| Infrastructure Security Management | 0.445 | 0.079 | 0.390 | 5.619 | 0.000 |
| Email Security Management | 0.073 | 0.070 | 0.068 | 1.041 | 0.300 |
| Organizational Security Policy | 0.224 | 0.086 | 0.197 | 2.594 | 0.010 |
| Organizational Support and Training | 0.166 | 0.066 | 0.161 | 2.510 | 0.013 |
| Perception of Security | 0.180 | 0.092 | 0.163 | 1.954 | 0.053 |

a. Dependent Variable: Information Security Behavior
b. R=0.865; R2=0.748; F=68.935; Sig (p-value) = 0.000

### *3.3.1. Password Management*

Password management, with a p-value of 0.563 shown in Table 7, does not necessarily contribute to information security behavior. Some earlier studies indicate that passwords induce anxiety in users and make it challenging for them to keep track of their passwords (Kovačević et. al., 2020). Datt and Tewari's study in 2021 also revealed that most users are unaware of the value of using strong passwords; users often find it challenging to remember such complex passwords. As a result, they resort to various coping strategies to avoid forgetting or resetting them, such as creating passwords that are easily associated with their accounts as a way to assist their memory (Umejiaku et. al., 2023). Ray et. al.'s (2020) study on password managers revealed that users lacked faith in cloud-based password managers and wanted greater control over their passwords. As a result, users resort to reusing passwords on multiple accounts (Kovačević et. al., 2020) or create easy-to-guess passwords primarily composed of their personal data and common words or strings (Hitaj et. al., 2019).

### *3.3.2. Infrastructure Security Management*

Infrastructure security management was the only variable in the perceived behavior concepts that had a positive and significant effect on information security behavior, with a regression coefficient (β) of 0.39 and a p-value of 0.000, as shown in Table 7. The positive influence indicated that if the perception of infrastructure security management teleworkers increases by 1, information security behavior will improve by 39%. This study consistently supports the suggested influence of infrastructure security management and supports the findings of other earlier studies, such as Mandal et al. (2023), on the significance of a user's awareness of the various security technologies and tools available and administered within their workstations. Humans, as the weakest link in cybersecurity (Atstaja et al., 2021; Wu et al., 2021), pose a serious risk to the cybersecurity posture of an organization. Because teleworkers are aware of their company's IT infrastructure, they exhibit more information security-conscious behavior, which lowers the likelihood of human-induced cybersecurity incidents (Mandal et. al., 2023). Zhu et. al. (2021) also demonstrated that the reduction of security infections is tied to a user's increased security behavior.

### *3.3.3. Email Security Management*

Email security management also did not significantly influence information security behavior, with a p-value of 0.3 depicted in Table 7. This can be justified by the study of Kovačević et. al. (2020), wherein

although users demonstrated a certain level of knowledge on insecure systems and technologies, they lack awareness when it comes to using emails. Most users are not aware of the dangers of phishing emails, malware infections, and cybercriminals gaining access to sensitive information (Milhailovic et al., 2021). Such results are also supported by the study of Asker and Tamtam (2023), wherein they observed that users have a low level of understanding of what an email scam is and how to spot it, due to the fact that users are averse to email application threats.

### *3.3.4. Organizational Security Policy*

Organizational security policy yielded a positive and significant influence on information security behavior, with a regression coefficient (β) of 0.197 and a p-value of 0.01 shown in Table 8. It implies that the respondents are well aware of the existence of security policies within their respective organizations, including their responsibilities and obligations as end-users and infractions for non-compliance. The positive influence indicated that if normative beliefs combined with the motivation to comply with the organizational security policy of teleworkers increase by 1, information security behavior will improve by 19.7%. Previous studies, such as that of AlQadheeb et. al. (2022), revealed that aligning organizational security policies with observed user behavior can effectively influence and improve their information security behavior. The perceptions of respondents on the clarity of security policies and specific instances of policy non-compliance are positively associated with information security behavior (Saeed, 2023). Trang and Brendel (2019) investigated the applicability of deterrence theory to the study of compliance with information security policies. They found out that imposing sanctions for non-compliance had an overall effect on information security behavior. If sanctions are severe and implemented more promptly, the higher the likelihood that users will comply with the policies (Asfoor et. al., 2022).

