LEBANESE AMERICAN UNIVERSITY

Information Security Awareness in Lebanese Community:

Antecedents and Impact on Practice

By

Abir Mohammad Sinno

A thesis Submitted in partial fulfillment of the

requirements for the degree of Master of Business

Administration

Adnan Kassar School of Business

December 2017

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS APPROVAL FORM

Student Name: Abir Sinno I.D. #: 20140047

Thesis Title: Information Security Awareness in Lebanese Community: Antecedents and Impact on Practice.

Program: Masters in Business Administration

Department: Information Technology and Operations Management

School: Adnan Kassar School of Business

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

Masters in the major of Business Administration.

Thesis Advisor's Name	Dr. Manal Yunis	Signatu [redacted]	DATE: 18 / 12 / 2017 (Day / Month / Year)
Committee Member's Name	Dr. Abdelnasser Kassar	Signatu	DATE: 18 / 12 / 2017 (Day / Month / Year)
Committee Member's Name	Dr. Abbas Tashiri	Signatu	DATE: 18 / 12 / 2017 (Day / Month / Year)

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

By signing and submitting this license, you (the author(s) or copyright owner) grants the Lebanese American University (LAU) the non-exclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic formats and in any medium, including but not limited to audio or video. You agree that LAU may, without changing the content, translate the submission to any medium or format for the purpose of preservation. You also agree that LAU may keep more than one copy of this submission for purposes of security, backup and preservation. You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant LAU the rights required by this license, and that such third-party owned material is clearly identified and acknowledged within the text or content of the submission. IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN LAU, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT. LAU will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

Name: Abir Sinno

Signature: [redacted]

Date: 27/11/2017

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

1. I have read and understood LAU's Plagiarism Policy.
2. I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.
3. This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name: Abir Sinno

Signature: [redacted]

Date: 27/11/17

Dedication

I dedicate my thesis work to my family. I am grateful to my loving parents, whose words of encouragement and push for tenacity ring in my ears.

I really appreciate the support I had from my husband Abdullah and my kids, Layal and Hasan who never left my side and encouraged me throughout the process. I couldn't have done it without them!

Acknowledgement

I wish to thank my committee members, Dr. Manal Yunis, Dr. Abdul Naser Kassar and Dr. Abbas Tarhini who generously shared their expertise and precious time. A special thanks to Dr. Manal Yunis, my advisor, for the countless hours of reflecting, reading, and most of all her encouragement for me throughout the entire process.

Information security Awareness in Lebanese Community:

Antecedents and Impact on Practice

Abir Sinno

ABSTRACT

In an interconnected economy, as technology evolves and reliance on information increases, new information security threats emerge. These threats are becoming increasingly complex, expensive and more specific to the vulnerabilities identified in the different systems, applications, and infrastructures. Universities are considered to be easy targets because they are known to host vast computing power and at the same time, they provide open access to the public. Human errors are one of the top threats to information security; this is why many researchers considered security education, training and awareness key factors of information security in any organization, where they aim to educate staff on information security. This study aims to evaluate and examine user perceptions towards information security practices and the level of awareness amongst students in Lebanese universities. Based on a theoretical framework comprising KAB Model and Protection-Motivation Theory, the study employs an exploratory method by administering a survey that targets university students on both the graduate and the undergraduate level to evaluate the level of awareness and the antecedents that contribute to this awareness. Data analysis is done using PLS Path Modeling. Results are reported and interpreted, implications are discussed, and limitations and recommendations are presented.

Keywords: Information Security Awareness, Technical Approach, Non-Technical Approach, Knowledge, Attitude and Behavior

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 The Value of Information

The information revolution reshaped the world. Billions of people are now linked by networked connections, they have the information processing power that was undreamt of a century ago.Many countries are pursuing initiatives to exploit the full potential of cyberspace focusing on cloud computing, IoT (Internet of Things) and Big data, upon realizing that the importance and criticality of such initiatives to achieving national competiveness. Information and Communication Technologies (ICT) presented new opportunities for the development of the educational, social, economic, political and legal sectors. The advancement of the internet, the availability and affordability of broadband services on mobile devices resulted in a rise in the number of internet users. By the end of 2015, approximately 65% of all people who were using the Internet, were from developing countries (International Telecommunications Union (ITU), 2008).

Countries are pursuing digitization at a rapid pace and the ever increasing dependence on the aforementioned technologies come at a price: cyber threats (Beidleman, 2009).

In the past two decades, information technology became more and more important and key to the success of various organizations (Morton, 1991; Davenport, 2013). Due to the importance of the role that information plays in supporting business operations of any organization (Scott, & Davis, 2015). Information provides an

organization with the needed competitive advantage over others to survive the market (Posthumus, Von Solms, & King, 2010).

The fact that information is valuable and critical to organizations, highlights a point of vulnerability of an organization to the various types of internal or external attacks like hackers, viruses and worms, data loss, etc. (Loch, Carr, & Warkentin, 1992). Such information security breaches or risks can cause an organization actual and potential financial and legal losses, not to mention the reputation ramifications (Böhme, & Nowey, 2008; Wagner, & Disparte, 2016). Practitioners and academics are increasingly trying to find ways to implement effective information security.

Information systems are used by organizations for data processing, storage, and data transmission. Consequently, Organizations have to face the challenge of protecting the different information systems in an organization from the different possible security breaches (Posthumus, & Von Solms, 2004).In compliance with applicable laws, organizations have been investing heavily in the protection of their information systems and their data from various types of attacks (Weber, 2010).

Despite all these efforts and measures, information security breaches have been on the rise (Soomro, Shah, & Ahmed, 2016; Walters, 2016). Many intrusions around the globe have been reported resulting in the theft of money, assets, and sensitive military, commercial and economic information *(*Johnson, 2016). For example,

- Saudi Aramco's data breach in 2012 affected up to 30,000 workstations. This breach was aimed to stop the oil output of one of the biggest oil producers in the world (Al Balushi, Ali, & Rehman, 2016).

- That same year both RAKBank in UAE and BMI in Oman suffered from a hacking incident where hackers were able to hack into card processing firms, increase the available balance and withdrawal limits on prepaid debit cards and then code fake cards to facilitate the theft of 45 million dollars (Walters,2016).
- 7 million health records in the United States were exposed to a data breach in 2013, this represents a 137% increase from the breaches reported in 2012 (Collier, 2014)
- In 2013 Iranian hackers were able to gain control of Bowman Dam sluice system, luckily the controls were manually disconnected at the time (Walters, 2014).
- Between the period extending between August and December of 2015, Hyatt Hotels Corporation experienced a malware attack on payment processing systems in two hundred and fifty locations. The malware collected cerdit card payment information (Dillon, 2016).
- In 2016 , the Federal Bureau of Investigation(FBI) in USA, suffered a critical breach. A hacker was able to penetrate their systems, retrieve the names and contact information of 29,000 employees from the Department of Homeland Security and FBI and released the information online, exposing their identities and putting them in danger (Walters, 2016).
- In May 2017 , more than 100 countries suffered a ransomware attack that hit within 48 hours. It was believed that the WannaCry / WanaCrypt0r 2.0 malware attack was the biggest ransomeware attack to ever be recorded (Kessem, 2017). Computers in at least 150 countries were crippled by the the "WannaCry" attack which

caused global financial and economic losses that almost totaled into billions of dollars, which makes this attack one of the most damaging ransomeware incidents (Berr, 2017)

Such threats not only caused physical losses but also compromised the security and the existence of the victims. As the types of threats evolve along with the massive advances in technology, information security and protection become more difficult to achieve and more of a critical need (Whitman, 2003).

In an attempt to secure their information systems, many organizations apply both the technical and the non-technical methods. Technical methods involve applying encryption, firewalls, security models and sometimes authentication methods to handle any attempts to breach their information systems. The non-technical approaches, however, focuses on improving users' security behaviors by raising information security awareness, educating the users or training them, and using products that support and encourage the secure use of information systems.

Many researchers believe that computer users are the weakest link behind many cyber-attacks (Hansman, & Hunt, 2005; Subrahmanian, Ovelgönne, Dumitras, & Prakash, 2015). Most users are low on computer literacy and they are incapable of setting up a secure personal computing system because simply they are not all IT professionals (Edwards, 2015; Jacobson, & Idziorek, 2016). This lack of security awareness is observed in peoples' practices like browsing unsafe websites, using open Wi-Fi connections, sharing passwords with friends and peers, disclosing personal information on social media or downloading unsafe software (Liang, & Xue, 2010).

User information security awareness (ISA) and behavior has been the center of attention of academicians over the past decade (Rezgui, & Marks, 2008). Many of them believe that universities as institutions of higher education play an important role in raising

the level of awareness, knowledge, skills, and values of the future workforce regarding information security. (Stanton, Stam., Mastrangelo, & Jolton, 2005).

This assumption is based on the knowledge-attitude-behavior (KAB) model that was proposed by Miller in 1998. The KAB model suggests that if we improve knowledge, our attitudes will change; and that these changes in attitude would promote behavior change.

Thus, it is suggested that as universities raise awareness on Information security, users will be more likely to practice safe information management. Universities prepare most of the professionals who are supposed to be in charge of developing, leading, managing, teaching, working in, and influencing society's future organizations, so they are considered to be key drivers for raising awareness on information security (Stanton, Stam., Mastrangelo, & Jolton, 2005).

1.2 Problem Statement

In order to secure information systems and to minimize the possibility of breaches, organizations take combinations of technical and nontechnical measures (Von Solms, & Von Solms, 2004). Technical methods involve applying encryption, firewalls, authentication methods and security models as ways to handle any attempts to breach their information systems (Barrows, & Clayton, 1996). Non-technical approaches however, aim to improve users' behavior through education and training, raising information security awareness, and using products that encourage and support secure usage of information systems (Colwill, 2009). Lack of security awareness would impose many risks like viruses, phishing, social engineering and stolen passwords. Such risks would

impede an organization and hinder its growth (Saini, Rao, & Panda, 2012). Even though, user awareness is always proposed as a non-technical approach to secure information systems, it is the least practiced method and the least invested in (Merete Hagen, Albrechtsen, & Hovden, 2008).

Normally, organizations that implement information security awareness programs are less likely to have security incidents caused by user behaviors (Kankanhalli, Teo, Tan, & Wei, 2003). Yet in a country where no cybersecurity policy exists and no legislations pertaining to cybercrime are set, we need to have a closer look at the level of awareness of the Lebanese community because unfortunately this may be our only front-line defense in the face of any possible attack.

Previous studies did not examine information security in Lebanon as a country, therefore, it is of high importance to examine the levels of information security awareness in Lebanon in order to better comprehend the antecedents involved, the approaches applied, and the degree to which these approaches are effective in creating information security awareness and developing information security best practices.

1.3 Statement of Purpose

This study aims to examine user perceptions towards information security practices and the level of information security awareness amongst students in Lebanese universities. The study will employ an exploratory method by administering a survey that targets university students on both the graduate and the undergraduate level to assess the level of awareness and identify the factors that contribute to this awareness and that result from it. Many stake holders would benefit from this study to enforce policies and regulations like administrators, IT departments, and curriculum designers. To start with,

administrators would be the front-line defense for any organization against any potential breaches. This study would shed some light on some of the information security practices that must be adopted, and would hence improve the level of information security in organizations. IT departments would also benefit since they will gain a better understanding of all the factors that need to be considered when setting information security policies and consequently they would have a better chance of successfully implementing and adopting the policies. Curriculum designers would also gain insight from this study and this would aid in creating rich curricula that integrate information security courses and practices thus preparing tomorrow's workforce for the evolving threats.

With the above purpose in mind, the study mainly aims to address the following questions:

1. What are the levels of users' awareness and preventive practice?

2. What are the factors that are most likely to be associated information security awareness?

3. What is the relationship between users' information security awareness and their information security related behavior?

The study will attempt to answer the above questions in light of the current body of literature and the results of our empirical study.

1.4 Significance of the Study

The significance of the study is attributed to the fact that it is the first to explore the level of information security awareness in an educational institution operating in

Lebanon by examining the factors that may promote this awareness and how this would impact the behavior of users in terms of information security related behaviors. The findings of the study would provide general assessment of the current level of security awareness in the Lebanese community and these findings would guide information security decision makers in the development of better strategies to improve user awareness and consequently elevate the level of information security.

This study will also highlight the importance of non-technical approaches which mostly focus on user behavior. It will also help end users realize their level of involvement and the role they can play in securing the information systems of their organizations. In other words, while previous studies highlighted technical approaches related to information security, this study emphasizes the perceptual and behavioral aspects related to information security awareness and practices.

1.5 Outline of the Study

The study will follow the following outline:

Chapter 1 is an introduction that presents the importance of information security awareness and highlights the need for examining the factors that could be related to it in an educational setting. It also presents the research problem, the purpose of the study, the research questions, and the significance of the study.

