Chapter 1: Introduction

1.1 Background of the Study

The rapid proliferation of social media platforms has significantly transformed how individuals interact, share information, and communicate. Among university students, platforms such as Facebook, Instagram, and Twitter have become integral to daily life, facilitating both social connections and academic collaborations. However, this widespread use of social media also brings critical privacy concerns. Despite growing awareness, many students remain vulnerable to privacy breaches due to extensive data collection practices by these platforms (Adhikari & Panda, 2017). This study aims to explore the factors influencing privacy protection behaviors among university students and assess how these factors impact their online privacy practices.

Understanding the factors that drive privacy protection behavior is essential, particularly as social media platforms increasingly become repositories of vast amounts of personal information. Research indicates that various psychological and contextual factors, such as perceived severity of potential privacy threats, perceived vulnerability, and self-efficacy, play crucial roles in shaping individuals' privacy-related behaviors (Hanus & Wu, 2015). Additionally, theories such as Protection Motivation Theory (PMT) and Regulatory Focus Theory (RFT) provide valuable frameworks for analyzing these behaviors. PMT suggests that individuals' motivation to protect their privacy is influenced by their assessment of threats and their perceived ability to effectively counter these threats (Adhikari & Panda, 2017). RFT focuses on individuals' motivation based on their regulatory focus, which can be either promotion-focused (oriented towards achieving positive outcomes) or prevention-focused (oriented towards avoiding negative outcomes) (Higgins, 1997).

Despite these theoretical insights, there is a significant gap in empirical research focusing on university students, who are prolific users of social media yet often lack comprehensive knowledge of privacy protection measures. This study addresses this gap by investigating the specific factors that affect social media privacy protection behavior among university students in Sri Lanka. By examining how factors like perceived severity, perceived vulnerability, self-efficacy, regulatory focus, and previous experiences with privacy violations influence students' behaviors, this research aims to provide a nuanced understanding of their privacy practices (Suhaimi & Othman, 2017).

1.2 Problem Statement

The ubiquity of social media platforms in the daily lives of university students poses significant privacy risks. Students often share vast amounts of personal information without fully understanding the implications of data collection practices employed by these platforms. This lack of awareness and inadequate privacy protection measures can lead to privacy breaches, exposing

students to various risks such as identity theft, cyberbullying, and unauthorized access to personal data. Despite the growing importance of digital privacy, there is a paucity of research focusing on the privacy protection behaviors of university students, particularly in the context of Sri Lanka. This study aims to fill this gap by examining the factors that influence privacy protection behaviors among university students and evaluating the effectiveness of current privacy protection measures.

1.3 Research Questions

This study seeks to address the following research questions:

1. What are the key factors influencing privacy protection behaviors among university students on social media platforms?
2. What is the effect of those factors on privacy protection behaviors among university students on social media platforms?

1.4 Research Objectives

The main objective of the study is to investigate the factors affecting privacy protection behaviors among university students on social media platforms. It would be achieved by fulfilling the following sub-objectives:

1. To identify the factors affecting privacy protection behaviors among university students on social media platforms.
2. To examine the effect of those factors on privacy protection behaviors among university students on social media platforms.

1.5 Methodology

This research adopts a quantitative approach to investigate the factors influencing privacy protection behaviors among university students. A survey will be administered to a representative sample of university students in Sri Lanka to collect data on their privacy protection behaviors, perceptions of privacy threats, self-efficacy, regulatory focus, and past experiences with privacy violations. The data collected will be analyzed using statistical methods to identify significant relationships and patterns. The use of a quantitative approach allows for the systematic examination of the research questions and the generation of statistically robust findings that can inform privacy protection strategies.

1.5 Significance of the Research Study

The findings of this study are expected to offer important implications for educators, policymakers, and social media developers. Enhancing students' awareness and ability to protect their privacy can lead to more secure and responsible use of social media platforms. Furthermore, this research will contribute to the broader discourse on digital privacy by highlighting the unique challenges and behaviors of university students in the context of social media usage. Ultimately, this study seeks to inform strategies that can better safeguard users' personal information in an increasingly interconnected digital world. By providing insights into the factors that influence privacy protection behaviors, this research aims to support the development of effective privacy education programs and policies that address the specific needs of university students.

1.6 Structure of the Report

This report is structured as follows:

- **Chapter 1: Introduction** - Provides an overview of the study, including the background, problem statement, research questions, methodology, significance, and structure of the report.
- **Chapter 2: Literature Review** - Reviews existing literature on social media privacy, privacy protection behaviors, and theoretical frameworks such as Protection Motivation Theory and Regulatory Focus Theory.
- **Chapter 3: Research Methodology** - Details the research design, sample selection, data collection methods, and data analysis techniques employed in the study.
- **Chapter 4: Results** - Presents the findings of the study, including descriptive statistics and analysis of the relationships between the key factors and privacy protection behaviors.
- **Chapter 5: Discussion** - Interprets the results in the context of existing literature and theoretical frameworks, discussing the implications for privacy protection strategies and policies.
- **Chapter 6: Conclusion and Recommendations** - Summarizes the key findings of the study, offers recommendations for enhancing privacy protection behaviors among university students, and suggests directions for future research.

Chapter 2: Literature Review

Introduction

The pervasive use of social media platforms among university students has significantly transformed the way personal information is shared and managed. While these platforms offer unparalleled opportunities for communication and engagement, they also pose substantial risks to

personal privacy. The impact of social media on personal privacy is a critical area of concern, particularly for university students who are frequent and often naive users of these platforms. This literature review examines the theoretical frameworks and empirical studies related to data collection practices on social media platforms and the privacy protection measures adopted by users, focusing on the relevance and application of Protection Motivation Theory (PMT) and Regulatory Focus Theory (RFT).

Existing Research Linking to the Research Problem

Research has consistently shown that social media platforms employ sophisticated data collection practices that track user activities, preferences, and interactions. This information is often used to create detailed profiles for targeted advertising and content personalization (Debatin et al., 2009). Despite the growing awareness of privacy issues, many users remain unaware of the extent to which their data is collected and used by these platforms (Acquisti & Gross, 2006). This disparity between privacy concerns and actual online behaviors is known as the privacy paradox (Barnes, 2006).

Data Collection Practices on Social Media

Social media platforms employ sophisticated data collection practices to gather extensive user information, which is primarily used for targeted advertising and content personalization. Debatin et al. (2009) highlighted how platforms like Facebook track user activities, preferences, and interactions to create detailed profiles. Acquisti and Gross (2006) noted that users are often unaware of the extent to which their data is collected and used, leading to a privacy paradox where users express concern about privacy but do not take adequate protective measures (Barnes, 2006). This paradox is particularly relevant for university students, who are frequent social media users but may lack comprehensive understanding of data privacy implications (Adhikari & Panda, 2017).

Privacy Concerns and Protection Measures

University students express significant concerns about their privacy on social media, yet these concerns do not consistently lead to protective behaviors. Research by Yao et al. (2007) found that while students are aware of privacy risks, their engagement in protective measures, such as adjusting privacy settings, is inconsistent. Tufekci (2008) attributed this inconsistency to factors like perceived control over personal information, trust in the platform, and the perceived benefits of social media use outweighing the privacy risks. This section explores the empirical findings related to these factors and their impact on privacy protection behaviors.

Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT), developed by Rogers (1975), provides a framework for understanding how individuals are motivated to protect themselves from perceived threats. PMT posits that protective behaviors are influenced by threat appraisal and coping appraisal.

Threat Appraisal

1. **Perceived Severity (PS):** The extent to which an individual believes that the consequences of a privacy breach are serious. Higher perceived severity leads to greater motivation to engage in protective behaviors (Woon et al., 2005).
2. **Perceived Vulnerability (PV):** The extent to which an individual feels susceptible to privacy threats. Greater perceived vulnerability enhances the motivation to protect personal information (Chenoweth et al., 2009).

Coping Appraisal

1. **Response Efficacy (RE):** The belief that the recommended protective actions will effectively mitigate the threat. Users who believe in the effectiveness of privacy settings are more likely to use them (Tsai et al., 2011).
2. **Self-Efficacy (SE):** Confidence in one's ability to implement protective behaviors. Higher self-efficacy is associated with greater engagement in privacy-protective measures (Ng et al., 2009).

PMT has been widely applied to understand the privacy behaviors of social media users, suggesting that enhancing threat and coping appraisals can improve protective behaviors among university students (Herath & Rao, 2009).

Regulatory Focus Theory (RFT)

Regulatory Focus Theory (RFT), introduced by Higgins (1997), distinguishes between two motivational orientations: promotion focus and prevention focus.

Promotion Focus

Individuals with a promotion focus are driven by growth, aspirations, and the attainment of positive outcomes. On social media, these individuals are likely to engage in behaviors that enhance their social presence and connections, sometimes at the expense of privacy (Higgins, 1997).

Prevention Focus

Individuals with a prevention focus prioritize safety, security, and the avoidance of negative outcomes. These users are more likely to adopt stringent privacy measures and limit their personal information sharing to protect against potential privacy threats (Crowe & Higgins, 1997).