### *3.3.5. Organizational Support and Training*

Organizational support and training also offered a positive and significant effect on information security behavior, with a regression coefficient (β) of 0.161 and a p-value of 0.013, as depicted in Table 7. It implies that helpdesks and IT administrators are accessible to the respondents and that teleworkers receive regular awareness and training sessions on information security. The positive influence indicated that if normative beliefs toward organizational support and training increase by 1, information security behavior will improve by 16.1%. The proposed influence of organizational support and training is consistently supported by this study and confirms the results of other previous literature, such as Eisenberger et. al. (2020) and Grassegger and Nedbal (2021), on the importance of employees' perceived organizational support and training to the improvement of information security behavior. Zhen et. al. (2022) also found out that learning inertia is positively associated with information security awareness, indicating that the organization's capability to provide technical support services and training and awareness sessions influence the teleworker's information security behavior.

### *3.3.6. Perception of Security*

Perception of security, with a p-value of 0.053 shown in Table 7, does not necessarily contribute to information security behavior and was not aligned with the expectations of this study. Previous studies supported this result, such as the study of Sulaiman et. al. (2022), wherein the perceived vulnerability does not positively influence a user's security behavior. Internet users with moderate security awareness tend to use weak passwords, open email attachments from unfamiliar senders, and engage in other risky behaviors.

Despite being aware of the potential risks, they underestimate their significance (Custers et al., 2019; Jampen et al., 2020). Saeed (2023) also found out that the perception of security does not significantly influence information security behavior and could be attributed to password management and email security management not being significant predictors as well.

### *3.4. Hypothesis Testing*

This study will reject the null hypothesis if the p-value is less than 0.05 (Di Leo & Sardanelli, 2020). Based on Table 8, the null hypotheses for infrastructure security management ($\beta = 0.390$, $p = 0.000$), organizational security policy ($\beta = 0.197$, $p = 0.01$), and organizational support and training ($\beta = 0.161$, $p = 0.013$) are rejected. However, the results failed to reject the null hypotheses for password management ($p = 0.563$), email security management ($p = 0.3$), and perception of security ($p = 0.053$).

Table 8: Summary of Hypotheses and Results

| Hypothesis | Standardized Coefficients (Beta) | p-value | Testing Result |
|---|---|---|---|
| Ho1: Password management does not significantly influence information security behavior. | 0.034 | 0.563 | Fail to Reject Ho |
| Ho2: Infrastructure security management does not significantly influence information security behavior. | 0.390 | 0.000 | Reject Ho |
| Ho3: Email security management does not significantly influence information security behavior. | 0.068 | 0.300 | Fail to Reject Ho |
| Ho4: Organizational security policy does not significantly influence information security behavior. | 0.197 | 0.010 | Reject Ho |
| Ho5: Organizational support and training do not significantly influence information security behavior. | 0.161 | 0.013 | Reject Ho |
| Ho6: Perception of security does not significantly influence information security behavior | 0.163 | 0.053 | Fail to Reject Ho |

## 4. Conclusion

In recent years, there has been a growing interest among academics and practitioners regarding the most effective way to enhance employees' information security behavior. This research offers insights into the various predictors that influence the information security behavior of teleworkers. On the basis of TPB, the researcher developed and empirically tested the constructs that linked perceived behavior concepts (password management, infrastructure security management, and email security management), subjective norms (organizational security policy and organizational support and training), and behavioral attitudes (perception of security) with information security behavior. Multiple linear regression was used to analyze the data collected from 146 respondents from different companies situated in NCR and CALABARZON. It was found that infrastructure security management, organizational security policy, and organizational support and training significantly influence information security behavior, therefore rejecting the corresponding null hypotheses. Such findings provided proof of the importance in mitigating human-induced cybersecurity risks among teleworkers and the significance of clear policies, normative beliefs, and effective enforcement mechanisms in fostering compliance and reducing risks related to information security. On the other hand, this research failed to reject the null hypotheses for password management, email security management, and perception of security.

