End-User Security & Privacy Behaviour on Social Media: Exploring Posture, Proficiency & Practice

By

Amir Akbari Koochaksaraee

A thesis submitted to the

Faculty of Graduate and Postdoctoral Studies

In partial fulfilment of the degree requirements of

Master of Science in System Science

University of Ottawa

Ottawa, Ontario, Canada

April 2019

Abstract

Security and privacy practices of end-users on social media are an important area of research, as well as a top-of-mind concern for individuals as well as organizations. In recent years, we have seen a sharp increase in data breaches and cyber security threats that have targeted social media users. Hence, it is imperative that we try to better understand factors that affect an end-user's adoption of effective security safeguards and privacy protection practices.

In this research, we propose and validate a theoretical model that posits several determinants of end-user security and privacy practices on social media. We hypothesize relationships among various cognitive, affective and behavioral factors identified under the themes of posture, proficiency, and practices. These constructs and hypotheses are validated through empirical research comprising an online survey questionnaire, and structural equation modeling (SEM) analysis.

The key findings of this study highlight the importance of cyber threat awareness and social media security and privacy self-efficacy, which have a direct impact on end-user security and privacy practices. Additionally, our research shows that use of general technology applications for security and privacy impacts the adoption of security and privacy practices on social media. In totality, our research findings indicate that proficiency is a better predictor or security and privacy practices as compared to the posture of an end-user. Factors such as privacy disposition, privacy concerns, and perceived risk of privacy violations do not have as significant or direct effect on security and privacy practices.

Based on our research findings, we provide some key take-aways in the form of theoretical contributions, suggestions for future research, as well as recommendations for organizational security awareness training programs.

Acknowledgments

Completion of master thesis was like passing a long road full of hardships that I shared with many wonderful people. It is always during the hard period that you can fully understand the value of having a great mentor, family and friends.

Foremost, I would like to express my deepest gratitude to Dr. Umar Ruhi. Despite having a heavy workload, he helped refine my research, and guided me throughout the duration of my studies with his critical and instructive comments. In addition, his immense knowledge and care about details were the key factors for successful completion of the work.

I have been blessed with a supportive family who always encouraged me in the challenging times. Without whom I could not have made it here. My greatest gratitude to my mother who her love and encouragements accompanied me thought out my way for following my dreams. I would like to thank my father and brother for their support in this project.

Contents

List of tables

List of figures

1. Introduction

Social Media plays a significant role in people's lives all around the world, and it is a technology that has affected and changed many of our personal and professional activities and interactions. Leading social media platforms such as Facebook, Twitter and LinkedIn have become the preferred method of communication for many users, and users spend a significant amount of time posting and reading content, and interacting with other end-users through these platforms (Z. Zhang & Gupta, 2018).

Based on recent reports by Statistica (2019), the total number of social media users is estimated to be around 2.77 billion as of January 2019, whereas in 2010, it was about 970 million. This represents a three-fold increase in the user base from 2010 to 2019. As of January 2019, Facebook ranked first in the social media market with about 2.271 billion users. The second and third-ranked social networks are YouTube and WhatsApp with 1.9 and 1.5 billion users respectively, and LinkedIn has 303 million active users, a threefold increase in just three years (Statistica, 2019). Based on a survey by Gruzd, Jacobson, Mai, & Dubois (2018), the majority of online Canadian adults (94%) have at least one social media account. Facebook is the most prevalent with 84% of Canadian adults using it, followed by YouTube with 59% and LinkedIn with 46%.

The use of social media has not been limited to communication between people, but has spread to fields like marketing and advertising, academia and education, and politics. Social media helps firms to form a virtual environment to interact with their stakeholders including customers, clients, business partners, as well as the general public (Culnan, Mchugh, Zubillaga, Uarterly, & Xecutive, 2010). This exponential increase of the number of users has prompted social network companies to provide personalized services, friends/content recommendations and upgrade users' quality of experience (Z. Zhang & Gupta, 2018).

With the rise of social media use among end-users and businesses alike, the frequency and prevalence of cybersecurity attacks, data breaches and privacy violations have also increased (Krishnamurthy & Wills, 2008). Attackers now have a new platform to target end-users and to gain unauthorized access to personal information (Gharibi & Shaabi, 2012).

In 2018, the growth rate of social media fraud was 43% compared to the number and scale in the previous year. A notable incident is Quora putting 100 million user accounts on the verge of a data breach because of unauthorized access. In September, 2018, a security breach of 90

million user accounts on Facebook occurred. Cybercriminals are abusing social networks like Facebook, Instagram and WhatsApp for their sinister intentions more than ever.

End-users themselves can be a source of security and privacy risks, since their carelessness, lack of awareness of threats, or negligence can lead to security and privacy breaches. Even unintentional actions can lead to significant setbacks or adverse outcomes in terms of security and privacy. Cybercriminals often count on users' lack of awareness or carelessness in order to obtain their personal information or gain unauthorized access to their social or financial accounts (trendmicro, 2018).

As the technical aspect of the social network defence system improves, the attackers apply different strategies. Social engineering is one of the effective ways for cybercriminals to bypass security protocols that they may not be able to overcome through technology alone. Cybercriminals use social engineering techniques to abuse human trust and elicit information based on human behavioural mistakes (Australian Cyber Security Centre, 2017). Social engineering can be tailored to specific people through targeted phishing messages. Other types of cyber threats include those that steal end users' login details and account numbers through account takeovers. In even worse scenarios, identity thefts could be perpetrated by attackers who introduce themselves as the victim to undertake actions using another's identity (Australian Cyber Security Centre, 2017).

The capability of sharing information between different social networks, location sharing, and development of information sharing habits by end users makes it even more probable for others to gain access to potentially sensitive information. The combination of these technological advances with enthusiastic end users who intend to interact with other people in social networks makes social media an environment presenting very high-level security and privacy risk (Tayouri, 2015). This opportunity makes social networks attractive for cybercriminals, due to the opportunity to produce a significant profit with low risk of identification.

The risks and problems mentioned above endanger end users' security control and personal privacy protection, and this is why it is crucial to study and understand human behaviour related to social media security and privacy. Such research will allow us to devise sufficient end-user safeguards for protection against cyber threats, and help identify ways to influence user behaviour through attitudinal changes.

There are many mitigation strategies in the form of policies and guidelines to reduce social media security and privacy risks (He, 2012). Policies and guidelines specify the appropriate behaviours such as the acceptable use of social media, content sharing instruction, privacy settings, password management, etc., that help end users to establish proper practices toward privacy and security in social media. However, the policies and guidelines are insufficient to counter cyber threats. The risk of cyber threats can exist when end users receive training but they do not know how to implement it in a real scenario. These issues show the criticality of the establishment of complementary layers of education and training for end users to ensure they are capable of adopting adequate privacy and security practices.

In this study, we study users' perceptions, attitudes and behaviours towards mitigating security and privacy threats within the context of social media. Toward this objective, a theoretical model is developed and empirically validated to uncover the influential constructs that affect social media security and privacy practices.

1.1. Research Rationale & Objectives

Social network companies invest financially and technically in cybersecurity safeguards as well as end-user training and education to prevent breaches (Rhee, Kim, & Ryu, 2009). To make the most of these investments, we need to first understand the potential causes for different types of social media security and privacy practices, and understand the role of relevant personal cognitive and affective factors. This study aims to contribute towards this type of research and provide insights that can potentially improve security awareness training, the overall use of end-user security controls, and privacy protection tools for social media.

While other studies have attempted to separately investigate security practices (Anwar et al., 2017; Egelman & Peer, 2015; Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018; Wan, Wang, & Haggerty, 2008) and privacy behaviours (Bada, Sasse, & Nurse, 2015; Bolhuis & Giraldeau, 2005; Dolan, Halpern, Hallsworth, King, & Vlaev, 2010; Halevi et al., 2016), little attention has been paid to investigating these concepts together. Instead, they either considered a limited number of predictor constructs like risk perception (Van Schaik, Jansen, Onibokun, Camp, & Kusev, 2018) or used security and privacy perception as a predictor and not as the final step of end users' interaction toward cyber threats in social media (Shin, 2010). Moreover, there have been few studies examining critical security and privacy constructs in the context of social media, studying the variables related to the general concept of cybersecurity. In addition to the

existing literature gaps, this study aims to define some layers for independent constructs, and to identify the effect of general online security and privacy constructs on specific social media security and privacy constructs.

In this study, we study users' perceptions, attitudes and behaviors towards mitigating security and privacy threats within the context of social media. Toward this objective, a theoretical model is developed and empirically validated in order to find the influential constructs that affect social media security and privacy practices.

1.2. Conceptual Framework

To study the effects of some predictors of end users' security and privacy practices in social media, a theoretical model is formulated comprising three major components: Posture, Proficiency and Practice. The major components of the conceptual framework are summarized in Table 1-1. The table represents the constructs associated with each dimension, their definition and origin.

Table 1-1 Conceptual Framework and its components

Dimension	Constructs	Definition
Posture	Online Privacy Disposition (OPD)	An inherent personal trait that set the limitation of control of own cyberspace (Xu, Dinev, & Smith, 2011)
	Social Media Privacy Concern (SMPC)	End users' sensitivity and fear about social media privacy threats and unauthorized third-party access to their information
	Social Media Risk Perception (SMRP)	End users' extent of concern and perception toward cyber threats
Proficiency	Social Media Security Threat Awareness (SMSTA)	Level of familiarity with security threats in social media
	Technological Self-efficacy (TSE)	User's perception of their control and capability over their information (Bada et al., 2015)
	Social Media Security & Privacy Self-efficacy (SMSPSE)	Technological capability over social media tools
Practice	Online Security Tools use (OSTU)	Security tools and techniques that end users use to protect their security in an online information system
	Online Privacy Tools use (OPTU)	Techniques and activities that end users undertake to increase their information privacy
	Social Media Security Practices	Consists of: - Authentication (Auth): Login and account access behaviour on social media - Security Settings (Sec Sett): Proactive action towards security threats
	Social Media Privacy Practices	Consists of: - Discoverability (Disc): Profile access or location detection through a search engine - Communication (Comm): limiting other users' access to our profile - Content Sharing (Content): managing what shared with whom in social media

Based on our model, Posture and Proficiency factors affect social media security and privacy practices. It also considers the effect of online security and privacy behaviour on social media security and privacy practices.

1.2.1. Posture Factors

The first component of the framework is Posture, which we define as users' mindsets and perceptions toward cyber risk and threats. According to the structure, Posture factors directly or indirectly affect Social Media Security and Privacy Practices. As illustrated in Table 1-1, Online Privacy Disposition, Social Media Privacy Concern and Social Media Risk Perception are important factors related to Posture.

1.2.2. Proficiency factors

Proficiency is the second component of our framework, which represents end users' knowledge and capability in the general online environment and the social media environment. It is divided into two factor groups. One group is for general online proficiency constructs, designated as Technological Self-efficacy in our model. The other group is called Social Media Proficiency constructs, consisting of Social Media Security Threat Awareness and Social Media Security & Privacy Self-efficacy.

Proficiency reflects end users' perceptions toward security threats, and their control and ability toward cyber threats in general online and social media environments.

1.2.3. Practice Factors

The third component of our conceptual model is called Practice. This component has two groups – general online and specific social media factors – and represents the behavioural aspects of end users regarding security and privacy. The first group consists of Online Security Tools Use (OSTU), and Online Privacy Tools Use (OPTU), which represents end-users' behaviour toward general online security and privacy threats.

Additionally, we address Social Media Security Practices and Social Media Privacy Practices in the second group, which are the major factors investigated in this model. In the context of our research, privacy and security are related to the behavioural aspect of human traits, and they are considered as practical specifications.

1.3. Research Questions & Approach

This research attempts to answer the following questions about end-users security and privacy behaviour on social media:

- RQ1: What are the pertinent cognitive, affective and behavioural factors associated with end-user security and privacy practices on social media?
- RQ2: How does general online security and privacy behaviour influence social media security and privacy practices?
- RQ3: What are the interrelationships among various cognitive, affective and behavioural factors associated with end-user security and privacy practices on social media? (Identified through answering RQ1).

RQ1 will primarily be answered through a comprehensive review of the relevant literature. RQ2 and RQ3 will utilize the findings from the literature review to develop a theoretical model with relevant constructs and hypotheses. Using a deductive approach, the theoretical model will be empirically validated through a survey questionnaire completed by a cross-section of social media end-users.

1.4. Structure of the Research

This thesis is organized as follows. The first chapter outlines the premise, rationale, objectives, and research questions for this study. Chapter 2 provides a literature review of various socio-technical factors related to end-user security and privacy practices on social media. Based on the literature review, Chapter 3 presents the theoretical model and describes the research design and methods used to validate the model. The results from our empirical investigation are presented in Chapter 4. Finally, Chapter 5 provides a detailed discussion of the research findings, and highlights the contributions to theory and implications for practice.

2. Literature Review

2.1. Security and privacy in social media

The rapid increase in using social media symbolizes the fact that these networks are becoming the preferred way of connecting, communicating and information sharing for many people, and this is an essential facet of modern daily life (Z. Zhang & Gupta, 2018).

Despite the popularity of the massive social networks like Facebook and Twitter, many other social networks with many different functions have emerged to attract a specific group of users. Some popular social networks like Tumblr and Instagram have emerged, which have been used by almost everyone. However, the new social networks can be categorized based on their applicability, for example:

- anonymous social networks like Whisper and Wut,
- those designed for teens like Tumblr,
- those capable of location sharing like Foursquare and Yelp,
- dating apps like Tinder and Bumble,
- video sharing social networks like YouTube and Vimeo (Moreau, 2019).

The multi-functional nature of social networks highlights the fact that these networks are not only useful for regular communication (Reuben, 2008). Table 2-1 illustrates the major features of some popular social networks. It should be noted that there is no clear boundary between business/professional and private activities in social networks; thus, the risk of harm affects both the users and the companies they are working at (Oehri & Teufel, 2012). From the executives' perspective, some advantages of social media are cutting communication cost, powerful expert finding tools, and marketing that is more productive. Reaching these and various other benefits of social media require a procedure to guide users (Schlienger & Teufel, 2002). Based on a survey by Oehri & Teufel (2012), two-thirds of Swiss companies have been active in social media, even though only 30% of these companies have had a social media communication procedure, instructing the proper behaviour toward social networks. The percentage also decreases to 22% for the established social media strategy.

Table 2-1 - features of some social networks (Moreau, 2019)

No.	SN title	Advantages	Disadvantages
1	Facebook	- Capability of setting groups - Massive community - Easy to find long lost friends - Integrated messenger - Exciting groups and pages to join	- Highly addictive - Difficult to keep up with updates - Complicated to adjust privacy
2	Twitter	- the real-time, public microblogging network - Vast community - Easy to use - Get updates from major brands - Integrates with third party services	- Can feel disorganized - Not easy to find specific people - Difficult to develop followers
3	LinkedIn	- A social network for professionals - Easy to make new connections - Simple to find people you know - Well organized website - The capability of posting job adds & applying to jobs	- Too much information at times - Frequent messages from marketers
4	Google+	- Useful for network - Improves search authority - Integrated with hangouts - Easy to set up a profile	- Not as popular as other platforms - The interface is not intuitive - Cannot combine with other social networks
5	Snapchat	- Very easy to use - Millions of users - Loaded with editing and filtering features - More personal and intimate than other platforms	- Small demographic of users - Content disappears every day - A large amount of useless content - Difficult to find people you know
6	Instagram	- More interesting than most social networks considering the real-time photo and video sharing - Useful filtering feature - See into the lives of others	- Strictly enforces policies - Ads can be a nuisance - Many images are over edited
7	Pinterest	- Very entertaining to use. - New ideas to discover. - Loaded with inspiring messages. - Intuitive interface - Becoming a massive influencer in social shopping	- Loaded with affiliate posts. - Limited range of topics - Can get cluttered

The daily usage of social media requires some considerations for using it effectively, and monitoring and preventing threats that violate security and privacy, such as cyberbullying or identity theft (Van Schaik et al., 2018). This risk usually impacts non-specialist end-users, and the high probability of these types of incidents make it necessary to develop models of human behaviour in social media (Garg & Jean Camp, 2015). To study and analyze human factors in cyber-security, it is useful to understand the concepts and terminology in this field, and the effect of human factors on the primary construct in cybersecurity (Veksler et al., 2018). Besides the various benefits of Social Network sites, end users' security and privacy have emerged as two major issues in these platforms.

2.1.1. Social Media Security

Security is about actions taken to protect information, accounts and devices from unauthorized entities, and be assured that the information will be preserved and shared by granted access, and the system is always available for use (Rhee et al., 2009).

It can be said that technical tools are critical for the success of an effective security system, which will involve a vast domain of encryption, access control techniques, and monitoring devices. However, even with reliable software and cyber systems, there is always the vulnerable human factor (Jones & Colwill, 2008). For example, there can be a high-standard authentication system, but if users use a very easy-to-guess password, this nullifies the capability of the system toward confidentiality.

2.1.1. Social Media Privacy

Security threats occur whenever an unauthorized entity gains access to a website, platform or a user's account. On the other hand, Privacy involves undeclared access to private information, and does not necessarily consist of a security breach. This fact shows that privacy issues can occur by just watching a person type his/her password to log into a social network (Shin, 2010).

Internet Privacy is about the control of people over their personal information and the procedure of sharing their knowledge with others. This concept has been highlighted ever since the capabilities of search and collection of online personal information emerged in social networks (A. L. Young & Quan-Haase, 2013). Social networks help end users to share personal information such as sexual preferences, political and religious views, phone numbers, occupations, and photographs. When users agree to an acceptable use policy, they are agreeing to provide

accurate information about themselves, and also grant the social media provider the right to sell that information (Baden et al., 2009).

The social network always offers privacy settings and sharing filters, which are usually different among platforms and confusing for ordinary users. The other possible issue is related to changing or updating privacy settings, in addition to the probability of misunderstanding the environment. End users need to know the appropriate level of privacy required in social networks, which is different for each user (Clark, 2012).

Both types of security and privacy breaches are increasing in social networks, mainly because anyone who violates a social network's security, gains access to the private information of users in that network (Dwyer, Hiltz, & Passerini, 2007).

2.1.2. Research Studies about Human security and Privacy Behaviour in Social Media

Research about the human aspect, known as the weakest link of cybersecurity, can be grouped into three categories; the first category is the conceptual identification of the weakest link. The second category consists of works examining a broad set of factors that are related to cyber threats, to find the relationship between human traits and cybersecurity breaches (Yan et al., 2018). It can be a relationship between gender with self-efficacy or cybersecurity behaviours, which showed the higher level of self-efficacy that women report compared to men, showing the effect gender can have on users' attributes and self-reported security behaviours (Anwar et al., 2017). The third category of research attempts to design cybersecurity technologies to mitigate the human-related risks and develop cyber training and education programs to improve this delicate aspect of the cyber environment. There can be some security imposed tools to direct users toward more secure behaviour, but it can make users frustrated (Veksler et al., 2018), and in the case of social media, reduce the number of users.

However, some items should be noted when examining a human entity in cyber security. The first involves the full range of users with many different attributes and characteristics, which requires identifying the exact points of end users' weaknesses. In addition, considering that weakness recognition is a qualitative process, it should be converted to some quantitative assessment. The other concern is related to the fact that there are various cyber threats such as password intrusion, privacy disclosure, malware infections, and service disruption, which need

further investigation with respect to the possibility of different security behaviours toward these hazards (Yan et al., 2018).

One of the problematic aspects of cybersecurity is its paradoxical nature, like the dilemma many corporations deal with: whether it is worth investing in cybersecurity compared to the loss of data. The other paradox involves the advantages of data collected and used for improvement in the quality of life of citizens compared to the abuse of data by hackers. However, the problem in end users' scale is about them not being worried about the risks of a data breach, because they have not experienced any impact until the attack happens, at which point it is too late to take some preventive actions. This means that the end-user is known as the weakest entity in cybersecurity (De Bruijn & Janssen, 2017).

2.1.3. Security and privacy threats in social media

In social media, there is a dependency of privacy on security; it is possible to have security without privacy, but it is different when it comes to having privacy without security (Symanovich, 2019).

Social media privacy threats can be exemplified by the situation that end users' posting in social media can be available to all followers or subscribers. These threats cannot be prevented because end users' connections are able to copy, use, or republish the data and make it available to the public. As well, social network search engines can index users' personal information, which is a breach of privacy, which can be used by attackers to gain access to end users' personal information. This weakness can help cyber criminals to guess victims' passwords and authentication information and get access to their accounts, which is a matter of social media security threats (Boyd, 2008).

With the advance of technology, our dependency on technology makes us more vulnerable to security threats in social networks. Data breaches occur because of insufficient security, and its growing existence cannot be ignored (Symanovich, 2019). On the other hand, end users usually make mistakes and risks when they use social networks like misusing corporate programs, unauthorized access, password management mistakes, transferring sensitive information between their work and personal computers, and using unsafe programs. These sorts of carelessness can raise the probability of a data breach when combined with end users' excessive trust of social networks (Gharibi & Shaabi, 2012). Based on Lemos (2013), it is estimated that

roughly 90% of data breaches are related to end users in the cyber environment choosing passwords in a careless manner.

Proportional to the increasing number of end users, the number of cyber-attacks have also increased. These attacks can be operated for many purposes, such as unauthorized messages, stealing money from victims' accounts, cyber bullying, etc. (Gharibi & Shaabi, 2012). However, a cyber-threat can be unintentional or intentional, targeted or non-targeted, and it can come from a variety of sources. We present some major cyber threats with examples of related incidents for each in recent years.

2.1.3.1. Phishing

A phishing attack is a practice of sending emails that seem trustworthy in order to gain users' personal information or direct them to do something that the hacker wants them to do. The other type of phishing attack is to send a URL to the users that trick them into downloading malware or unwanted programs. One of the most targeted types of Phishing is called Spear Phishing, in which the attacker first researches the targets and creates messages that look personal and relevant. An example of spear phishing is sending an email that has been made to look like your manager sent it (Melnick, 2018). The capability of data mining through the social network to gather people's preferences, common interests and relationships makes these platforms potential places for phishing (Debatin, Lovejoy, Horn, & Hughes, 2009).

In 2016, Yahoo! reported two significant data breaches. One incident occurred in 2014 compromising half a billion-user accounts; the second was in October 2017, which disclosed all 3 billion users' accounts. The tool of the second phishing attack was a simple spear-phishing email to a semi-privileged engineer. These breaches were the most massive discovered breaches in the history of the internet, compromising user details, including names, e-mail addresses, phone numbers, security questions, birth info, even passwords. These scandals were made public to criticize Yahoo!; the news impacted the company's share price dramatically, and it was finally sold to Verizon (Allen, 2018).

2.1.3.2. Social Engineering

Social engineering is the type of attack that deceives people into giving up their confidential information like social security number and access code. The social engineers apply psychological tricks instead of technological exploits. These attacks usually take advantage of human emotions, habits or trust, directing them to click on a URL or visit a malicious website.

These attacks are generally focused on specific human weaknesses, making it the most considerable risk for online users, which requires training about the importance of information, and methods to use internet security concepts and tools (Korpela, 2015).

2.1.3.3. Identity Theft

Identity theft happens when someone steals a victim's personal information without their knowledge and uses it for theft or fraud. The risk of identity theft is related to everything end users put online, and social media has made it so much easier for criminals to steal this information and even victims' identities (Brokerlink Insurance, 2018). The risk of identity and information theft requires users to improve their awareness and learn how to adapt their behaviour in this environment (Grobler, Flowerday, von Solms, & Venter, 2011).

Most social media companies generate revenue from advertising, which requires users to share their social security number and driving license. This sensitive information can lead to the risk of identity compromise, as it happened for 6.5 million passwords leaked at LinkedIn in 2012. However, this was not the end of this story, as it became clear that the attack compromised the hashed passwords of 167 million accounts (Hackett, 2016).

2.1.3.4. Account Takeover

Account takeover is a form of identity theft in which a third party gains access to victim's unique details of online accounts. Hackers usually abuse the victims' information to conduct financial transactions using the victims' money. This will be more dangerous nowadays because many end-users apply their social network account when logging into any other website to get access to their services.

In April 2013, the Associated Press (AP) Twitter account tweeted to its more than 2 million followers about two explosions in the White House causing an injury to Barak Obama. The issue started with an email that seemed to be from others within the company, while it was initially from the Syrian Electronic Army. The email included a link that led to a page requesting the details for the AP Twitter account. When the attacker gained the login details, he posted a single tweet, sending the stock market into chaos (Allen, 2018).

2.1.3.5. Clickjacking or Like jacking

Clickjacking is an attack in which the victim’s personal information can be hijacked through clicking on a web link or URL, which seems to be just a simple click on a button (Jyotiyana &

Maheshwari, 2018). Facebook has been one of the biggest targets for clickjacking, by luring end users to click on an invisible hyperlink.. It works using a transparent layer that is inserted over the main hyperlink. Clickjacking is a useful tool in social media, like the method used on Twitter to load a user's page on the top of another page (Bradbury, 2012).

In 2012, users were like-jacked on Facebook, showing them a link for a news article. Users who clicked on the link were taken to a blank screen, showing them the message "Click here to continue." The attacker overlaid a Facebook page with a like button, which causes the users to like the page, and posted the link on their web page, which spread the virus (Bradbury, 2012).

2.2. Security & Privacy Practices

The social platforms try to maintain and increase the number of their users by providing new features like customized personal services and recommendations, new experiences and content suggestions (Nepal, Paris, Pour, Freyne, & Bista, 2015). These features will also have some disadvantages, increasing the risk of sharing personal ideas, sentiments, and experiences with friends, and more importantly, friends of friends. This can include a broad, and to some extent unknown, range of people having access to photos, videos, and our daily routine (Nepal et al., 2015). One of the most critical risks for end-users comes from themselves toward each other, for violating each-others' privacy, sharing too much information, or posting false information about themselves or others.

Humans are considered one of the primary sources of cyber breaches, considering the fact that even the best technical solution is at risk of being nullified by human carelessness. This makes it critical for executives and researchers to study end-user security and privacy behaviour and the factors affecting it (Gratian et al., 2018). However, the first step is to determine a framework involving the significant predictors of end users security and privacy behaviour (Halevi et al., 2016).

A potential problem that some researchers have identified while studying end-users' security and privacy behaviours is related to the fact that academic groups, which do not have enough knowledge and subject expertise, have developed cybersecurity cognitive models (Veksler et al., 2018). Organizations usually use academic researchers to study and establish online security and privacy behaviour, whether it was dividing the behaviour into more groups (Stanton, Stam, Mastrangelo, & Jolton, 2005), or using a model to develop a measurement scale (Ng, Kankanhalli, & Xu, 2009).