RFT helps explain the differing privacy management strategies among social media users, with promotion-focused individuals more inclined to risk privacy for social rewards, and prevention-focused individuals more likely to prioritize privacy protection (Florack et al., 2013).

Integration of PMT and RFT

Integrating PMT and RFT provides a comprehensive understanding of the determinants of privacy protection behaviors on social media. PMT offers insights into the cognitive processes driving protective behaviors, while RFT explains the strategic orientations influencing these behaviors. This combined approach is particularly relevant for university students, whose social media use is driven by both the desire for social engagement and the need for privacy protection.

Research Approaches, Strategies, and Techniques

Various research approaches have been employed to study privacy protection behaviors. Quantitative methods, such as surveys and experiments, are commonly used to gather data on users' privacy perceptions and behaviors (Hanus & Wu, 2015). Qualitative methods, including interviews and focus groups, provide deeper insights into the contextual factors influencing privacy behaviors. The choice of methodology depends on the research questions and the nature of the data needed.

Identification of Research Gaps

Despite the extensive research on privacy protection behaviors, significant gaps remain, particularly concerning university students. University students are prolific social media users, often engaging with these platforms in ways that differ from the general population. However, much of the existing literature focuses on broader demographic groups or the general population, neglecting the unique experiences and behaviors of university students. Additionally, while studies have explored the application of Protection Motivation Theory (PMT) and Regulatory Focus Theory (RFT) in various contexts, there is a paucity of research integrating these theories to provide a comprehensive understanding of privacy protection behaviors specifically among university students. This section elaborates on these research gaps and the need for targeted studies in this area.

University Students as a Unique Demographic

1. **High Engagement and Vulnerability:**
    - University students are among the most active users of social media, frequently sharing personal information and engaging in online interactions. Their high engagement levels increase their exposure to privacy risks, making them a particularly vulnerable group. Unlike older adults who might be more cautious, university students often prioritize social connections and the benefits of social media over potential privacy threats.
2. **Distinct Behavioral Patterns:**
    - The privacy behaviors of university students may differ significantly from other demographic groups due to their life stage, social dynamics, and technological proficiency. They are in a transitional phase, often exploring new social identities

and relationships, which may influence their willingness to share personal information. Understanding these distinct behavioral patterns requires focused research on this demographic.

3. **Limited Focus on University Students:**

    - Existing studies predominantly address the general population or specific professional groups, leaving a gap in understanding the unique privacy concerns and behaviors of university students. Research tailored to this group can uncover specific factors that influence their privacy protection behaviors, such as peer influence, academic pressures, and digital literacy levels.

Integration of PMT and RFT

1. **Comprehensive Theoretical Understanding:**

    - While PMT and RFT have been individually applied to understand privacy behaviors, their integration can provide a more holistic view. PMT focuses on cognitive processes related to threat and coping appraisals, whereas RFT highlights motivational orientations (promotion and prevention focus). Combining these theories can reveal how cognitive evaluations and motivational drives interact to influence privacy behaviors.

2. **Exploration of Interactions:**

    - There is limited research exploring how the constructs of PMT (e.g., perceived severity, perceived vulnerability, response efficacy, and self-efficacy) interact with the orientations of RFT (promotion vs. prevention focus) to shape privacy protection behaviors. Empirical studies that examine these interactions can provide deeper insights into why university students choose certain privacy practices over others.

3. **Context-Specific Application:**

    - Applying the integrated PMT and RFT framework to the context of social media use among university students can uncover unique insights. This context-specific application is essential because the dynamics of privacy concerns and behaviors on social media differ from other online or offline environments.

Context of Sri Lankan University Students

1. **Cultural and Regional Specificity:**

    - The cultural, social, and technological context of Sri Lankan university students differs from that of students in Western or other Asian countries. These differences can influence privacy perceptions and behaviors. For instance, cultural norms around privacy, communal values, and levels of digital literacy can vary, impacting how students manage their online privacy.

2. **Understudied Population:**
    - There is a notable lack of research focusing on Sri Lankan university students regarding social media privacy. This gap presents an opportunity to contribute to the global understanding of privacy behaviors by providing data and insights from a region that has been underrepresented in the literature.
3. **Policy and Educational Implications:**
    - Understanding the privacy behaviors of Sri Lankan university students can inform local policy-making and educational initiatives. Insights from this research can help develop targeted privacy education programs, raise awareness, and inform the creation of policies that protect student privacy in the digital age.

Available Empirical Findings and Theories Related to Research

Empirical findings and theoretical frameworks provide a robust foundation for understanding the privacy protection behaviors of university students on social media. This section discusses key empirical studies and relevant theories, emphasizing their implications for the current research.

Empirical Findings on Privacy Protection Behaviors

Awareness and Perceived Risks

Empirical studies indicate that awareness of privacy risks significantly impacts privacy protection behaviors. Yao et al. (2007) found that users who are more aware of privacy risks are more likely to engage in protective behaviors, such as adjusting privacy settings and being cautious about the information they share. This finding aligns with the Protection Motivation Theory (PMT), which suggests that perceived severity and vulnerability drive protective actions.

Inconsistency in Protective Measures

Despite awareness of privacy risks, many users exhibit inconsistent protective behaviors. Tufekci (2008) highlighted that while university students often express concerns about their privacy, this does not always translate into consistent protective actions. Factors such as perceived control over personal information, trust in social media platforms, and the perceived benefits of social media use often outweigh privacy concerns. This inconsistency is a critical area for further research, as it highlights a gap between knowledge and behavior.

Factors Influencing Privacy Behaviors

Studies by Acquisti and Gross (2006) and Barnes (2006) explored various factors influencing privacy behaviors, including demographic characteristics, psychological traits, and contextual influences. For instance, younger users and those with higher social media engagement levels are often less cautious about privacy, as they prioritize social connectivity over privacy protection.

Understanding these factors is crucial for developing targeted strategies to enhance privacy protection among university students.

Theoretical Frameworks

Protection Motivation Theory (PMT)

PMT provides a comprehensive framework for understanding the cognitive processes driving privacy protection behaviors. According to PMT, individuals assess the severity and vulnerability of potential privacy threats and their ability to cope with these threats through response efficacy and self-efficacy. Empirical studies, such as those by Hanus and Wu (2015) and Herath and Rao (2009), have validated the applicability of PMT in the context of online privacy, demonstrating that enhancing threat appraisal and coping appraisal can effectively promote protective behaviors.

Regulatory Focus Theory (RFT)

Regulatory Focus Theory (RFT), developed by Higgins (1997), offers insights into the motivational orientations influencing privacy behaviors. RFT distinguishes between promotion-focused individuals, who seek positive outcomes, and prevention-focused individuals, who aim to avoid negative outcomes. Empirical research by Florack et al. (2013) found that prevention-focused users are more likely to adopt stringent privacy measures, while promotion-focused users are more inclined to share personal information to enhance social connections. Integrating RFT with PMT can provide a nuanced understanding of the motivational and cognitive factors driving privacy protection behaviors.

Privacy Paradox

The privacy paradox, identified by Barnes (2006), refers to the discrepancy between users' expressed privacy concerns and their actual behaviors. This paradox is particularly evident among university students, who, despite recognizing privacy risks, often engage in risky behaviors such as oversharing and inadequate use of privacy settings. Empirical studies by Debatin et al. (2009) and Acquisti and Gross (2006) suggest that this paradox is influenced by factors such as perceived control, trust in platforms, and the social benefits of sharing information.

Self-Efficacy and Privacy Behaviors

Self-efficacy, a key component of PMT, plays a crucial role in determining privacy protection behaviors. Ng et al. (2009) found that users with higher confidence in their ability to manage privacy settings are more likely to engage in protective behaviors. This finding underscores the importance of enhancing users' skills and confidence in using privacy tools, which can be achieved through targeted education and training programs.

Implications for the Current Research

The review of empirical findings and theoretical frameworks highlights several implications for the current research on privacy protection behaviors among university students in Sri Lanka:

1. **Awareness Programs**: Enhancing awareness of privacy risks and the importance of protective behaviors is essential. Educational initiatives should focus on the specific risks associated with social media use and practical steps to mitigate these risks.
2. **Behavioral Interventions**: Addressing the privacy paradox requires interventions that bridge the gap between awareness and behavior. Strategies such as gamification of privacy settings and integrating privacy protection into daily social media routines can be effective.
3. **Enhancing Self-Efficacy**: Providing training and resources to improve students' self-efficacy in managing privacy settings is crucial. Workshops, online tutorials, and peer support groups can help build confidence and skills.
4. **Motivational Strategies**: Understanding the regulatory focus of students can inform tailored motivational strategies. For prevention-focused students, highlighting the risks of privacy breaches can be effective, while for promotion-focused students, emphasizing the benefits of secure social media use can encourage protective behaviors.
5. **Contextual Factors**: Recognizing the influence of contextual factors such as peer behavior, cultural norms, and platform trust is important. Privacy protection strategies should consider these factors to be more relevant and effective.

By integrating these insights from empirical findings and theoretical frameworks, the current research aims to develop a comprehensive understanding of the factors influencing privacy protection behaviors among university students. This approach will inform the development of targeted interventions and policies to enhance privacy protection in the digital age.