Chapter 2 presents a review of the literature that discussed the topic in similar and different contexts. The factors presented by previous researchers as antecedents to information security awareness as well as the relationships between these factors and users' behavior related to information security practices will be explored and presented.

Chapter 3 discusses the theoretical frameworks that the study is based upon. Different frameworks related to behavioral approaches and adoption of relevant practices will be presented and discussed. Based on the literature review and the theoretical frameworks, the conceptual model of the study will be developed and presented.

Chapter 4 presents the study design and methodology. The instrument used to measure the various study variables, as well as the sampling technique, the sample selected, and the data analysis methods to be used to test the study model will be presented and discussed.

Chapter 5 reports the study findings and displays the statistical analysis results with possible interpretations and discussions.

Finally, Chapter 6 wraps up the study by presenting the main research conclusions, basic implications, limitations, and recommendations for future research.

Chapter 2

Literature Review

2.1 Information Threats

Information is anything that is communicated in any form publicly or privately. Any threat to the privacy of information could have a significant impact on all stakeholders; damage could vary from the loss of reputation, theft of assets, or other losses, depending upon the nature of the information (Nayak, & Rao, 2014). Thirty years ago, securing Information used to be viewed as a technical process. However, with the rush towards digitization and the change in the way computers and networks operate, information security evolved and exceeded technical boundaries. (Carr, N. G., 2003; Pérez, Murray, Fluker, Fluker, & Bailes, 2017).

Information security is generally defined by the properties that characterize secure information that include, but are not limited to, confidentiality, integrity and availability of information (Wood, 2004).

In 1975, Saltzer and Schroeder confirmed that security specialists identified three categories of threats to information:

- Threat to Confidentiality which can be comprimised by the unauthorised release of information
- Threat to integrity when unauthorised modification of information takes place

- Threat to availability which can be comprimised if one suffered from unauthorised denial of use

According to Posthumus & Von Solms (2004), information security can be defined as the protection of confidentiality, integrity, and availability of information. This definition was also backed by Whittman and Mattord (2011) who described it as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information".

The majority of research on information security focuses on the means to protect the components of the "CIA" model of information security information namely confidentiality, integrity, and availability (McCumber, 1991; Schneier, 2000).

- Confidentiality restricts the access to information in an organization to authorized personnel only.
- Integrity ensures and manages the processing method used on information and the accuracy and completeness of this information after the processing

.

- Availability emphasizes the accesibility and the precessability of information to authorized users .

Many researchers like Dhillon & Backhouse (2000), Parker (2002), Siponen, & Oinas-Kukkonen (2007), and Von Solms & Van Niekerk (2013) adopted and extensively used and applied this model of information security

Whittman and Mattord(2011) examined the CIA Triad which expounded that the value of information lies in its confidentiality , integrity and availability but they disagreed on the basis that the value of information is not limited to these three

characteristics. The authors suggested that accuracy, authenticity, utility, and possession should also be protected and that the CIA model no longer solely addresses the fast changing environment of information security.

The evolution of technology increases the need for information security since information security threats target all technologies that have to deal with information like the internet, ATMs, bank web portals, university webpages, credit cards etc. (Matbouli, & Gao, (2012, March)).

The Internet of things (IoT), the extensive use of the electronic chips in the daily things around us (like cars, toys, etc.) and the interconnectedness of all these gadgets are additional concerns because the possibility of an attack exists (Samaila, Neto, Fernandes, Freire, & Inácio, 2017).

The IoT term is used to refer to the process of connecting smart devices and enabling them to interact with other objects, or more complex and legacy computing devices and the surrounding environment (Rose, Eldridge, & Chapin, 2015). Smart devices have excessively populated and interacted with our lives and our environment by receiving, delivering, and processing any sort of information. Sensors have been integrated in vehicles, buildings, and our surrounding environment, some are even carried by people, and in some cases attached to animals. These sensors are able to communicate locally and remotely for the purpose of providing integrated services. With this deep penetration of technology, that introduced a new kind of remote interaction, and automation came some new security and privacy concerns (Weber, 2010).

Cloud computing is another factor that elevates the need for information security. This computing model has been getting a lot of attention lately, probably due to the many benefits it brings like increasing flexibility, improving access to data, and cutting costs.

Yet at the same time, it also presents many new risks to the security of the data that is stored in cloud environments (Van der Molen, 2012; Behl, & Behl, 2012, October).

As technology evolves, new threats emerge with their increasing complexity. These threats are more specific to the vulnerabilities identified in the different systems, applications, and infrastructures (Egan, 2007). According to Nayak & Rao, (2014) "every product, whether software or hardware, has vulnerabilities that, when exploited, can lead to extensive damage."

2.2 Information Security Threats

Recently information security violations have been a hot topic. These threats are costing businesses a lot of money. Unauthorized intrusions, identity thefts, privacy violations, and inference problem are also occurring frequently (Franchi, Poggi, & Tomaiuolo, 2015).

Deploying state of the art security products does not guarantee improved security. In many cases users do not follow security procedures, like checking for viruses or encrypting emails. Security products are often rendered ineffective by their users' unawareness and inability to behave in a way that ensures the effectiveness of security mechanisms (Mitnick, & Simon, 2011).

User behavior has been considered the factor that contributes to many security failures. Consequently, many researchers refer to users as the "weakest link in the security chain" Humans were considered the "weakest link in the security chain" because they provide the one error that attackers are waiting for to exploit (Karlof, Shankar, Tygar, & Wagner, 2007; Whitten, & Tygar, 1998).

Many factors dictate the approach that users choose to deal with Information security threats (Alfawaz, Nelson, & Mohannak, 2010), such as user's perception of threat, user's trust, and user's knowledge of information security best practices (Hedström, Karlsson, & Kolkowska, 2013).

2.3 Perception of threat

According to Witte (1992), whether a threat is perceived or not by users, it exists as an external stimulus. A user is considered to have awareness of a threat when he or she perceives the threat. This means that when an individual identifies a threat, he/she would assess the degree of seriousness of the threat and the probability of being subjected to it.

Rogers (1975) first coined the term "Perceived threat severity" as a factor that impacts user behavior. It refers to users' perception of the degree of significance of a threat which is also the ability to affect the intensity of a response (Rogers 1975; Witte 1992).

On an individual level, studies in this domain often investigated the effect of perceived threat on attitude change by relaying persuasive messages to users, conveying a potentially harmful outcome associated with a specific course of action followed by a declaration of a recommended course of action to alleviate the threat, thus avoiding negative outcomes. This approach has proven to be effective in instilling change in attitude, behavioral intention, and behavior (Rogers 1983; Sherer and Rogers 1984; Schneider et al. 2001)

In general, users tend to exhibit positive bias through their belief that they are less likely to be at risk of being attacked. This means that people generally tend to expect positive outcomes more than negative outcomes when it comes to information security

(Jøsang, Ismail, & Boyd, 2007).Some studies found that information security managers are more to be optimistically biased where they understand the possibility of a negative occurrence, yet believe that they are less prone to be targeted (Rhee, Ryu, & Kim, 2012). Thus, it can be said that threat perception affects the motivation of adopting and complying with measures to counter a threat, and people tend to modify their behavior based on their perception of the significance of risk (Liang, & Xue, 2010).

When the user understands the impact of threat, if it materializes, he/she will also understand the factors that determine the changes in behavior. This is why if a user believes that he/she may be at risk of a higher threat, he/she will change his/her behavior in order to counter the consequences .On the other hand, when a user believes that he/she is not at risk, he/she tend to be less cautious and less likely to comply with safety measures (Lacey, 2009). Moreover, having security related products installed on computers may give users a false sense of safety and this may encourage their incompliance with safety measures (Zinatullin, 2016).

2.4 User's Trust

One popular definition of trust is: "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another". This definition fails to fully cover the restraints involved that are dynamic and varied in nature (Pearson, & Benameur, 2010; Urban, Amyx, & Lorenzon,

2009). Trust, being a complex concept, requires a multi-level analysis to try to comprehend it (Pearson, & Benameur, 2010).

Trust can be established through many different ways, and even though security does not necessarily imply trust, it can still be one of these ways (D Harrison McKnight, 2001; Suh, & Han, 2003). Nissenbaum on the other hand refutes this idea and stresses that trust and security do not contribute to one another (Nissenbaum, 2001). Researchers who advocate the suggestion above defend their belief with a simple example: "increasing security to increase trust comes from people being more willing to engage in e-commerce if they are assured that their credit card numbers and personal data are cryptographically protected" (Pearson, & Benameur, 2010).Trust was defined by Mayer et al. (1995), as the "willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other party." In the field of Information Security research, the term "trust" refers to the user's beliefs and expectations about trust-related characteristics of information technology (Koufaris, & Hampton-Sosa,2002; Pavlou, 2003). Most information security studies confirm that trust plays an important role in determining user actions regarding a threat. Consequently, users need to take "trust" into consideration as a critical factor when a user assesses the credibility of online information content or when a user decides to behave responsibly/irresponsibly to maintain information security (Safa, Sookhak, Von Solms, Furnell, Ghani, & Herawan, 2015). Some researchers opine that trust increases the possibility of a user neglecting security measures (Albrechtsen, 2007).

2.5 User's computer knowledge

Another major factor that contributes to the information security level in any organization, is the computer knowledge that the user has (Raskin, Hempelmann, Triezenberg, & Nirenburg, 2001).

The importance of Knowledge lies in the fact that as it accrues in a relevant behavior, say for example in information security, it eventually triggers alterations in attitude that will slowly translate into an alteration in behavior (Kaur, & Mustafa, 2013). This concept is based on Kruger and Kearney's research in the field of social psychology. They developed a model for measuring information security awareness using what was known as the KAB model which comprised: knowledge, attitude and behavior (Beavers, Kelley, & Flenner, 1982; Thomson, & von Solms, 1998; Kruger, & Kearney, 2006). Knowledge is mostly observed when a user knows how to act in certain situations. A user cannot maximize confidentiality, integrity and availability of information, unless he/she are able to know what these concepts mean (Wolmarans, 2003; Van Niekerk, 2005). Users play a major role in detecting and preventing security breaches, they are responsible for always following security countermeasures, such as choosing to protect their information by protecting their passwords (Ng, Kankanhalli, & Xu, 2009).

However, users vary in their background knowledge of computer and information security issues, and they may not be fully aware of all the best practices needed to maintain information security within their work environment. That makes them the most vulnerable to an attack. Thus, if we want to examine information security practices of a group of users, we have to consider their knowledge first (Aytes, & Connolly, 2004).

In many cases, users fail to conform with information security best practices and fail to adopt information security practices because they lack the knowledge of the basic information security threats and consequences and the measures that should be taken to prevent them. User's knowledge and technical skills affect his/her attitude and behavior and leads him/her to be more security-conscious. However, theoretical empirical information systems research on the behavior of individuals in practicing secure computing are rarely found (Workman, Bommer, & Straub, 2008; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005).

The inadequacy of the human user of computer system is the result of the neglect that the human factor has suffered from both the developers of security technology and from the security personnel in their organizations. Attackers have given the human element in security a lot of attention, much more than security designers have, and they have managed to take this advantage enormously (Workman, Bommer, & Straub, 2008).

In order to be able to design effective security systems, security designers need to identify the causes of undesired user behavior, and address these causes (Viega, & McGraw, 2001). For example if a user doesn't recognize the characteristics and limitations of human memory, he/she will have the tendency to make unattainable or inconsistent task demands, and will most probably lack the support, training and motivation and consequently he/ she are more likely to act irresponsibly with passwords.

2.6 Common Information Security Threats

This section will cover the most common information security threats that are affected by the human factor.

2.6.1 Social engineering

- Social engineering can be defined as the art and science of convincing people to do as one wishes. (Thornburgh, 2004; Hadnagy, 2010). Social engineering happens when a hacker tries to gain access into a system by acquiring the information that he needs to do so by playing psychological tricks on authorized users (Granger, 2001; Schneier ,2000; Schneier, 2011). In other words, it is the the act of getting required information (for example, a password) from a person as an alternative to breaking into a system (Sasse, Brostoff, & Weirich, 2001).It is a hacker's clever manipulation of people by incorporating threats, and a sense of fear and urgency to obtain information that will grant him access to a system and consequently compromising the information on that system (Mitnick, & Simon, 2011).

2.6.1.1 Phishing

One type of social engineering is phishing**,** phishing attacks start with an email that is broadcasted to recipients, it aims to trick the recipient into giving the attacker the information he/she is after by claiming to be from a well-known and trustworthy source, (Hong, 2012). Most of the time the user is instructed to click a link that directs him/her to a website where he/she is requested to enter their credentials such as credit card or bank account numbers, passwords, or social security numbers . The website usually has a look

and feel similar to that of the organization in question and may redirect the unsuspecting user to the actual website after collecting the data. (Jakobsson, 2005, Ramzan, 2010).