There are also some developments over the definition of scales for privacy, such as the Westin Index, which is used to divide consumers into three categories: fundamentalists, pragmatists, and the unconcerned (Kumaraguru & Cranor, 2005). There has been some development to the Westin Index, in order to measure more aspects of privacy attitudes, such as the Internet Users' Information Privacy Concerns (IUIPC) scale that measures privacy concerns based on three dimensions of control over information, awareness of privacy practices, and attitudes about information collection (Malhotra, Kim, & Agarwal, 2004). There has also been an extension of

privacy scales to more than disposition, such as general behaviours, and the use of technical solutions (Buchanan, Paine, Joinson, & Reips, 2007).

2.2.1. The importance of studying factors affecting end-user security & privacy behaviours

The research on the human aspect of cybersecurity has made some changes in research patterns (Kuhn, 1996). There is a shift from technological advances to human ability examination to improve the effectiveness of the cyber defence system. There should be an analysis of human error vs. technical problems, clarifying the importance of each aspect of cyber security (Yan et al., 2018).

This will lead to studying average end users instead of cybersecurity professionals. Professional users have many pieces of training and education, making them capable against cyber threats (Burley & Goodman, 2013; Newhouse, Keith, Scribner, & Witte, 2017), while the average end users have a lack of knowledge and efficacy that makes them vulnerable to cyber hazards (Bennett & Maton, 2010). The direction of research will shift from creating a secure system to improving the weakest entity, which can maximize the performance of the entire system (Yan et al., 2018). The best line to describe the importance of end users in cybersecurity is that security is only as good as its weakest link, which are the people (Schneier, 2011). This shows that improving end users' abilities is the most robust cybersecurity strategy (Sasse, Brostoff, & Weirich, 2001).

This weakness has been a source of tension between online companies and users. At the first stages of entering a website, users usually form their cognitive processing or privacy belief based on privacy affections such as joy or fear. After information sharing, awareness of privacy policy and information relevance will adjust privacy protection and perceived privacy risk. Privacy protection practices are dynamic, considering the factors related to the characteristics of social network websites. These characteristics derive the perception and attitude reactions by its users (H. Li, Sarathy, & Xu, 2011).

A few strategies have been suggested to be taken into consideration. The first one is taking general caution, just having some personal protective steps, like strategies undergraduate students use to control their Facebook accounts. These strategies, which include contact information restriction, using the limited profile option, photograph management by removing tags and opportunities, and limiting friend requests, can be taught to end users to mitigate the

risk of disclosing personal information on social networks (A. L. Young & Quan-Haase, 2013). The other approach is more technical and advanced: using software and hardware tools, such as checking spyware, and control of cookies and history. This will give people a different level of privacy protection based on their knowledge and self-efficacy (Oakleaf, 2009).

Unlike the dynamic nature of social networks and the related privacy protection practices (H. Li et al., 2011), human behaviour is a static factor, and it does not change just by awareness training. There are three human factor components in each system: the IT expert, the threat entities and target entities. The threat entities imply the attackers and people who deliberately pose a threat to the system. The target entities are people who work inside an organization or any system that is protected by cybersecurity tools. Also, there are IT experts who provide cybersecurity services. Based on these categories, there are different categorizations of behavioural attitudes to achieve a better analysis of the human factor in cybersecurity, like the classification by H. Young, Vliet, Ven, & Jol (2018) as: reflex, habitual and thoughtful actions.

Reflex behaviour is the result of cues perceived by one's senses, like clicking on hyperlinks with the risk of instalment of malware. It can be said that reflexes are derived from end users' most basic cognitive thoughts. The second type is the habitual behaviour, which needs greater cognition and needs more cognitive analysis like the agreement to the condition of installing new software. The third type is thoughtful behaviour, like the training and awareness related to cyber risks, and the mitigation strategies toward those threats. Considerate behaviour is usually accomplished through thoughtful consideration of the situation and logical processing. It can be said that most security-related behaviour is habitual behaviour, which can be improved through an awareness training program and effective educational methods (H. Young et al., 2018).

One smart approach that can help the researchers is tailoring the model to reach better precision and applicability, which can be done at the start and during the modelling, using a progressive elaboration approach. Most of the model tailoring is done by adjusting parameters, and the adjustment based on users' experiences called "model-tracing". It can be helpful through detecting users' cognitive states, to predict potential biases, error and ignorance. The current method of end users' behaviour prediction is conducted by statistical analysis, and researchers recently recommended an extension of cognitive modelling-based tools to help to improve the effectiveness of awareness training (Veksler et al., 2018). However, there is a limitation of a standard measurement model for end-user security behaviour, which necessitates finding the

correlation between human traits and security practices, and determining what will cause users to fall prey to security or privacy breaches online (Egelman & Peer, 2015).

2.3. Determinants of Security and Privacy Practices

There has been some previous work modelling proposed human behaviour prediction in web browsers based on current goals (Fu & Pirolli, 2007). Moreover, there are models related to human behaviours such as social network use (Hannon, McCarthy, O'Mahony, & Smyth, 2012), chat behaviour (Ball et al., 2010), team-based performance evaluation (Ball et al., 2010), and email monitoring (Dredze & Wallach, 2008). Some models of human cognition show much effort by researchers to study and simulate human interaction in the cyber environment (Fu & Anderson, 2006; Nason & Laird, 2005).

Some researchers attempt to analyze the users' intentions to establish security practices, considering the case that they become aware of the cyber risks (Anwar et al., 2017). The Protection motivation theory (PMT) is an extended version of the health belief model, and the self-protection intention is dependent on perceived susceptibility, perceived severity, self-efficacy, and response efficacy (Rogers, 1983). PMT deciphers how and why end users decide to undertake protective behaviours, as behaviours motivated by threat appraisals and coping appraisals. Threat appraisals and coping appraisals are vital factors determining behavioural intentions to undertake security practices. End users usually undertake security and privacy practices that they believe are effective and require a reasonable expenditure (Tsai et al., 2016).

2.3.1. Demographics and network attributes

Demographic factors like gender can be a basis for the analysis of behavioural differences (Anwar et al., 2017). It can make a difference in users' perceptions of privacy and security, and affect users' attitudes toward online privacy in social media (Mathiyalakan, Heilman, & White, 2002) or toward security perception against cyber-attacks such as phishing (Halevi, Lewis, & Memon, 2013).

Based on Chen, Rea Jr, & Rea (2004), a direct relationship between demographic variables and privacy practices was not detected. However, women are found to have more sensitivity to detail, and are more aware of the changes and possible risks in their environment. On the other hand, men usually feel more comfortable in using software tools and new technologies, which can be interpreted by their higher level of self-efficacy (Arbaugh, 2000). From the perspective of age,

Dienlin & Trepte (2015) stated the age factor would cause a difference in awareness toward cyber threats, which will affect information self-disclosure, number of posted blogs and number of friends on social media (H. Li et al., 2011).

2.3.2. Disposition

The first step in cybersecurity action for a user is their perception of the concept. Because the way people think can form their attitude, this can be an independent variable to direct end users' intentions toward cybersecurity (Lallmahamood, 2007). Based on pre-disposition, users decide to use a social platform (Shin, 2010) or other internet tools such as internet banking (Lallmahamood, 2007).

End users have many reasons to be concerned about their privacy; for example, whether it is accessible to unauthorized entities, or if service providers will use their information without permission or share private information with third parties. Information privacy has been one of the major obstacles to the growth of e-commerce, as consumers may refuse to enter their personal information, or provide falsified information to online vendors (H. Li et al., 2011). Privacy concerns worry users due to potential harms from personal information disclosure, which increases the perceived risk (Zhou, 2015).

The trace of a person in an online environment is called a "digital footprint," which can give personal or critical information about the user and put them at risk (O'Keeffe & Clarke-Pearson, 2011). This risk can be a reason for users' to employ more privacy settings, as it has been reported that Facebook users who have been compromised by privacy invasion tend to establish more privacy settings than others. This concern intensifies when it comes to a lack of trust toward the company that has their personal information (Debatin et al., 2009). In contrast, there is another claim which goes against the existence of a relationship between trust and privacy, as it has been stated that trust is not that necessary to form an online relationship compared to its importance in face to face communication, indicating less sensitivity toward internet privacy (Dwyer et al., 2007).

It should be notified that trust should involve both the privacy and security aspects of a social platform. It is based on perceived privacy and security that governments (Shareef, Kumar, Kumar, & Dwivedi, 2011) and academic institutions (Almadhoun, Dominic, & Woon, 2011) can establish trust with end-users to use their online services. Although executives are expending much effort to establish a reliable cyber security system, there are problems such as the many

routes for access to social platforms, impersonation and anonymity, the last of which is a challenge in social media like Twitter (Everett, 2010).

2.3.3. Privacy Concerns

Security and access control tools of social media are weak purposefully, to make it easy for users to join and interact in a network. The concern for security will make it essential to establish a stronger security mechanism for using social networks. Executives should create harmony between privacy and security concerns and the usability and sociability of the system (C. Zhang, Sun, Zhu, & Fang, 2010). The number of participants in a community, the number of messages per unit of time, members' satisfaction, and some less apparent measures such as the amount of reciprocity, the number of on-topic messages, trustworthiness and several others are the key factors of sociability. Also, the number of errors, productivity and user satisfaction are the major factors for the usability of a social network (Tsai et al., 2016).

From the privacy perspective, the advantages of communication and information sharing in Social Networks has another aspect, which is the disadvantage of raising privacy, security and trust concerns (Almadhoun et al., 2011). The concern users have leads to mistrust, which causes users not to share or interact with others. Doubt concerning privacy directs the research to not only investigate the "site trust," but overall "social trust" (Brandtzæg, Lüders, & Skjetne, 2010). This paradox can be seen as users share information while having privacy concerns (Debatin et al., 2009).

The problem does not end here because even if people express concerns about their privacy, they will perform contradictory actions in a real-world scenario (Jensen, Potts, & Jensen, 2005). Some researchers examined users' behaviours in social networks, like Acquisti & Enhancing (2006) that examined the effect of privacy concerns on users' behaviour on Facebook, which showed that privacy concerns have a weak predictive power in behaviour analysis. Christofides, Muise, & Desmarais (2009) also examined young and adult users' behaviour, especially their content sharing on Facebook. They suggest finding the factors by focusing on users' different desires to share their information. Gross, Acquisti, & Heinz (2005) identified that users would share their knowledge without worrying about privacy risk, while this attitude changed in older age groups (Livingstone & Brake, 2010). The lack of understanding of online privacy issues raised the risk of using social media, which of course, is accompanied by other reasons such as inappropriate content, and the outside influence of third-party advertising groups. However, lack of trust and

high privacy concern can raise the intention to deceive organizations by not being honest when they perceive a violation of their privacy (Smith, Milberg, & Burke, 1996).

2.3.3.1. The relationship between privacy concern and behaviour

There are different types of privacy in social media, such as informational, social and psychological (Dienlin & Trepte, 2015), and study factors include privacy intention, attitude and behaviour. In addition, privacy concern has not been considered individually as a particular type of privacy, but as a general factor, because privacy concern is an indirect predictor of privacy behaviours, which has privacy intention and privacy attitude as mediating variables (Fishbein & Ajzen, 2011), in addition to being a direct predictor of content sharing and its breadth (L. Becker & Pousttchi, 2012).

Users undertake privacy behaviours to optimize their relationship and information sharing with others in a social network (Dienlin & Trepte, 2015). The informational privacy concern investigates individual control over the information sharing with others in a social network. Privacy concerns are related to attitude, and the integration of cognitive and affective factors related to an object (Crano & Prislin, 2006), described as the desire to safeguard personal information from others (Buchanan et al., 2007). Privacy concerns are unipolar; and refer to the incidents that can only be considered harmful, like identity theft or misuse of personal data. On the other hand, attitudes have two dimensions, cognitive and affective, and can be either negative or positive; they also can be extended to every online action (Dienlin & Trepte, 2015).

Dienlin & Trepte (2015) considered a multi-dimensional approach toward privacy behaviour, considering prior singular behaviour studies. They also tried to clarify the different definitions related to privacy concern, and privacy attitudes. There was a lack of sufficient variables, which made it challenging to detect a strong and robust relationship with privacy behaviour (Schmidt, Hunter, & Urry, 1976). This prompted the idea of using both privacy concern and privacy attitude to predict privacy behaviour. In addition, the answers that respondents give about their attitudes can be disrupted due to the pressure or situational constraints they feel, which may make their answers deviate from the correct judgement (Dienlin & Trepte, 2015). The other concern is about the effect of the mass media's report on respondents' answers, which may cause a deviation in their responses (Teutsch & Niemann, 2016). The significance of personal experience should not be forgotten; it can intensify the effect an attitude may have on behaviour (Trepte, Dienlin, & Reinecke, 2014). Dienlin & Trepte (2015) suggested the possibility of using

privacy attitude as a mediator between privacy concern and privacy behaviour, considering the difficulty of using privacy concern as a direct predictor of privacy behaviour.

2.3.4. Risk Perception

Many features and benefits of social media platforms are ignored because of the privacy risks they bring for social media users (Fogues, Such, Espinosa, & Garcia-Fornes, 2015). Social media provides big data based on users' sensitive personal information that can be collected and used for profit. The lack of a smart access control tool makes users unable to realize which data should be limited, which causes confusion between confidential and non-confidential information (Viejo & Sánchez, 2016).

The interesting fact about social media is that there is less developed research on security compared to privacy. There are findings about the relation between security perception and cyber victimization, and the fact that users with high perceived control over security and users that apply social networks for more than just the single purpose of information sharing are less likely to be victims of cyber-attacks (Saridakis, Benson, Ezingeard, & Tennakoon, 2016). One of the significant sources of vulnerability for social media comes from the weak security and privacy architecture of these media (Acquisti & Enhancing, 2006); and considering the main objective of social media, which is the sharing of information with other people, necessitates the understanding of users with regards to risk perception and privacy disposition (Van Schaik et al., 2018).

In order to establish a safe, reliable and lasting social platform, some factors should be considered in order to mitigate the current risks that many platforms have. Two of these significant factors are security and trustworthiness, in addition to adding other factors such as risk perception, and users demographic and security and privacy behaviours, which make the analysis more sophisticated and challenging (Z. Zhang, 2015; Z. Zhang & Gupta, 2018).

Risk perception is one of the significant variables in designing security and privacy models, indicating the extent to which users and executives recognize cyber threats. The security consists of dimensions like confidentiality, integrity, and availability (Schneier, 2011). Moreover, online privacy consists of different types, such as information privacy, social privacy, and personal privacy (Dienlin & Trepte, 2015).

In studying risk perceptions, there are different measures used to convert users' knowledge into quantitative scales. Gerber, Gerber, & Volkamer (2018) explored some predictive factors for

perceived privacy risk: privacy concern, the level of trust, personalization, recognized privacy regulatory protection, initial joy, trust, and demographic variables. It has been noted that there are no strong predictive variables in most studies. In addition, users will perceive more risk if they are more aware of general privacy risk, have experience with privacy violation, deal with sensitive information, or gain understanding from their own encounters with privacy threats (Gerber et al., 2018). One of the factors affecting risk perception is the availability of the risk, which means "the ease with which instances come to mind" (Kahneman & Egan, 2011), depending on the impact of the event, nature of the game, and the nature of the experience, which can increase availability (Van Schaik et al., 2017).

Fogel & Nehmad (2009) examined the effect of privacy concern on the perceived risk in an online social network, and they consider there to be a relevant relationship between risk-taking and privacy concern on these websites. This relevance has been re-examined by Lancelot Miltgen, Popovič, & Oliveira (2013), who detect the factors affecting an end-users' acceptance model for biometric technology. They confirm the influence of privacy concern on risk perception of customers, even though there is a medium correlation between these two factors, which affect the acceptance of the biometric access system. Later, they examined the effect of perceived privacy regulatory protection on perceived privacy risk, assuming this factor besides trust influences privacy risk. According to their study, trust will reduce the perceived privacy risk; besides the theory that users' perception of regulation/legal policies will have a positive effect on perceived risk.

Zhou (2015) examined the effect of perceived risk in location-based services, which explained that user behaviour depends on both perceived risk and perceived usefulness. The balance between these two factors determined their behaviour toward these services, and both of these factors have a significant relationship with privacy concern. The abovementioned concept has been developed by Dinev & Hart (2006), as a cost-benefit analysis called “privacy calculus”. Based on this concept, H. Li et al. (2011) proposed two factors: privacy protection belief, which is the expected belief consumers have about vendors’ capability to safeguard their personal information; and privacy risk, which consumers take on by sharing their information with vendors. A combination of both cognitive and affective-based factors have been applied to examine how users make decisions and behave based on “privacy calculus”. The findings in this paper show that privacy concern influences both perceived privacy risk and personal information disclosure.

Keith, Thompson, Hale, Lowry, & Greer (2013) examined privacy concern and privacy risk awareness as predictors of perceived privacy risk; in addition to the perceived risk and perceived benefit affecting intent to information disclosure. Based on their analysis, the privacy risk perception plays a more significant role than perceived benefit in the prediction of information disclosure.

The problem regarding risk perception and precautionary behaviour is the lack of study with respect to the correlation of these two factors with each other (Garg & Jean Camp, 2015), except for limited research such as the study on the disclosure of new information (Keith et al., 2013), or research by Shin (2010) about the effect of perceived privacy on perceived security. It was van Schaik et al. (2018) who studied the relationship between risk concern and precautionary behaviours related to privacy and security in social media, claiming that the previous research did not have a measurable scale for risk concern (perception) to establish a relationship with behaviour.

2.3.5. Awareness

Taddicken (2014) examined the relationship between self-disclosure, which shows a willingness to be discovered, and privacy concern and rejected it, while suggesting that the perceived social relevance of a social media, number of social networks used by a user, and willingness to share have a significant effect on the prediction of self-disclosure. Acquisti & Enhancing (2006) stated that users' attitudes do not affect their information sharing, followed by the fact that there was a lack of awareness about privacy and discoverability settings on Facebook.

Almost all Facebook users share their real name in their profile, while the majority of them share other significant information such as educational information, contact details, birth date, personal and social pictures, and in a smaller portion, sexual orientation, relationship status, and other interests (A. L. Young & Quan-Haase, 2009). On the other hand, considering the privacy concerns of aware users, they control their shared information regularly. Two of the most important reasons for users not following the safe online behaviour is because they are not fully aware of the risks and their impact, and they haven't fully perceived the correct action (Bada et al., 2015).

Up until now, organizations and governments have mostly focused on the technical aspects of cyber security, and not paid enough attention to the human dimension, and this has made their efforts and achievements ineffective (Oehri & Teufel, 2012). Increased emphasis on human

aspects of cybersecurity such as improving end-user awareness of security standards and best practices can help to boost end users' security awareness and help them engage in better security practices (Schlienger & Teufel, 2002). Social and cultural measures in social media guidelines can increase security awareness, which leads to improved security behavioural practices (Oehri & Teufel, 2012). This improvement will require discovering the mediating factors between these two constructs.

2.3.6. Social Media Self-efficacy

Social media end users need to realize the threats within the internet, and to establish the proper behaviour to deal with these threats. The realization usually comes from experiences users have in the cyber environment (Scott & Weems, 2010). This led to the definition of perceived control or self-efficacy, users' realization of their control over their information (Bada et al., 2015), which is really applicable for predicting users' behaviours (J. Lee, 2012). The more self-efficacy users feel they have, the more information they share (Hajli & Lin, 2016). With more perception, end users can develop their level of awareness to be more knowledgeable and cautious in risky situations. The home users usually feel a high level of controllability since they have the ability to choose the site they want to open, open an attachment or apply system updates (More, 2011).

Although cybersecurity plays the role of the foundation for each system and company, making people aware of the risks in cybersecurity does not remove the threat imposed by end users' carelessness (De Bruijn & Janssen, 2017). Improvement of end users' cyber behaviour is limited to training and awareness plans, in addition to technical tools, which have a limited effect. It cannot protect or warn users away from responding to phishing emails or clicking on anonymous sources (Tamrakar, Russell, Ahmed, Richard III, & Weems, 2016). There are some studies about users' knowledge and their practices against security risks which showed that there is no relationship between technical self-efficacy and the practices people adopt towards safeguarding against cyber threats, even though the knowledge can affect their awareness toward potential risks (Kang, Dabbish, Fruchter, & Kiesler, 2015). On the other hand, Egelman & Peer (2015) studied users' security behaviour using a set of questions to measure four dominant security traits: device securement, password generation, proactive awareness, and updating. These four variables are subsets of awareness and self-efficacy; it was concluded through statistical analysis that these factors are predictive of end users' security behaviours.

2.3.7. Security Awareness Training

Security awareness training programs and campaigns are to guide users on how to apply secure internet behaviour. The awareness training program is a significant part of the security chain, transferring security information and knowledge to users, and applying data on security breaches to improve end users' security behaviour (Bada et al., 2015). This will require more than just informing participants of the knowledge related to the subject. They should understand the importance of the information, perceive the procedure of behaviour toward cyber threats, and most of all, intend to apply the practices they have been taught (Bada et al., 2015; Witte, 1993).

The problem with educational programs is the limited effectiveness, considering that the most applications are awareness campaigns (Coventry, Briggs, Blythe, & Tran, 2014), and these campaigns present some highlights of the topic, which focus on the quality of the information. The issue is about the nature of the information delivery to the audiences, and which factors such as personal knowledge, attitude, perception and the efficacy of coping strategies are ignored in training (Gouveia, Lopes, & de Carvalho, 2011; Van Dijk, Spil, Van der Burg, Wenzler, & Dalmolen, 2015). The current challenge in cybersecurity is about the ineffectiveness of information delivery (Cook & Allan, 2018) for security awareness, indicating that warning and threatening messages make users stressed to the extent of ignoring the existence of the security threats (Bada et al., 2015).

Users are tired of material that is too general being presented in training programs; they would rather hear or see some simple, current and compelling content. Awareness is about the people who perceive the security concern and behave accordingly (Wilson & Hash, 2003). This highlights that awareness is not just about getting the information or recognition of the concept of cyber security, but also about enacting the appropriate security behaviour in a timely manner (Bada et al., 2015).

Many organizations have tried to establish an awareness training program to teach their employees about security breaches, which can be a reliable guide for practitioners and researchers studying information security behaviour (Abraham, 2011). There have been many discussions about how much a good training program can affect security behaviour (Choi, Kim, Goo, & Whitmore, 2008).

In the public environment, government and national organizations try to disseminate secure online behaviour to ordinary users, but it does not prevent incidents from happening. It is mostly because of the progressive nature of attacks, and difficulties of non-professional users to perceive security interfaces (Bada et al., 2015). The problem in most cases is that users are capable of understanding the awareness challenges and their relative answers, while they are not capable of performing the proper behaviour in real-life situations. Social media guidelines are meant to be practical, to direct users to low-risk security behaviour (Oehri & Teufel, 2012). The privacy and security practices should be designed to be user-friendly and easy-to-learn so that users do not avoid learning and applying the information (Coventry, Briggs, Blythe, et al., 2014). The usability challenge is a significant obstacle which has been troubling cyber specialists from the start of the 21st century (Cranor & Garfinkel, 2005) until now (Nurse, Creese, Goldsmith, & Lamberts, 2011a).

There are guidelines (Wilson & Hash, 2003) and a monthly awareness program (Department of Homeland Security, 2018) to improve awareness and education for end-users, even though they lack an evaluation criterion. There are many organizations advising end-users about staying safe online. The problem to this approach is the full range of tips and procedures are hard to follow, which make end-users confused, considering the diversity and number of items. This shows the need for an optimized set of behaviours to follow in the cyber environment (Egelman & Peer, 2015).

The risk of security being perceived as an obstacle can make users tired of following the security steps and instructions, especially when it prevents users from doing their tasks. The other side of this constant alertness is the phenomenon of security fatigue. There are three elements: security, functionality and usability (Waite, 2010), which should be in balance for the system to work effectively (Bolhuis & Giraldeau, 2005).

It is neither possible nor cost effective to attain absolute security, which means that we will always have to deal with residual risk, and its extent should be defined in security guidelines (Schlienger & Teufel, 2002). It is better to first detect gaps in behaviour, prioritize these gaps and then direct training and education for the most important ones (Oehri & Teufel, 2012). Executives are trying to modify the training system because the best way to reduce the risk of the human factor is through awareness (Korpela, 2015). Psychology plays a role in analyzing the behaviour of end users in high-risk cybersecurity actions (Whitty, Doodson, Creese, & Hodges, 2015).

In the case of passwords and content sharing, it can be said that age can make a difference in the level of knowledge and impulsivity that shows the difference in users' self-control and self-monitoring that can make users more considerate towards other people's requests. The other factor is called Locus of control, which is the users' perception toward their control over their environment. Users with an external locus of control believe that events depend more on luck than their own actions. These users engage in riskier online behaviour in social media (Whitty et al., 2015). This can help to detect weaknesses in each group of people, in order to form a customized training plan, although one of the significant challenges in defining the behavioural traits is the lack of knowledge about the level of influence each variable has on end users' awareness (Coventry, Briggs, Jeske, & Van Moorsel, 2014).

Some researchers believe in developing cybersecurity awareness training based on gender differences, considering their different security behaviours that affect users' perceptions, attitudes and behaviours (Anwar et al., 2017; Nosek, Banaji, & Greenwald, 2002). Anwar et al. (2017) state that women's self-efficacy is significantly lower than men's, while men are influenced more by attitude. On the other hand, women are more driven by subjective norms, social roles, and behavioural control. These differences in the level of self-efficacy and its associated factors direct researchers to develop gender-specific training programs.

Some factors can make a training system ineffective, such as the inability to detect users at risk or understand how the end users learn cybersecurity the best. It has been suggested to develop security awareness based on the risk each end user encounters instead of having a role-based training system. A survey can help to determine the level of risk each user has to deal with, which categorizes the users based on the level of human risk (Korpela, 2015). Nevertheless, the inevitable risk lies in the fact that much of the knowledge about cybersecurity is passive, and it is somewhat challenging to make people think actively about cyber risk through training alone. The other factor that should be considered is the difference between self-claimed cyber knowledge and the real-scenario capability of end users, which is difficult to evaluate (Larson, 2015).

2.4. Privacy Paradox

There are some privacy concerns over using the social network (European Commission, 2011; Yao, Rice, & Wallis, 2007), even though it does not affect the overall use of these social platforms by end-users (Gross et al., 2005).