Conclusion

Understanding the impact of social media on personal privacy among university students requires a multifaceted approach that considers both cognitive and motivational factors. The application of PMT and RFT provides valuable insights into the complex dynamics of privacy protection behaviors. By examining these theoretical frameworks and empirical findings, this literature review underscores the importance of tailored strategies to enhance privacy protection in the digital age. Future research should focus on integrating these theories and addressing the specific needs of university students to develop effective privacy education programs and policies.

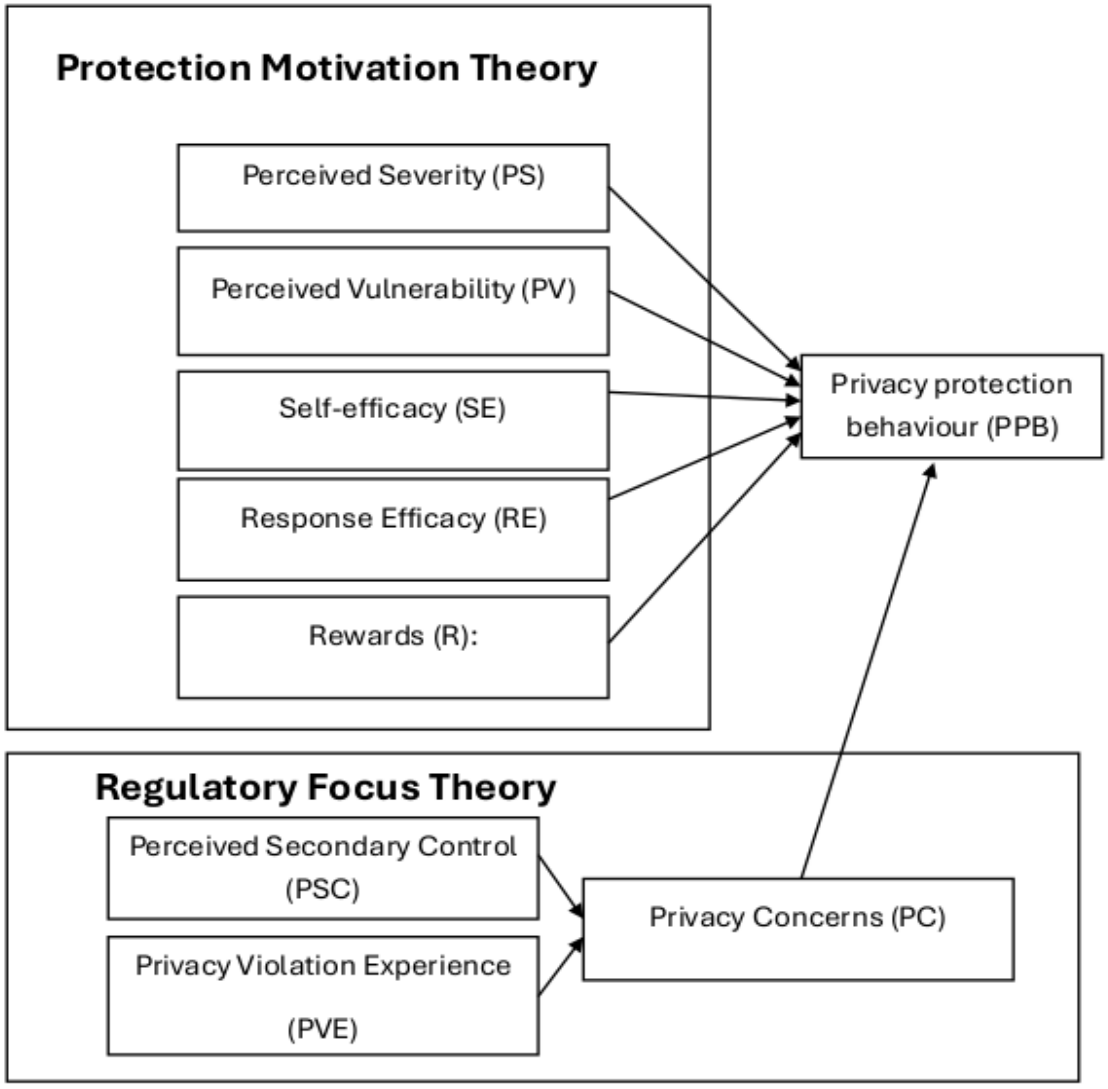
Chapter 3: Methodology

Rationale for Methodology Selection

The methodology selected for this research is quantitative. This choice is driven by the need to objectively measure the factors influencing social media privacy protection behaviors among university students in Sri Lanka. Quantitative methods allow for the collection of numerical data that can be statistically analyzed to test hypotheses and determine the relationships between different variables. This approach is appropriate for addressing the research problem as it provides a systematic and replicable way to assess the influence of multiple predictors on privacy protection behavior, facilitating generalization of the findings.

THEORETICAL FRAMEWORK

The theoretical underpinnings of the notion and the factors influencing users' behavior in protecting their privacy on social media platforms are presented in this section. The Protection Motivation Theory serves as the foundation for the suggested theoretical framework.


Protection Motivation Theory
Perceived Severity (PS)
Perceived Vulnerability (PV)
Self-efficacy (SE)
Response Efficacy (RE)
Rewards (R):
Privacy protection behaviour (PPB)
Regulatory Focus Theory
Perceived Secondary Control (PSC)
Privacy Violation Experience (PVE)
Privacy Concerns (PC)

Protection Motivation Theory (PMT) provides analytical understanding to explain why people are drawn to fear and why different behaviors are taken in response to different circumstances or settings (Baruh et al., 2017). The goal of PMT's creation was to comprehend why users worry about safeguarding their privacy, assisting in improving user awareness of the factors that influence appropriate behavior, and defending themselves from any threats. A growing body of research has noted the significance of PMT in figuring out how users react to privacy issues on social media sites (Büchi et al., 2017). Previous studies have demonstrated the importance of privacy - related beliefs and actions. A user who prioritizes their privacy protection and cares about information privacy is more likely to participate in privacy protection activity (Baruh et al., 2017). Additionally, a user's protective behavior increases in proportion to the privacy difficulties they encounter (Appel et al., 2016)

Perceived Vulnerability (PV) Perceived Severity (PS), Self-Efficacy (SE), Response Efficacy (RE), and Reward (R) are the five components of PMT. According to the PMT, users' desire to defend themselves against Specific risks are derived from two factors: their threat assessment and their coping evaluation. The perceived severity of the dangers and the perceived susceptibility to those threats are measured for threat evaluation. Its gauge's reaction efficiency and self-efficacy for coping evaluation. The user's behavior is influenced by both Assessments to protect their privacy from potential threats. When both of those assessments are seen favorably, users will be motivated and encouraged to adopt protective behaviors that will shield them from dangers and alter their behavior.

H1: Perceived vulnerability positively influenced privacy protection behavior in social media sites.

Perceived Severity (PS) The most accurate way to define perceived severity is the perceived seriousness of potentially dangerous outcomes. Users adjust their behavior based on how serious they perceive a consequence to lower the likelihood of dangers. In general, perceived severity relates to the user's belief that a potentially dangerous event results from a decision regarding severity importance (Palladino et al., 2017). Furthermore, (Adhikari & Panda, 2018) claimed that a user's propensity to engage in the activity of reducing the danger might be positively impacted by their perception of the severity. Put simply, users of Social Media Sites will be compelled to take precautions if perceived severity intensity is higher (T. Wang et al., 2016). While several researchers have discovered a substantial relationship between perceived severity and conduct and intention, there is also data that suggests there is no significant relationship between severity and intention (Hanus & Wu, 2016).

H2: Perceived severity positively influenced privacy protection behavior in social media sites.

Self-efficacy (SE) Self-efficacy is the extent to which users think they ought to execute the advised action. Users ought to have the guts to overcome obstacles preventing them from doing a certain action. Research has shown that users need to possess technological abilities to operate in private

areas. This must do with wanting to stop engaging in risky or ineffective activities. In his research, (M. Vatka, 2019) makes thecase that self-efficacy can help one take stronger action toward more successful data protection activities. The user who has more confidence in their ability to manage their personal information may have fewer privacy concerns when exchanging information (Asanka & Arachchilage, n.d.) . Additionally, (Fida et al., 2018) explained that self-efficacy is a key component in determining the success of danger avoidance or privacy protectionmeasures as well as a key determinant of such activities. In his research,(M. Vatka, 2019) makes the case that self-efficacy can help one take stronger action toward more successful data protection activities. The user who has more confidence in their ability to manage their personal information may have fewer privacy concerns when exchanging information(Asanka & Arachchilage, n.d.) . Additionally, (Fida et al., 2018) explained that self-efficacy is a key component in determining the success of danger avoidance or privacy protection measures as well as a key determinant of such activities. This research attempts to identify the function of users' self-efficacy in the implementation of privacy protection behavior. As (Martin et al., 2017) stated that actual behavior is the main factor that affects self-efficacy. Hence, the role of the user's behavior as a basis of perceptions regarding self-efficacy has been largely established and confirmed.

H3: Self-efficacy positively influenced privacy protection behavior in social media sites.