2.6.1.2 Pretext

Another type of social engineering is pretext .According ro Workman (2008), pretext is the act of creating the scenario that will manipulate the victim and get him/her to give away sensitive information, pay money or compromise confidential information. It differs from phishing, in that pretexts are mostly conducted in person by fostering a sense of trust with the victim and not fear (Parsons, McCormac, Butavicius, & Ferguson, 2010).

2.6.1.3 Pharming

Pharming is a more complex version of phishing. In a pharming attack, the culprit inserts Trojans or worms into the victim's computer or DNS server causing the initiation of different types of attacks .Such an attack would mislead the user to give their private information or passwords to a forged webpage. Pharming attacks are considered to be a very serious threat to the security of users on the client-side because even if the users double check the URL before they visit a website, they would not be able to detect any exception (San Martino, & Perramon, 2010; Karlof, Shankar, Tygar, & Wagner, 2007)

2.6.2 Malware

Malware is a program that has numerous malicious objectives and often bypasses security checks or antivirus software by applying anti-reverse engineering techniques.

As a software, a malware instance is created to cause damage. Malicious code as defined by McGraw, & Morrisett, (2000), is “any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system”. Malware was also defined as “a generic term that encompasses viruses, trojans, spywares and other intrusive code” (Vasudevan and Yerraballi, 2006).

Malware is a general term, it includes any spyware that may attack a victim’s computer for illegal purposes. Viruses, Trojans, and worms are different types of malware.

2.6.3 Viruses

A computer virus is a code that attaches itself to executable files or what may be referred to as ‘virus hosts’ and inserts itself into other programs, replicating itself in the process. When the user launches the virus host the virus is activated so it duplicates itself and disables malware detectors installed and enabled on the computer system. According to Schneier (2000), viruses may infect applications, data files, or system files in computer memory or hard disk. And although using an antivirus software may help in detecting and removing computer viruses, but users are still the front line defense. If users are trained to frequently update their antivirus software so that the virus definition files are up to date, and if users are made aware of potential sources of viruses and are encouraged to have good security practices then and only then would they be safe (Szor,2005; Skoudis, & Zeltser, 2004).

2.6.4 Worms

Worms are self-directed threats that infect computer programs in a different way than that of viruses. Worms replicated themselves and depend on many means to spread

for example it may be passed on to uninfected computers via network system, e-mail, instant messaging programs, peer-to-peer file-sharing networks and software vulnerabilities . Worms were considered a big concern to information security because of the way they propagate and the way they consume valuable computer resources. In many cases worms can cause a system to fail or crash (Campbell, 2016; Gross, 2011)

2.6.5 Trojan Horse

A Trojan horse may seem like legitimate application while in fact it is a harmful program in disguise. It is used by cyber-thieves and hackers to gain unauthorized access to computers. Once inside the system and activated, a Trojan horse may delete, block, modify, or copy data (Wu, Narang, & Clarke, 2014). It can also cause a major disruption to the performance of the computer system of network. A Trojan horse can also open "a back door" that allows an outsider to infiltrate the system and control the compromised computer remotely. There are major technical differences between Trojan horses, worms and viruses. Trojan horses and other types of malware have something in common, they "take advantage of the very conveniences and features that make the Internet so appealing" (Taylor, Fritsch, & Liederbach, 2014) and may cause serious problems for the users of the compromised device and those who rely on them.

2.6.6 Password attacks

Information systems rely on passwords to authenticate their users. That is why passwords are the target of varied attacks that are undertaken in different approaches that if successful would lead to identity theft or a major compromise in the privacy and the

security of the users.Below are the most common methods used to undertake such an attack:

- In some cases attackers simply “guess” the password either based on their personal knowledge of the user or based on the assumption that they did not change the default password setting .
- Attackers may also launch what is refered to as the “ Dictionary attack” where the attackers deploy programs to crack the passwords and to encrypt the words in the dictionary. The success of such an attack relies on people’s tendency to use passwords that are altered from a dictionary words.
- Another more sophisticated method called Brute force attack may be used. In this method attackers generate a large number of consecutive possibilities using an automated software to match the value of each character in a password.

2.7 Security Approaches

There are two approaches to information security: the technical approach and the non-technical approach (Vroom & Solms, 2004).

2.7.1 Technical Approaches

The technical approach fixates on deploying technology like cryptography, authentication methods, firewalls, and security models to mitigate threats. The technical approach applies technical controls to computer hardware, software, or firmware (Stoneburner, Goguen, & Feringa, 2002; Baskerville, Spagnoletti, & Kim, 2014).

- Authentication

Authentication ensures and validates that the individual is who he says he is and he is allowed access to the information. When considering authentication mechanisms, an unauthorized access takes place when an unauthorized user accesses the resources on an information system or when an authorized user accesses a level to which he is not authorized to access. This is why all users must be identified and authenticated before they are allowed to access information. This fact is also confirmed by Schneier (2000) when he stated "no matter what kind of computer security system you're using, the first step is often identification and authentication"

There are many ways to validate users who are attempting to access or retrieve information:

1. Th Knowledge approach: relies on something that a user knows

2. The Token approach: relies on an item that a user has for example a smart card.

3. The Biometrics approach: relies on something that a user is like fingerprints.

Due to the fact that the token based approach and the biometric approach are costly, the knowledge based approach is the one most commonly used. Yet the choice of the approach to be applied depends on the nature of the information that requires protection.

Another critical step for securing information systems, is using strong passwords. However, the limitations of the human brain presented a problem when people started forgetting their passwords and some wrote them down to remember them. This was a big problem especially if the system is not frequently used and the "reset password" option is not available. So we can conclude that technical approaches alone cannot secure information systems, and although some threats may be resolved using the technical

solutions only but many times when the level of complexity rises, it becomes evident that the technical solution cannot be sufficient.

2.7.2 Non-Technical approaches

With all the advancements in technology, it has been noticed that the number of breaches due to the human factor have risen. This is why some researchers refer to users as "the weakest link in the security chain", many researchers examined the culprit "human factor" without which technology cannot seem to function as it should (Metalidou, Marinagi, Trivellas, Eberhagen, Skourlas, & Giannakopoulos, 2014; Von Solms, & Van Niekerk, 2013). Many researchers considered failure to understand the technology and failure to implement the features are key factors that affect information security (Herath& Rao, 2009; Leach, 2003; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015).So as a way to transform the weakest link to the first line of defense, researchers suggested that security approaches should be user oriented (Siponen, 2000; Wang, Wu, Chen, & Wang, 2014).

These approaches can be categorized as follows:

- **Punishment approaches:**

This approach uses punishment as an external deterrence to force users to abide by security rules and policies (Siponen, Pahnila, & Mahmood, 2007; Chen, Ramamurthy, & Wen,2012).Some researchers and practitioners in the information security industry advocate the use of a deterrent strategy as a precaution to undesirable behaviors that could compromise information security as in the case of computer abuse or failing to comply with the information security policy (D'Arcy, & Hovav, 2007).Some researchers disagreed on the punishment approach, they considered punishment as a low priority choice to be applied by managers because they expect this approach to generate negative

consequences that would outweigh any benefits, it would cause users to experience negative emotions such as distress, anxiety, or withdrawal. (Kerr, 1975; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2015). Users may even display hostile behavior towards the punishing agent in the organization. Other researchers drawing from theories in organizational literature, advocate positive enforcement strategy for example offering a reward. They argue that the reward motivate users to comply , and if combined with sanction it can influence user's rational cost–benefit assessment of their compliance and noncompliance behaviors. If we examine reward and punishment from a control perspective we would certainly consider both as control mechanisms to achieve organizational goals and ensure compliance with policies. Many scholars on the other hand drew from the "General deterrence theory" to support punishment as a "negative" enforcement strategy. This theory proposes that by increasing the certainty and severity of punishment, organizations can deter unwanted behavior and minimize user incompliance with security policies. Advocates of punishment argue that punishment may improve the standards of social norms within an organization, highlight acceptable / unacceptable behaviors to users, and discourage incompliance with policies . Thus, punishment can actually result in positive outcomes if applied as a strategy to discourage undesirbal;e behavior . (Shariff, Greene, Karremans, Luguri, Clark, Schooler, & Vohs, 2014).According to Arvey and Ivancevich (2007) " punishment is a frequent and naturally occurring event in all of our lives and that it shapes a large part of our psyche and behavior. Therefore, a careful examination of punishment, particularly factors influencing the effectiveness of punishment, is necessary."

- **Non-punishment approaches**

Non-pinishment approaches empower users to modify their behaviors without the use of punishment. This approach can be further divided into an approach that promotes security either by information security awareness (Stanton, Stam, Mastrangelo, & Jolton, 2005) or by education and training which are the main factors to prevent things like social engineering (Tsohou, Karyda, & Kokolakis, 2015). Researchers who support this approach argue that security issues are greatly affected by the usability of the user interface (Huang, Rau, Salvendy, Gao, & Zhou, 2011).

Many researchers believe that user mistakes that are caused by user interface could compromise information security (Reeder, Karat, Karat, & Brodie, 2007) and consequently user interface design is considered to be one of the cornerstones of designing a secure system (Shneiderman, 2005; Wu, Huang, Xu, & Yang, 2013).

This focus on user interface doesn't negate the fact that users should be the ones controlling the user interface as long as the user interface is designed in such a way to ensure a threshold level of security. Here, we are just highlighting that as long as the goals of the user and those of the mechanism that he/she is using are in alignment, mistakes can be minimized (Schumacher, Fernandez-Buglioni, Hybertson, Buschmann, & Sommerlad,2013; Agrawal, & Khan, 2014; Endsley, 2016;D'Arcy, Herath, & Shoss, 2014).

A good approach to promoting information security in any organization is to make users aware of the threats they are up against and the consequences of their actions before allowing them to make any decision about security issues. This approach was strongly supported by Thomson, M. & von Solms (1998), where they stated that: "it is now necessary to educate the users in the discipline of information security. Their behavior has to be modified to such a degree that they carry out their day-to-day activities

in a security supporting manner. It is important that this behavior be subconscious, i.e. they must carry it out without having to think about what they are doing."

2.8 Information security in the Middle East and Lebanon

What measures have countries in the Middle East taken to enhance their Information security?

On a country level the terms Information security and cyber security are usually interchangeably used even though they may have some differences in context.

According to the International Telecommunications Union (ITU), Cybersecurity can be defined as follows:

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability;
- Integrity, which may include authenticity and non-repudiation; and
- Confidentiality" (International Telecommunications Union (ITU), 2008).

When governments adopt and execute cybersecurity policies, they are actually seeking safety from cyber-attacks and they are protecting information and other assets from being compromised and they are investing in improving their ability to mitigate the harms of such risks and their readiness to address all new emerging threats (Amoroso, 2011).Many measures were taken by countries of the Middle East in order to secure the information of the organizations that support their economy and protect them (Guazzone, 2016).

Since there was a need to ensure the adoption of security means, many governments around the world adopted certain regulations and legislations that would enable them to do so. Countries in the Middle East are following the lead, they are seeking digitization as well. Digitization takes place when consumers, enterprises, and governments extensively adopt connected digital technologies and applications (Sabbagh, Friedrich, El-Darwiche, Singh, Ganediwalla, & Katz, 2012). The overall compound annual growth rate(CAGR) of the digital markets in the Middle east was expanding at a rate of 12% equivalent to 35 Million dollars in 2015, it is expected to grow to 13.07% equivalent to 9.56 billion in 2019 (Morgan, 2017).

The major revenue generating industries in the Middle East are utilities, gas, oil and energy. These industries highly relied on Networks and industrial Control systems in their structure and operation. During the past few years these systems and networks were connected to the internet, and this means that they are more vulnerable to cyber attacks (Anderson, & Fuloria, 2010).

Many organizations are seeking ex-military personnel to handle cyber espionage. They tend to apply military-like strategies to counter the threat. This is due to the surge in

the volume and variety of cyberattacks, and the increase in vulnerability (Andress, & Winterfeld, 2013).

This exposure to information security threats is forcing many industries to adopt the latest technology solutions, thereby speeding up the development and growth of information security in this region (Yeoh, 2017). Where does Lebanon stand when it comes to information security?

Unlike the active measures undertaken by other countries in this region, Lebanon needs to work a lot to meet the required standards. According to the Telecommunications Regulatory authority reports, currently, Lebanese efforts did not meet the national requirements to deal with the high levels of information security risks and threats (Telecommunications Regulatory Authority, 2017).

In fact, Lebanon is still in the process of developing a vision and a strategy for information security.Lebanon has yet to establish legislations that deal with information security. Such legislations could be the basis for a solid framework for protecting individuals and corporations; Lebanon lacks effective integral information security awareness plans and dedicated campaigns. However, these challenges can be overcome if the private and the public sectors join forces to at least raise awareness (Telecommunications Regulatory Authority, 2017).