This provided insights regarding the gap on Filipino teleworkers' ability to practice secure methods for managing passwords and identify email-related threats leading to a lower level of perception of security. These findings contribute to the body of knowledge in the fields of information security and teleworking. They also provide cumulative knowledge to organizations, security practitioners, and national policymakers on how to enhance information security programs for teleworkers.

## 5. Recommendations

Significant variables, such as infrastructure security management, organizational security policy, and organizational support and training, represent crucial focal points where organizations should direct their efforts to strengthen security measures and improve information security behavior. By investing resources and attention in these key areas, businesses can effectively bolster their security frameworks and mitigate potential risks. Combined with effective training initiatives, this can promote a culture of security consciousness and enhance the overall information security posture. Monitoring and consistency are pivotal for gauging the effectiveness of this strategy. Therefore, integrating information security into employee performance management is essential. Compliance can be measured through various means, such as the completion of security training courses and the outcomes of phishing simulation exercises. Furthermore, fostering a culture of continuous improvement in security practices, encouraging open communication channels for reporting security concerns, and regularly evaluating and updating security policies and practices can further reinforce the organization's resilience against evolving threats and promote a proactive approach to cybersecurity.

Conversely, non-significant variables such as password management, email security management, and perception of security suggest areas where efforts may be less impactful in influencing security behavior. In these areas, organizational effectiveness hinges on employees' comprehensive understanding of their roles and responsibilities as end-users, as outlined in security policies. The efficacy and impact of these non-significant factors ultimately depend on employees' adherence and engagement, regardless of the clarity of information security policies addressing these aspects. As such, organizations should consider alternative approaches, such as targeted education campaigns, soliciting feedback from teleworkers, or reassessing existing practices, to better align with organizational goals and industry best practices.

## 6. Limitations of the Study

Similar to the majority of published empirical studies, this study presents several limitations that provide opportunities for future research. This study was conducted with a limited number of respondents and may not fully represent the entire spectrum of the information security behavior of Filipino teleworkers. Consequently, this study did not account for the demographic characteristics of the respondents or the specific industries in which they were employed. For instance, age and industry type within the sample might offer different perspectives on how individuals approach cybersecurity practices. Future studies should delve deeper into these demographics, examining how they intersect with other predictors, to provide a more comprehensive understanding of the information security behavior of teleworkers. Another key limitation is the chosen set of predictors that explain a teleworker's information security behavior. This limitation stems from the adoption of the TPB as the theoretical lens of this research. While this theory offers valuable insights into the determinants of behavior, it may not encompass all potential predictors related to information security behavior. This opens avenues for further research from a variety of theoretical perspectives, allowing for a more comprehensive understanding of teleworkers' information security practices.

## References

Adjei Nyarko, D., & Fong, R. (2023). Cyber Security Compliance Among Remote Workers (pp. 343–369). https://doi.org/10.1007/978-3-031-20160-8_18

Almansoori, A.; Al-Emran, M.; Shaalan, K. (2023) Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories. Appl. Sci., 13, 5700. https://doi.org/10.3390/app13095700

Almehmadi, T., & Alsolami, F. (2019). Password Security in Organizations: User Attitudes and Behaviors Regarding Password Strength (pp. 9–13). https://doi.org/10.1007/978-3-030-14070-0_2

AlQadheeb, A., Bhattacharyya, S., & Perl, S. (2022). Enhancing cybersecurity by generating user-specific security policy through the formal modeling of user behavior. Array, 14, 100146. https://doi.org/https://doi.org/10.1016/j.array.2022.100146