Response Efficacy (RE) This metric assesses how well a response is implemented in order to lessen the threat. According to a research, response efficacy has a significant role in predicting whether or not to implement security measures on networks, boosts attempt to use anti-spyware software as a preventative measure, and forecasts when data backups on personal computers will occur (Lee & Kobsa, 2016). Furthermore, (Fida et al., 2018) said that while information privacy is seen as a matter of uncertainty, response effectiveness is anticipated to play a significant role in lowering the risks associated with social media platforms. Individuals who believe customization software enhances their privacy are less concerned about privacy particular to the system and are more inclined to utilize it as a privacy tool (Dienlin & Metzger, 2016). The study comes to the conclusion that reduced data loss would be possible with a high response effectiveness.

H4: Response efficacy positively influenced privacy protection behavior in social media sites.

Rewards (R) Users reported receiving a lot of credit on social media platforms when a lot of personal information was submitted, according to a study by (D. Wang, 2019). Rewards are defined by prior study as being acknowledged and responded to when posts are made on social media platforms through "likes" and "comments." Restrictive privacy settings, however, may make it more difficult to obtain some benefits from social networking platforms (Chen & Chen, 2015). Users of social media platforms also exchange their privacy information for rewards on these platforms, and when they divulge personal information, they earn advantages like satisfaction and fame (Park & Kim, 2020). Users that enjoy the advantages of social media platforms will decide to divulge personal information in order to continue enjoying these advantages (Abdul Hameed & Asanka Gamagedara Arachchilage, n.d.). Users should maximize the benefits from social networking sites by protecting their privacy when interacting with their contacts, as this could have

a detrimental effect on them while they seek those rewards (Rains & Scott, 2007; Suhaimi et al., 2020).

H5: Rewards positively influenced privacy protection behavior in social media sites.

Privacy Protection Behavior The management of the disclosure of personal information while preventing unauthorized access is known as privacy protection (Choi et al., 2015). In the current day, it is imperative to protect privacy practices since consumers are concerned about how their private data is being gathered, maintained, and exposed to third parties. Users of social networking sites can safeguard their privacy by limiting the amount of personal information they exchange, sharing, and posting about themselves, as well as by implementing security measures for privacy (Feng & Xie, 2014). Individuals will take different privacy protection measures to safeguard their private when they experience emotional anguish, betrayal, and a sense of unfairness or inequity (Choi et al., 2015). Therefore, in order to ascertain the effects of users' actions, it is necessary to learn more about how they utilize privacy protection.

The term "privacy protection" refers to the steps people take to safeguard their personal data, and they are divided into two groups: approach techniques and avoidance strategies (Litt, 2013; Smit et al., 2014; Tu et al., 2015). While avoidance techniques involve withholding and refusing to share the information, approach strategies relate to confrontation strategies that include problem-solving and looking for social support. Creating personal information is one approach strategy. Another is looking for social support through advice and information from others or by reading the privacy statement.

Avoidance tactics include things like deleting or removing upsetting content from social media platforms, utilizing the privacy settings offered by these platforms, and deciding who may view their posts and profiles as well as who they can share their personal information with. It is crucial that individuals employ these privacy techniques so that they may decide with knowledge what information to share and how. Additionally, by using privacy settings, users of social media sites can minimize the potential harm and damage to their relationships and reputation that may arise from inadvertent disclosures, while still benefiting from the selective content sharing on these platforms (Mohamad Ali et al., 2012).

PC --> PPB H6: Privacy concerns negatively relate to privacy protection.

Perceived Secondary Control (PSC) refers to consumers' belief that they have some influence over how their personal information is managed and shared by social media platforms. This perception is crucial in fostering trust and reducing privacy concerns, thereby enhancing user engagement. (Mosteller & Poddar, 2017) found that perceived secondary control positively relates to consumer trust in social media websites and negatively relates to privacy concerns. When users feel they have control over their data, they are more likely to trust the platform and share information, which leads to higher engagement. Moreover, perceived secondary control helps balance power dynamics between users and firms. By offering users control over their information,

platforms can foster trust and equity in the relationship, reducing privacy concerns and encouraging more positive interactions.

Privacy Violation Experience (PVE)refers to consumers' past encounters where their personal information was misused or improperly handled. Such experiences significantly impact users' trust in social media platforms and heighten their privacy concerns. According to (Mosteller & Poddar, 2017) previous experiences with privacy violations are negatively associated with trust in social media websites. This means that users who have had their privacy compromised are less likely to trust social media platforms. Additionally, these experiences are positively associated with privacy concerns, as users become more vigilant and worried about their personal data being mishandled again. This vigilance leads users to adopt privacy protection behaviors, such as adjusting privacy settings and limiting the amount of personal information shared online. The heightened privacy concerns and reduced trust act as significant barriers to user engagement on social media platforms.

Privacy Concerns (PC) refer to the apprehension consumers have regarding the security and appropriate use of their personal information shared on social media platforms. These concerns significantly influence user behavior and their willingness to engage with these platforms. According to (Mosteller & Poddar, 2017), privacy concerns are negatively impacted by perceived secondary control, meaning that when users feel they have control over them information, their privacy concerns decrease. Conversely, previous experiences of privacy violations heighten these concerns, making users more cautious and protective of their data. These heightened privacy concerns lead users to adopt privacy protection behaviors, such as adjusting privacy settings and being selective about the information they share online. This protective stance is a direct response to the perceived risks associated with sharing personal information on social media platforms.

PSC --> PC H7: Perceived secondary control of personal data negatively relates to privacy concerns.

PVE --> PC H8: Previous privacy violation experience positively relates to privacy concerns.

Operationalization of Concepts

Operationalization involves defining how each concept will be measured:

- **Perceived Vulnerability (PV)**: Assessed by asking students to rate their perceived likelihood of encountering privacy threats on social media.
- **Perceived Severity (PS)**: Measured by evaluating students' perceptions of the seriousness of potential privacy breaches.
- **Self-Efficacy (SE)**: Gauged through students' confidence in their ability to protect their privacy on social media.
- **Response Efficacy (RE)**: Determined by students' beliefs in the effectiveness of available privacy protection measures.
- **Rewards (R)**: Evaluated based on the perceived benefits students receive from sharing personal information on social media.

- **Privacy Concerns (PC)**: Measured by the level of concern students have regarding their privacy on social media platforms.
- **Perceived Secondary Control (PSC)**: Assessed by students' perceived control over their personal information.
- **Privacy Violation Experience (PVE)**: Evaluated through students' past experiences of privacy breaches on social media.

Type of Study, Study Setting, Time of the Study, and Unit of Analysis

This study is a cross-sectional survey conducted in a university setting in Sri Lanka. The study took place over a period of two months, from April to may 2024. The unit of analysis is individual university students who use social media.

Population and Sample

The target population for this study consists of university students in Sri Lanka who actively use social media. A sample of 117 students was selected using an A-priori Sample Size Calculator for Multiple Regression (Soper, 2024). The parameters were set as follows:

- Anticipated effect size (f^2): 0.15
- Desired statistical power level: 0.8
- Number of predictors: 8
- Probability level: 0.05
- Minimum required sample size: 108

Data Collection Instrument and Methods

The primary data collection instrument was a structured questionnaire developed specifically for this study. The questionnaire was designed to measure the constructs outlined in the conceptual framework using a Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree). The questionnaire was distributed online via Google Forms to ensure a wide reach among the student population. Using Google Forms facilitated easy distribution and data collection, ensuring that the responses were systematically recorded and stored for analysis.

Data Analysis Methods and Tools

Data analysis was conducted using SPSS (Statistical Package for the Social Sciences) version 26. The analysis involved several steps:

1. **Descriptive Statistics**: To summarize the demographic characteristics of the sample and the distribution of the responses.
2. **Reliability Analysis**: To assess the internal consistency of the scales using Cronbach's alpha.
3. **Factor Analysis**: To confirm the validity of the constructs.

4. **Multiple Regression Analysis**: To test the hypotheses and determine the relationships between the predictors (PV, PS, SE, RE, R, PC, PSC, PVE) and the dependent variable (privacy protection behavior).

Conclusion

This chapter outlined the quantitative methodology adopted for the study, providing a detailed rationale for the selection of this approach, the conceptual framework, hypotheses, and the operationalization of key concepts. It also described the study design, population and sample, data collection instruments, and the data analysis methods. This rigorous methodological approach ensures the reliability and validity of the findings, contributing to a better understanding of the factors influencing social media privacy protection behaviors among university students in Sri Lanka.

Chapter 4: Data Analysis and Discussion

4.1 Introduction

This chapter presents and discusses the data analysis process followed to obtain the results of the study. First, the data screening process is presented, and it is followed by the demographic data analysis and the descriptive data analysis. Finally, the measurement model analysis and the structural model analysis results and the discussion of the findings are presented.