Users try to apply privacy protection strategies such as limiting access to content shared, restricting photo tags, or blocking the capability of private messaging, all of which control the information disclosure in social networks. These strategies do not show a high degree of privacy concern (A. L. Young & Quan-Haase, 2013), which should be the opposite of willingly sharing information in social networks (Barth & de Jong, 2017). End-users know their privacy concerns and needs, but their behaviour does not necessarily align with their concerns (Buck, Horbel, Germelmann, & Eymann, 2014). This has been introduced as the privacy paradox: users exhibit different behaviour compared to their attitude. The paradox is highlighted in situations in which the perceived risk is high, and yet users show a high level of information disclosure (Acquisti & Enhancing, 2006), which highlights the mistake users make in assessing the cost-benefit trade-off.

It is almost undeniable that social network users have a behavioural tendency to compromise privacy over the benefit they perceive (Barnes, 2006). Risk perception can prompt users to acquire knowledge of privacy protection, but it cannot suffice to motivate users to apply privacy practices (Oomen & Leenes, 2008). The other issue is that end users usually share more information than they intend to (Norberg, Horne, & Horne, 2007). Information disclosure is based on immediate and clear benefits, while the risks and threats are abstract concepts, which cause the benefits to outweigh the risks at the time of actual behaviour (Barth & de Jong, 2017).

End users' attitudes and behaviour can be affected by people around them, e.g. family, friends or significant others. Influencers have the potential to make users adapt their behaviour within the groups they are members of, either positively or negatively (Crutchfield, 1955). Individuals do not like to be excluded from the social group, and this causes them to accept information disclosure by ignoring privacy concerns (Flender & Müller, 2012). This issue is one of the potential side effects of social media, which has become a habit that is a part of people's daily routines. This habit will inhibit privacy protection strategies and will cause a weak relationship between privacy concern and behaviours (Quinn, 2016).

2.4.1. Privacy Concern, Perceived Risk and Privacy Behaviours

There are contradictory results causing the privacy paradox, such as the relationship between perceived privacy risk (resembling privacy concern) and users' scale of self-disclosure (Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010), as well as the relationship between privacy disposition and the application of privacy tools (Mohamed & Ahmad, 2012).

There is also research about users' change of privacy behaviour when they become insulted online; here, the change in their behaviour is limited to their informational privacy behaviour, but not their social or psychological aspects (Trepte et al., 2014). These paradoxes lead to the need to investigate how to change users' behaviour effectively.

In sum, the paradox between privacy concern and information disclosure highlights these questions as to why users behave as they do in response to the risk they perceive from cyber threats (Barth & de Jong, 2017). It seems that users are capable of identifying and weighting privacy disclosure disadvantages, but there is a probability of not calculating the benefit-risk relationship rationally, or not even being aware that they are negatively affected by factors such as time limitation, immediate gratification or positive bias. End-users do not usually recognize the preferences; however, it cannot be denied that these biases have a significant effect on users' behaviour. Behaviours are typically made rapidly and without all-aspect analysis, and determined by experience instead of analytical judgement (Barth & de Jong, 2017).

The biased behaviour can be explained by users' cognitive limitations, making them incapable of assessing the risks thoroughly, which is natural for users not having access to all factors and information, causing the benefit to outweigh the risks (Deuker, 2010; Pötzsch, 2009). Users usually show reluctance to become aware of the privacy threats, even in the situation that the necessary knowledge and tools are available (Acquisti & Grossklags, 2005). This may be because of the subjective nature of awareness, which makes users unaware of the actual level of privacy risk. Although end users perceive privacy concerns, it can be different with their actual privacy behaviour, which can be altered in the 'heat of the moment' (Barth & de Jong, 2017; Sundar, Kang, Wu, Go, & Zhang, 2013).

According to Acquisti & Enhancing (2006), Facebook users have more concern about disclosing their personal information such as their living whereabouts or class schedule compared to people with no Facebook profile, but there is no relationship between concern with privacy behaviour like information disclosure (European Comission, 2011). This paradox has also been shown by Stutzman (2006), which found that students consider it essential to safeguard their identity information, but they rated as "neutral" whether they agree or not, that strangers have access to their profile through social media.

The risk assessment requires the time and cost of the process, and calculation and aggregation of information about the privacy concern, which necessitates a high-level cognitive process, causing individuals to replace it with other methods of risk analysis (Barth & de Jong, 2017).

End-users tend to make decisions using mental shortcuts instead of thorough information analysis (Tversky & Kahneman, 1974). End users usually underestimate their risk of privacy threats while overestimating this risk for others, which causes the idea that their own risk and others are different, which can end in more exposure risk (Acquisti, 2004). There is a theory called "Under Insurance" for analyzing low probability but high impact events; the possibility is underestimated because of lack of experience, lack of awareness about the threat, or overestimation of the cost of privacy protection strategies (Kunreuther, 1984).

The concept of underestimating self-risk compared to risk consideration for others, which is affected by the mass media (Davison, 1983), will lead users to not exhibit the intended behaviours; this shows that users consider themselves to have the advantage of using the positive aspect of social networks (Debatin et al., 2009). This can clarify the fact that individuals do not apply security safeguards, even though they have enough awareness of knowledge of cyber threats (Barth & de Jong, 2017). End users have a tendency to choose smaller short-term benefits instead of the long-term benefit, showing that privacy concern may not be able to influence users' behaviour in the instant of decision-making. This lack of awareness ends in choosing immediate advantages and dealing with a future risk (Barth & de Jong, 2017). This will give the impression that end-users underestimate the low probability of future risk for the sake of an immediate yet small benefit (Acquisti, 2004; Acquisti & Grossklags, 2005; Flender & Müller, 2012).

The cognitive resolution for engagement in social networks can overcome the privacy concern and appropriate behaviour of mitigating the risks, which will negatively affect both private and social life (Barth & de Jong, 2017). There are some needs and goals along with the entertainment and routine social activities that can be achieved through acting in social networks, which justify interaction with all the privacy concern and risks (Debatin et al., 2009).

Integrating all the themes in the literature review, Table 7-1 illustrates the critical takeaway from the critical papers referred to in the study. Based on the table, it can be interpreted that there are many studies examining privacy concern, perceived risk, security awareness training and privacy paradox, which shows the focus that researchers have put on end users' perceptions and practices. On the other hand, there is a lack of studies on privacy disposition and self-efficacy. This shows the lack of research about the role of knowledge and technology capability in end users' security and privacy practice.

3. Research Design and Methodology

This chapter provides a general description of the design and methodology for our research. We elaborate on the theoretical model developed for deductive research, data analysis technique, the design of the survey instrument, the data collection, and data analysis procedures used in this study.

3.1. The Proposed research theoretical model

To study the effects of different factors on security and privacy behaviour on social media, we propose a framework to analyze the interrelationship between significant constructs of the model to specify the crucial variables that influence end-users' behaviours, privacy and security practices. The major dimensions of the model are posture, proficiency and practice, completed by end users' attributes and demographic information.

This model has been developed based on the major constructs affecting end users' behaviours and practices in social media. Figure 3-1 illustrates the details of the dimensions, constructs and relationships between these components. The dimensions, variables and relationships between these items will be discussed thoroughly in the next chapter.

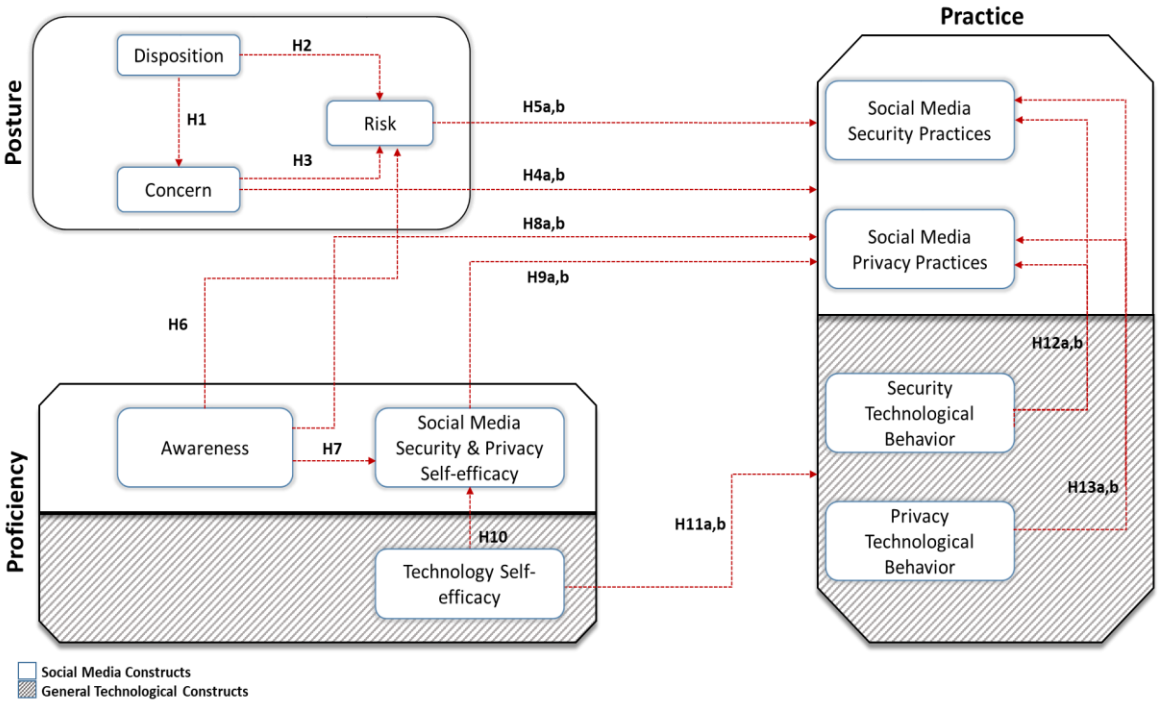

Figure 3- 1 – Theoretical model of the interplay among posture, proficiency and practice

This empirical model aims to evaluate the research questions presented earlier, to find the answer about the inter- and intra-relationships between posture, proficiency and practice factors, which can influence the end-users' security and privacy behaviours in social media. For this objective, we will investigate the relationship between factors from different dimensions of this research in both the context of global online and social media. One of the less studied aspects of our study is related to the investigation of both social media security and privacy practices. We aim to explore whether there is any difference between security and privacy practices, and their influential factors in social media.

In addition, there is a lack of elaborate research on the effect of proficiency factors on social media security and privacy behaviours. As posited in the model, both the posture and proficiency constructs will affect the practice construct, besides the effect of social media threat awareness on Social media risk perception. The relationship between these three dimensions of end users' traits will be investigated in this research.

3.2. Theoretical Model Dimensions and Constructs

We describe the conceptualization of the significant constructs of the conceptual model in section 1.2, in addition to the presentation of the theoretical model in the previous section. As discussed before, the model consists of three major dimensions, which are Posture, Proficiency and Practice. Posture can be defined as a set of end users' perceptions toward privacy and security, and related concerns and risks in social media. Proficiency involves the attitudes and capability end users perceive that they have, in both online technology and social media context. Practice is a set of constructs that measure the end users' behavioural practices toward security and privacy in online technology and social media. Table 3-1 illustrates different dimensions with associated constructs and their operationalization.

Table 3-1 – Model's construct with their operationalization

Dimension	Constructs	Operationalization
Posture	Online Privacy Disposition (OPD)	Unidimensional construct with reflective indicators
	Social Media Privacy Concern (SMPC)	Unidimensional construct with reflective indicators
	Social Media Risk Perception (SMRP)	Unidimensional construct with reflective indicators
Proficiency	Social Media Security Threat Awareness (SMSTA)	Unidimensional construct with reflective indicators
	Technological Self-efficacy (TSE)	Unidimensional construct with reflective indicators
	Social Media Security & Privacy Self-efficacy (SMSPSE)	Unidimensional construct with reflective indicators
Practice	Online Security Tools use (OSTU)	Unidimensional construct with reflective indicators
	Online Privacy Tools use (OPTU)	Unidimensional construct with reflective indicators
	Social Media Security Practices	Second-order formative construct with two dimensions, each with its formative indicators
	Social Media Privacy Practices	Second-order formative construct with two dimensions, each with its formative indicators

3.3. Proposed Model Paths and related hypotheses

In addition to the three major dimensions described in the previous section, there are some propositions that should be validated, to finalize our theory about end users' privacy and security practices in social media.

3.3.1. Posture

The first dimension of the model is posture, which encompasses three major constructs: disposition, concern, and risk. These constructs have five major propositions, as shown in Table 3-2.

Table 3-2 - Path Propositions for Posture constructs

Proposition	Model Path	Basis in Extant Literature
H1	Online Privacy Disposition has a positive effect on Social Media Privacy Concern	End users' lack of privacy disposition can negatively affect privacy concern in social media (Xu et al., 2011).
H2	Higher Online Privacy Disposition increases Social Media Risk Perception	According to Xu et al. (2011), privacy disposition has a positive effect on risk perception.
H3	Social Media Privacy Concern has a positive effect on Social Media Risk Perception	As privacy concern negatively affect trust, it has a positive impact on perceived privacy risk (Lo, 2010).
H4a,b	Higher Social Media Privacy Concern leads to better Security and Privacy Practices in social media	Considering privacy concern as a predictor for end users' beahvior in the online environment, Li (2014) validated that higher privacy concern leads to better privacy behaviour.
H5a,b	Social Media Risk perception has a positive effect on Security and Privacy Practices	According to Lo (2010), perceived risk has a positive effect on privacy practices.

3.3.2. Security & Privacy Proficiency

The second dimension is proficiency, which has three constructs called: Awareness, Social Media Security & Privacy Self-efficacy, and Technology Self-efficacy. Table 3-3 illustrates the five propositions related to these constructs.

Table 3-3 - Path Propositions for Proficiency constructs

Proposition	Model Path	Basis in Extant Literature
H6	Social Media Security Threat Awareness has a positive effect on social media Risk Perception	Security awareness positively affects risk perception in the information system (Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011).

H7	Higher Social Media Security Threat Awareness leads to better Social Media Security and Privacy Self-efficacy	The study considered both factors having a positive effect on the other one (Yao, 2011).
H8a,b	Higher Social Media Security Threat Awareness leads to better Social Media Security and Privacy Practices	The research for the relationship between these two constructs is not much; especially it is limited when it comes to assessing these construct in social media.
H9a,b	Social Media Security and Privacy Self-efficacy has a positive effect on Social Media Security and Privacy Practices	there has not been any reference in the literature based on our knowledge and research
H10	Technology Self-efficacy has positive effect on Social Media Security and Privacy Self-efficacy	there has not been any reference in the literature based on our knowledge and research
H11a,b	Technology Self-efficacy has a positive effect on Online Security and Privacy Tools Use	End users with higher Self-efficacy in Information Security show more security protection behaviour (Rhee et al., 2009)

3.3.3. Security and Privacy Practices

The last dimension is practice, which consists of four significant constructs, Social media security practices, Social media privacy practices, Online Security tools use, and Privacy technological behaviour. There is some internal relationships between the two sub-dimensions of this section, which are presented in Table 3-4.

Table 3-4 - Path Propositions for Practice constructs

Proposition	Model Path	Basis in Extant Literature
H12a,b	Online Security Tools Use has a positive effect on Social Media Security and Privacy Practices	there has not been any reference in the literature based on our knowledge and research
H13a,b	Online Privacy Tools Use has a positive effect on Security and Privacy Practices	there has not been any reference in the literature based on our knowledge and research

3.4. Theoretical Model Validation Techniques

The primary analysis technique for this study is Structure Equation Modeling (SEM). As a diverse set of statistical models, Structure Equation Models examine and analyze the relationship between hypothetical or unobserved (Latent) variables (P. Lei, Wu, & Pennsylvania, 2007), which fits well for testing and analysis of our exploratory theory (Kline, 2015). The latent variables used in SEM are the variables that cannot be measured directly, but are required to be operationalized through other indicator variables (manifest variables), which can be measured through an appropriate instrument such as a survey questionnaire, as both variables illustrated in *Figure 3-2*. SEM is a robust technique for modelling complex models that includes latent

variables, formative variables, moderator variables, and multiple group analysis (Lowry & Gaskin, 2014). Besides these advantages, using both structure and measurement makes it a precise analysis technique (Chin, 1998).

We use Partial least square (PLS), which is a variance-based SEM analytical technique (Kaplan & Haenlein, 2010). Unlike the first generation techniques, Partial Least Square has extensive and flexible casual modelling capabilities, which makes it superior to the first generation modelling (such as correlation, regression, etc.), and is especially advantageous for studies that include formative constructs (Lowry & Gaskin, 2014). The other two advantages of using SEM-PLS are the attributes of non-normal data and small sample size. SEM-PLS is an excellent technique to use for non-normal data, where there is the risk of underestimated standard error and inflated goodness-of-fit in techniques like CB-SEM (M. Lei & Lomax, 2005). PLS-SEM necessitates smaller sample sizes compared to covariance-based SEM, which can be influential for highly complex models (Hair, Sarstedt, Hopkins, & Kuppelwieser, 2014). We apply SmartPLS for path modelling and analysis of latent variables of the model.

The SEM-PLS model is presented in two different sub-categories; the inner model shows the relationship between the dependent and independent latent variables, and the outer model gives the relationship between latent variables and their indicators. In addition, some parts of our inner model have hierarchical components, which drives us to use a high-order model of SEM.

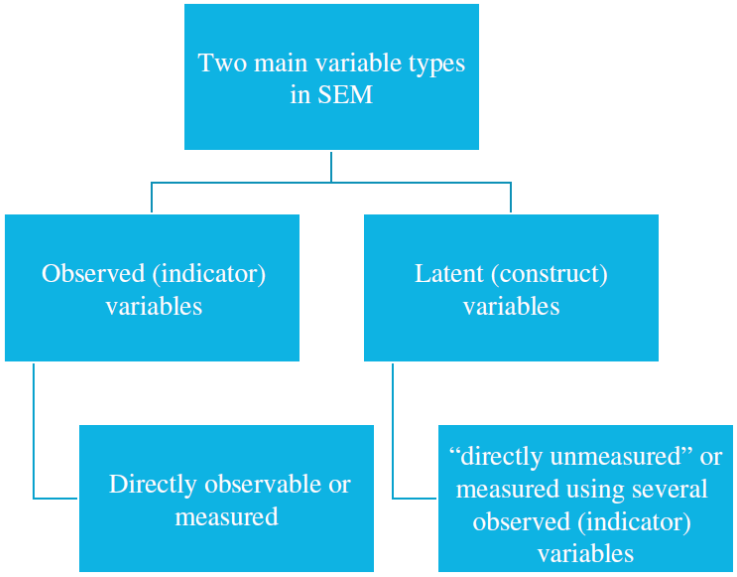

Figure 3-2 - Variable types in SEM

3.4.1. The Hierarchical Model of Structure Equation Modeling (SEM)

PLS path modelling has the advantage of using manifest variables repeatedly for hierarchical models (Guinot, Latreille, & Tenenhaus, 2001; Wetzels, Odekerken-Schröder, & van Oppen, 2017). This modelling connects all the indicators (manifest variables) of the lower-order latent variables to the higher-order variable. Manifest variables are used twice, in both the lower and higher-order latent variables, as primary and secondary loadings. By determining the outer model, we can also specify the inner model for the hierarchical component in the model. After determining the latent variables in first-order using path analysis, then they can be used as manifest variables for path analysis of second-order latent variables (Wetzels et al., 2017).

Hierarchical latent variables are one of the advantages of using PLS-SEM, which allows researchers to have more advanced and sophisticated models. The most used models in previous research are the reflective models, which have a different outer model than formative models (J. M. Becker, Klein, & Wetzels, 2012).

The number of levels (Rindskopf & Rose, 1988) and the nature of the relationship between the constructs in the model specify the type of hierarchical latent variables (Wetzels, Odekerken-Schröder, & Van Oppen, 2009). The reflective higher-order shows that the general concept consists of some unobserved variables, which in the case of the formative higher-order construct is the combination of several latent variables that include manifest variables (Edwards, 2001; Wetzels et al., 2009).

Based on the relationship between first-order variables vs. their manifest variables; and second-order variables vs. their related first-order latent variables, there are four types of the second-order hierarchical model (J. M. Becker et al., 2012). In the reflective-reflective type, the first-order variables are correlated and reflectively measured, which is a hierarchical standard factor model (Lohmöller, 1989). According to N. Lee & Cadogan (2013), this type of model is meaningless, and in the worst-case, misleading. Reflective constructs should be unidimensional and interchangeable, which does not adapt to the concept of multiple reflective dimensions, or it is better to use a reflective-formative model instead (N. Lee & Cadogan, 2013). Besides the formative-reflective, that is rather scarce, the lower-order constructs in the reflective-formative model are not interchangeable, but form a standard higher-order latent variable (Chin, 1998).

At last, the formative-formative type model helps us to subtotal some concepts into one general variable. This model can be useful to categorize many indicators into some sub-constructs (J. M.

Becker et al., 2012). The model in this study has two aspects: one consists of unidimensional reflective constructs, and the other ones are two second-order Formative-Formative sub-models.

3.5. Research Design and Method Appropriateness

The research design will define our research plan, which specifies the whole idea of performing the research using data and information we can acquire. One of the essential steps in research is to choose the research methodology, which determines the steps to collect and analyze data (Draper, 2004). In this research, we will employ explanatory research; since it is based on using a dataset to investigate some theories, we already have some previous research. Considering the specification of our study, we will use a dataset cultivated from a sample population of end users to study behavioural attitudes, which indicates the necessity of using a quantitative methodology for the research.

One most common classification of methods is quantitative vs. qualitative. The selection of the methodology depends on factors such as research context, purpose and nature of the study (Bryman & Burgess, 1999). We apply the quantitative method in this research, considering the advantages of better presentation capability (Weidemann & Fitzgerald, 2008) and being recommended for social studies (Cohen & Manion, 1980).

Advantages of Quantitative Research for This Study

The quantitative methodology is used for two reasons; first, to find the relationship between different factors in the model and see the degree of relationship using analytical techniques such as correlation and cluster analysis. Moreover, by using the quantitative method, we can have a basis for comparing our research with other research, and future studies can compare their results with this study.

3.6. Survey Instrument Design and Data Collection

To use the quantitative method, a survey is designed to collect data from a sample population, which later will be analyzed using Partial Least Square (PLS) method. An online Web Survey questionnaire was developed through various social media platform since electronic surveys have the advantage of expanding the capabilities of questionnaire development, and are more efficient for data collection and analysis (Alshumaimeri, 2001). We called for participation on various email lists. The survey comprised multiple questions about security and privacy practices of individuals, clustered into demographic information systems, technographic behavioural items, and psychographic perception based questions, to correlate the primary independent determinant for security and privacy primitives.

There are multiple groups of questions; each of them has one or more questions under each category. According to Felt et al. (2012), users do not take smartphone permission warnings seriously mainly because of the frequency of notices they receive. As such, there is a need to define traits that show the differences in various groups of users, which requires scales representing the different behavioural aspects of users.

The preferred method is self-reporting of security behaviour by end-users, resulting in a reliable set of factors affecting users' practices (Egelman & Peer, 2015). On the other hand, there is always the concern that participants answer the questions with a bias of not wanting to show the wrong attitude or behaviour toward cyber security (Crowne & Marlowe, 1960). The probability of biased self-stated data by users shows the necessity of adding other factors to make the data more reliable (Acquisti & Grossklags, 2005). For this matter, there has been much effort paid to finding a relationship between major human characteristics and their behaviour in cyber space.

In addition to the demographic information of respondents, there are psychographic questions to measure all aspects of latent variables, from all types of descriptive, multi-optional, 5-point and 7-point Likert. The Likert scale is a psychometric response scale used in questionnaires to investigate the degree of agreement respondents have toward a set of statements (Bertram, 2007). The Likert scale used in our study ranges from "Very low" to "Very high", "Strongly disagree" to "Strongly agree", "Not at all concerned" to "Extremely concerned", and "Not at all aware" to "Extremely aware". This approach is used to analyze the users' behaviours with a range of questions about their self-awareness and traits toward internet privacy and security.

It should be noted that data collection is conducted through an electronic (online) survey aimed at diverse groups of social media end-users. The online survey was created and hosted at the Telfer School of Management, University of Ottawa.

3.6.1. Construct Measurement Items

The questions designed for each construct are shown in Table 3-5. Moreover, The questionnaire is presented in the appendix.

Table 3-5 - Measurement Items for model constructs

Construct	Measurement Items	Extant Literature
Disposition	Scale of 1 (Strongly disagree) to 5 (Strongly agree) - Compared to others, I am more sensitive about the way online companies handle my personal information. - I am concerned about threats to my personal privacy in online activities. - It is important for me that my personal information is only available to people or organizations whom I have authorized	Adopted from Malhotra et al. (2004)
Concern	Scale of 1 (Not at all concerned) to 5 (Extremely concerned) - Impact of my online activities and interactions on my reputation or image - Social media sites sharing my information with other third-party organizations - Use of my social media profile and activities for data mining by other organizations. - Disclosure of location information to third-parties or strangers - Privacy of my personal or professional information	Adapted from Y. Chen & Zahedi (2016)
Risk	Scale of 1 (Very low) to 5 (Very high) - The risk of social media security threats to the average user is: - The risk of social media privacy breaches to the average user is: - The chance that an average user will fall victim to a security breach through social media is: - The chance that an average user's privacy will be compromised on a social network is: - A social media user's vulnerability to security and privacy issues is:	Adapted from Y. Chen & Zahedi (2016)
Awareness	Level of familiarity, 1 (Not at all aware) to 5 (Extremely aware) - Phishing - Social Engineering - Account Takeover - Clickjacking or Likejacking - Identity Theft	Created using new scales
Social Media Security & Privacy Self-efficacy	Scale of 1 (Strongly disagree) to 5 (Strongly agree) - I have the required skills and knowledge to protect against security threats on social media. - I am able to avoid security threats on social networks. - I have the technologies and resources to protect myself from security threats on social media. - I can take appropriate steps to avoid compromising my private information through social networks. - I am well informed about ways in which I can safeguard my privacy on social networks.	Created using new scales

Technological Self-efficacy	Scale of 1 (Strongly disagree) to 5 (Strongly agree) - I can figure out how to use new technologies reasonably quickly. - I can use new technologies without the help of other people. - I have the knowledge and skills to learn to use new technologies reasonably well on my own.	Adapted from Rhee et al. (2009)
Social Media Security Practices	Scale of 1 (Never) to 5 (Always) attempted/performed - Receive alerts for logins from new devices or browsers - Use my phone as a second-step for logging into social networks - When did you last check or modify the privacy and/or security settings of your social network accounts? - Which of these statements best reflects how you manage your passwords across social media sites?	Created using new scales
Social Media Privacy Practices	Scale of 1 (Never) to 5 (Always) attempted/performed - Limit whether search engines can link to my social media profile - Disable location information to be included automatically with my posts - Limit how others can discover or find me on the social network - Select who can send me friend or follower requests - Review posts or pictures that I am tagged in - Select specific people to share certain content or updates with - Maintain a Restricted List contacts (who won't see posts shared with friends) - Block users so they can't see my activity stream - Limit who can see my connections or friends list	(Kezer, Sevi, Cemalcilar, & Baruh, 2007)
Online Security Tools Use	Scale of 1 (Never) to 5 (Always) attempted/performed (Aggregate Score was used) - Anti-Virus or Anti Malware Software - Anti-Spam Rules or Filters in Email - Safe Web Browsing Tools - Password Management Tools - Two-Step Authentication - Biometric Authentication - Security Apps on the Phone	Created using new scales
Online Privacy Tools Use	Scale of 1 (Never) to 5 (Always) attempted/performed (Aggregate Score was used) - Clear Cookies and Browser History - Delete/Edit something I have posted - online in the past - Use a temporary username or email - address online - Browse or Post anonymously	Created using new scales

3.6.2. Design Consideration and Validity of the Survey

The validity of the research is a key requirement of the study since it confirms that the survey measures the items it is supposed to measure (Alshumaimeri, 2001). It is recommended to follow guidelines from similar studies to conduct the survey (Andrews, Nonnecke, & Preece, 2003). As suggested by Bagozzi (1994), this method of designing the survey validates its measurement.