2.9 Information Security Awareness in Higher education institutions

With the increasing use of Internet based information systems and services and students extreme immersion in online social networks along with the rapid advances of technology, the spread of online courses and digital libraries educational institutions,

especially universities, have been subject to several cyber-attacks (Marcella & Greenfield, 2002; Hylén, 2006; Al-Janabi, & Al-Shourbaji, 2016). Universities were considered as easy targets because they were known to host vast computing power and at the same time they provided open access to the public and its constituencies thus with the power came the vulnerabilities (Rid, & Buchanan, 2015).

Many researchers recognized the importance of information security awareness in institutes of higher education (Rowley, 2000; Marks, & Rezgui, 2009; Lehman, 2016). Some even considered it one of the top areas of concern for universities in the USA for several years (Rezgui, & Marks, 2008). Even though the importance of information security awareness in universities has been recognized, yet studies examining this issue are actually few and the ones available focus on threats rather than the students, assessing their information security awareness or the ways to educate them properly (Lebek, Uffen, Breitner, Neumann, & Hohler, 2013).

Not all higher education institutions are ahead of the game when it comes to information security. The well-established universities in Lebanon are investing in their information security infrastructure to protect their intellectual property and their users (Aloul, 2012), however the complexity of their information systems makes the process very challenging. These systems are complex because they are a combination of operating systems, networks and platforms that operate together to cater for the needs of the users.A university may be an attractive target for attackers because first they are exposed to numerous potential human threats to the security of the information that is processed on a daily basis and second because the systems are mostly open access and are structured to serve users on and off campus (Rezgui, & Marks, 2008).

Even though they are at high risk of an attack, the level of information security applied does not match the value of the data being protected and they hardly make the effort to spread awareness amongst their users. Decision makers in the Information technology departments of higher education institutions focus on deploying all the physical measures to secure their systems like firewalls, intrusion detection software, routers, or proxy servers and they neglect the human factor (Rezgui, & Marks, 2008; Safa, Von Solms, & Futcher, 2016).

Human errors are considered to be one of the top threats to information security, this is why many researchers considered security education, training and awareness key factors of information security in any organization, where they aim to educate staff on information security (Drevin, Kruger, & Steyn, 2007). According to Katz (2005), in his study of the level of information security awareness among staff members of universities, staff fully understood and applied the suitable measures to keep their information safe, but they lacked the technical awareness.

The main purpose of educating staff on information security is to convince them of the need for it and its importance in any given situation. They need to be aware of the rules that they should work by. Awareness can prevent staff from performing inappropriately and can improve their effective use of security controls (Thomson, & von Solms, 1998).

According to a study by Kvavik and Voloudakis (2003), only 145 out of the 435 universities invested in information security awareness training for staff and students. Their study also concluded that information security awareness is the 2nd largest barrier to information security and accordingly suggested that universities deploy awareness programs for their users to ensure their understanding and their trust in the IT security

policy. Usually organizations that invest in information security awareness are those who believe that the cost of educating their employees on Information security is far less than the penalties incurred if the rules were not followed or their systems were attacked (Krausz, & Walker, 2013).

Taking into account the disparity in the literature, an assessment of information security awareness of students in Lebanese educational institutions is deemed important. Following will be a discussion of the theoretical framework underlying this study, and the conceptual model that will be proposed accordingly.

Chapter 3

Theoretical Framework & Conceptual Model

3.1 Theoretical Framework

Researchers in the field of information security proved over and over that successful implementation of information security policies depends on people/ end users as much as it depends on the technology (Whitman, & Mattord, 2011). In order to maximize the chances of successful IS implementations, researchers tried to understand and predict users' behavior towards information systems (Ives, & Olson, 1984; Venkatesh, Morris, Davis, & Davis, 2003; Wallace, & Sheetz, 2014).

As we mentioned earlier they proposed two approaches to improve users' behavior:

1. punishment approach
2. non-punishment approach

The punishment approach applies criminology theories, and focuses on deploying external deterrence when handling cases of information system misuse. Even though the non-punishment approach does not refer to any theoretical foundation, it focuses on influencing users to modify their behaviors (Siponen, 2000).

Researchers have referrred to several theories in their quest to determine the factors that encourage user's to perform certain security action (Herath, & Rao, 2009). We can classify these theories into two main categories (Bulgurcu, Cavusoglu, & Benbasat, 2010): Behavioral theories (e.g. Theory of Reasoned Action/Theory of Planned Behavior (TRA/TPB), General Deterrence Theory (GDT)…) and Learning theories (e.g. Constructivism, Social cognitive theory (SCT), Social learning theory (SLT)...).

According to Siponen (2000) behavioral theories must be highly considered when researching behavioral issues. Dinev and Hu (2007) proposed the importance of applying concepts from behavioral and adoption theories when researching the field information security, especially after observing the success with which the use of adoption theories such as The Technology Acceptance Model (TAM) and the Task-Technology Fit Theory (TTF), which explained IT adoption.

Behavioral theories would help us explain, predict and eventually modify how people respond to different security activities (Siponen, 2000); this is why they will be adopted in this study.

3.1.1 Theory of Reasoned Action (TRA) & Theory of Planned Behavior (TPB)

One of the most commonly used theories is the Theory of Planned Behavior (TPB).TPB can be considered an extension of Theory of Reasoned Action (TRA) which was developed by Ajzen and Fischbein in 1967.

TPB postulates that behavioral intentions are what determines individual behavior. Behavioral intentions comprise three major elements, which are:

1. the degree of negative /positive evaluation that a person has of the behavior in question which is known as attitude (A)
2. the degree of social pressure that an individual considers to perform or not perform a certain behavior which is known as the Subjective norms (SN)
3. the perceived ease / difficulty of performing the behavior, known as Perceived behavioral control(PBC) (Davis, 1985).

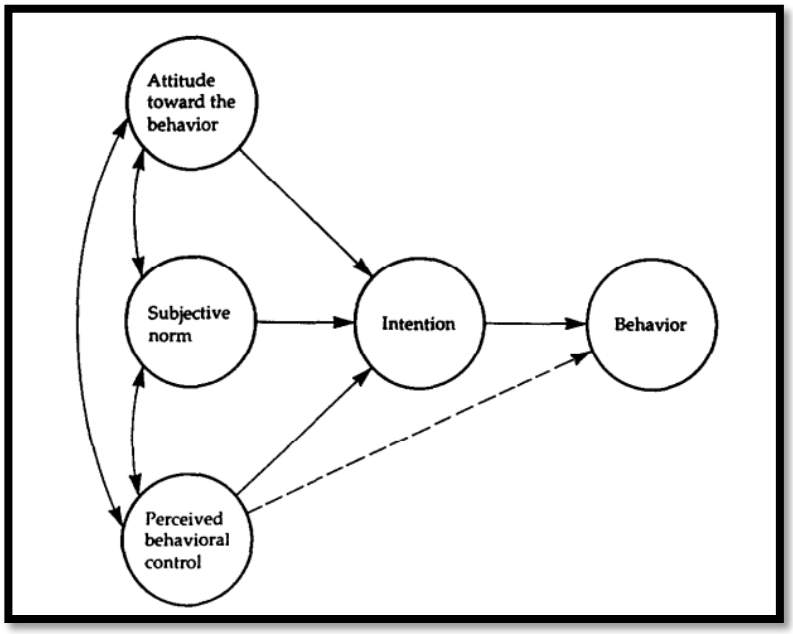

Figure 1 Theory of Planned Behavior (Source : Ajezn, 1991)

TPB has been examined by many studies that closely examined the factors that affected BI and A. Some researchers considered TPB to be a theoretical model that can be referred to, to explain ethical IT behavior (Yoon, 2011). Awareness of consequences was another factor that was found to have an impact on attitude (Guagnano, Stern, & Dietz, 1995).

In fact many factors are considered to have some effect on an individual's attitude, such as personal, legal, and business environments, society, professional, personal values, moral obligation and awareness of consequences (Leonard, Cronan, & Kreie, 2004).

Based on these findings, many organizations commit to continually assess employees' ethics, and they focus on addressing the aforementioned factors in information security. These efforts were mostly translated in terms of developing and implementing security awareness programs (Hu, Dinev, Hart, & Cooke, 2012).

3.1.2 General deterrence Theory (GDT)

The early works of philosophers such as Thomas Hobbes (1588–1678), Jeremy Bentham (1748–1832), and Cesare Beccaria (1738–1794) resulted in the existence of GDT . GDT has been the base of computer abuse studies for quite a while now (Lee, Lee, & Yoo,2004). It proposes that individuals' rational decisions are based on the rule of maximum benefit & minimum cost (Bennis, Medin, & Bartels, 2010). So as long as a person expects the benefit to be greater than the cost of punishment a person would almost always make a criminal decision (Akers, 2013; Jacobs, 2010).

For the past 15 years, researchers have relied on GDT to explain and analyze computer misuse/ abuse in employees of information system corporations. The theory examined mechanisms like systems, policies and information security awareness programs that were designed to elevate the perceived consequences of the crime. Unfortunately these mechanisms did not succeed in reducing criminal behaviors(Crossler, Johnston, Lowry, Hu, Warkentin, & Baskerville,2013; D'arcy, & Herath, 2011).

Researchers believe that this ineffectiveness was because of the following factors:

- Some organizations were enforcing inappropriate security policies in organization enforcement of inappropriate security policies in organizations
- Punishments of computer abusers were not sever enough and in many cases were minimal

- Some organizations discriminated sanctions based on the level / privilege of employees
- Few organizations actually go as far as report to the public (Knapp, Morris, Marshall, & Byrd, 2009; D'Arcy, Hovav, & Galletta, 2009).

Even though security systems are expected to prevent computer abuse effectively by reducing the vulnerability of an organization's information system and raise the level of fear of detection for computer abusers yet these systems often proved ineffective in extenuating security abuse because either organizations didn't invest enough money to develop and maintain these systems or these systems were not built in sync with organization's specific IT environments and requirements (Schneier, 2009).

Security awareness programs aimed at a conveying security knowledge to users there by reducing computer abuse by increasing perceived cost of such acts. And again some of these programs seemed useless since employees' perceived security knowledge to be restrictive, difficult to acquire, and inconvenient (Wheeler, 2011; Kirlappos, 2016).

Even though researchers were able to better understand computer abuse by using GDT yet the theoretical model didn't lead to practical success ,this is because organizations did not adequately apply it to their real environments and because the theory does not address all the factors involved in computer abuse (Herath, & Rao, 2009).

3.1.3 Protection Motivation Theory (PMT)

Rogers first introduced Protection Motivation Theory (PMT) in 1975, he initially aimed to study how health related decisions were affected by fear (Rogers, 1975). PMT

was later applied in various fields as a theoretical model intended to explain /predict users' intentions to take protective measures when a threat is perceived.

An individual's experience when faced with a threat is the base of the cognitive appraisal process that makes up PMT (Rogers ,1983).

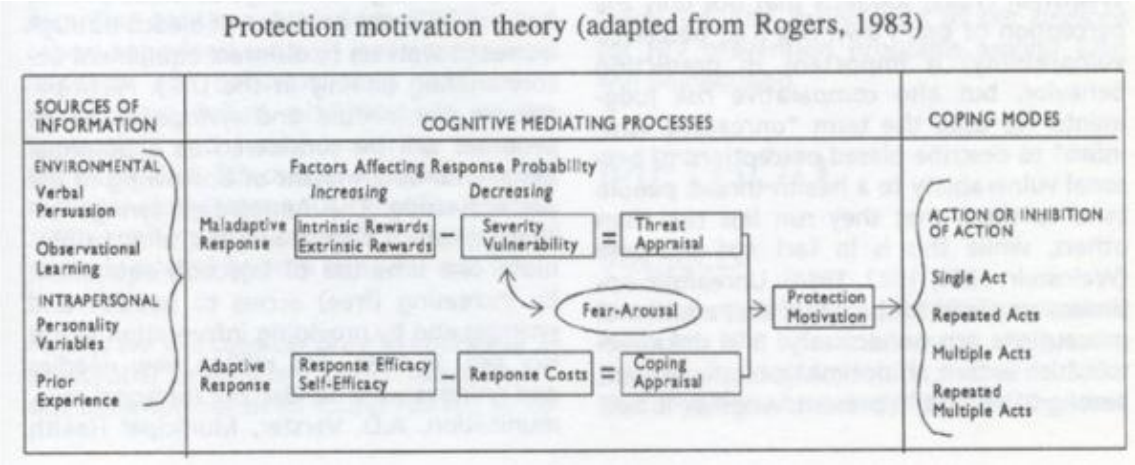

Figure 2 Protection Motivation Theory (Rogers, 1983)

The cognitive process comprises 2 aspects :

1. The first aspect is the threat appraisal process (TAP) (Floyd, Prentice-Dunn, & Rogers, 2000)

TAP assesses a maladaptive behavior . It comprises elements such as maladaptive response rewards, extrinsic , intrinsic, and the perception of threat, vulnerability and severity . where the reward factors motivate individuals to select the maladaptive behavior, and the threat factors hdiscourages indiviuals from selecting the maladaptive behavior .