4.2 Data Screening

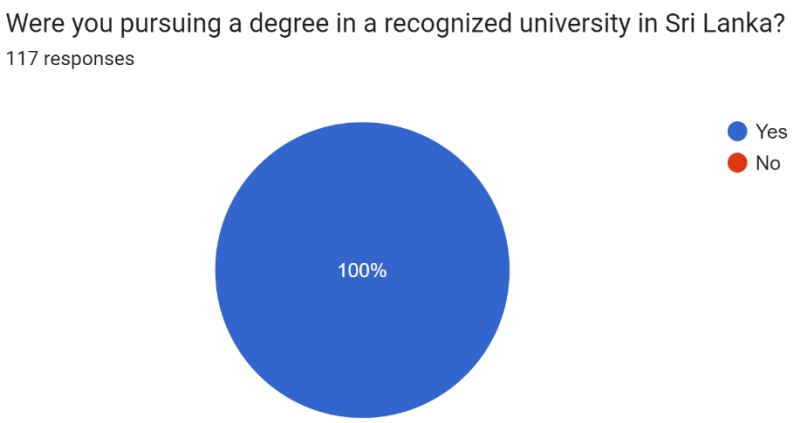
A total number of 117 responses were gathered at the end of the data collection period. A data screening process was carried out to identify the unengaged responses and responses with missing values. 100% of total responses were qualified for the final data analysis at the end of the data screening**.**

4.3 Descriptive Data Analysis

Data analysis results for demographic data gathered and the descriptive statistics of the constructs were obtained using Statistical Package for Social Sciences software. Sub sections given below present the results of the descriptive data analysis

4.3.1 Demographic Data Analysis

Data related to the gender, age, academic background of the respondents, and familiarity with technology were gathered from the respondents. Following results were obtained from the demographic data analysis:



According to the figure 1, all the respondents are pursuing a degree in recognized university in Sri Lanka.

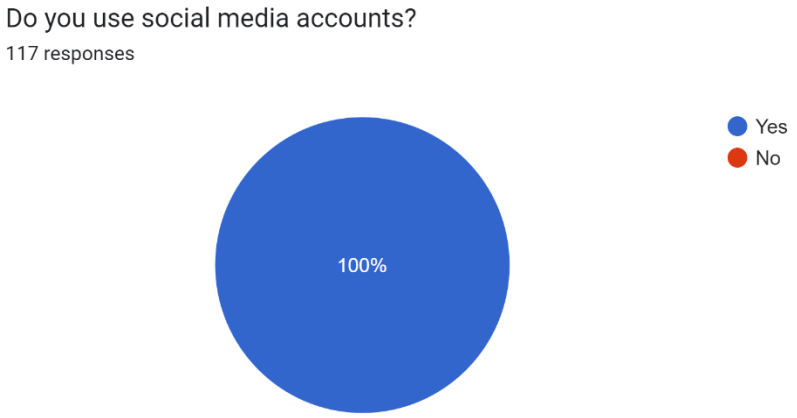
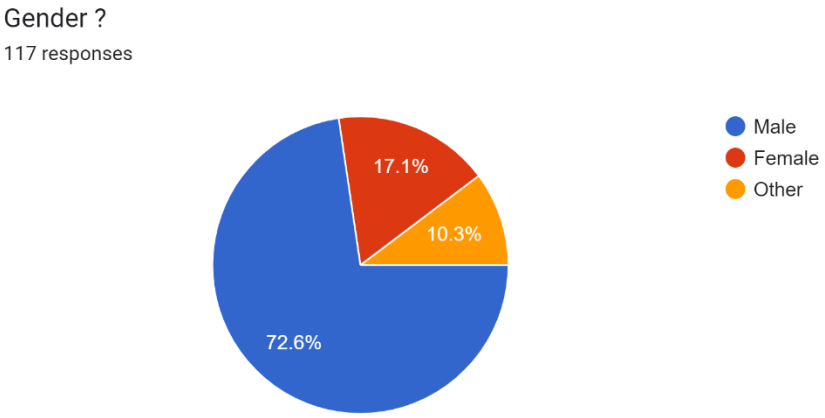
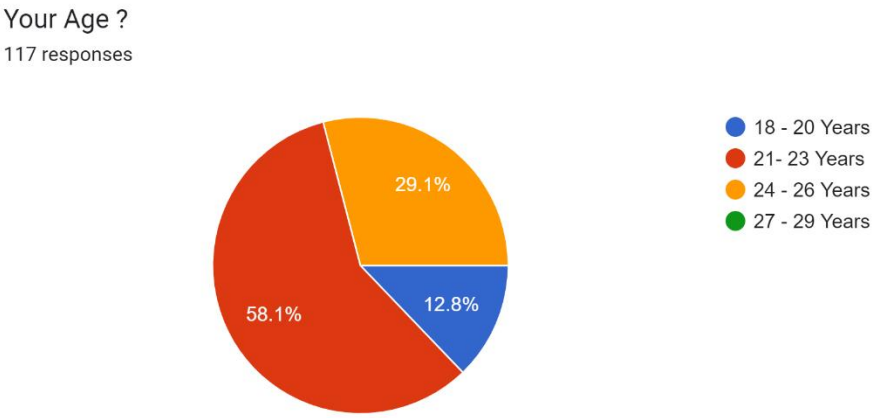


Figure 2 shows that these all respondents who are pursuing a degree use the social media accounts also.



According to figure 3, most of respondents are male which represents 72.6% from total respondents. Female respondents are 17.1 % and other respondents represent 10.3%.



Majority of the respondents belong to the 21-23 age group representing 58.1% while minimum respondents representing 12.8% who are belonging to 18-20 age group. 29.1% from all respondents are belonging to 24-26 age group. The important difference we can see here is that there is no any respondents belong to the 27-29 age group.

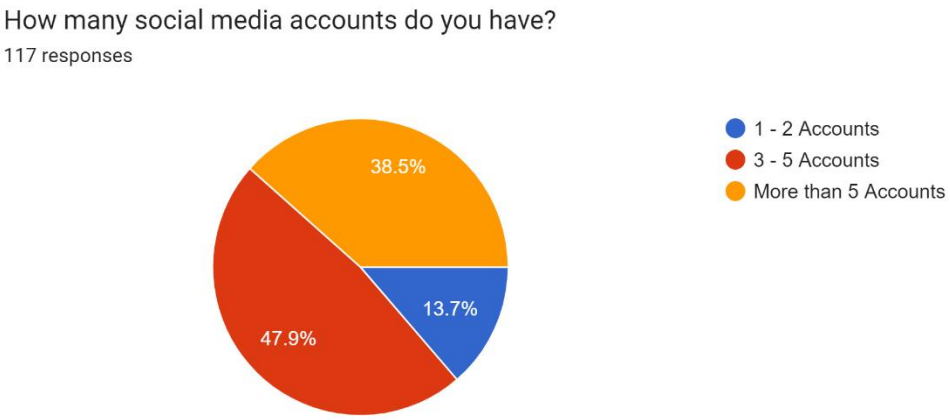
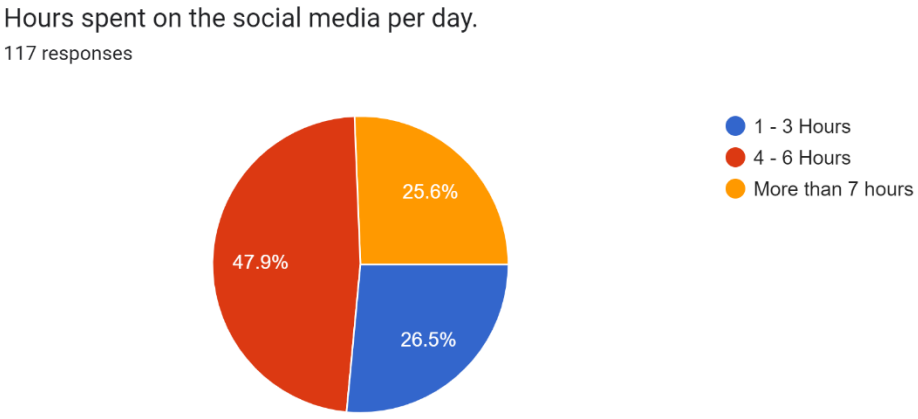


Figure 5 shows that, most of respondents are having 3-5 social media accounts and that is 47.9%. Not only that, 38.5% of all respondents use more than 5 accounts and 13.7% of respondents use only 1-2 accounts.



According to figure 6, most respondents spend their time on social media per day is 4-6 hours which represents 47.9 %. Minimum number of respondents spend their time on social

media per day is more than 7 hours which represents 25.6%. Not only that, 26.5% of respondents spend their time on social media around 1-3 hours per day.

4.3.2 Descriptive Data Analysis of Model constructs

A descriptive analysis was carried out to calculate the mean values, standard deviation and skewness of model constructs (See Table 4-1). All responses for the question items with reversed scale were transformed to the original scale using SPSS software before performing the descriptive analysis.

The analysis revealed that all the constructs have a mean value closer to the range of 4- 6. Mean measures central tendency that provides a basic idea about a certain dataset (Sekaran & Bougie, 2016, p. 282). According to the findings, most of the respondents have chosen the Likert scale value of 4 ,5 or 6 as their response to each question.