We use Likert questions, as an easily constructed and reliable scale (Nurse, Creese, Goldsmith, & Lamberts, 2011b), having a higher chance to be answered by respondents and be measured easily by the researcher (LaMarca, 2011).

3.6.3. Survey Pre-Test Procedure

To ensure that our survey is error-free, we did the survey pre-test. This helps ensure the data gathering procedure is reliable (Andrews et al., 2003; Preece, Rogers, & Sharp, 2015). A survey pilot is conducted in two steps. At first, the researcher supervisor will assess the survey based on the extensive experience in the field to improve the technical, grammatical and logical aspect of the survey. Then, 20 students from the University of Ottawa participated in the survey, to examine and improve the survey before applying it to the research. It should be noted that the data collected at this stage were not used in the main dataset.

3.7. Data Collection and Survey Administration Procedures

3.7.1. Sampling Frame

The method of representative selection from a dataset is called sampling (Latham, 2007) in order to generalize it to the whole population (Trochim, 2006). Considering the inclusive effect of social media on societies, we can consider everybody as a potential social media end-user. We collected the respondents from a diverse set of demographic specifications, making the sampling more convenient.

3.7.2. Sample Size Requirement

The other important factor for data collection is sample size, which must be determined. In this study, two prospective methods are used (determined before data collection) for estimation of sample size.

We employed the '10-times rule' method which is commonly used in PLS, and has been recommended by many researchers (Hair, M.Ringle, & Sarstedt, 2011; Peng & Lai, 2012). According to this rule, the sample size should be greater than 10 times the maximum number of indicators for a latent construct, or 10 times the maximum number of inner model paths for any latent variable in the model (Chin, Marcolin, & Newsted, 2003; Goodhue, Lewis, & Thompson, 2018).

For our structural model, the maximum number of indicators is nine for the formative second-order social media privacy practices construct; and the same construct has six incoming paths, which are the maximum number of incoming paths for a latent variable. Hence, our minimum sample size using this heuristic was determined to be 90 valid responses. Accounting for non-response rates and incomplete results in the range of 60%, a sampling frame of 150 responses within the duration of our designated data collection period was determined to be adequate.

Secondly, the inverse square root procedure was used as recommended by Kock & Hadaya (2018). This procedure has been shown to yield more precise and safe estimates for the sample size for both normal and non-normal data (Kock & Hadaya, 2018). Using the recommended procedure, the significance level was set to $P < 0.05$, the statistical power to 0.80, and we used the smallest beta coefficient in the results of the structural model estimation from the pilot test ($\beta = 0.15$). This yielded a minimum suggested sample size of 275 respondents. Once again, accounting for non-response rates and incomplete responses in the range of 60%, a sampling

frame of 440 responses was deemed to be adequate for the live survey.

Overall, the goal was to collect at least 440 responses for our survey in order to obtain a minimum of 275 valid responses. Meeting these minimum thresholds would help establish the statistical validity of the statistical analysis.

3.8. Data Analysis and Reporting Procedures

In this section, the data analysis methods and techniques are discussed. At the first step, some numerical features for the demographic and technographic information of the model are highlighted. Then, the relevancy of the exploratory constructs in the model is validated and overviewed. In the end, the testing of the empirical model using SEM technique is thoroughly discussed.

3.8.1. Demographic and Technographic Analysis and Reporting

Descriptive and nonparametric statistical data illustrates the analysis results related to demographic and technographic questions. The graphical features and numerical measures are the advantages of descriptive statistics in presenting useful information (Keller, 2015). Tableau was used as advanced software for visualization and descriptive statistics. Also, nonparametric statistics can be used for nominal or ordinal data (Zhao & Suganthan, 2012), and can compare propositions related to categories of various variables.

3.8.2. Exploratory Factor Analysis

Before the application of SEM, the validity of measurement items will be examined by exploratory factor analysis. It is defined as a statistical procedure used to detect relationships between variables and enables the researcher to condense variables with high correlation into fewer variables in the model (Zhao & Suganthan, 2012). In this study, factors represent the rate of agreement with end users' beliefs, cognitions, attitudes and behaviours toward online privacy and security in social media.

3.8.2.1. Procedures for Extraction and Rotation

For the analysis of the model, factor rotation type, number of factors used and the extraction method are used, in addition to the typical factor analysis or Principal Axis Factoring (PAF). PAF looks for the minimum number of factors for common correlation among different variables, and it does not depend on distributional assumptions of multivariate normality (Mercer, 2013). Besides, in order to represent attitudinal and belief dimensions, Promax rotation will be used to enable correlation among factors (Norusis, 1990). It will help as a fast and conceptually simple solution to fix a target matrix with a simple structure (Abdi, 2003).

At last, in order to specify the dimensionality of factor space, screen cut-off points suggested by Velicer & Jackson (1990) were used as a guide, with consideration of the number of factors in the analysis.

3.8.2.2. Assessment Criteria for Item Validity and Construct Dimensionality

The weight loading of items related to each construct should exceed 0.7 (Nunnally, 1978), or at least 0.6 for new items (Chin, 1998). After finalizing items related to each construct, another iteration of factor analysis is conducted, and the results are compared with the recommended acceptable range (above 0.7 of the Cronbach's alpha) (Allen & Yen, 1981).

3.8.3. Evaluation of Measurement Model Reliability and Validity for Reflective Constructs

The first step of model analysis is to examine the outer model of the study, which should be grouped in two sections: reflective measurement model and formative measurement model. The steps required ensuring the validity, reliability and accuracy of the reflective measurement in the model, and are explained as follows:

- **Outer Loadings on related Construct:** the acceptance rate is 0.7 or higher for outer loadings, and 0.60 for new measurement scales (Chin, 1998). Outer loadings show how strong the relationship is between indicators and their related construct.
- **Item Cross-Loadings:** this item explains that Indicators should have a stronger relationship with their relative construct than other constructs. Item Correlations with Target Construct should be higher compared to its correlations with other constructs in the model (Chin, 1998).
- **Inter-Correlation among constructs cross-tabulated with square roots of AVE:** this validates that a reflective construct should share more variance with its indicators than other constructs in the model. For that matter, It should exceed the inter-correlations between a reflective construct with other constructs in the model (Chin, 1998; Fornell & Larcker, 1981)
- **Average Variance Extracted (AVE) for a Construct:** AVE refers to the proportion of construct variance measured by its relative indicators: AVE above 0.50 shows that the construct explains more than half of the variance in its indicators (Fornell & Larcker, 1981; Hair, M.Hult, M.Ringle, & Sarstedt, 2016).
- **Composite Reliability:** this is a measure of internal consistency reliability of a construct as compared with other constructs in the model, which does not underestimate the internal consistency reliability, as may happen with Cronbach's alpha. Composite reliability prioritizes indicators based on their reliabilities during model estimation, which makes it adaptive to PLS-SEM algorithm method (Hair et al., 2014). It should be higher than 0.60 (Bagozzi & Yi, 1988); or 0.70, according to some researchers (Fornell & Larcker, 1981).
- **Cronbach's alpha:** this also measures the internal consistency reliability of a construct on a single basis, which tests the extent to which all the indicators in a test measure the same

construct (Cronbach, 1951; Tavakol & Dennick, 2011); and its value should exceed 0.70 (Chin, 1998; Cronbach, 1951; Gefen, Straub, & Boudreau, 2000).

3.8.4. Evaluation of Measurement Model Reliability and Validity for Formative Constructs

The steps required to ensure the validity, reliability and accuracy of the formative measurements in the model are explained as per the following:

- **Variance Inflation Factor (VIF):** Opposite to reflective indicators, formative indicators are expected to show unique variance, which means not having high correlations between indicators. The high correlation can lead to unstable indicator weights (Mathieson, Peacock, & Chin, 2001), which make it difficult to determine the influence of each indicator on the related formative construct (Bollen, 1989). VIF examines the risk of multicollinearity of the indicators, which gives the signal for conceptual redundancy among chosen indicators (Cenfetelli & Bassellier, 2017). Considering the higher level of the problems caused by multicollinearity for formative measures (Petter, Straub, & Rai, 2007), VIF should not exceed 3.3 (Diamantopoulos & Siguaw, 2006).
- **Outer Weight:** The outer weights of each indicator expresses each indicators' relative contribution to the construct, or its importance to form the construct. The evaluation of the significance of an indicator creating a construct is done by significance test through Bootstrapping procedure (Hair et al., 2016).

3.8.5. Evaluation of the Structural Model

In order to assess the significance of relationships in the structural model, a round of bootstrapping is conducted. Using the re-sampling technique with 200 replications provides more conservative testing of the parameters. In the following, the various evaluation techniques that apply to the assessment of the inner model are explained.

- **Path Validity Coefficients Significance (p-values):** A path coefficient shows that the relationship between two latent variables is not random. This path should be significant at the <0.05 level to provide support for the proposition in the theoretical model.
- **Predictability:** The quality assessment of a model is its ability to predict the endogenous constructs. It represents the endogenous variables predicted by its predictors; or to put it simply, a measure of the model's predictive accuracy (Hair et al., 2014). Falk et al. (1992)

recommended a minimum value of 0.10 for a construct to be considered viable within the nomological network.

- **Global Criterion of goodness-of fit (GoF):** GoF values allow a scalar-based assessment (summative index) of the model as a whole, which allows comparison between competing models. The baseline values: Low fit: 0.1; Medium fit: 0.25; High fit; 0.36 (Falk & Miller, 1992; Wetzels et al., 2009).

4. Data Analysis and Results

This chapter presents highlights of demographic characteristics and social media use attributes for the participants who responded to the survey questionnaire. This is followed by the results of the statistical analysis of the empirical model using PLS-SEM.

4.1. Participant Characteristics and Descriptive Statistics

There was no obligation for the respondents to fill out the questionnaire, which led to some incomplete data records. In addition, there is the risk of error in our dataset, and sometimes the only option is discarding the invalid data (Batista & Monard, 2003). In order to clean the dataset, first we removed the outliers by filtering the responses that were filled out at random, like respondents that answered all questions too positively or negatively. In addition, we discarded responses that had more than 10% missing data.

When data randomness was checked, it was found to be MCAR (Missing Completely at Random). This class of randomness occurs when the missing value for an attribute does not depend on known values or missing data. It allows applying any missing data imputation technique without being concerned about bias (Batista & Monard, 2003). For the remaining records, missing data were imputed using the NIPALS algorithm (Geladi & Kowalski, 1986; Wold, 1966). Our final dataset consisted of 630 valid responses out of 866 responses (approx. 72% valid responses).

4.1.1. Demographic and Attributional Questions

The final dataset comprises 630 participants, with classification as per the following: 60% male, 40% female, 40% with graduate school degree, 52% undergraduate, 8% finished their education with secondary school degree, and ages reached from less than 18 to +65, with 43% between 26-35 as the biggest age group.

Moreover, we tried to recruit participants from different regions, just to avoid the focus of our analysis being based on a single cultural context (Kim, Sohn, & Choi, 2011). The variety of respondents from a geographical perspective allows us to analyze the security and privacy behaviours based on a global trend, which helps us to examine the possibility of differences in users' behavioural traits in different regions and situations. It also should be mentioned that a high percentage of participants completed higher education, and this helps us to predict their higher level of knowledge and self-efficacy toward cybersecurity.

Table 4-1 - Demographic Characteristic of the survey sample

Question	Specification	Category	Frequency	percentage
2	Age	Less than 18	3	0.48%
		18-25	119	19%
		26-35	318	50%
		36-45	117	19%
		46-55	42	7%
		56-65	18	3%
		65+	13	2%
3	Gender	Male	380	60%
		Female	250	40%
4	Degree	Diploma	40	6%
		Undergraduate	297	47%
		Graduate Degree	293	47%
5	Region	North America	171	27%
		Western Europe	51	8%
		East Asia & Oceania	110	17%
		Baltics, Eastern Europe & Near East	133	21%
		Northern & Sub-Saharan Africa	158	25%
		Latin America & Caribbean	7	1%

As illustrated in Figure 4-1 and Figure 4-2, male respondents had a higher average rate of proficiency, whether in general aspects (Technological Self-Efficacy), or Social Network aspects (Social Media Security & Privacy Self-efficacy, and Awareness). The same trend happens in two variables of Security practices, showing that males have a higher rate of self-claimed security practice.

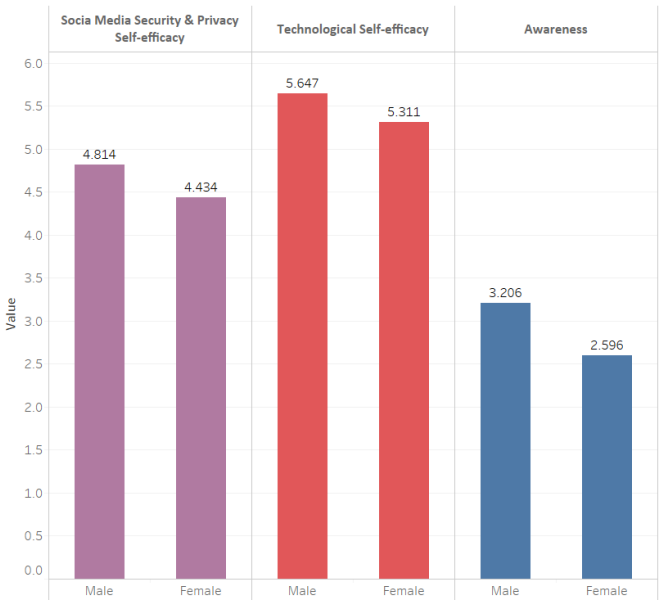

Figure 4-1 - Average rate of major proficiency variables based on Gender

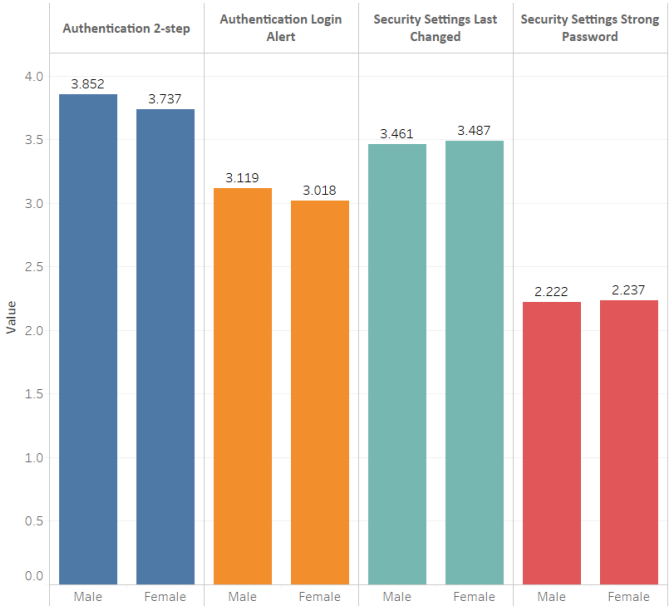

Figure 4-2 - Average rate of Security Practices based on Gender

This trend is the opposite with respect to Social Media Privacy Practices as illustrated in Figure 4-3, in which females show a higher rate of behavioural characteristics. This indicates females tend to be more cautious about privacy-related behaviour in social media. In addition to gender, the educational level can indicate some discrimination among end users' characteristics. Based on Figure 4-4, the higher the educational level, the greater the disposition, concern and risk perception.

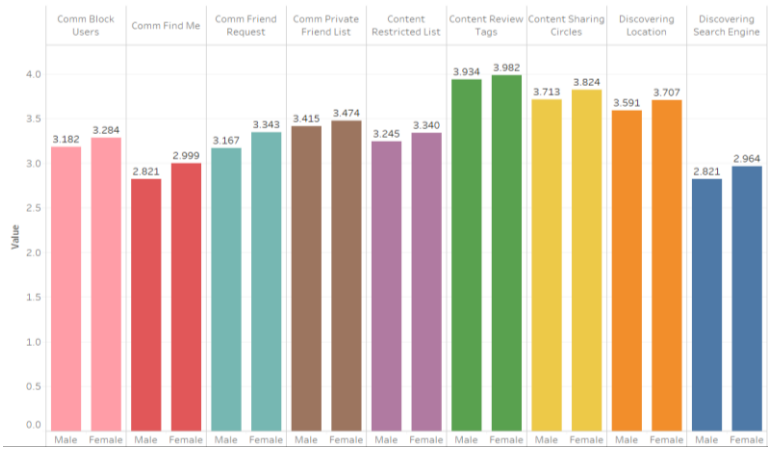

Figure 4-3 - Average rate of Privacy Practices in Social Media based on Gender

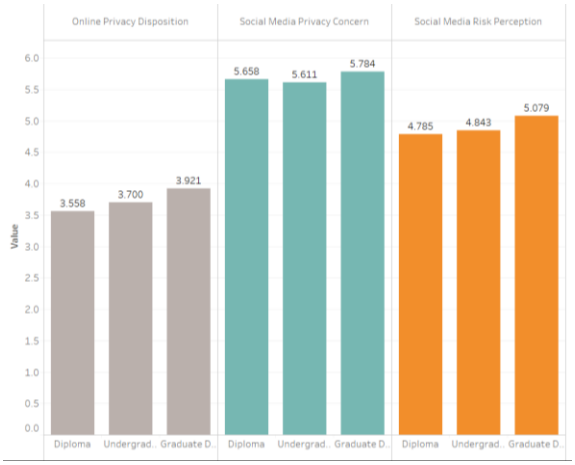

Figure 4-4 - Average rate of Posture variables based on Degree Status

From the perspective of technographic questions, most users tend to have 2-3 social networks (Figure 4-5). The interesting fact from this figure is the number of respondents that have five or

more social platforms: 148 out of 630 (22.2%). In addition, end users usually spent 1-10 hours per week on social networks (Figure 4-6).

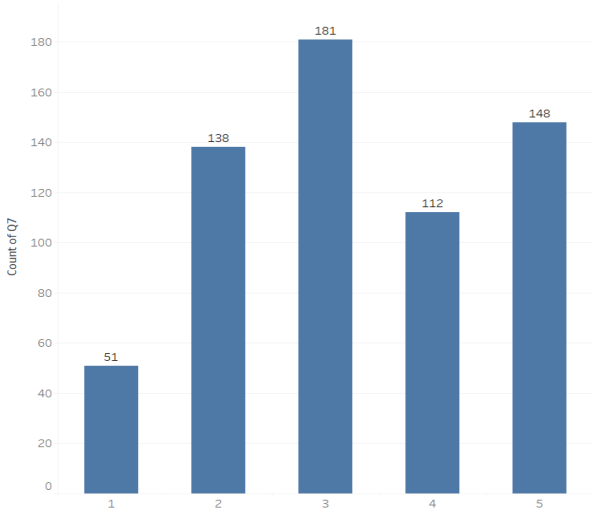

Figure 4-5 - Number of Social Platforms Used by Users

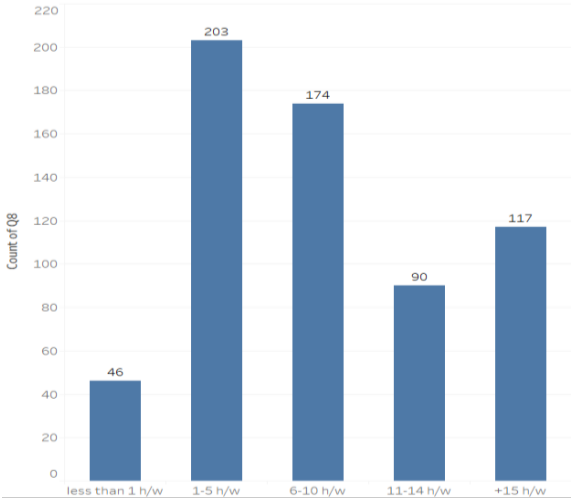

Figure 4-6 - Total Hours Spent on Social Media per week

As illustrated in Figure 4-7, end users tend to have a very small or large network size for their first platform, which shows the completely different functionality they expect from various social networks. About 24% of end users have more than 500 connections in their first platform choice, which shows a diverse type of end user connection. However, the tendency to have a large-scale network size makes end users resistant to sharing too much information as depicted in Figure 4-8.

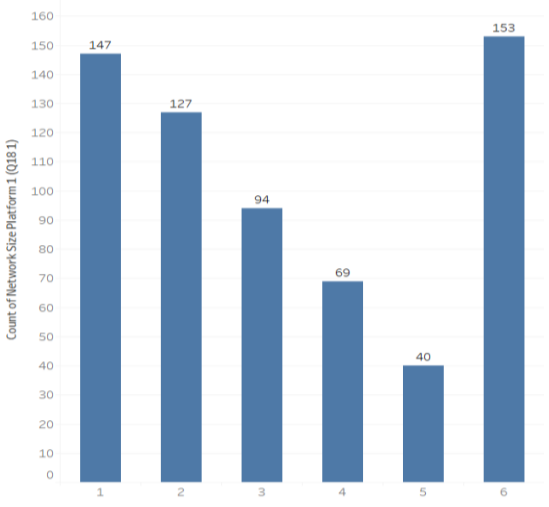

Figure 4-7 - Network Size for First Platform

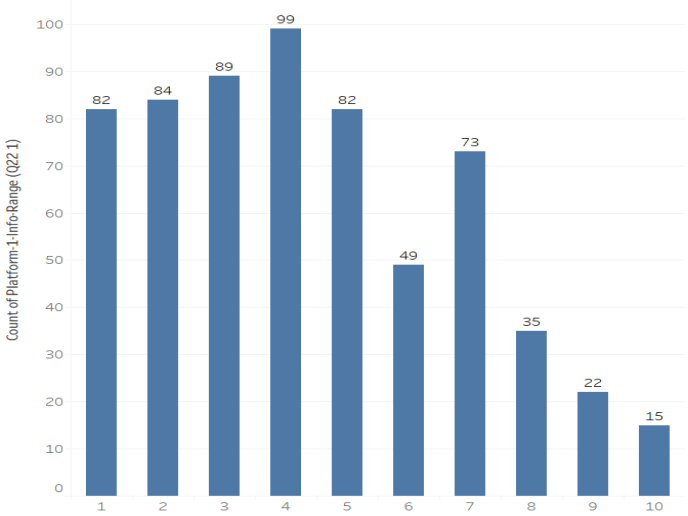

Figure 4-8 - First Platform Information Shared Range

4.2. Measurement Model Evaluation:

In this study, we will evaluate our model through two groups of measurements: first validating the reflective constructs using techniques like composite reliability, AVF and Cronbach's alpha; and validating the formative constructs using collinearity assessment and significance & relevance assessment for outer weights.

4.2.1. Evaluation of Reflective Constructs Measurement

The first step in model validation is to ensure the validity of constructs by measuring discriminant and convergent validity. As subcategories of the construct validity, these two-validity tests work together, and if both discriminant validity and convergent validity occur in a model, it shows sufficient evidence for construct validity. The discriminant validity is the measure of constructs that should not be related to each other, which means that it is possible to discriminate between different constructs. On the other hand, convergent validity relates to measures of constructs that should be related to each other, showing a convergence between similar constructs (Trochim, 2007).

The matrix of loadings and cross-loadings of the model is presented in Table 4-2, showing a high degree of significance for items related to each construct. The criterion here is that the average loading of each construct be higher than 0.7, and this criteria is met or exceeded for all the reflective constructs in our theoretical model.

4.2.1.1. Measurement Model Assessment: Discriminant Validity at Item level

There are two conditions for discriminant validity at the item level for reflective constructs. The first one is that the magnitude of the loadings exceeds 0.7, and the second one is that the loading of each item be higher with the related constructs compared to the loadings with other constructs. As seen in Table 4-2, these criteria are met, and this leads us to infer that our model demonstrates adequate discriminant validity at the item level.