2. The second aspect is coping appraisal process. (CAP)

CAP assesses the ability to cope with a threat . It comprises elements such as response efficacy, response costs , and self-efficacy. Response efficacy is a person's perception that a recommended action would protect him/her.

- Response costs are any cost the individual may incur for taking the adaptive response ,this element minimizes the probablity of an individual choosing an behave adaptively .

Self-efficacy refers to a person's perception of his/her ability to carry out the adaptive response. (Woon, Tan, & Low, 2005; Floyd, Prentice-Dunn, & Rogers, 2000)

Response efficacy and self-efficacy are the two factors that positively contribute to the probability of an individual selecting to behave adaptively. Even though PMT was first developed to examine how fear reflects on health related attitudes and behaviors, the theory also reaped great empirical support. It started being used as the base theory in many studies examining information security in organizations. These studies verified the theory when many of them concluded that in order to avoid social or interpersonal risks, individuals will always choose to avoid risk (Xu, Dinev, Smith, & Hart, 2011; Witte, 1992).

3.1.4 Technology Acceptance Model (TAM)

As an attempt to explain information systems user behavior, Davis proposed the technology acceptance model as a theoretical approach to his study in 1986 (Venkatesh, & Davis, 2000).

He wanted to examine the determining factors of computer acceptance which lead to explaining and modifying information systems users' behavior (Davis, 1993).

The basic TAM comprised and tested two specific components:

- Perceived Usefulness (PU) which can be defined as the user's conviction that the use of a system will be of benefit (Venkatesh, 2000).
- Perceived Ease of Use (PEU) can be defined as the degree to which the user believes that the system in question is easy to operate with little effort (Davis, & Vekatesh, 1986).

The present study investigates whether the these theories explain variances in students intention to use IS measures, based on how useful they perceive these measures to be , and how easy to use, controlling for their perceptions of support and their age; the study focused on university students in the Lebanese universities.

3.1.5 Knowledge-Attitude-Behavior Model

It makes sense to believe that Knowledge is a prerequisite to the intentional adoption of information security practices. Many researchers examined knowledge, its types and its different levels, yet few focused on the relationship between knowledge and information security behavior (Ezingeard, & Bowen-Schrire, 2007; Crouse, & Farmer, 2016). It was found that the different types of knowledge could affect decisions we make

and the degree to which we abide by the best information security practices (Locke, & Latham,2004; Leach, 2003).

The Knowledge -Attitude -Behavior (KAB) model has been used to explain the correlation between knowledge as it accumulates , the change in attitude and the change in behavior, to explain this relationship we can state that as knowledge accumulates , it starts to affect attitude or motivation and as motivation accumulates ,it becomes the motivational driving force that steers behavior (Schrader, & Lawless, 2004; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014)Attitude can be considered a simple set of beliefs about a certain behavioral mechanism. (Dinev, Albano, Xu, D'Atri, & Hart, 2016).

Thus, the main resource in the KAB model seems to be the accumulation of knowledge, and even though the KAB model has been around for quite a while, researchers have not specified the means by which behavioral change occurs in the model (Baranowski, Cullen, Nicklas, Thompson, & Baranowski, 2003).

The most recognized factor for nurturing change through this model is the provision of information or raising awareness through curricula or special programs (Schrader, & Lawless, 2004; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

In many cases, researchers applied the KAB model to modify or eradicate behavioral issues by assessing user knowledge in specific, recording deficits, and tailoring programs to address the gaps identified, but no further attention is given to the process through which the behavior or practices are changing. Thus, the knowledge component of the KAB model is not strongly supported maybe because the concept of knowledge is not well specified (Khan, Alghathbar, Nabi, & Khan, 2011).

Researchers in the field of information security found that people who exhibit self-control and perceive information security practices/behaviour as beneficial are able to change their practices/behaviour to comply with pre-set information security policies.

This means that knowledge can change behavior in the right kind of people, it does not work for everyone (Siponen, Pahnila, & Mahmood, 2007). If knowledge was found to be the key driver of behavioral change then changing knowledge must be made on the basis of clear specified objectives (Haas, 1990). According to a study by Safa et al (2016), knowledge is highly correlated with attitude in the field of information security practices. The theory of planned behavior also proposed that a user's intention to perform a behavior is highly correlated to their attitude toward the behavior.

Based on the above the proposed the researcher hypothesized the following:

H1: *There is a relationship between Knowledge and Attitude*

H2: There is a relationship between Attitude and Information security behavior

The term Knowledge in this study refers to general knowledge of basic IS practices. According to Frank, Shamir, & Briggs (1991) there exists a positive relationship between knowledge, Information Security awareness and Information Security Behaviors (Dinev, & Hu, 2007). This was also confirmed in a study by Gaston (1996.) states that Information technology staff in an organization has more Knowledge in the field of information security than employees in other departments and consequently exhibit higher level of IS awareness (Gavin ,1998). Based on the above the researcher hypothesized the following:

H3: *There is a relationship between the Knowledge and Information security awareness.*

A user's attitude towards information security practices is affected by two cognitive appraisals: threat and coping appraisal (Johnston, & Warkentin, 2010). Threat

Appraisal comprises two items: perceived severity, perceived vulnerability and threat perception (Lee, Larose, & Rifon, 2008). Threat perception can be determined by and perceived behavior control, response costs, response efficacy which refers to the user's ability to cope with potential threat (Tu, & Yuan,2012). A user who has been made aware of information security issues through IS training forms attitudes n towards perceptions of these threats to security and the coping response (Vance, Siponen, & Pahnila, 2012) and this would definitely translate into information security behavior (Miller, 1998). Based on the above the researcher hypothesized the following:

H4: There is a relationship between Information Security Training and Attitude

H5: There is a relationship between Information Security Training and Information Security Awareness.

H6: There is a relationship between Information Security Awareness and Information security behavior

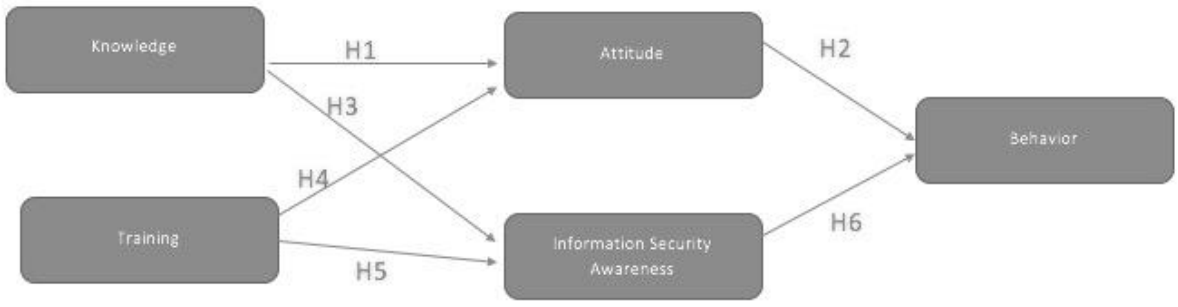

Figure 3 The Conceptual Model: Information Security Awareness

Chapter 4

Methodology

4.1 Design and Methodology

This chapter explains the methodology implemented to address the research questions and pave the way for examining the hypotheses of this study. It also provides an overview of the process that will be used for data collection and the methods that will be implemented to collect information from various groups participating in the study.

This research aims to find answers to the research questions mentioned before and the sub questions that may arise in order to validate my thesis and show the need for improving the level of security awareness among internet users, in general, and students in particular, in order to ensure their compliance with good information security practices.

4.2 Research methodology

Quantitative and qualitative research methods are two most commonly used methodologies in academic research. Qualitative research can be defined as a positioned activity that aims to detect the observer in the world. It makes the world visible by applying a set of interpretive, material practices. Qualitative research is more focused on seeking insights rather than statistical perceptions of the world (Mason, 2017; Harwell, 2011).

Quantitative research on the other hand, involves collecting data and examining the connection between the different components of the data. This methodology

implements techniques that are most likely to produce quantifiable measurable, and generalizable conclusions (Bernard, Wutich, & Ryan, 2016; Denzin, & Lincoln, 2000).

Since this study aims to gain insight on the level of information security awareness levels of Lebanese students in Universities in order to identify their level of IS awareness, the different factors affecting their IS awareness and the areas that need improvement, it is thus, an exploratory study.

Exploratory research comprises a combination of primary research methods and secondary research methods such as literature review. In our case, a survey that helped obtain the needed quantitative data was developed and administered (Sekaran, & Bougie, 2016). Therefore, this study requires the quantitative methodology to be adopted and literature review was performed to gain insight into the topic of information security awareness.

4.3 Sample

One of the most important steps in the research process is sampling. It requires careful consideration of time, and the resources available, keeping in mind that a sample has to be representative and generalizable at the same time.Thus, the outcome depends on the sampling method the researcher plans to use, whether it is probability or non-probability sampling.

Probability sampling is a method usually adopted to minimize researcher's bias and is usually generalizable. Non-probability sampling, on the other hand, is every other method that does not follow the guidelines provided by probability samples (Bryman & Bell, 2015). The sampling method that has been chosen for this study is non-probability

sampling method which is usually used when the sampling frame is not completely known and resources are limited. More specifically, the sampling method used was the convenience sampling where personal connections and acquaintances were used to spread the word about the survey link. The survey was mostly announced to students of AUB, BAU and LAU.

In this research, the factors that have had a major focus are the differences in the level of information security awareness of students in their university. It is believed that the level of IS awareness and information security practices will vary across different universities and may therefore to some extent be generalizable.

4.4 Sample Size

It is not straightforward to decide on the size of a sample, because this decision depends on various considerations and may not have a definite answer.The two factors that mostly affect the decision of the sample size are time and money. That's why researchers usually compromise the size of the sample for these two factors. This study's sample size was mainly affected by the limitations of time and money. The target sample size that was set by the research based on the time and money available was 400 respondents, which seemed to be an acceptable target with the time available. The survey managed to generate 139 responses and therefore the target sample size was reached less a small margin. This enabled the researchers to generate grounded relationships and findings.

Due to the choices of sampling methods in this study it is impossible to guarantee a heterogeneous sample because of the lack of a sampling frame. A response rate is the

percentage of the sample frame that actually ends up participating in the data collection. Due to the lack of a sampling frame, this research will have no possibility on reporting the response rate, and will therefor only report the total number of respondents that have participated.

4.5 Questionnaire

The questionnaire is the primary source of data, which will be analyzed and examined to draw the final conclusions and results. The researcher chose the information oriented selection to be used for this research and this is because the study must maximize utilization of information from small samples. Since information security is essential for all students, Responses from students enrolled in different Lebanese universities are included as a part of this study and students from all majors were selected in the study sample.

Kruger, Drevin, & Steyn (2010) and Kruger, & Kearney (2006), all prominent researchers in the the topic of information security awareness, confirmed the importance of using questionnaires when gauging information security awareness since it proved to be very beneficial and practical in this area , thus a questionnaire was used for this exploratory study .

4.6 Data Collection

Google Forms was used to create and deploy the questionnaire since it's a secure platform and it can store a large number of responses. After the data collection, the

responses can be exported into a statistical format like: Microsoft Excel. Google forms can be used to generate different types of questions for example multiple-choice, text boxes, it also has support for selectively display questions based on responses from previous questions. Google forms is widely used by many researchers. The link to the online questionnaire was distributed to all students of LAU via the internal email system. The email invited all employees to voluntarily take part in the research. Further, the invitation included a message that stated clearly that the responses to the survey will remain strictly anonymous and that no individuals can possibly be identified in the collected data. The purpose and details of the research was clearly stated in the email.

4.7 Questionnaire Design

The questionnaire was designed according to a study conducted by Kruger, Drevin & Steyn (2010). The questionnaire comprising six sections and totaling to seventy-two questions, was developed to assess the levels of information security awareness and the information security practices of university students in relation to various aspects of information security. On average, respondents need 10 minutes to complete the questionnaire and the resulting collected data is immediately available on excel for download.

The fact that the survey was administered online presented the researcher with some limitations, for example, an online questionnaire may be viewed by potential respondents as spam and thereby has a high chance of being disregarded. With the purpose of the study in mind , the questionnaire was built to include 4 areas to examine:

1. respondent’s demographic attributes;

2. respondent's information security awareness which comprises respondent's knowledge of common information security concepts, respondent's attitude towards information security threats, respondent's behavioral tendencies with respect to information security threats, and the confidentiality , integrity and availability in place in the institution under study;

3. respondent's awareness of the university's information security and password policies' existence and of some information security terminology; and

4. respondent's level of trust and perceived threat which may relate to the possibility of the respondent's being exposed to information security incidents or breaches in the past.

The ensuing sections will provide an overview of the questionnaire design and the questionnaire can be found in Appendix.

Section 1 – The first section of the questionnaire consists of 6 questions aiming to identify each respondent's demographic groups according to age, gender, current status, years of work experience, university of choice, major.