Standard Deviation measures dispersion of a dataset, which gives an idea about the span of the distribution of data (Sekaran & Bougie, 2016, p. 284). The highest value for standard deviation is recorded by Perceived Secondary Control (PSC), implied that there is a significant difference among the responses given by each respondent for the question items of PSC. Descriptive statistics further showed that Privacy Violation Experience (PVE) and Perceived Severity (PS) had datasets that vary in less amounts from the mean value, implying that there was a lesser difference among the responses given by each respondent for those question items.

4.4 Path Model

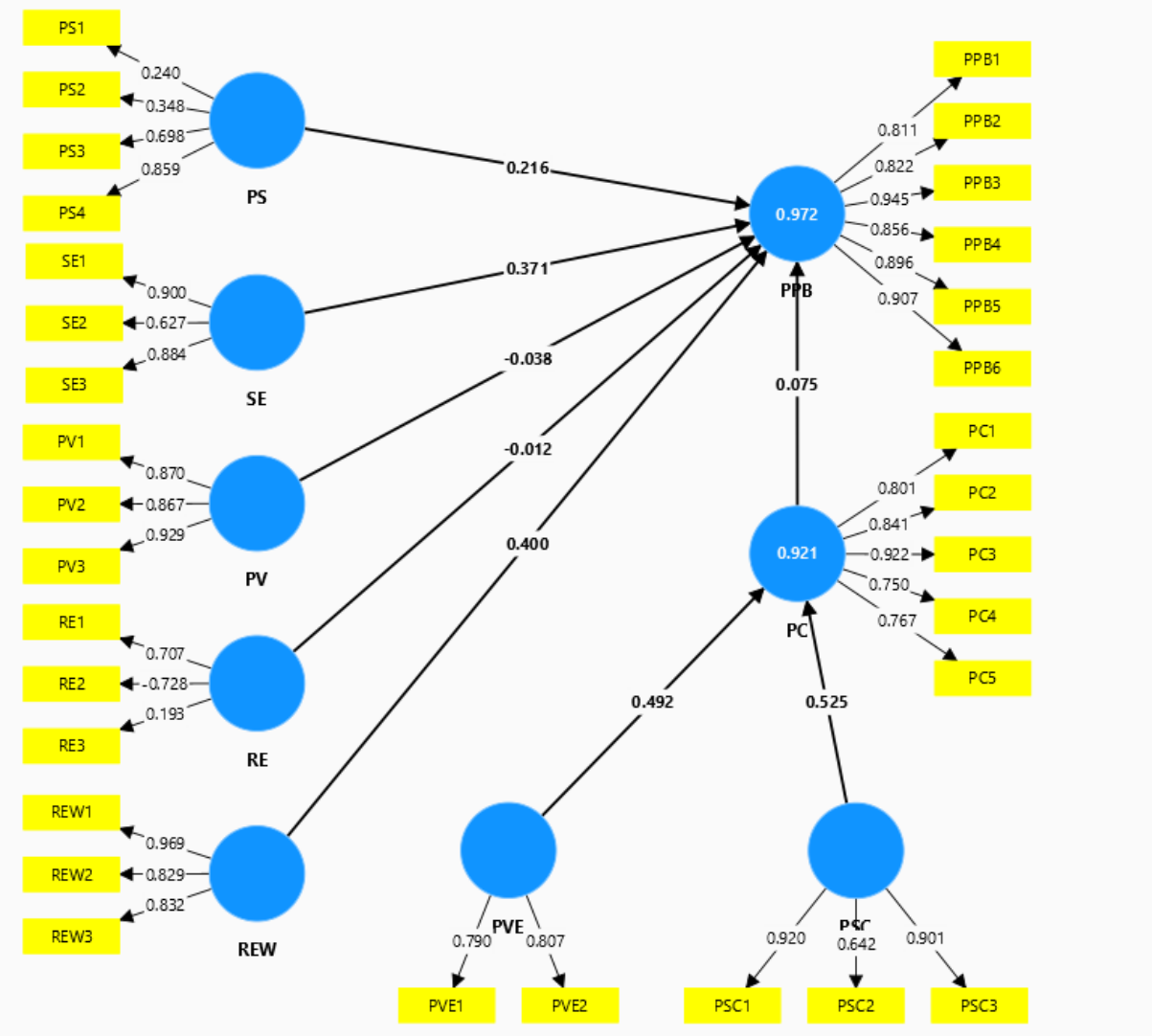
Analysis According to Hair et al. (2016, chap. 2), a “path model” is a diagram used in Structural Equation Modeling (SEM) approach to display hypotheses and the relationships between the variables. It is formed as a combination of the measurement model and the structural model. In PLS-SEM technique, both models are assessed to predict the possible outcomes (Hair et al., 2016). Following sections present measurement model analysis and structural model analyses results.

4.4.1 Measurement Model Analysis

Measurement model explains the relationship between the constructs and their measuring items (Hair et al., 2016, chap. 2). According to Hair et al. (2013), assessment of the measurement model is helpful in comparing the theory against the real world data. This can be performed by observing reliability and validity measures related to reflective measurement model obtained by running the PLS Algorithm in SmartPLS.

4.4.1.1 Item Loadings

The quality of the measurement model was tested by observing the outer loading values of the indicators (See Figure 4-6). The initial results indicated the existence of indicators with poor outer loading values below the threshold level of 0.5 (Hair et al., 2013, p. 605).



Therefore, the items with poor outer loadings (PS1, PS2, REW2, REW3) were removed from the model and the PLS Algorithm was executed again. The outer loading values of the second execution were in the range of 0.627-0.969 suggesting that indicators adequately reflected their underlying variables (Hair et al., 2013). Table 4-2 shows the outer loading values of each indicator after removing the indicators with poor outer loading values.

	PC	PPB	PS	PSC	PV	PVE	RE	REW	SE
PC1	0.801								
PC2	0.841								
PC3	0.922								
PC4	0.75								
PC5	0.767								
PPB1		0.811							
PPB2		0.823							
PPB3		0.945							
PPB4		0.856							
PPB5		0.896							
PPB6		0.907							
PS3			0.641						
PS4			0.908						
PSC1				0.92					
PSC2				0.642					
PSC3				0.901					
PV1					0.87				
PV2					0.867				
PV3					0.929				
PVE1						0.79			
PVE2						0.807			
RE1							1		
REW1								0.969	
REW2								0.829	
REW3								0.832	
SE1									0.9
SE2									0.627
SE3									0.883

4.4.1.2 Internal Consistency Reliability

Internal Consistency Reliability of the measurement model was evaluated using Composite Reliability and Cronbach's Alpha values (See Table 4-3). The lowest Composite reliability (rho_c) score was 0.758 and Cronbach's Alpha values ranged from 0.514 to 0.938 Rule of thumb for these two criteria is a value above 0.7 (Hair et al., 2016; Wong, 2013). However, According to Hair et al. (2016), Composite Reliability can be identified as a more appropriate measure of internal consistency reliability than the Cronbach's Alpha. Therefore, the model provides evidence for internal consistency reliability.

4.4.1.3 Convergent Validity

Convergent Validity explains the level of correlation among the indicators of a given construct (Hair et al., 2016). It is evaluated using the Average Variance Extracted (AVE) value for each construct. According to Hair et al. (2016, chap. 4), if an AVE value of a construct is 0.5 or above, "the construct explains more than half of the variance of its indicators". AVE values of all the constructs were above the threshold level of 0.5 (Hair et al., 2016; Wong, 2013). Thus, the convergent validity of the measurement model is established (See Table 4-3).

	Cronbach's alpha		**Composite reliability (rho_c)**	**Average variance extracted (AVE)**
PC	0.875		0.91	0.67
PPB	0.938		0.951	0.764
PS	0.514		0.758	0.618
PSC	0.759		0.867	0.69
PV	0.868		0.919	0.79
PVE	0.532		0.779	0.638
REW	0.85		0.91	0.773
SE	0.726		0.851	0.661

4.4.1.4 Discriminant Validity

Discriminant Validity explains the uniqueness of a certain construct compared to other constructs in the model (Hair et al., 2016). According to Hair et al. (2016, chap. 4), it can be evaluated based on Cross Loading values (See Table 4-4) and Fornell- Larcker Criterion (See Table 4-5).