Table 4-2 - Matrix of Loading and Cross Loadings

Measurement Items	Model Construct												
	Reflective Constructs								Formative Constructs				
	OPD	OPTU	OSTU	SMPC	SMRP	SMSPSE	SMSTA	TSE	Auth	Sec_sett	Comm	Cont	Disc
OPD_1	0.837	0.114	0.16	0.407	0.351	0.13	0.126	0.113	0.131	0.096	0.171	0.132	0.173
OPD_2	0.9	0.07	0.121	0.505	0.444	0.076	0.111	0.102	0.072	0.028	0.106	0.094	0.144
OPD_3	0.769	-0.006	0.064	0.343	0.273	0.108	0.066	0.119	0.074	0.07	0.122	0.101	0.11
OPTU_Agg	0.076	1	0.484	0.138	0.181	0.363	0.382	0.273	0.32	0.344	0.378	0.325	0.347
OSTU_Agg	0.14	0.484	1	0.164	0.179	0.407	0.437	0.276	0.437	0.412	0.356	0.343	0.38
SMPC_1	0.43	0.1	0.145	0.859	0.349	0.065	0.14	0.144	0.073	0.007	0.116	0.141	0.219
SMPC_2	0.427	0.148	0.174	0.844	0.284	0.087	0.105	0.126	0.075	-0.01	0.137	0.138	0.205
SMPC_3	0.384	0.116	0.14	0.797	0.296	0.077	0.057	0.073	0.081	0.037	0.133	0.118	0.169
SMPC_4	0.438	0.093	0.092	0.831	0.32	0.035	0.045	0.102	0.076	-0.04	0.097	0.121	0.184
SMPC_5	0.428	0.115	0.13	0.81	0.346	0.008	0.079	0.093	0.087	0.003	0.166	0.131	0.218
SMRP_1	0.434	0.088	0.149	0.327	0.806	0.077	0.142	0.119	0.122	0.031	0.094	0.109	0.15
SMRP_2	0.343	0.118	0.145	0.264	0.841	0.102	0.202	0.148	0.077	0.01	0.072	0.069	0.159
SMRP_3	0.328	0.172	0.136	0.353	0.836	0.078	0.144	0.132	0.122	0.01	0.073	0.056	0.127
SMRP_4	0.338	0.186	0.151	0.343	0.845	0.052	0.15	0.157	0.061	0.04	0.051	0.062	0.143
SMRP_5	0.359	0.194	0.16	0.316	0.831	0.076	0.212	0.131	0.087	0.062	0.109	0.098	0.169
SMSPSE_1	0.119	0.313	0.323	0.081	0.126	0.864	0.452	0.432	0.285	0.362	0.259	0.249	0.27
SMSPSE_2	0.084	0.276	0.289	0.032	0.06	0.869	0.44	0.405	0.296	0.329	0.275	0.245	0.325
SMSPSE_3	0.078	0.332	0.379	0.00	0.031	0.845	0.468	0.375	0.262	0.365	0.299	0.258	0.261
SMSPSE_4	0.135	0.273	0.338	0.087	0.106	0.829	0.433	0.384	0.308	0.312	0.236	0.241	0.323
SMSPSE_5	0.1	0.351	0.403	0.074	0.073	0.862	0.488	0.394	0.359	0.427	0.285	0.267	0.354
SMSTA_1	0.113	0.279	0.343	0.06	0.172	0.468	0.851	0.366	0.297	0.324	0.198	0.177	0.283
SMSTA_2	0.132	0.36	0.417	0.086	0.199	0.499	0.896	0.386	0.308	0.339	0.235	0.217	0.301
SMSTA_3	0.11	0.324	0.392	0.101	0.183	0.481	0.906	0.409	0.34	0.299	0.235	0.24	0.328
SMSTA_4	0.081	0.393	0.371	0.052	0.156	0.419	0.814	0.295	0.333	0.307	0.293	0.251	0.322
SMSTA_5	0.089	0.269	0.34	0.149	0.16	0.417	0.806	0.4	0.291	0.241	0.211	0.221	0.332
TSE_1	0.116	0.268	0.275	0.144	0.146	0.474	0.429	0.915	0.305	0.234	0.198	0.237	0.273
TSE_2	0.105	0.226	0.212	0.101	0.16	0.384	0.371	0.907	0.224	0.213	0.152	0.193	0.214
TSE_3	0.137	0.253	0.266	0.11	0.149	0.414	0.386	0.928	0.289	0.248	0.187	0.213	0.248
Auth_1	0.031	0.238	0.389	0.049	0.029	0.225	0.172	0.118	0.777	0.316	0.323	0.304	0.267
Auth_2	0.136	0.288	0.343	0.101	0.145	0.35	0.408	0.352	0.872	0.354	0.389	0.357	0.386
SecSett_1	0.086	0.321	0.352	0.023	0.036	0.372	0.272	0.205	0.334	0.823	0.253	0.245	0.226
Sec Sett_2	0.033	0.244	0.325	-0.02	0.026	0.321	0.309	0.21	0.333	0.818	0.254	0.254	0.254
Comm_1	0.057	0.305	0.25	0.108	0.065	0.245	0.169	0.169	0.272	0.187	0.767	0.577	0.392
Comm_2	0.104	0.319	0.298	0.107	0.103	0.232	0.25	0.135	0.366	0.256	0.737	0.483	0.476
Comm_3	0.131	0.237	0.269	0.108	0.047	0.21	0.166	0.063	0.304	0.235	0.729	0.497	0.444
Comm_4	0.183	0.309	0.293	0.153	0.09	0.285	0.266	0.219	0.402	0.281	0.844	0.579	0.509
Content _1	0.115	0.315	0.331	0.142	0.145	0.268	0.23	0.178	0.349	0.287	0.65	0.906	0.431
Content_2	0.083	0.179	0.202	0.104	0.004	0.201	0.175	0.227	0.309	0.219	0.405	0.64	0.396
Content_3	0.105	0.245	0.251	0.123	0.01	0.23	0.21	0.199	0.315	0.206	0.565	0.809	0.411
Disc_1	0.164	0.243	0.265	0.204	0.135	0.256	0.306	0.237	0.349	0.201	0.475	0.407	0.807
Disc_2	0.116	0.321	0.353	0.19	0.158	0.329	0.29	0.204	0.307	0.275	0.481	0.419	0.822

4.2.1.2. Measurement Model Assessment: Discriminant Validity at Construct level

The next step is to examine discriminant validity among constructs by evaluation of correlations between reflective variables. In order to do so, according to the Fornell-Larcker criterion, the square root of Average Variance Extracted (AVE) should be compared with the calculated correlations. Table 4-3 shows the square roots of AVE are higher than the correlation of the same constructs with other constructs, which leads to the inference that the discriminant validity of the model is acceptable (Fornell & Larcker, 1981). An AVE value of 0.50 or higher indicates that the construct explains more than the half of its indicators. Inversly, AVE values of less than 0.50 indicate that more variance remains in the error than the variance explained (Hair et al., 2016).

Table 4-3: Average Variance Extracted and Inter-Construct Correlations

Measurement Items	Model Reflective Constructs							
	OPR	OPTU	OSTU	SMPC	SMRP	SMSPSE	SMSTA	TSE
Online Privacy Disposition	**0.837**	-	-	-	-	-	-	-
Online Privacy Tools Use	0.076	**1**	-	-	-	-	-	-
Online Security Tools Use	0.14	0.484	**1**	-	-	-	-	-
Social Media Privacy Concerns	0.509	0.138	0.164	**0.829**	-	-	-	-
Social Media Risk Perceptions	0.436	0.181	0.179	0.386	**0.832**	-	-	-
Social Media Security Privacy Self-Efficacy	0.121	0.363	0.407	0.064	0.092	**0.854**	-	-
Social Media Security Threats Awareness	0.124	0.382	0.437	0.104	0.204	0.535	**0.855**	-
Technology Self Efficacy	0.131	0.273	0.276	0.131	0.165	0.466	0.434	**0.917**

4.2.1.3. Measurement Model: Convergent Validity

The convergent validity is assessed by evaluating three criteria, which are Cronbach's alpha, the composite reliability, and AVE. In the first step, the internal consistency reliability will be evaluated. The Cronbach's alpha is applied to measure the reliability for a set of construct indicators based on the inter-relatedness of indicators (Tavakol & Dennick, 2011). A value of 0.70 or above is considered a good indicator of internal reliability. Additionally, the composite reliability of all model constructs is over 0.7. The final step for examining convergent validity is to assess AVE. The rate of above 0.68 (almost all of them above 0.7) for all the constructs ensures the constructs are reliable and reflective in the model (Chin, 1998; Fornell & Larcker, 1981).

Table 4-4: Constructs Statistics – Convergent Validity

Construct	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Online Privacy Disposition	0.788	0.875	0.7
Online Privacy Tools Use	1	1	1
Online Security Tools Use	1	1	1
Social Media Privacy Concerns	0.886	0.916	0.686
Social Media Risk Perceptions	0.889	0.918	0.692
Social Media Security Privacy Self-Efficacy	0.907	0.931	0.729
Social Media Security Threats Awareness	0.908	0.932	0.732
Technology Self-Efficacy	0.905	0.94	0.84

4.2.2. Evaluation of Formative Constructs Measurement

The most significant difference between formative variables and reflective variables is that the formative variables are assumed to be error free (Diamantopoulos & Siguaw, 2006), which makes them useless in assessing internal reliability. Unlike reflective constructs, we apply formative measures to compose a construct, which necessitates detecting all the extreme measures through content validity. Otherwise, the omission of essential indicators can affect the incomplete representation of the construct (Petter et al., 2007).

In our research, we utilized indicators for social media security and privacy practices from other studies and added to these indicators based on our own research into security and privacy best practices that are recommended for end-users. Content validity was hence addressed through literature review, as well as validation among research team members.

4.2.2.1. Assess Formative Measurement Models for Collinearity Issues

Unlike reflective indicators, we do not expect formative indicators to be interchangeable, which means that indicators should not have a high correlation with each other. The high correlation is referred to as collinearity, and when there are more than two formative indicators, it is called multicollinearity, which should not happen in formative constructs.

A high level of collinearity can cause the risk of false path weights, show many indicators to be low or non-significant, or even show an opposite sign for indicator's correlation with its construct (Cenfetelli & Bassellier, 2017). The weight path for formative indicators represents each indicator's contribution to its construct. As standard error for formative indicators

increases, it leads to underestimated significance of these indicators with their related constructs (Hair et al., 2014). As Table 4-5 illustrates, all the outer VIFs (Variance Inflation Factor) in the model are below 3.3, which shows there is no collinearity between our formative constructs in the model (Diamantopoulos & Siguaw, 2006).

Table 4-5 - Assessment of Collinearity for formative constructs

Formative Indicators	VIF
Auth_1	**1.159**
Auth_2	**1.159**
SecSett_1	**1.136**
Sec Sett_2	**1.136**
Comm_1	**1.42**
Comm_2	**1.564**
Comm_3	**1.434**
Comm_4	**1.742**
Content_1	**1.474**
Content_2	**1.354**
Content_3	**1.727**
Disc_1	**1.121**
Disc_2	**1.121**

4.2.2.2. Assessment of the Significance and Relevance of the Formative Indicators

The other criterion for evaluation of the formative indicators in our model is the outer weights. The outer weights of each indicator express each indicator's relative contribution to the construct, or its importance in forming the construct. To find out whether the formative indicators are essential in developing a construct, we should evaluate its significance by bootstrapping procedure (Hair et al., 2016). Bootstrapping is also crucial in the examination of structural model path coefficient, which is presented in the next section.

Table 4-6 illustrates the outer weights between each formative indicator and their related construct, which shows that all relationships between formative constructs and their indicators are significant at $P < 0.01$.

Table 4-6 - Formative Outer Weights

Formative Indicators	1st Order Formative Constructs				
	Authentication	**Security Settings**	**Communication**	**Content Sharing**	**Discoverability**
Auth_1	0.527	-	-	-	-
Auth_2	0.677	-	-	-	-
SecSett_1	-	0.613	-	-	-
Sec Sett_2	-	0.606	-	-	-
Comm_1	-	-	0.362	-	-
Comm_2	-	-	0.242	-	-
Comm_3	-	-	0.299	-	-
Comm_4	-	-	0.387	-	-
Content_1	-	-	-	0.634	-
Content_2	-	-	-	0.25	-
Content_3	-	-	-	0.328	-
Disc_1	-	-	-	-	0.602
Disc_2	-	-	-	-	0.625

4.3. Structural Model Evaluation

In this section, the path validity coefficient in the model is examined using bootstrapping mode in SmartPLS. The P-value is examined to determine which paths are significant. Figure 4-9 represents the details that indicate which relationships are significant in the model.

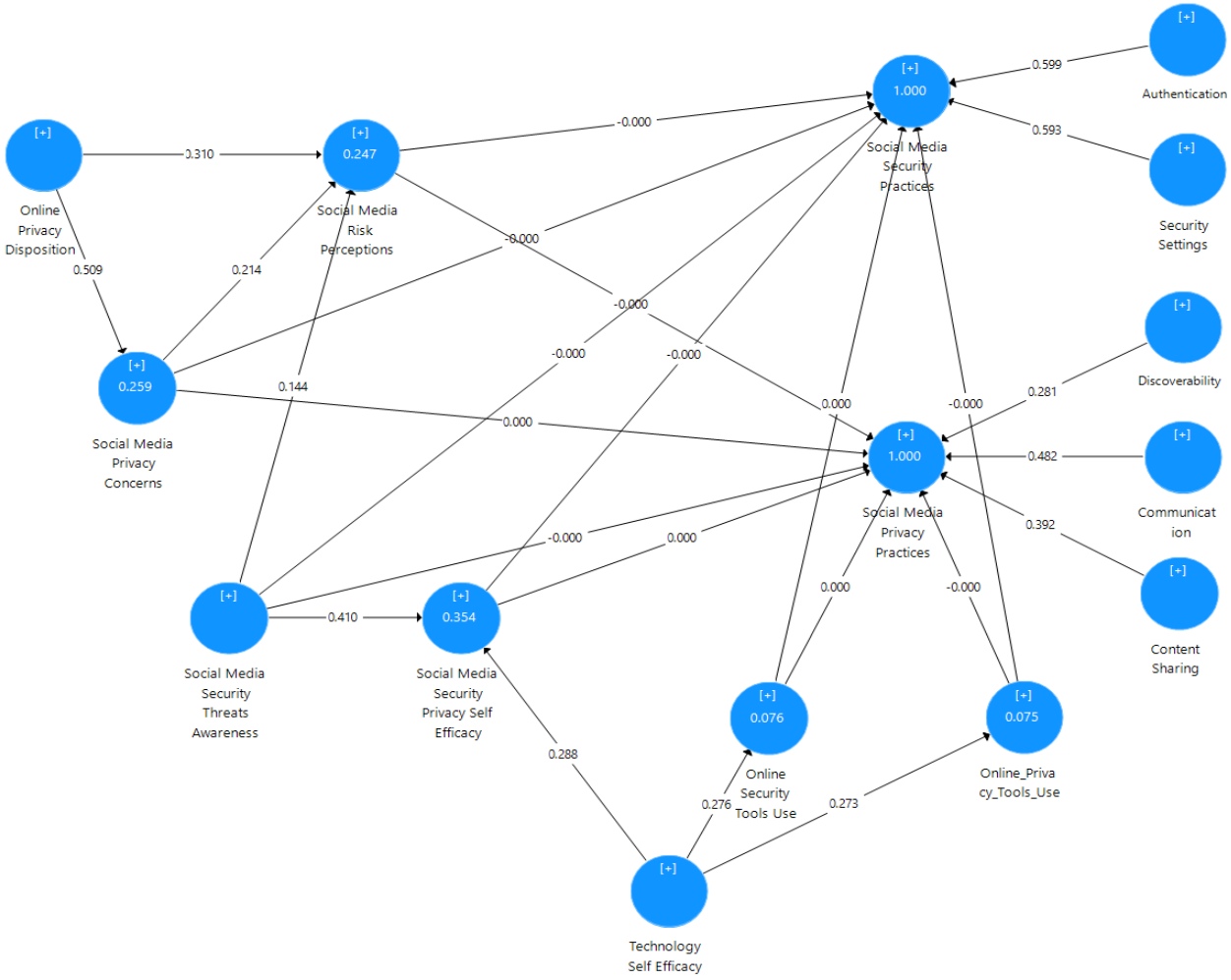

Figure 4-9: Structural Model Result

4.3.1. Predictability of Model Constructs

The next criterion for model analysis is R^2, the assessment predictability and coefficient of determination, which explains the variance of the construct that can be predicted by its antecedent constructs. All the R^2 values in our model are above twenty percent, as shown in Table 4-7, validating the predictability of the endogenous constructs in our model.

Table 4-7: Constructs Coefficients of Determination (R^2)

Latent Variable	R Square
Social Media Privacy Concerns	0.259
Social Media Privacy Practices	0.277
Social Media Risk Perceptions	0.247
Social Media Security Practices	0.362
Social Media Security Privacy Self-Efficacy	0.354

Based on the above table, we can see that all the endogenous constructs in our model have a strong correlation with their connected constructs.

4.3.2. Path Validity

Table 4-8 shows the path validity of the first-order formative constructs with their related second-order constructs using bootstrapping with 2000 sub-samples. Based on this table, all the relationships between first and second order formative constructs are significant in the model.

Table 4-8 - Path validity of first order formative variables with their related second-order constructs

Formative Path	Sample Mean (M)	P Values	Significance Level	Validation
Authentication -> Social Media Security Practices	0.599	0	< 0.001	**Supported**
Security Settings -> Social Media Security Practices	0.593	0	< 0.001	**Supported**
Communication -> Social Media Privacy Practices	0.483	0	< 0.001	**Supported**
Content Sharing -> Social Media Privacy Practices	0.391	0	< 0.001	**Supported**
Discoverability -> Social Media Privacy Practices	0.281	0	< 0.001	**Supported**

Moreover, Table 4-9 shows the relationship between the constructs in the empirical models, showing that the majority of the relationships in the model are significant. The P-value in both tables shows that most relationships have significance at 0.01 of the alpha level.

Table 4-9: Combined Data Path Validity Analysis

Inner Model Relationship	Path Coefficient	Sample Mean (M)	P Values	Sign. Level	Validation
Online Privacy Disposition -> Social Media Privacy Concerns	**0.509**	**0.509**	**0**	< 0.001	**Supported**
Online Privacy Disposition -> Social Media Risk Perceptions	**0.310**	**0.31**	**0**	< 0.001	**Supported**
Online Privacy Tools Use -> Social Media Privacy Practices	**0.209**	**0.21**	**0**	< 0.001	**Supported**
Online Privacy Tools Use -> Social Media Security Practices	**0.123**	**0.122**	**0.001**	< 0.001	**Supported**
Online Security Tools Use -> Social Media Privacy Practices	**0.193**	**0.191**	**0**	< 0.001	**Supported**
Online Security Tools Use -> Social Media Security Practices	**0.304**	**0.304**	**0**	< 0.001	**Supported**
Social Media Privacy Concerns -> Social Media Privacy Practices	**0.133**	**0.133**	**0.001**	< 0.001	**Supported**
Social Media Privacy Concerns -> Social Media Risk Perceptions	**0.214**	**0.212**	**0**	< 0.001	**Supported**
Social Media Privacy Concerns -> Social Media Security Practices	-0.030	-0.03	0.4	N. Sig.	Rejected
Social Media Risk Perceptions -> Social Media Privacy Practices	-0.019	-0.02	0.609	N. Sig.	Rejected
Social Media Risk Perceptions -> Social Media Security Practices	-0.023	-0.025	0.51	N. Sig.	Rejected
Social Media S/P Self Efficacy -> Social Media Privacy Practices	**0.171**	**0.17**	**0**	< 0.001	**Supported**
Social Media S/P Self Efficacy -> Social Media Security Practices	**0.225**	**0.225**	**0**	< 0.001	**Supported**
Social Media Security Threats Awareness -> Social Media Privacy Practices	0.071	0.074	0.116	N. Sig.	Rejected
Social Media Security Threats Awareness -> Social Media Risk Perceptions	**0.144**	**0.144**	**0**	< 0.001	**Supported**
Social Media Security Threats Awareness -> Social Media Security Practices	**0.138**	**0.138**	**0.001**	< 0.001	**Supported**
Social Media Security Threats Awareness -> Social Media S/P Self Efficacy	**0.410**	**0.411**	**0**	< 0.001	**Supported**
Technology Self Efficacy -> Online Privacy Tools Use	**0.273**	**0.273**	**0**	< 0.001	**Supported**
Technology Self Efficacy -> Online Security Tools Use	**0.276**	**0.277**	**0**	< 0.001	**Supported**
Technology Self Efficacy -> Social Media S/P Self Efficacy	**0.288**	**0.286**	**0**	< 0.001	**Supported**

4.3.3. Global Goodness of Fit

The goodness-of-fit is the geometric mean of the average AVE and the average of the R^2 (for endogenous constructs), as a global validation of the model (Tenenhaus, Vinzi, Chatelin, & Lauro, 2005).

The following formula is used to present the Goodness-of-fit:

$$GoF = \sqrt{\overline{AVE} \times \overline{R^2}}$$

$\overline{AVE}$ and the $\overline{R^2}$ are the weighted averages of AVE and average R^2 respectively.

Considering the fact that there are no specific heuristics for GoF, and the proposed validation criteria for AVE is expected to be above 0.5 (Fornell & Larcker, 1981), as presented by formulation, this results in a baseline value for GoF as Gof small= 0.1; GoF medium = 0.25; and

GoF large = 0.36 (Wetzels et al., 2009). After calculation of the GoF, it is compared with the baseline considered. As illustrated in Table 4-10, having a GoF = 0.468 exceeds the large effect size of above 0.36.

Table 4-10 Goodness of Fit

Construct	Average Variance Extracted (AVE)	R Square
Online Privacy Disposition	0.700	Exogenous
Social Media Privacy Concerns	0.686	0.259
Social Media Risk Perceptions	0.692	0.247
Social Media Security Privacy Self-Efficacy	0.729	0.354
Social Media Security Threats Awareness	0.732	Exogenous
Technology Self-Efficacy	0.840	Exogenous
Social Media Privacy Practices	Formative	0.277
Social Media Security Practices	Formative	0.362
Average	0.730	0.300
Goodness-of-Fit	**0.468**	

5. Discussion and Conclusion

Following the quantitative analysis in the previous chapter, this chapter will present the main results from our analysis in the context of the extant literature and also offer our key take-aways. The chapter concludes with a discussion of our study's contributions to theory and practice, its limitations, and some suggestions for future research directions.

5.1. Theoretical Model Validation

The final results of our analysis are presented in Figure 5-1, with all path coefficients for hypotheses posited in our theoretical model We will discuss each hypotheses within the themes of posture, proficiency, and practices individually in this section

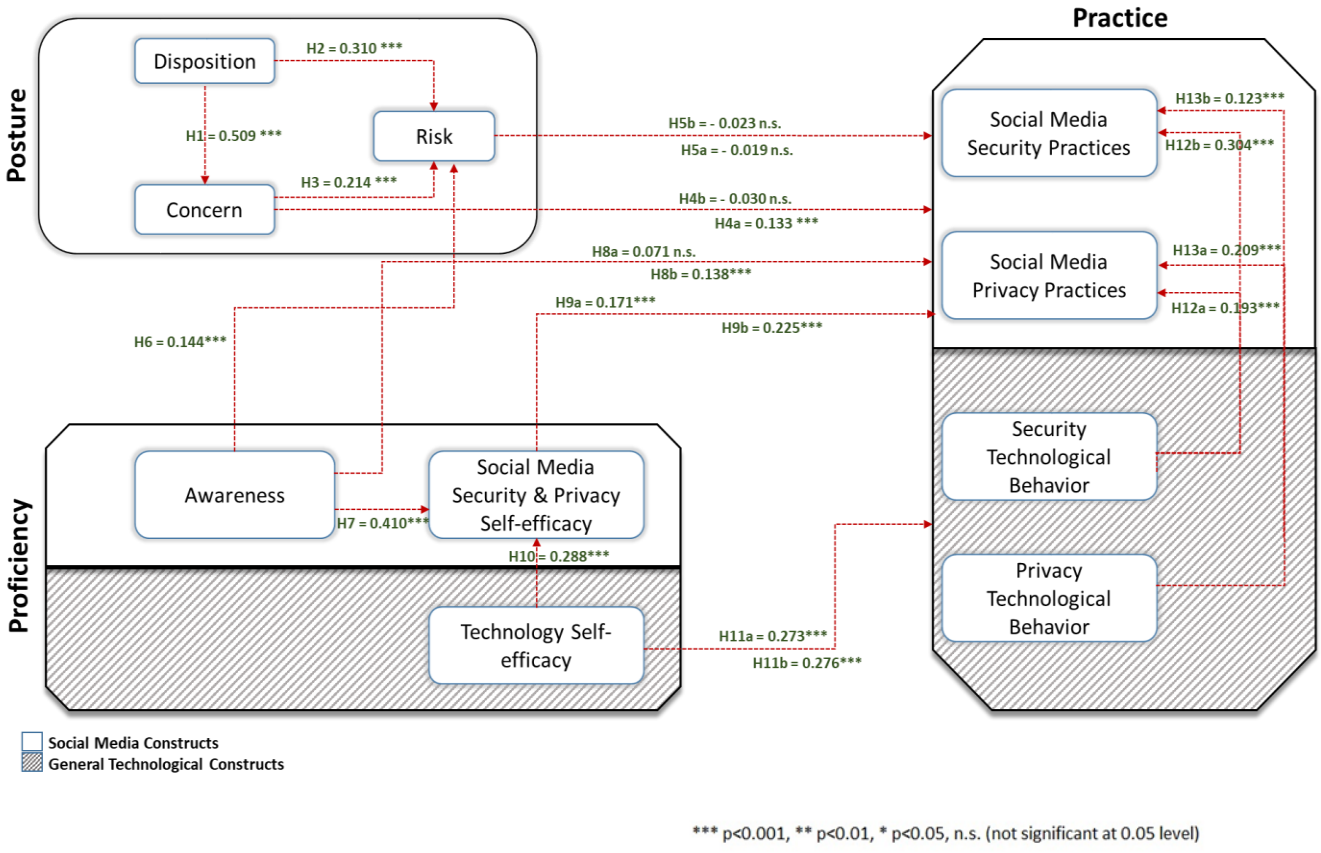

Figure 5-1 - Structural Model Validity

5.1.1. Posture

The analyzed data shows that posture variables have strong relationships among them, but their relationships to security and privacy practices are not as strong. Surprisingly, three out of four hypotheses posited between posture and practices variables were not supported in our analysis. These results are discussed in the next subsections.

5.1.1.1. Online privacy disposition and social media privacy concern

Online Privacy Disposition affects Privacy Concern as an influential antecedent based on many studies. Li (2014) investigated the relationship between Privacy Disposition and Online Privacy Concern, also uncovering the moderating and antecedent factors for disposition. They proposed that users' privacy disposition has a positive impact on their privacy concern, especially for websites with lower popularity and familiarity. The relationship between privacy disposition and privacy concern highlights the fact that privacy issues are not just related to technological factors but also the psychological aspects of Internet users (Yao et al., 2007).

It makes intuitive sense that users who do not value privacy do not exhibit as many concerns about privacy violations on social media (Xu, Dinev, & Smith, 2011). Similar to Xu et al. (2011), the results of the analysis confirms the significant correlation between these two constructs.

- H1: Online Privacy Disposition has a positive effect on Social Media Privacy Concern (Supported - β=0.509, P<0.001).

5.1.1.2. Online privacy disposition and social media risk perception

The privacy disposition is a personality attribute and a general tendency to preserve personal information, and the higher this disposition, the more it affects risk perception (Xu et al., 2011). Xu et al. (2011) specified disposition as the inherent personal trait that set the limitation to control users' own space in the cyber environment.

The reverse relationship has also been validated, investigating the positive impact of risk perception on users' privacy disposition according to Y. Li (2014), privacy experiences will increase users' awareness, which will lead to more concern and disposition for privacy.

The results from our model confirm the significant correlation between these two constructs. It can be justified that the cognitive perception of users toward privacy increases their awareness

toward privacy issues, which make them more sensitive about the risk impacts. Consequently, users will be more aware of the risks in social networks, which can drive them to form cognitive recognition to behavioural change.

- H2: Higher Online Privacy Disposition increases Social Media Risk Perception (Supported - β=0.310, P<0.001).