Section 2 – This section is designed to evaluate respondents' information security awareness, it consists of 31 items. Instrument contained five point Likert-scale to measure for knowledge, attitude, behavior, confidentiality, integrity and availability attributes. The scale refers to 1 as strongly disagree to 5 as strongly agree. This tool was used and validated in a study by Kaur, & Mustafa (2013).

Section 3- This section aims to examine the current information security practice of respondents at their universities. The section also queried about the type of information security training that they have attended and the learning methods that they have been exposed to. Respondents were also asked if they were aware of a list of security threats

terms. The list of terms also included a couple of fake terms –Whooping, Phlopping – this would make it possible to identify arbitrary responses.

This tool was used and validated by Talib, Clarke & Furnell (2010).

Section 4- This section aimed to examine respondents' trust and perceived threats. Instrument contained five point Likert-scale to measure for the level of the respondent's perceived threat and degree of trust. The Likert scale was used with 1 indicating strongly disagree to 5 indicating strongly agree. This section draws from a study by Slusky, & Partow-Navid (2012).

4.8 Data Analysis

The study used SPSS, a statistical package, to apply some simple statistical techniques like:

- Descriptive statistics (frequencies, percentages…)
- Reliability Testing and Factor analysis for the main parts of the questionnaire: Knowledge, Attitude, Behavior, Information Security training, and Information Security Awareness.

Since the sample size is considerably small and the study aims to predict outcomes the researcher chose to use Smart PLS3 for Structural Equations Modeling (SEM).

Chapter 5

Findings

In chapter 3, the main hypothesis were stated as follows:

H1: *There is a relationship between Knowledge and Attitude*

H2: There is a relationship between Attitude and Information security behavior

H3: *There is a relationship between the Knowledge and Information security awareness.*

H4: There is a relationship between Information Security Training and Attitude

H5: There is a relationship between Information Security Training and Information Security Awareness.

H6: There is a relationship between Information Security Awareness and Information security behavior

This chapter is meant to discuss the statistical results of the questionnaire and it includes the following sections: Demographics, reliability tests, factor analysis and the structural model to address these hypotheses and answer the research questions.

5.1 Demographics

Table 1 Demographics

Gender	**Age**
Female: 56.8% Male: 43.2 %	19 to 22: 64.7% 23 to 30: 28.8% Above 30 : 6.5%
Occupation	**Work Experience**
Undergraduate :61.2% Postgraduate:20.9% Employed: 18%	0 to 3 years: 49.6% 3 to 5 years:30.9% More than 5 years: 9.4%

As observed in the Table 1 listed above, the sample comprised 139 participants, with 56.8% females and 43.2 % of males. Since the survey targeted university students, both graduate and undergraduate, it was reasonable to find that 64.7% of participants were between the age of 19 and 22. 28.8% were between the age of 23 and 30 and only 9% were above 30. Consequently we have the majority of the participants 61.2% are undergraduate students and 20.9% are postgraduate students leaving only 18 % of students who actually concluded their studies and are working .

5.2 The Measurement Model

A reliability analysis was conducted for the major components of this study. The reliability results are shown below in Table 2. The results show a Cronbach's alpha value

of 0.780 for the five items of Knowledge, 0.81 for the five items of Attitude, 0.762 for the six items of Behavior, 0.895 for the two components of Training and 0.805 for the seven components of Information Security Awareness. From these results, we can conclude that the construct measured by this questionnaire have high reliability and they are all above 0.7 (Nunnally, 1978).

Table 2 Reliability Analysis

Reliability Statistics		
Component	Cronbach's Alpha	N of Items
Knowledge	.780	5
Attitude	.810	5
Behavior	.762	6
Information Security Training	.895	2
Information Security Awareness	.805	7

5.3 Score

According to Thompson (2004) a factor analysis can usually be used to test the fitness of the obtained model. It can be used to test the measurement model that assumes that each item is only loaded on its expected latent variable (Thompson 2004). A principal component analysis and factor analysis was conducted with verimax rotation. The factor analysis resulted in 1 score for Knowledge, 1 score for Attitude, 1 score for Information security training and 1 score for Information Security Awareness. However, the factor

analysis provided 2 scores for Behavior: General Information security behavior and email related information security behavior.

5.4 Factor Analysis

A factor analysis was conducted on the 5 major components of the questionnaire: Knowledge, Attitude, Behavior, Information Security Training, and Information Security Awareness.

5.4.1 Factor Analysis for Knowledge

The factor analysis for the Knowledge component of the questionnaire resulted in 1 factor. According to the component matrix shown below in Table 3, all items loaded highly well above the minimum threshold of 0.5 (Costello et al, 2005)

Table 3 Component Matrix: Knowledge

Component Matrix[a]	
	Component
	1
knowledge1	.818
knowledge2	.837
knowledge3	.874
knowledge4	.577
knowledge5	.545

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

5.4.2 Factor Analysis for Attitude

The factor analysis for the Attitude component of the questionnaire resulted in 1 factor. According to the component matrix shown below in Table 4, all items loaded highly well above the minimum threshold of 0.5.

Table 4 Component Matrix: Attitude

Component Matrix[a]	
	Component 1
Atittude1	.639
Atittude2	.811
Atittude3	.805
Atittude4	.768
Atittude5	.735
a. 1 components extracted.	

5.4.3 Factor Analysis for Behavior

Table 5 Component Matrix: Behavior

Component Matrix[a]		
	Component	
	1	2
Behavior1	.589	.466
Behavior2	.606	.470
Behavior3	.728	
Behavior4	.753	
Behavior5	.689	-.502
Behavior6	.686	-.477

Extraction Method: Principal Component Analysis.

a. 2 components extracted.

As seen in Table 5 the items which are related to Behavior resulted in 2 components based on the principal component analysis extraction method. The rotation matrix based on Varimax with Kaiser Normalization is shown in Table 6.

Table 6 Rotated Component Matrix : Behavior

Rotated Component Matrix[a]		
	Component	
	1	2
Behavior1		.743
Behavior2		.758
Behavior3		.744
Behavior4	.665	
Behavior5	.845	
Behavior6	.826	

Extraction Method: Principal Component Analysis.

Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in 3 iterations.

These results show that the two factors account for 72.6% of the variance. Moreover, the component matrix shown above reveals that all 6 items of Behavior loaded highly, above the minimum threshold of 0.6.

5.4.4 Factor Analysis for Information Security Training

Table 7 Component Matrix: IS Training

Component Matrix[a]	
	Component
	1
ISAtraining1	.952
ISAtraining2	.952
Extraction Method: Principal Component Analysis.	
a. 1 components extracted.	

The factor analysis for the Information Security Training component resulted in 1 factor. According to the component matrix shown above in Table 7, 2 items loaded highly well above the minimum threshold of 0.6.

5.4.5 Factor Analysis for Information Security Awareness

Table 8 Component Matrix: Information Security Awareness

Component Matrix[a]	
	Component 1
ISAwareness1	.783
ISAwareness2	.654
ISAwareness3	.739
ISAwareness4	.688
ISAwareness5	.674
ISAwareness6	.663
ISAwareness7	.539
Extraction Method: Principal Component Analysis.	
a. 1 components extracted.	

The factor analysis for the Information Security Awareness component resulted in 1 factor. According to the component matrix shown above in Table 8, all items loaded highly well above the minimum threshold of 0.6. Except for 1 which was 0.539, a bit close to 0.6.

In order to gauge the level of understanding that respondents had of some aspects of information security, the researcher asked some questions targeting their knowledge of terms of information security threats.

Table 9 Understanding of Information Security Threats (Real Terms)

	No	I don't Know	Yes
Virus/Worm	0%	0.7%	**99.3%**
Spam	0.7%	5%	**94.2%**
Social engineering	0%	71.2%	**28.8%**
Phishing	0.7%	44.6%	**54.7%**
Pharming	1.4%	80.6%	**18%**
Identity theft	0.7%	16.5%	**82.7%**
Key loggers	0.7%	52.5%	**46.8%**
Botnets	0%	82%	**18%**
Denial of service	0%	48.9%	**51.1%**
Packet sniffer	1.4%	72.7%	**25.9%**
Hacker	0%	2.2%	**97.8%**
Cracker	0.7%	28.8%	**70.5%**

Table 9 reflects the readings of respondent's awareness of a variety of security threats terms.

It was clear to see that, the long-standing, famous threats such as "virus", "identity theft", "spam", "hacker" and "Cracker" scored the highest percentages as being understood with percentages ranging between99.3% and 70.5%.

However, "Botnets" being a newer threat scored 18%, thus we can conclude that it is not commonly understood by university students. "Pharming", "social engineering" and "packet sniffer" scored 18%, 28.8%, and 25.9% respectively which also reflects a low understanding of the terms. Surprisingly 54.7% understood Phishing, a relatively smaller 28.8% understood Social Engineering, of which Phishing is an example of.

Table 10 Understanding of Information Security Threats - Fake Terms

	No	I don't Know	Yes
	Yes	I don't Know	No
Phlopping *	0%	89.2%	10.8%
Whooping*	0.7%	82.7%	16.5%

- Fake Terms

In order to identify respondents who might exaggerate their knowledge or provide arbitrary answers, the researcher included two fake terms "Phlopping" and

"Whooping" .As seen in Table 10, a relatively small percentage of respondents (10.8%-16.5%) thought they understood the terms. It can be a bit alarming that these terms were even acknowledged.

5.5 The Structural Model

After proposing the conceptual model and empirically testing it using survey data the researcher deployed the Partial least squares path analysis using Smart PLS 3.

Even though it is most common to analyze structural models using covariance based structural equation model technique (CB-SEM) the study deployed PLS path analysis instead because the data sample is not large enough to converge to acceptable results in CB-SEM and because PLS path analysis proved to be very powerful in studies that are explorative in nature (Shackman, 2013; Hair, Ringle, & Sarstedt, 2011); Joe , Sarstedt, Hopkins,& Kuppelwieser, 2014).

The PLS path analysis has its advantages over other methods in that it aims to maximize the explained variances of the latent variables (Henseler, & Chin, 2010). The PLS path analysis can be applied without any assumptions concerning the distribution on interval scales. As mentioned earlier, a further advantage of PLS path analysis is that the technique works in the case of relatively small sample sizes (Sarstedt, Henseler, & Ringle, 2011).

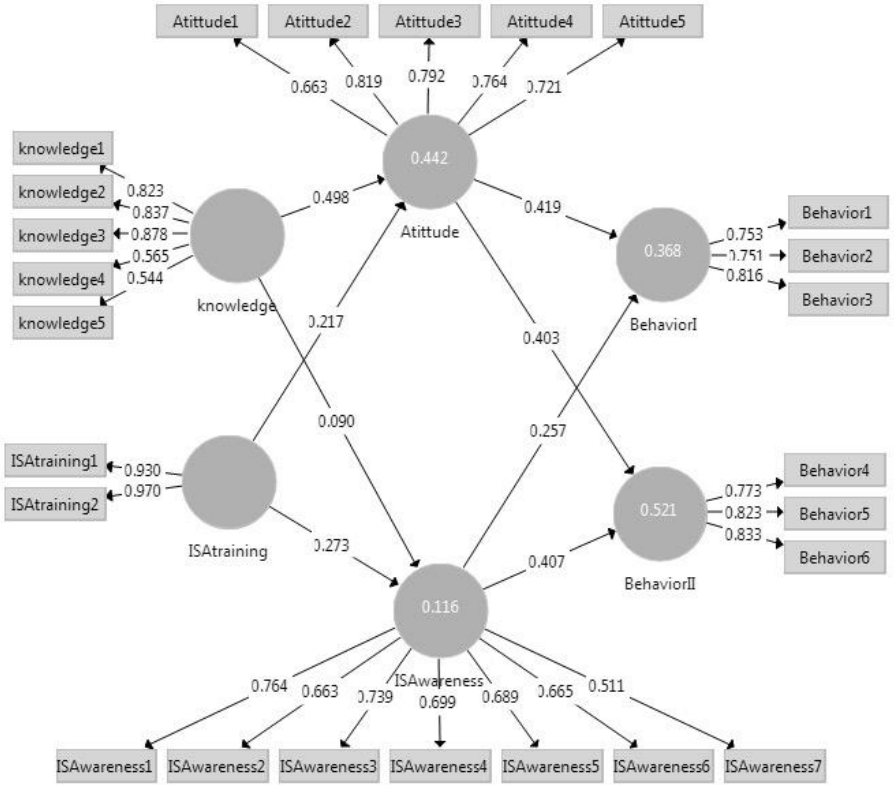

Figure 4 Structural Mode: IS Awareness

Bootstrap Method was implemented to determine the significance of the path coefficient as well as the indirect and total effect of the different components on IS Awareness and Behavior.