Alqahtani, M. (2022). Factors Affecting Cybersecurity Awareness among University Students. Applied Sciences, 12(5). https://doi.org/10.3390/app12052589

Alqahtani, M. (2022). Cybersecurity Awareness Based on Software and E-mail Security with Statistical Analysis. Computational Intelligence and Neuroscience, 2022, 6775980. https://doi.org/10.1155/2022/6775980

Altulaihan, E. (2023). Email Security Issues, Tools, and Techniques Used in Investigation. Sustainability, 15. https://doi.org/10.3390/su151310612

Asfoor, A., Kasim, H., Latif, A., Razali, R., Ibrahim, Z.-A., & Shanneb, A. (2022). Identifying Factors of Non-Compliance, Compliance with Information Security Policy, and Behavior Change to Compliance: Literature Review. Journal of Hunan University Natural Sciences, 49, 274–288. https://doi.org/10.55463/issn.1674-2974.49.12.28

Asker H. & Tamtam A. (2023). Knowledge of Information Security Awareness and Practices for Home Users: Case Study in Libya. ESI Preprints. https://doi.org/10.19044/esipreprint.2.2023.p22

Atstaja, L., Rutitis, D., Deruma, S., & Aksjonenko, E. (2021). Cyber Security Risks And Challenges In Remote Work Under The Covid-19 Pandemic (pp. 12–22).

Bansal, N. (2023). Awareness of Password Management and Adoption of Digital Awareness of Password Management and Adoption of Digital Banking Services in Rural India". 34, 861–874.

Brooks, R., Williams, K., & Lee, S.-Y. (2023). Personal and Contextual Predictors of Information Security Policy Compliance: Evidence from a Low-Fidelity Simulation. Journal of Business and Psychology. https://doi.org/10.1007/s10869-023-09878-8

Calónico, S., Cattaneo, M. D., Farrell, M. H., & Titiunik, R. (2019, July 1). Regression Discontinuity Designs Using Covariates. https://doi.org/10.1162/rest_a_00760

Campbell, L. (2023, June). The Philippines: Cyber Threats. Retrieved February 19, 2024, from https://apps.dtic.mil/sti/trecms/pdf/AD1213133.pdf

Chandel, S., Yu, S., Yitian, T., Zhili, Z., & Yusheng, H. (2019). Endpoint Protection: Measuring the Effectiveness of Remediation Technologies and Methodologies for Insider Threat. 81–89. https://doi.org/10.1109/CyberC.2019.00023

Chintala, R., Tentu, S. R. K., & Chandu, R. (2022). Email Security Framework and Virus Detection Techniques (pp. 189–197). https://doi.org/10.1007/978-981-19-4960-9_16

Custers, B. H., Pool, R. L., & Cornelisse, R. (2019). Banking malware and the laundering of its profits. European Journal of Criminology, 16(6), 728–745.https://doi.org/10.1177/1477370818788007

Di Leo, G., & Sardanelli, F. (2020). Statistical significance: p value, 0.05 threshold, and applications to radiomics—reasons for a conservative approach. European Radiology Experimental, 4(1). https://doi.org/10.1186/s41747-020-0145-y

Eisenberger, R., Rhoades Shanock, L., & Wen, X. (2020). Perceived Organizational Support: Why Caring About Employees Counts. Annual Review of Organizational Psychology and Organizational Behavior, 7(1), 101–124. https://doi.org/10.1146/annurev-orgpsych-012119-044917

Estrellado, V. (2023, August 18). Surprising work-from-home statistics of 2023. Retrieved from https://www.outsourceaccelerator.com/articles/work-from-home-statistics/

Farooq, A., Ndiege, J., & Isoaho, J. (2019, October). Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior. https://doi.org/10.1109/AFRICON46755.2019.9133764