However, it should be noted that the privacy disposition does not make the users utterly aware of the impact of the risks. There may be an issue that even though end-users are aware of the privacy risk, they have not recognized the extent of its impact, mostly because of the lack of experience about that threat.

5.1.1.3. Social media privacy concern and social media risk perception

Many research studies have investigated the relationship between these two constructs, considering privacy concern or the privacy risk as to the antecedent, but in the context of the general online environment. Based on Liao, Liu, & Chen (2011), perceived privacy risk has a significant correlation with privacy concern.

In this study, we aim to explore the reverse relationship, the social media privacy concern as antecedent and social media privacy risk as consequent. Malhotra et al. (2004) considered privacy concern as a reflection of users' privacy pre-disposition, which is regarded as an antecedent to privacy risk perception. In addition to the assessment of the relationship between general privacy concern and perceived privacy risk, there has been some research exclusively related to the field of social networks. Based on empirical studies in that field, it has been confirmed that privacy concern will positively influence the social media perceived privacy risk, considering that end users believe their personal information may be misused. Moreover, this privacy concern leads to a negative impact on trust in social networks (Lo, 2010).

The findings are entirely consistent with the previous studies regarding the impact privacy concern has on perceived privacy risk in social networks.

- H3: Social Media Privacy Concern has positive effect on Social Media Risk Perception (Supported - β=0.214, P<0.001).

The information shared in social networks makes users concerned about the risk to their privacy, which even can push them to stop using social networks (Zhou & Li, 2014). There have been other strategies for end users to deal with privacy risk, such as reporting falsified information, which with awareness and self-disclosure training, users can view social networks as a safe environment for self-presentation and identity construction (Krasnova, Günther, Spiekermann, & Koroleva, 2009).

5.1.1.4. Social media privacy concern and social media S/P practices

Many researchers have studied the relationship between general privacy concern and users' behavioural intention and practices. Li (2014) considered privacy concern an antecedent for users' behaviour in the online environment, while presenting privacy disposition as affecting privacy concern; considering privacy concern as a mediator between privacy pre-disposition and privacy behaviours. Privacy concern is an important factor in social cognitive and protection motivation theories, which aim to explain cybersecurity behaviours in social networks (Mohamed & Ahmad, 2012). Young & Quan-Haase (2009) investigate users' privacy practices, especially information content sharing on Facebook. They explain that information disclosure cannot be examined in isolation, but privacy protection practices show users' reaction to privacy concern in social media, which has a negative correlation with privacy concern.

Following these studies, we analyzed the relationship between social media privacy concern and cybersecurity practices, with the difference that we separated privacy and security practices and examined the relationship between privacy concern with these two constructs separately. The path validation result presents a significant relationship between privacy concern and privacy practices in social media. On the other hand, the relationship between privacy concern and security practices is not significant, and we reject that hypothesis.

- H4a: Higher Social Media Privacy Concern leads to better Privacy Practices in social media (Supported – $\beta = 0.133$, $P<0.001$).
- H4b: Higher Social Media Privacy Concern leads to better Security Practices in social media (Rejected – $\beta = -0.030$, $P<0.05$).

This difference shows that privacy practices are influenced by posture variables and how people think about privacy related breaches. Nevertheless, posture constructs do not have a substantial

impact on security practices, which distinguish the different antecedents for this construct compared to privacy practices.

5.1.1.5. Social media risk perception and social media S/P practices

Privacy risk perception is undeniably one of the critical antecedents for privacy and security practices in social media. Based on a study, awareness of privacy risk negatively affects users' self-disclosure behaviour in social media (Krasnova et al., 2010). Lo (2010) explained that perceived risk has a stronger impact on privacy practices compared to other factors like trust because self-disclosure sensitivity can hurt trust in social networks.

In our study, both hypotheses for the relationship between privacy risks with social media privacy/security practices were unsupported. This shows there is no significant relationship between these items, which contradicts previous studies examining this relationship.

- H5a: Social Media Risk perception has a positive effect on Privacy Practices (Rejected – $\beta = -0.019$, $P<0.05$).
- H5b: Social Media Risk perception has a positive effect on Security Practices (Rejected – $\beta = -0.023$, $P<0.05$).

One of the reasons for this insignificance can be related to the existence of other significant variables affecting privacy and security practices, which shows the risk is not the only influential construct as behaviour's antecedent. The benefits of social networks such as communicating and interacting with family, friends and new people; interacting with virtual communities and groups; and posting photos and news about our personal experience result in the acceptance of even high-level risks by end users (Acquisti & Enhancing, 2006). Perceived risk can push end users to acquire knowledge about social media risk, but it cannot prevent them from preferring short term benefits over risks that they have not experienced yet (Deuker, 2010; Pötzsch, 2009), which make it an abstract concept for them (Barth & de Jong, 2017).

5.1.2. Proficiency

Proficiency has not been investigated as much as posture and its constructs in social media. The research in cybersecurity has been more general, or has investigated the relationship of posture constructs with users' behavioural practices. Seven out of eight hypotheses between proficiency

with practice-related constructs were supported in our model, showing the importance of this aspect of end-users' characteristics in social networks.

5.1.2.1. Social media security threats awareness and social media Perceived Privacy Risk

Huang, Patrick Rau, Salvendy, Gao, & Zhou (2011) examined the relationship between information security perceived awareness and perceived security (reverse of perceived risk). They validate that perceived awareness is significantly correlated with perceived security, and as a result, with perceived risk. The reverse relationship has been examined by Egelman & Peer (2015) and Gratian et al. (2018), which validated that risk-taking is a significant predictor of threat awareness. They considered threat proactive awareness a component of security behaviour, which will be affected by end users' risk preferences.

The relationship in our study examines the correlation between these two constructs in the context of social media. Based on the statistical results, social media security threat awareness is significantly correlated with social media risk perception, which supports the hypothesis of a positive relationship between these two constructs.

- H6: Social Media Security Threat Awareness has a positive effect on social media Risk Perception (Supported – $\beta = 0.144$, $P<0.001$).

Based on this relationship, more security awareness will increase end users' knowledge toward security threats, which will have a positive effect on users' risk perception. This shows the effect that proficiency (as a cognitive construct) can have on posture (as an affective construct), towards security and privacy on social media.

5.1.2.2. Social media security threat awareness and social media S/P self-efficacy

The relationships between these two variables have not been studied frequently in social media privacy and security research, as most studies focus on the investigation of disposition, concerns and risk as antecedents of behaviour in cybersecurity studies. Arachchilage & Love (2014) investigate awareness of phishing and tried to find the relationship between this construct with technology self-efficacy, trying to highlight the educational needs of users to be prepared against phishing threats. They confirmed the relationship between phishing threat awareness and online

self-efficacy to be significant. There is a study that considers the two-direction relationship between awareness with privacy self-efficacy in social media, that both of those have effect on behavioural control, which has an impact on privacy self-protection (Yao, 2011).

On the other hand, there are some clear distinctions between our hypotheses and the previous ones. The first thing is that we tried to measure awareness for a set of threats, and the relationship in our study focuses on social networks. As validated by the results, social media threat awareness has a positive significant correlation with social media security and privacy self-efficacy. This shows that the more awareness users get about the online threats in social media, the more they feel confident to control their interaction in social networks.

- H7: Higher Social Media Security Threat Awareness leads to better Social Media Security and Privacy Self-efficacy (Supported – $\beta = 0.410$, $P<0.001$).

5.1.2.3. Social media security threat awareness and S/P practices

Threat awareness can make users realize the consequences of cyber threats, and drive them to take proactive or reactive actions towards security and privacy dangers. The relationship between online threat awareness and maladaptive security practices has been studied, which indicates a positive correlation between these two constructs. Maladaptive behaviours are explained as a reaction caused by fear of online threats (Milne, Labrecque, & Cromer, 2009). The research into the relationship between these two constructs is limited, especially when it comes to assessing these constructs in social media.

Based on the statistical results, social media security threat awareness does not have a significant relationship with privacy practices. On the other hand, the relationship between threat awareness and social media security practices is significant, which supports the hypothesis of there being a positive relationship between these two constructs.

- H8a: Higher Social Media Security Threat Awareness leads to better Social Media Privacy Practices (Rejected – $\beta = 0.071$, $P<0.05$).
- H8b: Social Media Security Threats Awareness has a positive effect on social media security practices (Supported – $\beta = 0.138$, $P<0.001$).

This finding can help to create more effective messages and training to increase end users' practical behaviours toward security. End users seem to show that awareness toward cyber threats makes them more active toward security, and privacy does not have a strong dependency over users' knowledge toward threats. In the context of our model, privacy practices include communication, content sharing and discoverability. Together, these practices may constitute benefits that end-users obtain from their use of social media, and once again, there may be a trade-off between benefits and privacy behaviour. In addition, many of the practices associated with privacy protection leave the onus on the end-user to implicitly engage in protective behaviour, without the explicit use of specific tools, and this makes these practices more challenging for end-users to adopt. Security practices, on the other hand, can be enabled through proper use of authentication, access control, and security settings available on the social media sites, and these are easier for end-users to comprehend and align with their awareness of different types of security threats.

5.1.2.4. Social Media S/P self-efficacy and social media S/P practices

This study, related to these two constructs, has been limited to the general concept of information security, which lacks the research focus on social networks and privacy practice behaviours.

Our statistical analysis validates the significant correlation between social media security and privacy self-efficacy and social media privacy practices. This significance shows that by making people more capable of cybersecurity, technologies can boost their privacy-related practices. The same scenario happens for the relationship between social media security and privacy self-efficacy and social media security practices, which clarify that the more users become capable of dealing with cyber threats, the more effective their security behaviour will become in social networks.

- H9a: Social Media Security and Privacy Self-efficacy has a positive effect on Social Media Privacy Practices (Supported – $\beta = 0.171$, $P<0.001$)
- H9b: Social Media Security and Privacy Self-efficacy has a positive impact on Social Media Security Practices (Supported – $\beta = 0.225$, $P<0.001$).

5.1.2.5. Technology self-efficacy and social media S/P self-efficacy

Based on this study, technology self-efficacy is a significant predictor in social media security and privacy self-efficacy. It has been validated through the statistical analysis between these two constructs that the better users' get at technological self-efficacy, the more effective they will become with respect to social media security and privacy.

- H10: Technology Self-efficacy has a positive effect on Social Media Security and Privacy Self-efficacy (Supported – $\beta = 0.288$, $P<0.001$).

5.1.2.6. Technology self-efficacy and Online S/P Tools Use

The effects of online security self-efficacy on security tools use have been tested and validated in a study by Milne et al. (2009), which showed that ultimate success of information security depends on boosting end users' self-efficacy with the use of technology in general. The development of these capabilities should not be limited to training users on what not to do and the negative implications of their negligent actions (Rhee et al., 2009). Similar to the results of that research, our results validated the significance of the relationship between technology self-efficacy and security tools use. Based on this validation, the more confident users are in their ability, the better their security behaviour will become.

The other relationship analyzed in this study is between technology self-efficacy and privacy tools use, which is also validated.

- H11a: Technology Self-efficacy has a positive effect on Privacy Tools Use (Supported – $\beta = 0.273$, $P<0.001$)
- H11b: Technology Self-efficacy has a positive effect on Security Tools Use (Supported – $\beta = 0.276$, $P<0.001$).

5.1.3. Practices

The downstream constructs in our model pertain to end-user practices for security and privacy on social media platforms. Within this theme, the aim is to investigate whether there is a spill-over between security and privacy practices that end-users exhibit in general technology use, and the realm of social media.

5.1.3.1. Online Security Tools Use and social media S/P practices

The assessment of the theoretical model has determined that security tool use influences social media privacy practices among participants.

- H12a: Security Tools Use has a positive effect on Social Media Privacy Practices (Supported – $\beta = 0.193$, $P<0.001$)
- H12b: Security Tools Use has a positive impact on Social Media Security Practices (Supported – $\beta = 0.304$, $P<0.001$)

It can be concluded that more effective users' behaviour toward using security safeguards such as anti-malware software, password management, and safe browsing, tends to have a positive impact on their attitudes and behaviours towards safeguarding security and privacy on social media.

5.1.3.2. Online Privacy Tools Use and social media S/P practices

The privacy technological behaviours examined in this study have a significant relationship with social media security and privacy practices.

- H13a: Privacy Technological Behaviour has a positive effect on Privacy Practices (Supported – $\beta = 0.209$, $P<0.001$)
- H13b: Privacy Technological Behaviour has a positive effect on Security Practices (Supported – $\beta = 0.123$, $P<0.001$).

Based on the analysis, Privacy Tools Use is a useful predictor of the users' privacy practice in social media. The same relationship has been validated between Privacy Tools Use and social media security practices. This clarifies the theory that the more users establish online privacy enhancing strategies (e.g. browsing anonymously, clearing cookies, etc.), the more effective their privacy-related behavioural practices will be on social media.

5.2. Theoretical and Practical Contributions

5.2.1. Contributions to Theory

This study hopes to have contributed further to the body of knowledge on end-users' behaviour toward security and privacy in social media in the context of analyzing users' posture, proficiency and practice. Our study addresses notable concerns in end users' behaviour in social media at the theoretical level. The theoretical contributions made by the research are presented in the following subsections.

5.2.1.1. Investigating both end-users' security and privacy practice

To the best of our knowledge, the previous research studies either examined end users' social media privacy behaviour (Bada et al., 2015; Halevi et al., 2016; Williams et al., 2009) or social media security behaviour (Anwar et al., 2017; Egelman & Peer, 2015; Gratian et al., 2018). In this model, the empirical model is developed to examine both constructs and its predictive factors.

While many antecedent constructs have similar effects on both privacy and security, there are some distinctions that we have been able to make between them, which allows us to have a better understanding the model and its influential dimensions. For example, by breaking down security and privacy into two distinct constructs, we were able to verify the differential effect of privacy concerns, and cyber threat awareness on both constructs. This leads us to believe that there may be other constructs which can be investigated in a similar vein, and future studies should investigate these constructs separately to gain a comprehensive perspective of end-user behaviour related to security and privacy on social media.

5.2.1.2. New insight into the privacy and security construct's relationships

The three constructs under posture are disposition, social media privacy concern, and social media perceived privacy risk. One of the highlights of our study is that these factors have a significant relationship with each other, whereas the relationship between these constructs with practice constructs are mostly non-significant. The relationship between perceived privacy risk with both social media security and privacy practices are non-significant, showing that privacy risk, on its own, is not a reliable predictor for these two constructs, or at best, it can only predict a small portion of the variance in end-user security and privacy behaviour.

In our model, some constructs have not been studied much in previous research, mostly disposition and self-efficacy. The relationship between these constructs with their consequent constructs was significant, which shows the influential effect they have in the model. Moreover, the significant relationship between awareness and perceived risk showed that proficiency does not only affect behavioural constructs, but it is also a strong predictor of perceived risk. On the other hand, the relationship between proficiency constructs with practices is validated to be significant, which shows the more important role this dimension plays in predicting security and privacy practices.

There is also a significant correlation between online technological behaviour with social media security and privacy behaviour, indicating the positive effect online practices have on social media related behaviours. Such relationships have not previously been explored in the extant literature.

5.2.1.3. A new measurement scale for end-user cyber threat awareness

In order to have a clear understanding of the concept of social media security awareness, we defined a new multi-item scale that inquires end-user awareness levels for different prevalent social media security threats. This is in contrast to generic scales of awareness that have been used in previous research. A more well-defined scale allows us to conceptualize the awareness construct broadly as well as granularly. For example, previous researchers have either used generic scales of awareness, or only investigation awareness of specific types of threats, e.g. phishing.

5.2.1.4. Multi-dimensional Conceptualization of Social Media Security & Privacy Practices

To our knowledge, no prior studies have conceptualized social media security and privacy as formative constructs with multiple dimensions. In this study, we aimed to categorize different measurement items for security and privacy practices into specific first-order dimensions. For example, authentication and security settings were conceptualized as dimensions of security practices on social media. Similarly, communication, content sharing, and discoverability were conceptualized as dimensions of privacy. Our path model analysis demonstrates this conceptualization to be valid.

5.2.2. Contributions to Practice

5.2.2.1. End users

For practice, the results of this study yield some important recommendations for an effective cybersecurity awareness training programs for social media end users.

The insignificant relationship between social media perceived risk, and social media privacy concern with social media security and privacy practices (except for privacy concern and social media privacy practice) make clear the fact that concern and risk perception do not cause users to follow appropriate practices in critical situations. It supports the fact that end users usually follow their short-term benefit when they get involved in social networks (Lancelot Miltgen & Smith, 2015). Based on this finding, there should be an analysis of benefit-risk trade-off in the examination of social media security and privacy behaviour. It can be helpful to extract both the threats and benefits of interacting in the social network for end users. It should be highlighted that one of the most important problems with risk and concern is that there is a different benefit for each social network, considering their various features. This difference causes end users to have different perceptions of benefits, which will result in different behavioural practices by end users. Training programs should highlight effective ways for end-users to balance benefits of social media use with managing risks associated with security and privacy threats.

This study highlighted the role of threat awareness in strengthening social media security practice. The lack of research on threat awareness in previous studies results in researchers focusing on posture-related constructs. This research highlights the importance of self-efficacy in improving end-user security and privacy practices. Furthermore, we also discern that this self-efficacy in the realm of social media security and privacy is dependent on the awareness of cyber threats as well as on self-efficacy with security and privacy tools and techniques in the general online environment.

Proficiency plays an essential role as a predictor for both security and privacy practices. This shows the dependency of social media security and privacy on users' knowledge and capability.

Cyber threat awareness and self-efficacy can be increased by proper training, which means it should make users aware of doing the right thing at the right time when they need to deal with cyber threats. Such training should also focus on improving end-user confidence with the use of technology in general. End users can take more effective behavioral practice if they truly realize

the impact and consequences of cyber threats, in addition to the realization of long-term loss, besides the short-term benefit of involvement in the social network.

Based on our analysis, we put forth the following five recommendations for organizational security awareness training programs for end-users:

Table 5- 1 – Recommendations for Organizational Security Awareness Training Programs

Recommendations
1. When talking about social media security and privacy, do not discount the benefits of social media use. Balance discussion around optimizing rewards while effectively managing security and privacy.
2. Don't focus on using scaring tactics to instill fear among end-users, but focus on improving their proficiency.
3. Aim to improve end-user knowledge of different types of cyber threats and their implications.
4. Combine training tools and techniques for social media security and privacy alongside other internet security and privacy safeguards. The application of computer simulations is a powerful technique to investigate human cognition and behaviours. Simulations provide the possibility of designing an optimized training procedure based on different end-users (Veksler et al., 2018).
5. Assess and measure end-user proficiency with internet as well as social media security and privacy tools and techniques, allowing users to improve themselves and develop confidence in their abilities.

5.3. Study Limitations

The findings of this study are restricted by limitations in the survey methodology and the generalizability of the results. This section highlights those limitations and some possible ways to address them in future research. This discussion is followed by additional suggestions that could extend the research in this area.

5.3.1. Limitations in the survey methodology

The survey used a combination of convenience and snow-balling sampling approach and consisted of self-reported answers. This is not ideal as respondent answers can be influenced by environmental pressure and self-overestimation or self-underestimation. Social influence is defined by Bandyopadhyay & Fraccastoro (2007) as "societal pressure on users to engage in a certain behaviour".

The other limitation of this study was about the non-significant relationship between social media privacy concern with social media security practice. Also, social media perceived privacy risk with social media security and privacy practice, which shows the existence and more influential constructs in prediction of security and privacy behaviour. Future studies should investigate additional constructs that potentially affect social media security and privacy behaviour.

5.3.2. Generalizability of the results

The other limitation of this study is that general security and privacy questions were asked about behaviour in social networks without considering the different features and benefits each social network has. These differences can discriminate its users from users of other social networks, which cause different concerns and risk perception, and consequently, various security and privacy practices. We believe that this study provides a platform for future efforts, and the research model should be tested for users of different social networks.

This study also dealt with the issue of the disproportionate category of respondents, and we did not have control over the size of age groups, gender, or educational backgrounds. Most of our respondents have a higher educational level, which highlights the behavioural aspect of end users with higher educational and possibly technological capability. Moreover, the other limitation of our dataset is related to the geographical constraints, because end users in some countries do not have easy access to the questionnaire via the social networks we used. Moreover,

there are different cultural attributes based on a geographical specification that can affect behavioural traits, which can be investigated in future studies. In addition, there is the risk that respondents will not answer with total integrity, especially about the victim experience they have had, which cause them to give overestimated answers.

5.4. Suggestions for Future Studies

In order to improve the quality of future studies on the analysis of end users' security and privacy practice in social media, a few points are suggested. The empirical model can be enhanced by examining new factors in the context of security and privacy in social media, especially by adding factors related to the benefits of social media, either for posture or as a mediator variable between posture and practice constructs.

There were a few suggested correlations in the previous studies that are not supported in our analysis results, like the relationship between perceived risk and social media privacy practices, or privacy concern and social media privacy practices. This could be due to our new operationalization of the security and privacy constructs, or due to the profile of respondents in our survey. Future research should replicate or extend our conceptualization of security and privacy practices to verify these and other potential relationships.

The other suggestion is about the expansion or discrimination between antecedents of security and privacy practices. Future studies can develop these two behavioural practices, the reactive and proactive, to examine and detect the factors that affect the end users' practices before and after cyber breaches. As end users recognize the potential risk to social media security and privacy, there are some actions they can undertake as risk responses to mitigate the risk of cyber threats before their occurrence. On the other hand, because the risk of the cyber threat cannot entirely be removed, end users should be ready for certain cyber risks, which necessitates the establishment of reactive social media security and security practices.

5.5. Conclusion

This study investigated the posture, proficiency and practices associated with end-user security and privacy behaviour in social media. After a comprehensive investigation of the available literature, a quantitative deductive research approach was adopted to formulate a theoretical model capable of explaining end-user social media security and privacy behaviour. We tested and analyzed the model using SEM-PLS to validate the defined hypotheses in our study.

Overall, our research indicates that social media security and privacy practices are multi-faceted, and they are dependent of different personal attributes related to posture and proficiency. Furthermore, in our research, proficiency appears to be a better predictor of social media security and privacy practices, as compared to posture. From a research standpoint, more research is required to investigate the differential effects of posture and proficiency on practices. The implications of this research for organizations is that they need to focus on improving knowledge, skills and abilities of end-users to foster better security and privacy behaviour among them.

6. References

Abdi, H. (2003). Partial least square regression (PLS regression). - *Encyclopedia for Research Methods for The*. Retrieved from http://www.utd.edu/~Herve/Abdi-PLSR2007-pretty.pdf

Abraham, S. (2011). Information Security Behavior: Factors and Research Directions. *17th Americas Conference on Information Security*, 4050–4062. Retrieved from http://aisel.aisnet.org/amcis2011_submissions%0Ahttp://aisel.aisnet.org/amcis2011_submissions

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce - EC '04* (p. 21). New York, New York, USA: ACM Press. https://doi.org/10.1145/988772.988777

Acquisti, A., & Enhancing, R. G. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. *International Workshop on Privacy*. Retrieved from https://link.springer.com/10.1007/11957454_3

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, *3*(1), 26–33. https://doi.org/10.1109/MSP.2005.22

Allen, C. (2018). 7 Most Famous Social Engineering Attacks In History (Updated). Retrieved April 7, 2019, from https://phoenixnap.com/blog/famous-social-engineering-attacks

Almadhoun, N. M., Dominic, P. D. D., & Woon, F. L. (2011). Perceived Security , Privacy, and Trust concerns within Social Networking Sites. *IEEE International Conference on Control System, Computing and Engineering*, 426–431. https://doi.org/10.1109/ICCSCE.2011.6190564

Alshumaimeri, Y. (2001). *Research Methodology Chapter*. http://faculty.ksu.edu.sa/yousif/Master%20Dissertation/Chapter%204%20Research%20Methodolog .pdf.

Andrews, D., Nonnecke, B., & Preece, J. (2003). Electronic survey methodology: A case study in reaching hard-to-involve Internet users. *International Journal of Human-Computer Interaction*, *16*(2), 185–210.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304–312. https://doi.org/10.1016/J.CHB.2014.05.046

Arbaugh, J. B. (2000). An Exploratory Study of the Effects of Gender on Student Learning and Class Participation in an Internet-Based MBA Course. *Management Learning*, *31*(4), 503–519. https://doi.org/10.1177/1350507600314006

Australian Cyber Security Centre. (2017). ACSC 2017 Threat Report, (February). Retrieved from https://www.acsc.gov.au

Bada, M., Sasse, A., & Nurse, J. R. C. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? In *Proceedings of the International Conference on Cyber Security for Sustainable Society* (pp. 118–131). https://doi.org/10.1142/S0219635211002816

Baden, R., Bender, A., Spring, N., Bhattacharjee, B., Starin, D., Baden, R., … Starin, D. (2009). Persona: an online social network with user-defined privacy. *Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication - SIGCOMM '09*, *39*(4), 135. https://doi.org/10.1145/1592568.1592585

Bagozzi, R. P. (1994). Measurement in marketing research: Basic principles of questionnaire design. *Principles of Marketing Research*, *1*(1), 1–49.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, *16*(1), 74–94. https://doi.org/10.1007/BF02723327

Ball, J., Myers, C., Heiberg, A., Cooke, N. J., Matessa, M., Freiman, M., & Rodgers, S. (2010). The synthetic teammate project. *Computational and Mathematical Organization Theory*, *16*(3), 271–299. https://doi.org/10.1007/s10588-010-9065-3

Bandyopadhyay, K., & Fraccastoro, K. A. (2007). THE EFFECT OF CULTURE ON USER ACCEPTANCE OF INFORMATION TECHNOLOGY. *… Association for Information …*, *19*(1).