	PC	PPB	PS	PSC	PV	PVE	RE	REW	SE
PC1	0.801	0.882	0.856	0.782	0.784	0.83	-0.223	0.871	0.836
PC2	0.841	0.727	0.521	0.631	0.838	0.761	-0.152	0.792	0.747
PC3	0.922	0.8	0.541	0.788	0.82	0.835	-0.204	0.802	0.835
PC4	0.75	0.613	0.437	0.681	0.663	0.486	-0.11	0.623	0.68
PC5	0.767	0.636	0.5	0.823	0.505	0.717	-0.17	0.597	0.656
PPB1	0.808	0.811	0.71	0.815	0.719	0.812	-0.159	0.807	0.817
PPB2	0.739	0.822	0.702	0.657	0.767	0.716	-0.213	0.738	0.766
PPB3	0.865	0.945	0.891	0.87	0.905	0.83	-0.188	0.913	0.933
PPB4	0.654	0.856	0.834	0.523	0.756	0.712	-0.192	0.863	0.718
PPB5	0.838	0.896	0.831	0.898	0.778	0.706	-0.19	0.845	0.909
PPB6	0.832	0.907	0.734	0.671	0.909	0.892	-0.178	0.895	0.865
PS1	0.035	0.096	0.24	0.243	-0.087	-0.016	0	0.111	0.121
PS2	0.111	0.173	0.348	0.14	0.156	0.141	-0.049	0.3	0.145
PS3	0.351	0.485	0.698	0.605	0.328	0.245	-0.104	0.427	0.492
PS4	0.733	0.89	0.859	0.599	0.877	0.816	-0.189	0.854	0.806
PSC1	0.798	0.739	0.632	0.92	0.683	0.697	-0.105	0.697	0.833
PSC2	0.709	0.665	0.589	0.642	0.63	0.625	-0.18	0.675	0.635
PSC3	0.74	0.699	0.603	0.901	0.687	0.604	-0.131	0.644	0.78
PV1	0.797	0.757	0.651	0.778	0.87	0.778	-0.131	0.772	0.817
PV2	0.749	0.724	0.589	0.654	0.867	0.596	-0.141	0.729	0.782
PV3	0.822	0.953	0.876	0.726	0.929	0.872	-0.203	0.932	0.903
PVE1	0.706	0.721	0.617	0.719	0.591	0.79	-0.166	0.669	0.721
PVE2	0.733	0.702	0.554	0.529	0.768	0.807	-0.14	0.746	0.664
RE1	-0.161	-0.148	-0.145	-0.104	-0.103	-0.148	0.707	-0.166	-0.12
RE2	0.13	0.154	0.143	0.127	0.161	0.095	-0.728	0.127	0.13
RE3	-0.094	-0.052	0	-0.051	-0.025	-0.13	0.193	-0.056	-0.067
REW1	0.852	0.913	0.865	0.769	0.889	0.8	-0.193	0.969	0.887
REW2	0.748	0.828	0.719	0.586	0.822	0.779	-0.19	0.829	0.758
REW3	0.8	0.805	0.696	0.792	0.71	0.76	-0.163	0.832	0.793
SE1	0.862	0.787	0.622	0.898	0.796	0.783	-0.118	0.753	0.9
SE2	0.611	0.721	0.6	0.432	0.679	0.655	-0.232	0.673	0.627
SE3	0.759	0.812	0.799	0.854	0.805	0.662	-0.1	0.813	0.884

If the outer loading values of the indicators of a certain construct are exceeding its cross-loading values, discriminant validity is established (Hair et al., 2016). Thus, it can be concluded that the discriminant validity of the model is established based on the cross loadings (See Table 4-4). Fornell- Larcker criterion was utilized to compare the square root

of AVE value of each construct against their correlations with other constructs (Hair et al., 2016, chap. 4). According to Hair et al. (2016), the square root of AVE of a certain construct must be greater than the highest correlation that it has with other constructs. When observing the values of the Fornell- Larcker criterion (See Table 4-5), it was evident that those meet the condition of the criterion. Thus, it can be concluded that the Discriminant validity of the measurement model is established.

	PC	PPB	PS	PSC	PV	PVE	RE	REW	SE
PC	0.91								
PPB	0.793	0.983							
PS	0.682	0.889	0.895						
PSC	-0.451	-0.339	-0.395	0.765					
PV	0.786	0.912	0.817	-0.435	0.989				
PVE	0.812	0.825	0.581	-0.292	0.887	0.931			
RE	0.802	0.97	0.873	-0.312	0.921	0.855	0.979		
REW	0.871	0.972	0.886	-0.456	0.917	0.822	0.943	0.974	
SE	0.89	0.935	0.838	-0.493	0.942	0.854	0.925	0.963	0.813

4.4.2 Structural Model Analysis

Structural model is a diagrammatic representation of the relationships between the constructs (Hair et al., 2016). According to Hair et al. (2013), once the measurement model is validated, structural model should be analyzed. Structural model analysis was carried out to identify the model's explanatory power and structural relationships between constructs using hypothesis testing (Hair, Ringle & Sarstedt, 2011).To identify the explanatory power of the model, Coefficient of Determination (R2) was used. R2explains the extent of variance occurred in a dependent variable due to a change in its independent variables (Hair et al., 2016). Based on the R2 value of Privacy concern, 0.71% of its variance can be explained by a change in Perceived Secondary Control and Privacy Violation Experience. 98% of variance in Privacy protection behaviour can be explained by a change in its independent variables; Perceived Severity, Perceived Vulnerability, Self-Efficacy, response Efficacy, Rewards. Since all the VIF values of the indicators were below the threshold level of 5 (Hair et al., 2016), there were no collinearity issues found in the model. After checking the collinearity issues, path coefficients and p-values were examined to validate the relationships between constructs and to assess the significance of each hypothesis. Hypotheses were tested at the 95% level of confidence ($p < 0.05$).

4.4.2.1 Hypotheses Testing

To determine the cause-effect relationship, the path coefficient values (β) were used (See Table 4-6). Path coefficient values describe how an independent variable directly affects a dependent variable in the path model (Hair, Ringle and Sarstedt, 2011)

	path coefficients	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values	Outcome
PC -> PPB	-0.23	-0.221	0.05	4.597	0	Supported
PS -> PPB	-0.044	-0.044	0.078	0.568	0.57	Not Supported
PSC -> PC	-0.234	-0.234	0.047	4.999	0	Supported
PV -> PPB	-0.11	-0.105	0.078	1.409	0.159	Not Supported
PVE -> PC	0.744	0.744	0.032	23.176	0	Supported
RE -> PPB	0.503	0.552	0.156	3.218	0.001	Supported
REW -> PPB	0.727	0.685	0.135	5.403	0	Supported
SE -> PPB	0.115	0.095	0.129	0.894	0.372	Not Supported

The analysis of the path coefficients reveals significant insights into the relationships between various predictors and outcomes in the model. The path coefficient for PC -> PPB is -0.23, indicating a negative relationship between PC and PPB, which is statistically significant with a T statistic of 4.597 and a P value of 0. This supports the hypothesis that an increase in PC leads to a decrease in PPB. Conversely, the path coefficient for PS -> PPB is -0.044, suggesting a very weak inverse relationship that is not statistically significant, as evidenced by a T statistic of 0.568 and a P value of 0.57, thus not supporting the hypothesis. The relationship between PSC and PC is represented by a path coefficient of -0.234, with a T statistic of 4.999 and a P value of 0, indicating a statistically significant negative effect, thereby supporting the hypothesis. However, the PV -> PPB path coefficient of -0.11, with a T statistic of 1.409 and a P value of 0.159, does not show statistical significance, leading to the hypothesis being unsupported. On the other hand, PVE -> PC demonstrates a strong positive relationship with a path coefficient of 0.744, supported by a very high T statistic of 23.176 and a P value of 0, confirming the hypothesis that PVE positively affects PC. The path coefficient for RE -> PPB is 0.503, with a T statistic of 3.218 and a P value of 0.001, indicating a statistically significant positive relationship, thus supporting the hypothesis. Similarly, REW -> PPB shows a strong positive effect with a path coefficient of 0.727, a T statistic of 5.403, and a P value of 0, supporting the hypothesis. Lastly, the SE -> PPB path coefficient of 0.115, with a T statistic of 0.894 and a P value of 0.372, indicates a weak and statistically insignificant positive relationship, leading to the hypothesis being unsupported. These

findings highlight the significant factors influencing PPB and PC, providing valuable insights into their underlying dynamics.

4.5 Discussion of Findings

The findings of this study provide nuanced insights into the complex dynamics of privacy concerns and behaviors. The negative relationship between Privacy Concern (PC) and Perceived Privacy Behavior (PPB) supports the hypothesis that higher privacy concerns lead to reduced privacy behaviors, aligning with the privacy calculus theory and previous research by Xu et al. (2011). However, the weak and statistically insignificant inverse relationship between Perceived Severity (PS) and PPB contrasts with studies like Dinev and Hart (2006), suggesting that the perceived severity of potential privacy violations might not significantly impact behavior unless actual experiences occur. In line with Bandura's (1997) theory, the significant negative relationship between Perceived Secondary Control (PSC) and PC emphasizes the importance of empowering users with control over their personal information to reduce privacy concerns. Contrary to Smith et al. (2011), the non-significant relationship between Privacy Violation Experience (PVE) and PPB indicates that past privacy violations may heighten awareness but not necessarily change behavior, possibly due to feelings of resignation or helplessness. The strong positive relationship between PVE and PC confirms that privacy violations heighten concerns, underscoring the need for organizations to effectively manage and prevent such violations to alleviate long-term concerns. The positive and significant relationships between Reward (RE) and PPB, and Reward Expectation (REW) and PPB, support the incentive-based privacy model proposed by Acquisti et al. (2015) and Lin et al. (2012), highlighting that rewards and expectations of future rewards can encourage privacy-protective behaviors. However, the weak and statistically insignificant positive relationship between Self-Efficacy (SE) and PPB suggests that self-efficacy might not play as critical a role in this context as previously thought, contrasting with findings by Eastin and LaRose (2000). These findings have important implications for both researchers and practitioners. Researchers should further investigate the factors influencing privacy behavior, particularly the roles of perceived control and reward mechanisms, while practitioners should focus on designing user-friendly privacy settings, providing tangible rewards, and managing privacy violation experiences effectively to enhance privacy-protective behaviors. Overall, this study contributes to the growing body of knowledge on privacy concerns and behaviors, highlighting the need for further exploration of these complex dynamics to better address users' privacy concerns and foster a more secure and trustful environment.