Further assessment of the structural model involved computing the path coefficients among knowledge, Information Security training, Attitude, Behavior I (General IS behavior), and Behavior II (Email related IS behavior) constructs. As mentioned earlier the path coefficients among these constructs were examined using bootstrapping. Figure4 depicts the results of both the inner model and bootstrapping. The path coefficients (Figure 4) showed that both Knowledge (path coefficient=0.498) and IS Training (path coefficient=0.217) had a significant positive impact on Attitude, thus

supporting H1 and H4, with Knowledge being the most important determinant of Attitude. The path coefficients (Figure 4) showed that both Knowledge (path coefficient=0.09) and IS Training (path coefficient=0.273) had a significant positive impact on IS Awareness, thus supporting H3 and H5, with IS Training being the most important determinant of IS Awareness in this case.

Moreover, Attitude had a significant direct impact on Behavior I (General IS behavior) with a path coefficient of 0.419 and Behavior II (Email related IS behavior) with a path coefficient of 0.403 thus supporting H2.

IS Awareness also had a significant impact on Behavior I (General IS behavior) with a path coefficient of 0.257 and Behavior II (Email related IS behavior) with a path coefficient of 0.407 thus supporting H6.

Moreover, the results of the path analysis support the indirect effects of Knowledge and IS Training on Behavior I (General IS behavior) and Behavior II (Email related IS behavior) through Attitude and IS Awareness. Knowledge showed the highest total (indirect) effect on Behavior I (0.498*419= 0.21) and (0.498*0.403 =0.2) on behavior II whereas IS training had a less significant total (indirect) effect on Behavior I (0.217*0.419= 0.09) and (0.273*0.407= 0.11) on Behavior II.

Table 11 Construct Reliability and Validity -PLS

	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Atittude	**0.808**	**0.867**	**0.568**
BehaviorI	**0.664**	**0.817**	**0.599**
BehaviorII	**0.738**	**0.851**	**0.656**
ISAtraining	**0.898**	**0.949**	**0.904**
ISAwareness	**0.804**	**0.856**	**0.462**
Knowledge	**0.787**	**0.856**	**0.553**

The reliability analysis results are listed above in Table 11, these results indicate that the measures are reliable as indexed by the Composite Reliability values, almost all exceeded the required minimum of 0.7. For each measure, the average variance extracted (AVE) is above the required value of 0.5 (Fornell and Larcker's, 1981). Except for Awareness it was 0.462 but it is acceptable since it is close to 0.5. Hence, more than 50% of the indicators' variance was captured by the constructs. This confirms a high level of reliability and the factors being unidimensional and reflective.

Table 12 Construct's Discriminant Validity

Furthermore, referring to Table 12, the construct's discriminant validity can be confirmed since each number in the diagonal exceeds the values in its row or column.

Table 13 Structural Model Results: Path Coefficients

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Atittude -> BehaviorI	0.419	0.421	0.102	4.100	0.000
Atittude-> BehaviorII	0.403	0.401	0.088	4.596	0.000
ISAtraining-> Atittude	0.217	0.214	0.092	2.350	0.019
ISAtraining-> ISAwareness	0.273	0.266	0.123	2.223	0.026
ISAwareness -> BehaviorI	0.257	0.256	0.094	2.725	0.006
ISAwareness -> BehaviorII	0.407	0.409	0.086	4.731	0.000
knowledge -> Atittude	0.498	0.506	0.099	5.030	0.000
knowledge -> ISAwareness	0.090	0.108	0.127	0.710	0.478

After observing Table 13 , we observe the following :

- Attitude has a positive significant influence on Behavior with a path coefficient of 0.419 on Behavior I component and 0.403 on Behavior II component with a corresponding Pvalue of 0.00 in both cases.

- Information Security Training (ISTraining) has a positive significant influence on Attitude with a path coefficient of 0.217 with a corresponding Pvalue of 0.019

- Information Security Training (ISTraining) has a positive significant influence on Information security Awareness (IS Awareness) with a path coefficient of 0.273 with a corresponding Pvalue of 0.026 .

- Information Security Awareness (IS Awareness)has a positive significant influence on Behavior with a path coefficient of 0.257 on Behavior I component and 0.407 on Behavior II component with a corresponding Pvalue of 0.006 for behavior I and 0.000 for behavior II

- Knowledge has a positive significant influence on Attitude with a path coefficient of 0.498 with a corresponding Pvalue of 0.000

- Knowledge doesn't have a significant influence on Information security Awareness it has a path coefficient of 0.090 with a corresponding Pvalue of 0.478 this indicates that there is no mediating effect of awarenes on the relationship between Knowledge and behavior.

Chapter 6

Discussion & Implications

This chapter will cover the results of the data analysis that was conducted to answer the research questions, it will outline the implications and limitations of the research and finally some suggestions and recommendations will be provided for future research.

6.1 Findings

The study was triggered by the fact that universities are considered to be easy targets to information security breaches because they are known to host vast computing power and at the same time they provide open access to the public. And since many researchers agreed that human errors are the top threats to information security, many researchers considered security education, training and awareness key factors of information security in any organization.

This study aimed to evaluate and examine user perceptions towards information security practices and the level of awareness amongst students in Lebanese universities. It employed an exploratory method by administering a survey that targeted university students on both the graduate and the undergraduate level to evaluate the level of awareness and the antecedents that contribute to this awareness. The quantitative analysis performed shed some light on the factors contributing to the levels of information security awareness of university students here in Lebanon.

First, there is no significant direct effect for the Knowledge on Behavior. In other words, Knowledge alone cannot lead to information security behaviors; it has a significant indirect effect on information security awareness through Attitude as a mediator. This of course makes sense because students who have the knowledge of information security may not have the will or the intention to maintain an information secure behavior. This is why information security trainings tend to target users' attitudes because they are just as important as knowledge ; unless users believe that maintaining the right information security behaviors is important, users are unlikely to work securely, regardless of how much knowledge they have about security requirements. Attitudes reflect the degree to which a student is disposed to act securely.

Second it was found that Knowledge and information security training both contribute to Attitude and information security awareness and this shows that we can modify students'/ employees' attitude or disposition to act safely and their level of information security awareness by employing information security training and improving the level of knowledge in the area of information security. This point aligns with the stream of Siponen (2000), D'Arcy, Hovav, & Galletta, (2009), and Sommestad, Hallberg, Lundholm, & Bengtsson, (2014).

Both Attitude and information security awareness contribute in steering information security behavior in both aspects: Email related information security behavior and General Information security behavior.

The facts that were observed supported aforementioned relationships which are:

- Knowledge → Attitude,

- Information security training → Attitude,
- Knowledge →IS Awareness ,
- IS training →IS Awareness ,
- Attitude → IS Behavior,
- IS Awareness → IS Behavior

So we found that students who have been exposed to IS training and had the knowledge in the area of information security with regards to threats and safety measures has a higher level of information security awareness and a better disposition to complying with Information security policies which we can refer to as Attitude.

And consequently students with higher levels of Information security awareness and the disposition to commit to information security behaviors are the ones who exhibit email related information security behaviors and general information security behaviors.

6.2 Implications & Recommendations

With relevance to the previously discussed points, Universities seeking to enhance their students' information security practices and behaviors are recommended to deploy several mechanisms that are capable of improving the level of Information security awareness and Information security practices and behaviors. One way of achieving these goals is to develop and implement information security awareness programs that target the areas that their students lack in. Since universities are the main players in preparing tomorrow's workforce they have to take what the market needs into consideration in their curricula. Today's workplace have an increasing demand for employees who are aware of

the ever evolving information security threats to their information security and the measures that need to be taken to protect themselves and their workplace. Universities in Lebanon need to cater for this rising need for safety and they can take several steps to achieve these goals like setting clear and well circulated Information security policies, running continuous assessment of the information security awareness of their students, providing customized information security trainings for their students would be a major leap for universities in Lebanon who are trying to achieve these goals.

Universities can also contribute by formulating programs and specializations in the field of information security to support the movement towards the information security aware culture. They can also support initiatives that raise information security awareness through seminars, competitions or trainings. The government can play a major role in achieving this objective by creating laws and regulations that can actually govern the management of various data types.

6.3 Limitations

This study evaluated university students' information security awareness and behaviors .One of the major limitations is that the sample included students from some and not all universities in Lebanon and this means that the findings do not represent the full range of university student's population in Lebanon.

The researcher faced many limitations with the sample whether in size, gender or in the affiliation of respondents. The sample size was 139 respondents which is considered small and that also was a major limitation to this study. There wasn't an equal representation of genders, this could have given us an idea of how awareness varies with

gender. The sample was unevenly distributed among universities, because the researcher sent the online survey to all LAU students, and to some friends and acquaintances who spread across other universities in Lebanon .That made it hard to observe the different measures of Information security Awareness in the population of each university. The time factor also presented a limitation to this study because with more time we could have addressed the limitations of the sample.

6.4 Future Work

This research has answered the research questions based on document analysis, and user survey results from different universities. Future research should include information on current information security breaches on the level of university students to get a complete picture of the how the occurrence of information security breaches correlates to low level of information security awareness and behavior. Future research might also look at the same issues but with a different approach. One of the approaches would be to send fake phishing emails and test students to see how they respond to breach attempts and how that relates to their current level of awareness and their information security awareness training if any.

Another approach is to explore the information security awareness of staff and faculty and to check if their level correlates to the information security awareness of their students. This would examine how information security practices are passed along from the culture of the university to students. Another possible approach would be to do a cross-university study comparing the results from the different universities and matching the findings with whether the university has an established information security policy

and if the university itself is investing in raising student information security awareness . Conducting a similar study among different organizations or industries might also highlight the differences and similarities between them.

References

Aboul Enein, S. (2016). Cooperation in addressing cyber security challenges.

Agrawal, A., & Khan, R. A. (2014). Usability Vulnerability: The Result of Disagreement between Psychology and Technology. *Computer Science and Applications*, *1*(3), 195-198.

Akers, R. L. (2013). *Criminological theories: Introduction and evaluation*. Routledge.

Al Balushi, T., Ali, S., & Rehm an, O. (2016). Economics of Cyber Security and the Way Forward. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *6*(4), 41-57.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & security*, *26*(4), 276-289.

Alfawaz, S., Nelson, K., & Mohannak, K. (2010, January). Information security culture: a behaviour compliance conceptual framework. In *Proceedings of the Eighth Australasian Conference on Information Security-Volume 105* (pp. 47-55). Australian Computer Society, Inc..

Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment in the Middle East. *Journal of Information & Knowledge Management*, *15*(01), 1650007.

Aloul, F. (2012). The need for effective information security awareness. *Journal of Advances in Information Technology*, *3*(3), 176-183.

Amoroso, E. G. (2012). *Cyber attacks: protecting national infrastructure*. Elsevier.

Anderson, R., & Fuloria, S. (2010). Security economics and critical national infrastructure. In *Economics of Information Security and Privacy* (pp. 55-66). Springer US.

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.

Aytes, K., & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing (JOEUC)*, *16*(3), 22-40.

Baranowski, T., Cullen, K. W., Nicklas, T., Thompson, D., & Baranowski, J. (2003). Are current health behavioral change models helpful in guiding prevention of weight gain efforts?. *Obesity*, *11*(S10).

Barrows, R. C., & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American Medical Informatics Association*, *3*(2), 139-148.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management*, *51*(1), 138-151.

Beavers, I., Kelley, M., & Flenner, J. (1982). Nutrition knowledge, attitudes, and food purchasing practices of parents. *Family and Consumer Sciences Research Journal*, *11*(2), 134-142.

Behl, A., & Behl, K. (2012, October). An analysis of cloud computing security issues. In *Information and Communication Technologies (WICT), 2012 World Congress on* (pp. 109-114). IEEE.

Beidleman, S. W. (2009). *Defining and deterring cyber war*. ARMY WAR COLL CARLISLE BARRACKS PA.

Bennis, W. M., Medin, D. L., & Bartels, D. M. (2010). The costs and benefits of calculation and moral rules. *Perspectives on Psychological Science*, *5*(2), 187-202.

Bernard, H. R., Wutich, A., & Ryan, G. W. (2016). *Analyzing qualitative data: Systematic approaches*. SAGE publications.

Berr, J. (2017). *"WannaCry" ransomware attack losses could reach $4 billion*. [online] Money Watch. Available at: http://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ [Accessed 27 Jul. 2017].

Böhme, R., & Nowey, T. (2008). Economic security metrics. In *Dependability metrics* (pp. 176-187). Springer Berlin Heidelberg.

Bonneil, D. & Harris, L. (2017). *Thales strengthens commitment to Middle East cybersecurity market | Zawya MENA Edition*. *Zawya.com*. Retrieved 1 March 2017, from https://www.zawya.com/story/Thales_strengthens_commitment_to_Middle_East cybersecurity_market-ZAWYA20160517082308/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information

security awareness. *MIS quarterly*, *34*(3), 523-548.

Campbell, T. (2016). Protection of Systems. In *Practical Information Security Management* (pp. 155-177). Apress.

Carr, N. G. (2003). IT doesn't matter. *Educause Review*, *38*, 24-38.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188.

Collier, R. (2014). US health information breaches up 137%.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information security technical report*, *14*(4), 186-196.