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday*, *11*(9). https://doi.org/10.5210/fm.v11i9.1394

Barth, S., & de Jong, M. D. T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), 1038–1058. https://doi.org/10.1016/J.TELE.2017.04.013

Batista, G. E. A. P. A., & Monard, M. C. (2003). An analysis of four missing data treatment methods for supervised learning. *Applied Artificial Intelligence*, *17*(5–6), 519–533. https://doi.org/10.1080/713827181

Becker, J. M., Klein, K., & Wetzels, M. (2012). Hierarchical Latent Variable Models in PLS-SEM: Guidelines for Using Reflective-Formative Type Models. *Long Range Planning*, *45*(5–6), 359–394. https://doi.org/10.1016/J.LRP.2012.10.001

Becker, L., & Pousttchi, K. (2012). Social Networks: The Role of Users' Privacy Concerns. In *Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services - IIWAS '12* (p. 187). New York, New York, USA: ACM Press. https://doi.org/10.1145/2428736.2428767

Bennett, S., & Maton, K. (2010). Beyond the 'digital natives' debate: Towards a more nuanced understanding of students' technology experiences. *Journal of Computer Assisted Learning*, *26*(5), 321–331. https://doi.org/10.1111/j.1365-2729.2010.00360.x

Bertram, D. (2007). Likert Scales… are the meaning of life: CPSC 681–Topic Report. *Poincare*, 1–11. https://doi.org/10.1002/9780470479216.corpsy0508

Bolhuis, J., & Giraldeau, L. (2005). *The study of animal behaviour*. *Blackwell Publishing*. Retrieved from https://www.researchgate.net/profile/Luc-Alain_Giraldeau/publication/46656210_The_study_of_animal_behavior/links/0f317532049969e421000000/The-study-of-animal-behavior.pdf

Bollen, K. (1989). *Structural equations with latent variables.* John Wiley and Sons. Retrieved from https://www.popline.org/node/362861

boyd, danah. (2008). Facebook's Privacy Trainwreck. *Convergence: The International Journal of Research into New Media Technologies*, *14*(1), 13–20. https://doi.org/10.1177/1354856507084416

Bradbury, D. (2012). Spreading fear on Facebook. *Network Security*, *2012*(10), 15–17. https://doi.org/10.1016/S1353-4858(12)70094-6

Brandtzæg, P. B., Lüders, M., & Skjetne, J. H. (2010). Too Many Facebook "Friends"? Content Sharing and Sociability Versus the Need for Privacy in Social Network Sites. *International Journal of Human-Computer Interaction*, *26*(11–12), 1006–1030. https://doi.org/10.1080/10447318.2010.516719

Brokerlink Inssurance. (2018). How social media is increasing your risk for identity theft. Retrieved April 7, 2019, from https://www.brokerlink.ca/blog/how-social-media-is-increasing-your-risk-for-identity-theft/?source=es

Bryman, A., & Burgess, R. G. (1999). *Qualitative research. Vol. 2,[Methods of qualitative research]*. Sage.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U.-D. (2007). Development of measures of online privacy concern and protection for use on the Internet. *Journal of the American Society for Information Science and Technology*, *58*(2), 157–165. https://doi.org/10.1002/asi.20459

Buck, C., Horbel, C., Germelmann, C. C., & Eymann, T. (2014). The unconscious app consumer: discovering and comparing the information-seeking patterns among mobile application consumers. *ECIS 2014 Proceedings*. Retrieved from https://aisel.aisnet.org/ecis2014/proceedings/track14/8

Burley, D. L., & Goodman, S. E. (2013). *Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making. Committee on Professionalizing the Nation's Cybersecurity Workforce: Criteria for Future Decision-Making*. https://doi.org/10.17226/18446

Cenfetelli, & Bassellier. (2017). Interpretation of Formative Measurement in Information Systems Research. *MIS Quarterly*, *33*(4), 689. https://doi.org/10.2307/20650323

Chen, K., Rea Jr, A. I., & Rea, A. I. (2004). Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques. *Journal of Computer Information Systems*, *44*(4), 85–92. https://doi.org/10.1080/08874417.2004.11647599

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly*, *22*.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study. *Info. Sys. Research*, *14*(2), 189–217. https://doi.org/10.1287/isre.14.2.189.16018

Choi, N., Kim, D., Goo, J., & Whitmore, A. (2008). Knowing is doing. *Information Management & Computer Security*, *16*(5), 484–501. https://doi.org/10.1108/09685220810920558

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? *CyberPsychology & Behavior*, *12*(3), 341–345. https://doi.org/10.1089/cpb.2008.0226

Clark, L. (2012). Privacy Settings in Social Media | Social Media Sun. Retrieved April 6, 2019, from http://socialmediasun.com/privacy-settings/

Cohen, L., & Manion, L. (1980). Research Methods in Education. London: Croom Helm Ltd. *Hyderabad: Orient Longman Private Limited*.

Cook, A., & Allan. (2018). Establishing cyber situational awareness in industrial control systems. Retrieved from https://www.dora.dmu.ac.uk/xmlui/handle/2086/17463

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Retrieved from http://nrl.northumbria.ac.uk/23903/

Coventry, L., Briggs, P., Jeske, D., & Van Moorsel, A. (2014). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 8517 LNCS, pp. 229–239). https://doi.org/10.1007/978-3-319-07668-3_23

Crano, W. D., & Prislin, R. (2006). Attitudes and Persuasion. *Annual Review of Psychology*, *57*(1), 345–374. https://doi.org/10.1146/annurev.psych.57.102904.190034

Cranor, L., & Garfinkel, S. (2005). *Security and usability: designing secure systems that people can use*. Retrieved from https://books.google.com/books?hl=en&lr=&id=wDVhy9EyEAEC&oi=fnd&pg=PR5&dq=Usability+cybersecurity&ots=BRNJyOLq4r&sig=WWNj5xVWh_vzpXIgX9hlsgJjvRQ

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, *16*(3), 297–334. https://doi.org/10.1007/BF02310555

Crowne, D., & Marlowe, D. (1960). A new scale of social desirability independent of psychopathology. *Journal of Consulting Psychology*, *24*, 349–354. Retrieved from http://psycnet.apa.org/record/1961-02183-001

Crutchfield, R. S. (1955). Conformity and character. *American Psychologist*, *10*(5), 191–198.

https://doi.org/10.1037/h0040237

Culnan, M. J., Mchugh, P. J., Zubillaga, J. I., Uarterly, M. Q., & Xecutive, E. (2010). the Need for a New Approach To Implementing Social Media. *MIS Quarterly Executive*, *9*(4), 243–259.

Davison, W. P. (1983). The Third-Person Effect in Communication. *Public Opinion Quarterly*, *47*(1), 1. https://doi.org/10.1086/268763

De Bruijn, H., & Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1–7. https://doi.org/10.1016/j.giq.2017.02.007

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. https://doi.org/10.1111/j.1083-6101.2009.01494.x

Department of Homeland Security. (2018). National Cybersecurity Awareness Month | Homeland Security. Retrieved January 22, 2019, from https://www.dhs.gov/national-cyber-security-awareness-month

Deuker, A. (2010). Addressing the Privacy Paradox by Expanded Privacy Awareness – The Example of Context-Aware Services (pp. 275–283). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14282-6_23

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison and Empirical Illustration. *British Journal of Management*, *17*(4), 263–282. https://doi.org/10.1111/j.1467-8551.2006.00500.x

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, *45*(3), 285–297. https://doi.org/10.1002/ejsp.2049

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Dolan, P., Halpern, D., Hallsworth, M., King, D., & Vlaev, I. (2010). Influencing behaviour through public policy _(Mindspace Short Guide). *The Institute for Government for the Cabinet Office*. https://doi.org/10.1111/j.1753-4887.2009.00206.x

Draper, J. (2004). The relationship between research question and research design. In *Research into Practice: Essential Skills for Reading and Applying Research in Nursing and Health Care* (pp. 69–84). Bailliere Tindall.

Dredze, M., & Wallach, H. (2008). User models for email activity management. *Workshop on Ubiquitous User Modeling, Int. Conf. Intelligent User Interfaces*, 2–4. Retrieved from https://www.cs.jhu.edu/~mdredze/publications/dredze_ubiqum_user_model_08.pdf

Dwyer, C., Hiltz, S. R., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *Americas Conference on Information Systems (AMCIS)*, *123*, 339–350. https://doi.org/10.1.1.148.9388

Edwards, J. R. (2001). Multidimensional constructs in organizational behavior research: An integrative analytical framework. *Organizational Research Methods*, *4*(2), 144–192.

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the ACM Conference on Human Factors in Computing Systems, Seoul;* Retrieved from https://dl.acm.org/citation.cfm?id=2702249

European Comission. (2011). Attitudes on Data Protection and Electronic Identity in the European Union, 330. https://doi.org/10.1007/s002270050518

Everett, C. (2010, June 1). Social media: Opportunity or risk? *Computer Fraud and Security*. Elsevier Advanced Technology. https://doi.org/10.1016/S1361-3723(10)70066-X

Falk, R. F., & Miller, N. B. (1992). A primer for soft modeling. *A Primer for Soft Modeling.* Akron, OH, US: University of Akron Press.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions. In *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12* (p. 1). New York, New York, USA: ACM Press. https://doi.org/10.1145/2335356.2335360

Fishbein, M., & Ajzen, I. (2011). *Predicting and changing behavior: The reasoned action approach*. Psychology Press. Retrieved from https://content.taylorfrancis.com/books/download?dac=C2009-0-04110-3&isbn=9781136874734&format=googlePreviewPdf

Flender, C., & Müller, G. (2012). Type Indeterminacy in Privacy Decisions: The Privacy Paradox Revisited (pp. 148–159). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-35659-9_14

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. https://doi.org/10.1016/J.CHB.2008.08.006

Fogues, R., Such, J. M., Espinosa, A., & Garcia-Fornes, A. (2015). Open Challenges in Relationship-Based Privacy Mechanisms for Social Network Services. *International Journal of Human-Computer Interaction*, *31*(5), 350–370. https://doi.org/10.1080/10447318.2014.1001300

Fornell, C., & Larcker, D. F. (1981). Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics. *Journal of Marketing Research*, *18*(3), 382–388. https://doi.org/10.1177/002224378101800313

Fu, W. T., & Anderson, J. R. (2006). From recurrent choice to skill learning: A reinforcement-learning model. *Journal of Experimental Psychology: General*, *135*(2), 184–206. https://doi.org/10.1037/0096-3445.135.2.184

Fu, W. T., & Pirolli, P. (2007). SNIF-ACT: A Cognitive Model of User Navigation on the World Wide Web. *Human–Computer Interaction*, *22*(4), 355–412. https://doi.org/10.1080/07370020701638806

Garg, V., & Jean Camp, L. (2015). Cars, Condoms, and Facebook (pp. 280–289). Springer, Cham. https://doi.org/10.1007/978-3-319-27659-5_20

Gefen, D., Straub, D., & Boudreau, M.-C. (2000). Structural Equation Modeling and Regression: Guidelines for Research Practice. *Communications of the Association for Information Systems*, *4*. https://doi.org/10.17705/1CAIS.00407

Geladi, P., & Kowalski, B. R. (1986). Partial least-squares regression: a tutorial. *Analytica Chimica Acta*, *185*, 1–17. https://doi.org/10.1016/0003-2670(86)80028-9

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226–261. https://doi.org/10.1016/J.COSE.2018.04.002

Gharibi, W., & Shaabi, M. (2012). Cyber Threats In Social Networking Websites. *International Journal of Distributed and Parallel Systems*, *3*(1), 119–126. https://doi.org/10.5121/ijdps.2012.3109

Goodhue, Lewis, & Thompson. (2018). Does PLS Have Advantages for Small Sample Size or Non-Normal Data? *MIS Quarterly*, *36*(3), 981. https://doi.org/10.2307/41703490

Gouveia, D., Lopes, D., & de Carvalho, C. V. (2011). Serious gaming for experiential learning. In *2011 Frontiers in Education Conference (FIE)* (pp. T2G-1-T2G-6). IEEE. https://doi.org/10.1109/FIE.2011.6142778

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, *73*, 345–358. https://doi.org/10.1016/J.COSE.2017.11.015

Grobler, M., Flowerday, S., von Solms, R., & Venter, H. (2011). *Proceedings of the first IFIP TC9/TC11 Southern African cyber security awareness workshop 2011*. Defence, Peace, Safety and Security Council for Scientific and Industrial Research. Retrieved from http://researchspace.csir.co.za/dspace/handle/10204/5164

Gross, R., Acquisti, A., & Heinz, H. J. (2005). Information revelation and privacy in online social networks. In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society - WPES '05* (p. 71). New York, New York, USA: ACM Press. https://doi.org/10.1145/1102199.1102214

Gruzd, A., Jacobson, J., Mai, P., & Dubois, E. (2018). The State of Social Media in Canada 2017, (February), 1–18. https://doi.org/10.5683/SP/AL8Z6R

Guinot, C., Latreille, J., & Tenenhaus, M. (2001). PLS Path modelling and multiple table analysis. Application to the cosmetic habits of women in Ile-de-France. *Chemometrics and Intelligent Laboratory Systems*, *58*(2), 247–259. https://doi.org/10.1016/S0169-7439(01)00163-0

Hackett, R. (2016). Microsoft LinkedIn: Lynda.com Resets 55,000 Passwords Post Data Breach | Fortune. Retrieved April 7, 2019, from http://fortune.com/2016/12/19/microsoft-linkedin-lynda-data-breach/

Hair, J. F., M.Hult, G. T., M.Ringle, C., & Sarstedt, M. (2016). *A Primer on Partial Least Squares Structural Equation Modeling*. *SAGE Publications*. https://doi.org/10.1016/j.lrp.2013.01.002

Hair, J. F., M.Ringle, C., & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hair, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V.-G. (2014). Partial least squares structural equation modeling (PLS-SEM). *European Business Review*, *26*(2), 106–121. https://doi.org/10.1108/EBR-10-2013-0128

Hajli, N., & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, *133*(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. In *Proceedings of the 22nd International Conference on World Wide Web - WWW '13 Companion* (pp. 737–744). New York, New York, USA: ACM Press. https://doi.org/10.1145/2487788.2488034

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., … Chen, J. (2016). Cultural and psychological factors in cyber-security. In *Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services - iiWAS '16* (pp. 318–324). New York, New York, USA: ACM Press. https://doi.org/10.1145/3011141.3011165

Hannon, J., McCarthy, K., O'Mahony, M. P., & Smyth, B. (2012). A multi-faceted user model for Twitter. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (Vol. 7379 LNCS, pp. 303–309). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-31454-4_26

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, *14*(2), 171–180. https://doi.org/10.1108/13287261211232180

Huang, D.-L., Patrick Rau, P.-L., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870–883. https://doi.org/10.1016/J.IJHCS.2011.07.007

Jensen, C., Potts, C., & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, *63*(1–2), 203–227. https://doi.org/10.1016/J.IJHCS.2005.04.019

Jones, A., & Colwill, C. (2008). Dealing with the malicious insider. In *Proceedings of 6th Australian Information Security Management Conference* (pp. 70–86). https://doi.org/10.4225/75/57b562dab876e

Jyotiyana, P., & Maheshwari, S. (2018). Techniques to Detect Clickjacking Vulnerability in Web

Pages (pp. 615–624). Springer, Singapore. https://doi.org/10.1007/978-981-10-7395-3_68

Kahneman, D., & Egan, P. (2011). *Thinking, fast and slow*. Macat International Ltd. Retrieved from https://content.taylorfrancis.com/books/download?dac=C2018-0-82622-6&isbn=9781912453207&format=googlePreviewPdf

Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. *Symposium on Usable Privacy and Security*, 39–52. https://doi.org/10.1093/gerona/glp002

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, *53*(1), 59–68. https://doi.org/10.1016/J.BUSHOR.2009.09.003

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B., & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. https://doi.org/10.1016/J.IJHCS.2013.08.016

Keller, G. (2015). *Statistics for Management and Economics, Abbreviated*. Cengage Learning.

Kim, Y., Sohn, D., & Choi, S. M. (2011). Cultural difference in motivations for using social network sites: A comparative study of American and Korean college students. *Computers in Human Behavior*, *27*(1), 365–372. https://doi.org/10.1016/J.CHB.2010.08.015

Kline, R. (2015). *Principles and practice of structural equation modeling*. Retrieved from https://books.google.ca/books?hl=en&lr=&id=Q61ECgAAQBAJ&oi=fnd&pg=PP1&dq=Kline,+R.+B.+(2005).+Principles+and+practice+of+structural+equation+modeling,+Guilford+Press&ots=jEji2wCdrl&sig=5QXvax4nypqs5n-87Y7RSaLPlZY

Kock, N., & Hadaya, P. (2018). Minimum sample size estimation in PLS-SEM: The inverse square root and gamma-exponential methods. *Information Systems Journal*, *28*(1), 227–261. https://doi.org/10.1111/isj.12131

Korpela, K. (2015). Improving Cyber Security Awareness and Training Programs with Data Analytics. *Information Security Journal*, *24*(1–3), 72–77. https://doi.org/10.1080/19393555.2015.1051676

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63. https://doi.org/10.1007/s12394-009-0019-1

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Krishnamurthy, B., & Wills, C. E. (2008). Characterizing privacy in online social networks. In *Proceedings of the first workshop on Online social networks - WOSP '08* (p. 37). New York, New York, USA: ACM Press. https://doi.org/10.1145/1397735.1397744

Kumaraguru, P., & Cranor, L. (2005). *Privacy indexes: a survey of Westin's studies*. Retrieved from http://reports-archive.adm.cs.cmu.edu/anon/anon/home/ftp/usr0/ftp/isri2005/CMU-ISRI-05-138.pdf

Kunreuther, H. (1984). Causes of Underinsurance against Natural Disasters. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *9*(2), 206–220. https://doi.org/10.1057/gpp.1984.12

Lallmahamood, M. (2007). An Examination of Individual ' s Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce : Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce*, *12*(3), 1–26. https://doi.org/Article

LaMarca, N. (2011). The Likert Scale: Advantages and Disadvantages | Field Research in Organizational Psychology. Retrieved April 13, 2019, from https://psyc450.wordpress.com/2011/12/05/the-likert-scale-advantages-and-disadvantages/

Lancelot Miltgen, C., Popovič, A., & Oliveira, T. (2013). Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context. *Decision Support Systems*, *56*, 103–114. https://doi.org/10.1016/J.DSS.2013.05.010

Lancelot Miltgen, C., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. https://doi.org/10.1016/J.IM.2015.06.006

Larson, S. (2015). The cyber security fair: an effective method for training users to improve their cyber security behaviors? Retrieved from www.dline.info/isej/fulltext/v2n1/2.pdf

Latham, B. (2007). Sampling: What is it? Quantitative research methods. *ENGL 5377, Spring 2007*.

Lee, J. (2012). Components of medical service users' dissatisfaction: a perceived control perspective. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2145038

Lee, N., & Cadogan, J. W. (2013). Problems with formative and higher-order reflective variables. *Journal of Business Research*, *66*(2), 242–247. https://doi.org/10.1016/J.JBUSRES.2012.08.004

Lei, M., & Lomax, R. G. (2005). The Effect of Varying Degrees of Nonnormality in Structural Equation Modeling. *Structural Equation Modeling: A Multidisciplinary Journal*, *12*(1), 1–27. https://doi.org/10.1207/s15328007sem1201_1

Lei, P., Wu, Q., & Pennsylvania, T. (2007). Introduction to Structural Equation Modeling : Issues.

Lemos, R. (2013). Targeted attacks, weak passwords top IT security risks in 2013. Retrieved from http://tomax7.com/asecplus/articles/Targeted Attacks 2013.docx

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434–445. https://doi.org/10.1016/J.DSS.2011.01.017

Li, Y. (2014). The impact of disposition to privacy, website reputation and website familiarity on information privacy concerns. *Decision Support Systems*, *57*, 343–354. https://doi.org/10.1016/J.DSS.2013.09.018

Liao, C., Liu, C.-C., & Chen, K. (2011). Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model. *Electronic Commerce Research and Applications*, *10*(6), 702–715. https://doi.org/10.1016/J.ELERAP.2011.07.003

Livingstone, S., & Brake, D. R. (2010). On the rapid rise of social networking sites: New findings and policy implications. *Children and Society*, *24*(1), 75–83. https://doi.org/10.1111/j.1099-0860.2009.00243.x

Lo, J. (2010). Privacy Concern, Locus of Control, and Salience in a Trust-Risk Model of Information Disclosure on Social Networking Sites. *Americas Conference on Information Systems (AMCIS) 2010 Proceedings*, Paper 110. Retrieved from http://aisel.aisnet.org/amcis2010/110

Lohmöller, J.-B. (1989). Predictive vs. structural modeling: Pls vs. ml. In *Latent variable path modeling with partial least squares* (pp. 199–226). Springer.

Lowry, P. B., & Gaskin, J. (2014). Partial Least Squares (PLS) Structural Equation Modeling (SEM) for Building and Testing Behavioral Causal Theory: When to Choose It and How to Use It. *IEEE Transactions on Professional Communication*, *57*(2), 123–146.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Mathieson, K., Peacock, E., & Chin, W. W. (2001). Extending the technology acceptance model. *ACM SIGMIS Database*, *32*(3), 86. https://doi.org/10.1145/506724.506730

Mathiyalakan, S., Heilman, G., & White, S. (2002). Gender Differences in Student Attitude toward Privacy in Facebook. *Communications of the IIMA*, *13*(4), 35. Retrieved from https://www.questia.com/library/journal/1G1-368623349/gender-differences-in-student-attitude-toward-privacy

Melnick, J. (2018). Top 10 Most Common Types of Cyber Attacks. Retrieved April 7, 2019, from https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Phishing and spear phishing attacks

Mercer, D. A. (2013). Nonparametric Discriminant Analysis in Forensic Ancestry Estimation : An Assessment of Utilitzed and Alternative Statistical Methods.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, *43*(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior*, *28*(6), 2366–2375. https://doi.org/10.1016/J.CHB.2012.07.008

More, J. (2011). Measuring Psychological Variables of Control in Information Security. *Information Security*. Retrieved from http://www.starmind.org/images/MeasuringPsychologicalVariablesOfControlInInformation Security-JoshMore.pdf

Moreau, E. (2019). The Top 25 Social Networking Sites People Are Using. Retrieved from https://www.lifewire.com/top-social-networking-sites-people-are-using-3486554

Nason, S., & Laird, J. E. (2005). Soar-RL: integrating reinforcement learning with Soar. *Cognitive Systems Research*, *6*(1), 51–59. https://doi.org/10.1016/J.COGSYS.2004.09.006

Nepal, S., Paris, C., Pour, P. A., Freyne, J., & Bista, S. K. (2015). Interaction-Based Recommendations for Online Communities. *ACM Transactions on Internet Technology*, *15*(2), 1–21. https://doi.org/10.1145/2774974

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. https://doi.org/10.6028/NIST.SP.800-181

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/J.DSS.2008.11.010

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

Norusis, M. (1990). SPSS/PC and Statistics 4.0 for the IBM PC/XT/AT and PS/2. Retrieved from http://www.sidalc.net/cgi-bin/wxis.exe/?IsisScript=BFHIA.xis&method=post&formato=2&cantidad=1&expresion=mfn=005355

Nosek, B. A., Banaji, M. R., & Greenwald, A. G. (2002). Harvesting implicit group attitudes and beliefs from a demonstration web site. *Group Dynamics: Theory, Research, and Practice*, *6*(1), 101–115. https://doi.org/10.1037/1089-2699.6.1.101

Nunnally, J. (1978). *Psychometric Theory: 2d Ed*. New York: McGraw-Hill.

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011a). Guidelines for usable cybersecurity: Past and present. In *2011 Third International Workshop on Cyberspace Safety and Security (CSS)* (pp. 21–26). IEEE. https://doi.org/10.1109/CSS.2011.6058566

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011b). Guidelines for usable cybersecurity: Past and present. In *Proceedings - 2011 3rd International Workshop on Cyberspace Safety and Security, CSS 2011* (pp. 21–26). https://doi.org/10.1109/CSS.2011.6058566

O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The Impact of Social Media on Children, Adolescents, and Families. *Pediatrics*, *127*(4), 800–804. https://doi.org/10.1542/peds.2011-0054

Oakleaf, M. (2009). Writing information literacy assessment plans: A guide to best practice. *Communications in Information Literacy*, *3*(2), 80–90. https://doi.org/10.1002/asi

Oehri, C., & Teufel, S. (2012). Social media security culture. In *2012 Information Security for South Africa* (pp. 1–5). IEEE. https://doi.org/10.1109/ISSA.2012.6320436

Oomen, I., & Leenes, R. (2008). Privacy Risk Perceptions and Privacy Protection Strategies. In *Policies and Research in Identity Management* (pp. 121–138). Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-77996-6_10

Peng, D. X., & Lai, F. (2012). Using partial least squares in operations management research: A practical guideline and summary of past research. *Journal of Operations Management*, *30*(6), 467–480. https://doi.org/10.1016/J.JOM.2012.06.002

Petter, S., Straub, D. W., & Rai, A. (2007). *Specifying Formative Constructs in Information Systems Research*. *MIS Quarterly* (Vol. 31). Retrieved from http://scholarworks.gsu.edu/cis_facpubhttp://misq.org/specifying-formative-constructs-in-information-systems-research.html.

Pötzsch, S. (2009). Privacy Awareness: A Means to Solve the Privacy Paradox? (pp. 226–236). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03315-5_17

Preece, J., Rogers, Y., & Sharp, H. (2015). *Interaction design: beyond human-computer interaction*. John Wiley & Sons.

Quinn, K. (2016). Why We Share: A Uses and Gratifications Approach to Privacy Regulation in Social Media Use. *Journal of Broadcasting & Electronic Media*, *60*(1), 61–86. https://doi.org/10.1080/08838151.2015.1127245

Reuben, R. (2008). The use of social media in higher education for marketing and communications: A guide for professionals in higher education. Retrieved from http://www.fullerton.edu/technologyservices/_resources/pdfs/social-media-in-higher-education.pdf

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Rindskopf, D., & Rose, T. (1988). Second order factor analysis: Some theory and applications. *Multivariate Behavioral Research*, *23*(1), 51–67.

Rogers, R. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social Psychophysiology*. Retrieved from https://ci.nii.ac.jp/naid/10004535663/

Saridakis, G., Benson, V., Ezingeard, J.-N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320–330. https://doi.org/10.1016/J.TECHFORE.2015.08.012

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, *19*(3), 122–131. https://doi.org/10.1023/A:1011902718709

Schlienger, T., & Teufel, S. (2002). Information Security Culture. In M. A. Ghonaimy, M. T. El-Hadidi, & H. K. Aslan (Eds.), *Security in the Information Society: Visions and Perspectives* (pp. 191–201). Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-35586-3_15

Schmidt, F. L., Hunter, J. E., & Urry, V. W. (1976). Statistical power in criterion-related validation studies. *Journal of Applied Psychology*, *61*(4), 473–485. https://doi.org/10.1037/0021-9010.61.4.473

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*. John Wiley & Sons. Retrieved from https://books.google.com/books?hl=en&lr=&id=z_7CAjmql6kC&oi=fnd&pg=PT8&dq=Schneier,+B.+(2011).+Secrets+and+lies:+Digital+security+in+a+networked+world.+Hoboken,+NJ:+John+Wiley+%26+Sons.&ots=NswT5kG3Zo&sig=gcSevsSk_Kbg_Acd0oG95n39jJk

Scott, B. G., & Weems, C. F. (2010). Patterns of actual and perceived control: are control profiles differentially related to internalizing and externalizing problems in youth? *Anxiety, Stress & Coping*, *23*(5), 515–528. https://doi.org/10.1080/10615801003611479

Shareef, M. A., Kumar, V., Kumar, U., & Dwivedi, Y. K. (2011). e-Government Adoption Model (GAM): Differing service maturity levels. *Government Information Quarterly*, *28*(1), 17–35. https://doi.org/10.1016/J.GIQ.2010.05.006

Shin, D. H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with Computers*, *22*(5), 428–438. https://doi.org/10.1016/j.intcom.2010.05.001

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, *20*(2), 167. https://doi.org/10.2307/249477

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124–133. https://doi.org/10.1016/J.COSE.2004.07.001

Statistica. (2019). Global social media ranking 2019 | Statistic. Retrieved April 8, 2019, from https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Stutzman, F. (2006). An evaluation of identity-sharing behavior in social network communities. *IN IDMAA AND IMS CODE CONFERENCE*, *3*. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.91.617

Sundar, S. S., Kang, H., Wu, M., Go, E., & Zhang, B. (2013). Unlocking the privacy paradox. In *CHI '13 Extended Abstracts on Human Factors in Computing Systems on - CHI EA '13* (p.