Fernando, P., Dissanayake, D., Dushmantha, S., Liyanage, C., & Karunatilake, C. (2023). Challenges and Opportunities in Password Management: A Review of Current Solutions. Sri Lanka Journal of Social Sciences and Humanities, 3, 9–20. https://doi.org/10.4038/sljssh.v3i2.96

Generalao, I. N. (2021). Measuring the telework potential of jobs: evidence from the International Standard Classification of Occupations. The Philippine Review of Economics, 58(1 & 2), 92–127. https://doi.org/10.37907/5erp1202jd

Goh, Z. H., Hou, M., & Cho, H. (2022). The impact of a cause–effect elaboration procedure on information security risk perceptions: a construal fit perspective. In Journal of Cybersecurity (Vol. 8, Issue 1). Oxford University Press (OUP). https://doi.org/10.1093/cybsec/tyab026

Grassegger, T., & Nedbal, D. (2021). The Role of Employees' Information Security Awareness on the Intention to Resist Social Engineering. Procedia Computer Science, 181, 59–66. https://doi.org/https://doi.org/10.1016/j.procs.2021.01.103

Gundu, T. (2019, October). Acknowledging and Reducing the Knowing and Doing Gap in Employee Cybersecurity Compliance.

Haque, Saw. Mu. S. (2023). THE IMPACT OF REMOTE WORK ON HR PRACTICES: NAVIGATING CHALLENGES, EMBRACING OPPORTUNITIES. European Journal of Human Resource Management Studies, 7(1). https://doi.org/10.46827/ejhrms.v7i1.1549

Hijji, M.; Alam, G. (2022). Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. Sensors, 22, 8663. https://doi.org/10.3390/s22228663

Hitaj, B., Gasti, P., Ateniese, G., & Perez-Cruz, F. (2019). Passgan: A deep learning approach for password guessing. In Applied Cryptography and Network Security: 17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings 17 (pp. 217-237). Springer International Publishing.

International Telecommunications Union. (2021). Global Cybersecurity Index 2020 [Website]. Switzerland: Author. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Jarlhem, J., & Stigsson, J. (2021). Digital Vulnerability Awareness : In a "working from home" environment during COVwID-19 (p. 37).

Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. Human-Centric Computing and Information Sciences, 10(1). https://doi.org/10.1186/s13673-020-00237-7

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a Theory of Information Systems Security Behaviors of Organizational Employees: A Dialectical Process Perspective. In Information Systems Research (Vol. 30, Issue 2, pp. 687–704). Institute for Operations Research and the Management Sciences (INFORMS). https://doi.org/10.1287/isre.2018.0827

Khan, M. (2023). Securing network infrastructure with cyber security. World Journal of Advanced Research and Reviews, 17, 803–813. https://doi.org/10.30574/wjarr.2023.17.2.0308

Kim, J., & Mou, J. (2020). Meta-analysis of Information Security Policy Compliance Based on Theory of Planned Behavior. Journal of Digital Convergence, 18(11), 169–176. https://doi.org/10.14400/JDC.2020.18.11.169

Mandal, D., Singhal, N., & Tyagi, M. (2023). Cybersecurity in the Era of Emerging Technology (pp. 108–134).

Mihailovic, A., Smolović, J., Radević, I., Rašović, N., & Martinović, N. (2021). COVID-19 and Beyond: Employee Perceptions of the Efficiency of Teleworking and Its Cybersecurity Implications. Sustainability, 13, 6750. https://doi.org/10.3390/su13126750

Mohajan, H.K. (2020). Quantitative Research: A Successful Investigation in Natural and Social Sciences. Journal of Economic Development, Environment and People.