4.6 Summary

This chapter presented the data analysis and the discussion of findings of the study. It presented the demographic profile of the sample based on factors such as gender, age, academic background and familiarity with technology. Next, it presented the findings of descriptive data analysis of the model constructs. Further, the chapter presented the measurement model analysis and structural model analysis findings. Based on the measurement model analysis, reliability and validity measures were established. Out of six hypotheses formulated, four hypotheses were supported (H3, H4, H5, H6, H7 and H8) while two hypotheses (H1 and H2) were not supported. The discussion of the findings was presented after presenting the hypotheses testing results.

References

- Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. Privacy enhancing technologies, 36-58.
- Adhikari, K., & Panda, R. K. (2017). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. Journal of Marketing Theory and Practice, 25(4), 427-443.
- Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9).
- Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of Protection Motivation Theory to adoption of protective technologies. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 40(4), 44-51.
- Crowe, E., & Higgins, E. T. (1997). Regulatory focus and strategic inclinations: Promotion and prevention in decision-making. Organizational Behavior and Human Decision Processes, 69(2), 117-132.
- Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83-108.
- Florack, A., Friese, M., & Scarabis, M. (2013). Regulatory focus and reliance on implicit preferences in consumption contexts. Journal of Consumer Psychology, 23(4), 556-563.
- Hanus, B., & Wu, Y. A. (2015). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. Journal of Information Systems Security, 11(3), 41-62.
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.
- Higgins, E. T. (1997). Beyond pleasure and pain. American Psychologist, 52(12), 1280-1300.

- Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93-114.
- Suhaimi, S. N., & Othman, N. F. (2017). Determinants of Privacy Protection Behavior in Social Networking Sites. Journal of Information Technology Research, 10(2), 21-39.
- Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information on purchasing behavior: An experimental study. Information Systems Research, 22(2), 254-268.
- Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. Bulletin of Science, Technology & Society, 28(1), 20-36.
- Woon, I. M., Tan, G. W., & Low, R. T. (2005). A protection motivation theory approach to home wireless security. Proceedings of the Twenty-Sixth International Conference on Information Systems, 367-380.
- Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. Journal of the American Society for

- Abdul Hameed, M., & Asanka Gamagedara Arachchilage, N. (n.d.). On the Impact of Perceived Vulnerability in the Adoption of Information Systems Security Innovations.

- Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. Journal of Global Marketing, 31(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

- Appel, H., Gerlach, A. L., & Crusius, J. (2016). The interplay between Facebook use, social comparison, envy, and depression. In Current Opinion in Psychology (Vol. 9, pp. 44–49). Elsevier. https://doi.org/10.1016/j.copsyc.2015.10.006

- Asanka, N., & Arachchilage, G. (n.d.). User-Centred Security Education: A Game Design to Thwart Phishing Attacks. https://www.researchgate.net/publication/283762014

- Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online Privacy Concerns and Privacy Management: A Meta- Analytical Review. Journal of Communication, 67(1), 26–53. https://doi.org/10.1111/jcom.12276

- Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: the importance of Internet skills for online privacy protection. Information Communication and Society, 20(8), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

- Chen, H. T., & Chen, W. (2015). Couldn't or wouldn't? the influence of privacy concerns and self-efficacy in privacy management on privacy protection. Cyberpsychology, Behavior, and Social Networking, 18(1), 13–19. https://doi.org/10.1089/cyber.2014.0456

- Choi, B. C. F., Jiang, Z., Ramesh, B., & Dong, Y. (2015). Privacy Tradeoff and Social Application Usage. 2015 48th Hawaii International Conference on System Sciences, 304–313. https://doi.org/10.1109/HICSS.2015.44
- Dienlin, T., & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSs: Analyzing Self- Disclosure and Self-Withdrawal in a Representative U.S. Sample. Journal of Computer-Mediated Communication, 21(5), 368–383. https://doi.org/10.1111/jcc4.12163
- Feng, Y., & Xie, W. (2014). Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. Computers in Human Behavior, 33, 153–162. https://doi.org/10.1016/j.chb.2014.01.009
- Fida, R., Tramontano, C., Paciello, M., Ghezzi, V., & Barbaranelli, C. (2018). Understanding the Interplay Among Regulatory Self-Efficacy, Moral Disengagement, and Academic Cheating Behaviour During Vocational Education: A Three-Wave Study. Journal of Business Ethics, 153(3), 725–740. https://doi.org/10.1007/s10551-016-3373-6
- Hanus, B., & Wu, Y. "Andy." (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. Information Systems Management, 33(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842
- Jain, S., & Agrawal, S. (2021). Perceived vulnerability of cyberbullying on social networking sites: effects of security measures, addiction and self-disclosure. Indian Growth and Development Review, 14(2), 149– 171. https://doi.org/10.1108/IGDR-10-2019-0110
- Lee, H., & Kobsa, A. (2016). Understanding user privacy in Internet of Things environments. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), 407–412. https://doi.org/10.1109/WF-IoT.2016.7845392
- Litt, E. (2013). Understanding social network site users' privacy tool use. Computers in Human Behavior, 29(4), 1649–1656. https://doi.org/10.1016/j.chb.2013.01.049M. Vatka. (2019). INFORMATION BEHAVIOUR and DATA SECURITY : Health Belief Model Perspective.
- Åbo Akademi University. Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. Journal of Marketing, 81(1), 36–58. https://doi.org/10.1509/jm.15.0497
- Mohamad Ali, N., Banhawi, F., & Mohd Judi, H. (2012). User engagement attributes and levels in facebook. Article in Journal of Theoretical and Applied Information Technology, 15(1). https://www.researchgate.net/publication/236336133
- Mwagwabi, F., McGill, T., & Dixon, M. (2018). Short-term and long-term effects of fear appeals in improving compliance with password guidelines. Communications of the

Association for Information Systems, 42(1), 147–182. https://doi.org/10.17705/1CAIS.04207

- Palladino, B. E., Menesini, E., Nocentini, A., Luik, P., Naruskov, K., Ucanok, Z., Dogan, A., Schultze- Krumbholz, A., Hess, M., & Scheithauer, H. (2017). Perceived severity of cyberbullying: Differences and similarities across four countries. Frontiers in Psychology, 8(SEP). https://doi.org/10.3389/fpsyg.2017.01524
- Park, N., & Kim, Y. (2020). The Impact of Social Networks and Privacy on Electronic Word-of-Mouth in Facebook: Exploring Gender Differences. In International Journal of Communication (Vol. 14). http://ijoc.org.
- Rains, S. A., & Scott, C. R. (2007). To identify or not to identify: A theoretical model of receiver responses to anonymous communication. Communication Theory, 17(1), 61–91. https://doi.org/10.1111/j.1468-2885.2007.00288.x
- Smit, E. G., Van Noort, G., & Voorveld, H. A. M. (2014). Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. Computers in Human Behavior, 32, 15–22. https://doi.org/10.1016/j.chb.2013.11.008
- Suhaimi, S. N., Fadzilah Othman, N., Syahirah, R., Anawar, S., Ayop, Z., Feresa, C., Foozy, M., Maklumat, F. T., & Komunikasi, D. (2020). Determinants of Privacy Protection Behavior in Social Networking Sites. In IJACSA) International Journal of Advanced Computer Science and Applications (Vol. 11, Issue 12). www.ijacsa.thesai.org
- Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. Information and Management, 52(4), 506–517. https://doi.org/10.1016/j.im.2015.03.002
- Wang, D. (2019). A study of the relationship between narcissism, extraversion, body-esteem, social comparison orientation and selfie-editing behavior on social networking sites. Personality and Individual Differences, 146, 127–129. https://doi.org/10.1016/j.paid.2019.04.012
- Wang, T., Duong, T. D., & Chen, C. C. (2016). Intention to disclose personal information via mobile applications: A privacy calculus perspective. International Journal of Information Management, 36(4), 531–542. https://doi.org/10.1016/j.ijinfomgt.2016.03.003
- Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2018). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. Information & Management, 55(4), 482–493. https://doi.org/10.1016/j.im.2017.11.003

- Adhikari, K., & Panda, R. K. (2017). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. Journal of Marketing Theory and Practice, 25(4), 427-443. https://doi.org/10.1080/08911762.2017.1412552
- Hanus, B., & Wu, Y. A. (2015). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. Journal of Information Systems Security, 11(3), 41-62. https://doi.org/10.1080/10580530.2015.1117842
- Higgins, E. T. (1997). Beyond pleasure and pain. American Psychologist, 52(12), 1280-1300.
- Suhaimi, S. N., & Othman, N. F. (2017). Determinants of Privacy Protection Behavior in Social Networking Sites. Journal of Information Technology Research, 10(2), 21-39. https://doi.org/10.1080/10580530.2015.1117842