811). New York, New York, USA: ACM Press. https://doi.org/10.1145/2468356.2468501

Symanovich, S. (2019). Privacy vs. security: what's the difference? Retrieved May 8, 2019, from https://us.norton.com/internetsecurity-privacy-privacy-vs-security-whats-the-difference.html

Taddicken, M. (2014). The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*, *19*(2), 248–273. https://doi.org/10.1111/jcc4.12052

Tamrakar, A., Russell, J. D., Ahmed, I., Richard III, G. G., & Weems, C. F. (2016). SPICE: A Software Tool for Bridging the Gap Between End-user's Insecure Cyber Behavior and Personality Traits. *Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy*, 124–126. https://doi.org/10.1145/2857705.2857744

Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Tayouri, D. (2015). The Human Factor in the Social Media Security – Combining Education and Technology to Reduce Social Engineering Risks and Damages. *Procedia Manufacturing*, *3*, 1096–1100. https://doi.org/10.1016/J.PROMFG.2015.07.181

Tenenhaus, M., Vinzi, V. E., Chatelin, Y.-M., & Lauro, C. (2005). PLS path modeling. *Computational Statistics & Data Analysis*, *48*(1), 159–205. https://doi.org/10.1016/J.CSDA.2004.03.005

Teutsch, D., & Niemann, J. (2016). Social network sites as a threat to users' self-determination and security: A framing analysis of German newspapers. *The Journal of International Communication*, *22*(1), 22–41. https://doi.org/10.1080/13216597.2015.1111841

trendmicro. (2018). Linking the Enterprise to Social Media Security - Security News - Trend Micro USA. Retrieved April 9, 2019, from https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/linking-the-enterprise-to-social-media-security

Trepte, S., Dienlin, T., & Reinecke, L. (2014). Risky behaviors: How online experiences influence privacy behaviors.

Trochim, W. (2006). Nonprobability sampling. *Research Methods Knowledge Base*, *1*(1), 1–10.

Trochim, W. (2007). The Research Methods Knowledge Base.

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/J.COSE.2016.02.009

Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases. *Science (New York, N.Y.)*, *185*(4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124

Van Dijk, T., Spil, T., Van der Burg, S., Wenzler, I., & Dalmolen, S. (2015). Present or Play.

International Journal of Game-Based Learning, *5*(2), 55–69. https://doi.org/10.4018/ijgbl.2015040104

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283–297. https://doi.org/10.1016/J.CHB.2017.10.007

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547–559. https://doi.org/10.1016/J.CHB.2017.05.038

Veksler, V. D., Buchler, N., Hoffman, B. E., Cassenti, D. N., Sample, C., & Sugrim, S. (2018, May 15). Simulations in cyber-security: A review of cognitive modeling of network attackers, defenders, and users. *Frontiers in Psychology*. https://doi.org/10.3389/fpsyg.2018.00691

Velicer, W.-F., & Jackson, D.-N. (1990). Component Analysis versus Common Factor Analysis: Some issues in Selecting an Appropriate Procedure. *Multivariate Behavioral Research*, *25*(1), 1–28. https://doi.org/10.1207/s15327906mbr2501_1

Viejo, A., & Sánchez, D. (2016). Enforcing transparent access to private content in social networks by means of automatic sanitization. *Expert Systems with Applications*, *62*, 148–160. https://doi.org/10.1016/j.eswa.2016.06.026

Waite, A. (2010). InfoSec Triads: Security/Functionality/Ease-of-use | Infosanity's Blog. Retrieved February 4, 2019, from https://blog.infosanity.co.uk/2010/06/12/infosec-triads-securityfunctionalityease-of-use/

Wan, Z., Wang, Y., & Haggerty, N. (2008). Why people benefit from e-learning differently: The effects of psychological processes on e-learning outcomes. *Information and Management*, *45*(8), 513–521. https://doi.org/10.1016/j.im.2008.08.003

Weidemann, B. R., & Fitzgerald, A. (2008). Mastering the art of writing quantitative research reports. *Marketing Research Review*, (April). Retrieved from https://www.quirks.com/articles/by-the-numbers-mastering-the-art-of-writing-quantitative-research-reports

Wetzels, M., Odekerken-Schröder, G., & Van Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly*, 177–195.

Wetzels, Odekerken-Schröder, & van Oppen. (2017). Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration. *MIS Quarterly*, *33*(1), 177. https://doi.org/10.2307/20650284

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. https://doi.org/10.1089/cyber.2014.0179

Williams, K., Boyd, A., Densten, S., Chin, R., Diamond, D., & Morgenthaler, C. (2009). Social Networking Privacy Behaviors and Risks.

Wilson, M., & Hash, J. (2003). *Building an Information Technology Security Awareness and Training Program*. Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-50

Witte, K. (1993). Message and conceptual confounds in fear appeals: The role of threat, fear, and efficacy. *Southern Communication Journal*, *58*(2), 147–155. https://doi.org/10.1080/10417949309372896

Wold, H. (1966). Estimation of Principal Components and Related Models by Iterative Least squares. *Academic Press, New York*, 391–420. Retrieved from https://ci.nii.ac.jp/naid/20001378860/

Xu, H., Dinev, T., & Smith, J. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*. Retrieved from http://faculty.ist.psu.edu/xu/papers/jais2011.pdf

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior*, *84*, 375–382. https://doi.org/10.1016/j.chb.2018.02.019

Yao, M. Z. (2011). Self-Protection of Online Privacy: A Behavioral Approach. In *Privacy Online* (pp. 111–125). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-21521-6_9

Yao, M. Z., Rice, R. E., & Wallis, K. (2007). Predicting user concerns about online privacy. *Journal of the American Society for Information Science and Technology*, *58*(5), 710–722. https://doi.org/10.1002/asi.20530

Young, A. L., & Quan-Haase, A. (2009). Information revelation and internet privacy concerns on social network sites. In *Proceedings of the fourth international conference on Communities and technologies - C&T '09* (p. 265). New York, New York, USA: ACM Press. https://doi.org/10.1145/1556460.1556499

Young, A. L., & Quan-Haase, A. (2013). PRIVACY PROTECTION STRATEGIES ON FACEBOOK: The Internet privacy paradox revisited. *Information Communication and Society*, *16*(4), 479–500. https://doi.org/10.1080/1369118X.2013.777757

Young, H., Vliet, T. Van, Ven, J. Van De, & Jol, S. (2018). Understanding Human Factors in Cyber Security as a Dynamic System (Vol. 593). https://doi.org/10.1007/978-3-319-60585-2

Zhang, C., Sun, J., Zhu, X., & Fang, Y. (2010). Privacy and security for online social networks: challenges and opportunities. *IEEE Network*, *24*(4), 13–18. https://doi.org/10.1109/MNET.2010.5510913

Zhang, Z. (2015). Security, Trust and Risk in Multimedia Social Networks. *The Computer Journal*, *58*(4), 515–517. https://doi.org/10.1093/comjnl/bxu151

Zhang, Z., & Gupta, B. B. (2018). Social media security and trustworthiness: Overview and new direction. *Future Generation Computer Systems*, *86*, 914–925. https://doi.org/10.1016/j.future.2016.10.007

Zhao, S.-Z., & Suganthan, P. N. (2012). Comprehensive comparison of convergence performance of optimization algorithms based on nonparametric statistical tests. In *2012 IEEE Congress on Evolutionary Computation* (pp. 1–7). IEEE. https://doi.org/10.1109/CEC.2012.6252910

Zhou, T. (2015). Understanding user adoption of location-based services from a dual perspective of enablers and inhibitors. *Information Systems Frontiers*, *17*(2), 413–422. https://doi.org/10.1007/s10796-013-9413-1

Zhou, T., & Li, H. (2014). Understanding mobile SNS continuance usage in China from the perspectives of social influence and privacy concern. *Computers in Human Behavior*, *37*, 283–289. https://doi.org/10.1016/J.CHB.2014.05.008

7. Appendix

Table 7-1 - Literature Review Reference Table

No.	Paper Title	Demographics & Attributes	disposition	Privacy Concern	Perceived Privacy Risk	Threat Awareness	Self-efficacy	Training & Awareness Strategies	Security & Privacy Practice	Privacy Paradox
1	Acquisti & Enhancing, 2006			√	√	√				√
2	Acquisti & Grossklags, 2005									√
3	Abraham, 2011							√		√
4	Acquisti, 2004									√
5	Almadhoun, Dominic, & Woon, 2011		√	√						
6	A. L. Young & Quan-Haase, 2009					√				
7	A. L. Young & Quan-Haase, 2013									√
8	Anwar et al., 2017	√						√		
9	Arbaugh, 2000	√								
10	Bada et al., 2015					√	√	√		
11	Barnes, 2006									√
12	Barth & de Jong, 2017									√
13	Bolhuis & Giraldeau, 2005							√		
14	Brandtzæg, Lüders, & Skjetne, 2010			√						
15	Buchanan, Paine, Joinson, & Reips, 2007			√					√	
16	Buck, Horbel, Germelmann, & Eymann, 2014									√
17	C. Zhang, Sun, Zhu, & Fang, 2010			√						
18	Chen, Rea Jr, & Rea, 2004	√								
19	Choi, Kim, Goo, & Whitmore, 2008							√		
20	Christofides, Muise, & Desmarais, 2009			√						
21	Cook & Allan, 2018							√		
22	Coventry, Briggs, Jeske, & Van Moorsel, 2014							√		
23	Crano & Prislin, 2006			√						
24	Crutchfield, 1955									√
25	Davison, 1983									√
26	de Bruijn & Janssen, 2017						√			
27	Debatin et al., 2009		√	√						√
28	Deuker, 2010; Pötzsch, 2009									√
29	Dienlin & Trepte, 2015	√		√	√					
30	Dinev & Hart, 2006				√					

31	Dwyer, Hiltz, & Passerini, 2007		√							
32	Egelman & Peer, 2015						√	√	√	
33	European Comission, 2011									√
34	Yao, Rice, & Wallis, 2007									√
35	Everett, 2010		√							
36	Fishbein & Ajzen, 2011			√						
37	Flender & Müller, 2012									√
38	Fogel & Nehmad 2009				√					
39	Fogues, Such, Espinosa, & Garcia-Fornes, 2015				√					
40	Garg & Jean Camp, 2015				√					
41	Gerber, Gerber, & Volkamer, 2018				√					
42	Gouveia, Lopes, & de Carvalho, 2011							√		
43	Gratian et al., 2018								√	
44	Gross, Acquisti, & Heinz, 2005			√						√
45	H. Li, Sarathy, & Xu, 2011	√	√		√				√	
46	H. Young, Vliet, Ven, & Jol, 2018								√	
47	Hajli & Lin, 2016						√			
48	Halevi, Lewis, & Memon, 2013	√							√	
49	J. Lee, 2012						√			
50	Jensen, Potts, & Jensen, 2005			√						
51	Kahneman & Egan, 2011				√					
52	Kang, Dabbish, Fruchter, & Kiesler, 2015						√			
53	Keith, Thompson, Hale, Lowry, & Greer 2013				√					
54	Korpela, 2015							√		
55	Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010									√
56	Kumaraguru & Cranor, 2005								√	
57	Kunreuther, 1984									√
58	L. Becker & Pousttchi, 2012			√						
59	Lallmahamood, 2007		√							
60	Lancelot Miltgen, Popovič, & Oliveira, 2013				√					
61	Larson, 2015							√		
62	Livingstone & Brake, 2010			√						
63	Malhotra, Kim, & Agarwal, 2004								√	
64	Mathiyalakan, Heilman, & White, 2002	√								
65	Mohamed & Ahmad, 2012									√
66	More, 2011						√			
67	Nepal, Paris, Pour, Freyne, & Bista, 2015								√	
68	Ng, Kankanhalli, & Xu, 2009								√	
69	Norberg, Horne, & Horne, 2007									√

70	Nosek, Banaji, & Greenwald, 2002							√		
71	Nurse, Creese, Goldsmith, & Lamberts, 2011							√		
72	O'Keeffe & Clarke-Pearson, 2011		√							
73	Oakleaf, 2009								√	
74	Oehri & Teufel, 2012					√		√		
75	Oomen & Leenes, 2008									√
76	Quinn, 2016.									√
77	Saridakis, Benson, Ezingeard, & Tennakoon, 2016				√					
78	Schlienger & Teufel, 2002					√		√		
79	Schmidt, Hunter, & Urry, 1976			√						
80	Schneier, 2001				√					
81	Scott & Weems, 2010						√			
82	Shareef, Kumar, Kumar, & Dwivedi, 2011		√							
83	Shin, 2010				√					
84	Smith, Milberg, & Burke, 1996		√	√						
85	Stanton, Stam, Mastrangelo, & Jolton, 2005								√	
86	Stutzman, 2006									√
87	Sundar, Kang, Wu, Go, & Zhang, 2013									√
88	Taddicken, 2014					√				
89	Tamrakar, Russell, Ahmed, Richard III, & Weems, 2016						√			
90	Teutsch & Niemann, 2016			√						
91	Trepte, Dienlin, & Reinecke, 2014			√						√
92	Tsai et al., 2016			√						
93	Tversky & Kahneman, 1974									√
94	van Dijk, Spil, van der Burg, Wenzler, & Dalmolen, 2015							√		
95	van Schaik et al., 2018				√					
96	Veksler et al., 2018								√	
97	Viejo & Sánchez, 2016				√					
98	Waite, 2010							√		
99	Whitty, Doodson, Creese, & Hodges, 2015							√		
100	Wilson & Hash, 2003							√		
101	Witte, 1993							√		
102	Z. Zhang, 2015; Z. Zhang & Gupta, 2018				√					
103	Zhou, 2015		√		√					

Default Question Block

Online Survey: Security & Privacy on Social Media

Thank you for your interest in participating in this study.

Before we start, there is some information that you may find useful.
You may want to print out a copy of this information sheet and consent form.

Please read through and scroll down to continue with the survey.

Once you have read the information, should you be interested in participating, *please click 'Continue' to start the questionnaire*.

Information and Consent Form

You are invited to participate in a research project conducted by researchers at the University of Ottawa concerning Social Media Security and Privacy Issues and Behaviours.

Purpose of the Research Project

The purpose of this research is to investigate users' attitudes towards information security and privacy threats within the context of social media use. The survey hopes to provide insights about users' perceptions and behaviors towards social media security and privacy issues. The findings from this research are expected to identify potential gaps in current practices for the mitigation of social media security and privacy threats, and to provide better guidelines to educate people about these issues.

This research project has been reviewed and approved by the University of Ottawa's Research Ethics Board (Certificate Number: 11-15-10).

If you have any concerns or questions about your rights as a participant or about the way the research project is conducted, you may contact:

Research Ethics and Integrity
University of Ottawa
Tabaret Hall, 550 Cumberland St. Room 154
Ottawa, ON, Canada K1N 6N5
Tel: +1(613)562-5387
Email: ethics@uottawa.ca www.research.uottawa.ca/ethics

Data Collection Procedures

You will be responding to questions in an online survey. This survey consists of general questions related to your knowledge, opinions and behavior pertaining to the use of social media platforms and associated security or privacy issues.

Completing this questionnaire will take about 15 minutes.

Privacy and Confidentiality

Your identity will remain anonymous and the data collected will be kept confidential and treated with respect.

To guarantee anonymity, no personally identifiable information will be asked in the survey.

Furthermore, all survey responses will be kept confidential and they will not be released to any third party organization. The data collected from this study will only be reported in aggregate form.

Please be advised that the data collected will be hosted and administered by Qualtrics.com whose servers are located in United States of America. Therefore, all data is subject to applicable laws, including, but not limited to the Patriot Act of the United States of America which allows American authorities to access such information.

Conservation of Data

After the completion of the research, data will be conserved in a secure digital environment for 5 years. Data will be stored digitally in a password-protected Excel file on the principal investigator's computer which has multiple layers of security.

Secondary Use of Data

The data gathered in this study may be used by members of the research team in subsequent research investigations exploring social media use and/or information security and privacy issues. Any secondary use of data will be treated with the same degree of confidentiality and anonymity as in the original project. As such, any research projects requiring access to the data collected for this project will also be reviewed by the University of Ottawa's Research Ethics Board for approval.

Potential Harms or Risks

There are no physical, psychological, or social risks expected as a result of participating in this research project.

Potential Benefits

There will be no direct incentives for the participants in the study. However, participants may feel some fulfillment in helping to carry out research that may lead to practical recommendations to improve user awareness of security and privacy on social media, and subsequently lead to safer online social media experiences.

Participation

Your participation in this study is strictly voluntary. If you do not want to answer all the questions in the survey, you do not have to.

If you decide to participate, you can decide to stop at any time, even after completing the consent form or halfway through the questionnaire.

As it is not possible to link your identity with the survey data, once you submit your survey data (at the end of the questionnaire) it will be impossible to delete the data you have submitted. However, if you wish to withdraw from the study prior to submitting your survey data, then all you need to do is close your web browser (tab). Terminating the survey session without clicking the final submission button will prevent your data from being sent to the research team.

Results of the Research Project

You can request a summary of the findings from the survey after the analysis of the responses has been completed. If you wish to receive a summary, please send an email to any one of the research team members listed above.

Informed Consent

I have read the information presented above about the research study being conducted by Dr. Umar Ruhi, Ms. Anita Bright, Mr. Ali Alshammasi, and Mr. Karim Sultan from the University of Ottawa.
I have had the opportunity to ask questions about my involvement in this study and to receive additional details I wanted to know. I understand that I may withdraw from the study at any time if I choose to do so.
I understand that my confidentiality and anonymity, as outlined above, will be guaranteed.
I understand that the data collected for this project could potentially be used in future research investigations.

- ○ I AGREE to participate in this study
- ○ I DECLINE to participate in this study

Please Indicate Your Age Group:

- ○ Less than 18
- ○ 18-25
- ○ 26-35
- ○ 36-45
- ○ 46-55
- ○ 56-65
- ○ 65+

Please Indicate Your Gender:

- ○ Male
- ○ Female

What is Your Highest Education Level (obtained or in-progress)?

- ○ Primary School
- ○ Secondary (High) School

- College or Undergraduate (Bachelor's Degree)
- Graduate (Master's / Professional/ Doctoral Degree)

What is your Country of residence?

▼

Information:
For purposes of this survey, the terms ***social media, social media platforms, or social networks*** refer to websites or mobile applications that facilitate connections among people. Examples include Facebook, Twitter, LinkedIn, Google+, Snapchat, Instagram, Pinterest etc.

How many social media platforms do you use on a regular basis (i.e. visit at least once a month):

- 1
- 2
- 3
- 4
- 5 or more

How many hours on average do you spend on social media per week?:

- Less than 1 hour per week.
- 1 - 5 hours per week.
- 6 - 10 hours per week.
- 11 - 14 hours per week.
- 15+ hours per week.

Information:
For purposes of this survey, the terms ***privacy and security*** are defined as follows:

Privacy refers to the ability of individual users to exercise control over when, how, and to what extent their personal information is shared with other people or organizations.

Security refers to measures taken by users to protect their devices, accounts or data against unauthorized access, changes or destruction.

On a scale of 1 to 7, where 1 indicates strongly disagree and 7 indicates strongly agree:
Respond to each statement about your online privacy preferences:

	(1) Strongly Disagree	(2) Disagree	(3) Somewhat Disagree	(4) Neutral	(5) Somewhat Agree	(6) Agree	(7) Strongly Agree
Compared to others, I am more sensitive about the way online companies handle my personal information.	○	○	○	○	○	○	○
I am concerned about threats to my personal privacy in online activities.	○	○	○	○	○	○	○
It is important for me that my personal information is only available to people or organizations whom I have authorized.	○	○	○	○	○	○	○

On a scale of 1 to 7, where 1 indicates very low and 7 indicates very high:
Respond to each statement about people's security and privacy on social networks:

	(1) Very Low	(2) Low	(3) Somewhat Low	(4) Average	(5) Somewhat High	(6) High	(7) Very High
The risk of social media security threats to the average user is:	○	○	○	○	○	○	○
The risk of social media privacy breaches to the average user is:	○	○	○	○	○	○	○
The chance that an average user will fall a victim to a security breach through social media is:	○	○	○	○	○	○	○
The chance that an average user's privacy will be compromised on a social network is:	○	○	○	○	○	○	○

	(1) Very Low	(2) Low	(3) Somewhat Low	(4) Average	(5) Somewhat High	(6) High	(7) Very High
A social media user's vulnerability to security and privacy issues is:	○	○	○	○	○	○	○

On a scale of 1 to 7, where 1 indicates strongly disagree and 7 indicates strongly agree:
Respond to each statement about your security and privacy in social networks:

	(1) Strongly Disagree	(2) Disagree	(3) Somewhat Disagree	(4) Neutral	(5) Somewhat Agree	(6) Agree	(7) Strongly Agree
I have the required skills and knowledge to protect against security threats on social media.	○	○	○	○	○	○	○
I am able to avoid security threats on social networks.	○	○	○	○	○	○	○
I have the technologies and resources to protect myself from security threats on social media.	○	○	○	○	○	○	○
I can take appropriate steps to avoid compromising my private information through social networks.	○	○	○	○	○	○	○
I am well informed about ways in which I can safeguard my privacy on social networks.	○	○	○	○	○	○	○

How many friends or followers do you have on various social networks?:

	0 – 100	101 – 200	201 – 300	301 – 400	401 – 500	500+
${q://QID55/ChoiceGroup/SelectedChoicesTextEntry}	○	○	○	○	○	○
${q://QID56/ChoiceGroup/SelectedChoicesTextEntry}	○	○	○	○	○	○
${q://QID57/ChoiceGroup/SelectedChoicesTextEntry}	○	○	○	○	○	○

On a scale of 1 to 5, where 1 indicates you are not at all concerned and 5 indicates you are extremely concerned:
Which of the following issues are you concerned about when you use social media platforms?

	(1) Not at all concerned	(2) Slightly concerned	(3) Somewhat concerned	(4) Moderately concerned	(5) Extremely concerned
Impact of my online activities and interactions on my reputation or image	○	○	○	○	○
Social media sites sharing my information with other third-party organizations	○	○	○	○	○
Use of my social media profile and activities for data mining by other organizations.	○	○	○	○	○

	(1) Not at all concerned	(2) Slightly concerned	(3) Somewhat concerned	(4) Moderately concerned	(5) Extremely concerned
Disclosure of location information to third-parties or strangers	○	○	○	○	○
Privacy of my personal or professional information	○	○	○	○	○

On a scale of 1 to 7, where 1 indicates that you strongly disagree and 7 indicates that you strongly agree:
Please indicate your responses to the following statements about your general confidence with the use of new technologies:

	(1) Strongly Disagree	(2) Disagree	(3) Somewhat Disagree	(4) Neither Agree or Disagree	(5) Somewhat Agree	(6) Agree	(7) Strongly Agree
I can figure out how to use new technologies reasonably quickly.	○	○	○	○	○	○	○
I can use new technologies without the help of other people.	○	○	○	○	○	○	○
I have the knowledge and skills to learn to use new technologies reasonably well on my own.	○	○	○	○	○	○	○

On a scale of 1 to 5, where 1 indicates you never do something and 5 indicates you do something very regularly while using the Internet:
To what extent do you use the following security safeguards in your day-to-day Internet use?

	(1) Never	(2) Rarely	(3) Sometimes	(4) Often	(5) Always	Don't Know
Anti Virus or Anti Malware Software						
Anti Spam Rules or Filters in Email						
Safe Web Browsing Tools						
Password Management Tools						
Two-Step Authentication						
Biometric Authentication						
Security Apps on the Phone						
	(1) Never	(2) Rarely	(3) Sometimes	(4) Often	(5) Always	Don't Know

On a scale of 1 to 5, where 1 indicates you never do something at all and 5 indicates you do something very regularly while using the Internet:
To what extent do you use the following privacy enhancing techniques in your day-to-day Internet use?

	(1) Never	(2) Rarely	(3) Sometimes	(4) Often	(5) Always	Don't Know
Clear Cookies and Browser History						
Delete/Edit something I have posted online in the past						
Use a temporary username or email address online						
Browse or Post anonymously						

When did you last check or modify the privacy and/or security settings of your social network accounts?:

	Within the past month	Within the past six months	Within the past year	When the account was first created	Never	Don't Know
${q://QID55/ChoiceGroup/SelectedChoicesTextEntry}						
${q://QID56/ChoiceGroup/SelectedChoicesTextEntry}						
${q://QID57/ChoiceGroup/SelectedChoicesTextEntry}						

Which of these statements best reflects how you manage your passwords across social media sites?

- I use unique strong passwords (using a combination of letters, numbers and/or special characters) for every social media site.
- I use the same strong password across multiple social media sites.
- I use different but simple passwords on different social media sites.
- I use the same simple password on different social media sites.

On a scale of 1 to 5, where 1 indicates that you have never attempted to perform a certain action and 5 indicates that you regularly perform that action, respond to the statements below:

I have attempted or opted to:

	(1) Never	(2) Rarely	(3) Sometimes	(4) Often	(5) Always	Don't Know / Not Sure
Limit whether search engines can link to my social media profile						
Select who can send me friend or follower requests						
Review posts or pictures that I am tagged in						
Select specific people to share certain content or updates with						
Maintain a Restricted List contacts (who won't see posts shared with friends)						
Block users so they can't see my activity stream						
	(1) Never	(2) Rarely	(3) Sometimes	(4) Often	(5) Always	Don't Know / Not Sure
Limit who can see my connections or friends list						
Disable location information to be included automatically with my posts						
Limit how others can discover or find me on the social network						
Receive alerts for logins from new devices or browsers						
Use my phone as a second-step for logging into social networks						