Monzon, A. M. (2023, March 2). Most PH job seekers now prefer hybrid, remote work setup | Inquirer News. Retrieved from https://newsinfo.inquirer.net/1737214/most-ph-job-seekers-now-prefer-hybrid-work-setup

National Privacy Commission. (2023, August). NPC 2022 Annual Report. Retrieved February 19, 2024, from https://privacy.gov.ph/wp-content/uploads/2023/08/NPC-2022-ANNUAL-REPORT_ver3_revised.pdf

Parker, C.; Scott, S.; Geddes, A. (2019). Snowball Sampling; SAGE: New York, NY, USA

Pimentel, J. (2019). Some Biases in Likert Scaling Usage and its Correction. International Journal of Sciences: Basic and Applied Research (IJSBAR). 45. 183-191.

Ray, H., Wolf, F., Kuber, R., & Aviv, A.J. (2020). Why Older Adults (Don't) Use Password Managers. ArXiv, abs/2010.01973.

Saeed, S. (2023). Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia. Sustainability (Switzerland), 15(7). https://doi.org/10.3390/su15076019

Simonet, J., & Teufel, S. (2019). The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users. 194–208. https://doi.org/10.1007/978-3-030-22312-0_14ï

Sulaiman, N., Fauzi, M., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information, 13, 413. https://doi.org/10.3390/info13090413

Tanrıverdi, N., & Metin, B. (2021). Enterprise Information Security Awareness and Behavior as an Element of Security Culture During Remote Work (pp. 119–138). https://doi.org/10.4018/978-1-7998-7513-0.ch008

Trang, S., & Brendel, A. (2019). A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. Information Systems Frontiers, 21. https://doi.org/10.1007/s10796-019-09956-4

Turner, C., Turner, C., & Shen, Y. (2020). Cybersecurity Concerns & Teleworking in the COVID-19 Era: A Socio-Cybersecurity Analysis of Organizational Behavior. Journal of Advanced Research in Social Sciences, 3, 22–30. https://doi.org/10.33422/jarss.v3i2.502

Umejiaku, A., Dhakal, P., & Sheng, V. S. (2023, May 9). Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation. https://doi.org/10.3390/electronics12102159

Wachira, J. (2021, August 17). Factors Affecting Information Security in Teleworking. Case Study: Kenya National Police DT Sacco. Retrieved September 21, 2023, from http://erepository.uonbi.ac.ke/bitstream/handle/11295/155828/Wachira_Factors%20Affecting%20Information%20Security%20in%20Teleworking.pdf?sequence=1&isAllowed=y

Wang, X., & Cheng, Z. (2020). Cross-Sectional Studies. In Chest (Vol. 158, Issue 1, pp. S65–S71). Elsevier BV. https://doi.org/10.1016/j.chest.2020.03.012

Wiley, A., McCormac, M., & Calic, D. (2019). More than the Individual: Examining the Relationship Between Culture and Information Security Awareness. Computers & Security, 88, 101640. https://doi.org/10.1016/j.cose.2019.101640

Wu, B., & Ngambeki, I. B. (2021). Assessing and Improving Security Awareness and Concerns in Teleworking [Purdue University]. In ProQuest Dissertations and Theses. https://www.proquest.com/dissertations-theses/assessing-improving-security-awareness-concerns/docview/2838635357/se-2?accountid=28547

Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. Journal of Systems and Software, 210, 111946. https://doi.org/10.1016/j.jss.2023.111946

Zhen, J., Dong, K., Xie, Z., & Chen, L. (2022). Factors Influencing Employees' Information Security Awareness in the Telework Environment. Electronics (Switzerland), 11(21). https://doi.org/10.3390/electronics11213458

Zhu, Q., Luo, X., & Liu, Y. (2021). Modeling and Analysis of the Spread of Malware with the Influence of User Awareness. Complexity, 2021, 6639632. https://doi.org/10.1155/2021/6639632
Zickar, M.J.; Keith, M.G. (2023). Innovations in Sampling: Improving the Appropriateness and Quality of Samples in Organizational Research. Annu. Rev. Organ. Psychol. Organ. Behav, 10, 315–337. https://doi.org/10.1146/annurev-orgpsych-120920-052946