Cordesman, A. H., & Cordesman, J. G. (2002). *Cyber-threats, information warfare, and critical infrastructure protection: defending the US homeland*. Greenwood Publishing Group.

Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: designing secure systems that people can use*. " O'Reilly Media, Inc.".

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security*, *32*, 90-101.

Crouse, P., & Farmer, R. (2016). Information Security Awareness: A Course Module Using Simulated Spear-Phishing.

D Harrison McKnight, N. L. C. (2001). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International journal of electronic commerce*, *6*(2), 35-59.

D'arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643-658.

D'Arcy, J., & Hovav, A. (2007). Deterring internal information systems misuse. *Communications of the ACM*, *50*(10), 113-117.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, *20*(1), 79-98.

Davenport, T. H. (2013). *Process innovation: reengineering work through information technology*. Harvard Business Press.

Davis, F. D. (1985). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* (Doctoral dissertation, Massachusetts Institute of Technology).

Davis, F. D. (1993). User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *International journal of man-machine studies*, *38*(3), 475-487.

Davis, F. D., & Vekatesh, V. (1986). A model of the antecedents of perceived ease of use. *Decision Sciences*, *27*(3), 451-481.

Davis, F. D., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies*, *45*(1), 19-45.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science*, *35*(8), 982-1003.

Denzin, N. K., & Lincoln, Y. (2000). Qualitative research. *Thousand Oaks ua*, 413-427.

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Dillon, L. (2016). Cyberterrorism: Using the Internet as. *Combating Violent Extremism and Radicalization in the Digital Era*, 426.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems*, *8*(7), 386.

Dinev, T., Albano, V., Xu, H., D'Atri, A., & Hart, P. (2016). Individuals' Attitudes Towards Electronic Health Records: A Privacy Calculus Perspective. In *Advances in Healthcare Informatics and Analytics* (pp. 19-50). Springer International Publishing.

Edwards, K. (2015). Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users.

Egan, M. J. (2007). Anticipating future vulnerability: Defining characteristics of

increasingly critical infrastructure-like systems. *Journal of contingencies and crisis management*, *15*(1), 4-17.

Endsley, M. R. (2016). *Designing for situation awareness: An approach to user-centered design*. CRC press.

Ezingeard, J. N., & Bowen-Schrire, M. (2007). Triggers of change in information security management practices. *Journal of General Management*, *32*(4), 53-72.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), 407-429.

Franchi, E., Poggi, A., & Tomaiuolo, M. (2015). Information and password attacks on social networks: An argument for cryptography. *Journal of Information Technology Research (JITR)*, *8*(1), 25-42.

Frank, J., Shamir, B., & Briggs, W. (1991). Security-related behavior of PC users in organizations. *Information & Management*, *21*(3), 127-135.

Gaston, S. J. (1996). Information security: Strategies for successful management, Toronto: CICA Publishing.

Gavin, T. A. (1998). Information Security: Strategies for Successful Management. *Issues in Accounting Education*, *13*(3), 769.

Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. *Security Focus, December*, *18*.

Gross, M. J. (2011). A declaration of cyber-war. *Vanity Fair*, *53*(4).

Guagnano, G. A., Stern, P. C., & Dietz, T. (1995). Influences on attitude-behavior relationships: A natural experiment with curbside recycling. *Environment and behavior*, *27*(5), 699-718.

Guazzone, L. (Ed.). (2016). *The Middle East in Global Change: The Politics and Economics of Interdependence versus Fragmentation*. Springer.

Haas, E. B. (1990). *When knowledge is power: Three models of change in international organizations* (Vol. 22). Univ of California Press.

Hadnagy, C. (2010). *Social engineering: The art of human hacking*. John Wiley & Sons.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19*(2), 139-152.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer

attacks. *Computers & Security*, *24*(1), 31-43.

Harwell, M. R. (2011). ReseaRch Design in Qualitative/Quantitative. *The Sage handbook for research in education: Pursuing ideas as the keystone of exemplary inquiry*, 147.

Hedström, K., Karlsson, F., & Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security*, *21*(4), 266-287.

Henseler, J., & Chin, W. W. (2010). A comparison of approaches for the analysis of interaction effects between latent variables using partial least squares path modeling. *Structural Equation Modeling*, *17*(1), 82-109.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Huang, D. L., Rau, P. L. P., 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.

Hylén, J. (2006). Open educational resources: Opportunities and challenges. *Proceedings of Open Education*, 49-63.

ISO/IEC 27002: code of practice for information security management (2005)

Ives, B., & Olson, M. H. (1984). User involvement and MIS success: A review of research. *Management science*, *30*(5), 586-603.

Jacobs, B. A. (2010). Deterrence and deterrability. *Criminology*, *48*(2), 417-441.

Jacobson, D., & Idziorek, J. (2016). *Computer security literacy: staying safe in a digital world*. CRC Press.

Jakobsson, M. (2005, February). Modeling and preventing phishing attacks. In *Financial Cryptography* (Vol. 5).

Joe Jr, F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review*, *26*(2), 106-121.

Johnson, M. (2016). *Cyber Crime, Security and Digital Intelligence*. Routledge.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Johnston, J., Eloff, J. H., & Labuschagne, L. (2003). Security and human computer interfaces. *Computers & Security*, *22*(8), 675-684.

Jøsang, A., Ismail, R., & Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, *43*(2), 618-644.

Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International journal of information management*, *23*(2), 139-154.

Karlof, C. K., Shankar, U., Tygar, D., & Wagner, D. (2007). Locked cookies: Web authentication security against phishing, pharming, and active attacks. *University of California at Berkeley, Technical Report UCB/EECS-2007-25*.

Karlof, C., Shankar, U., Tygar, J. D., & Wagner, D. (2007, October). Dynamic pharming attacks and locked same-origin policies for web browsers. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 58-71). ACM.

Katz, F. H. (2005, September). The effect of a university information security survey on instruction methods in information security. In *Proceedings of the 2nd annual conference on Information security curriculum development* (pp. 43-48). ACM.

Kaur, J., & Mustafa, N. (2013, November). Examining the effects of knowledge, attitude and behavior on information security awareness: A case on SME. In *2013 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 286-290). IEEE.

Kerr, S. (1975). On the folly of rewarding A, while hoping for B. *Academy of Management journal*, *18*(4), 769-783.

Kessem, L. (2017). *WannaCry Ransomware Spreads Across the Globe, Makes Organizations Wanna Cry About Microsoft Vulnerability*. [online] Security Intelligence Analysis and Insight for Information Security Professionals. Available at: https://securityintelligence.com/wannacry-ransomware-spreads-

across-the-globe-makes-organizations-wanna-cry-about-microsoft-vulnerability/. [Accessed 27 Jul. 2017].

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862.

Kirlappos, I. (2016). *Learning from" shadow security": understanding non-compliant behaviours to improve information security management* (Doctoral dissertation, UCL (University College London)).

Knapp, K. J., Morris, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493-508.

Koufaris, M., & Hampton-Sosa, W. (2002). Initial perceptions of company trustworthiness online: A comprehensive model and empirical test. *Report No.# CIS-2002*, *11*.

Krausz, M., & Walker, J. (2013). *The true cost of information security breaches and cyber crime*. IT Governance Publishing.

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *computers & security*, *25*(4), 289-296.

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security*, *18*(5), 316-327.

Kvavik, R. B., & Voloudakis, J. (2003). *Information technology security: Governance, strategy, and practice in higher education*. Educause.

Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. John Wiley & Sons.

Layton, T. P. (2016). *Information Security: Design, implementation, measurement, and compliance*. CRC Press.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685-692.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685-692.

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013, January). Employees' information security awareness and behavior: A literature review. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp.

2978-2987). IEEE

Lebek, B., Uffen, J., Breitner, M. H., Neumann, M., & Hohler, B. (2013, January). Employees' information security awareness and behavior: A literature review. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 2978-2987). IEEE.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, *27*(5), 445-454.

Lee, S. M., Lee, S. G., & Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, *41*(6), 707-718.

Lehman, D. W. (2016). *Identifying the Critical Success Factors for Information Systems to Manage Sponsored Research Activities at Institutions of Higher Education*. Robert Morris University.

Leonard, L. N., Cronan, T. P., & Kreie, J. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics?. *Information & Management*, *42*(1), 143-158.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, *11*(7), 394.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *Mis Quarterly*, 173-186.

Locke, E. A., & Latham, G. P. (2004). What should we do about motivation theory? Six recommendations for the twenty-first century. *Academy of management review*, *29*(3), 388-403.

Marcella Jr, A., & Greenfield, R. S. (Eds.). (2002). *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*. CRC Press.

Marks, A., & Rezgui, Y. (2009, September). A comparative study of information security awareness in higher education based on the concept of design theorizing. In *Management and Service Science, 2009. MASS'09. International Conference on* (pp. 1-7). IEEE.

Mason, J. (2017). *Qualitative researching*. Sage.

Matbouli, H., & Gao, Q. (2012, March). An overview on web security threats and impact to e-commerce success. In *Information Technology and e-Services (ICITeS), 2012 International Conference on* (pp. 1-6). IEEE.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709-734.

McGraw, G., & Morrisett, G. (2000). Attacking malicious code: A report to the Infosec Research Council. *IEEE software*, *17*(5), 33-41.

Merete Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377-397.

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., & Giannakopoulos, G. (2014). The human factor of information security: Unintentional damage perspective. *Procedia-Social and Behavioral Sciences*, *147*, 424-428.

Miller, W.C. (1998). *Negotiated peace: How to end the war over weight.* Boston: Allyn & Bacon.

Mitnick, K. D., & Simon, W. L. (2011). *The art of deception: Controlling the human element of security*. John Wiley & Sons.

Morgan, S. (2017). Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020. Forbes.com. Retrieved 1 March 2017, from: https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#6ec4d1ed10c3

Morton, M. S. S. (1991). *The corporation of the 1990s: Information technology and organizational transformation*. Oxford University Press on Demand.

Nayak, U., & Rao, U. H. (2014). *The InfoSec Handbook: An Introduction to Information Security*. Apress.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815-825.

Nissenbaum, H. (2001). Securing trust online: Wisdom or oxymoron. *BUL Rev.*, *81*, 635.

Nunnally, J. C. (1978). *Psychometric theory*. New York: McGraw-Hill.

Parker, D. B. (2002). Toward a New Framework for Information Security?. *Computer Security Handbook, Sixth Edition*, 3-1.

Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). *Human factors and*

information security: individual, culture and security environment.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & security*, *42*, 165-176.

Pavlou, P. A. (2003). Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International journal of electronic commerce*, *7*(3), 101-134.

Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In *Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on* (pp. 693-702). IEEE.

Pérez, J., Murray, M., Fluker, J., Fluker, D., & Bailes, Z. (2017). Connectivity and Continuity: New Fronts in the Platform War. *CAIS*, *40*, 8.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638-646.

Posthumus, S., Von Solms, R., & King, M. (2010). The board and IT governance: The what, who and how. *South African Journal of Business Management*, *41*(3), 23-32.

Ramzan, Z. (2010). Phishing attacks and countermeasures. In *Handbook of information and communication security* (pp. 433-448). Springer Berlin Heidelberg.

Raskin, V., Hempelmann, C. F., Triezenberg, K. E., & Nirenburg, S. (2001, September). Ontology in information security: a useful theoretical foundation and methodological tool. In *Proceedings of the 2001 workshop on New security paradigms* (pp. 53-59). ACM.

Reeder, R. W., Karat, C. M., Karat, J., & Brodie, C. (2007, September). Usability challenges in security and privacy policy-authoring interfaces. In *IFIP Conference on Human-Computer Interaction* (pp. 141-155). Springer, Berlin, Heidelberg.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7), 241-253.

Rhee, H. S., Ryu, Y. U., & Kim, C. T. (2012). Unrealistic optimism on information security management. *computers & security*, *31*(2), 221-232.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, *38*(1-2), 4-37.

Rogers, R. W. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

Rose, K., Eldridge, S., & Chapin, L. (2015). The internet of things: An overview. *The Internet Society (ISOC)*, 1-50.

Rowley, J. (2000). Is higher education ready for kowledge management?. *International journal of educational management*, *14*(7), 325-333.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *computers & security*, *56*, 70-82.

Safa, N. S., Von Solms, R., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud & Security*, *2016*(2), 15-18.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-9.

Samaila, M. G., Neto, M., Fernandes, D. A., Freire, M. M., & Inácio, P. R. (2017). Security Challenges of the Internet of Things. In *Beyond the Internet of Things* (pp. 53-82). Springer International Publishing.

San Martino, A., & Perramon, X. (2010). Phishing Secrets: History, Effects, Countermeasures. *Ij Network Security*, *11*(3), 163-171.

Sarstedt, M., Henseler, J., & Ringle, C. M. (2011). Multigroup analysis in partial least squares (PLS) path modeling: Alternative methods and empirical results. In *Measurement and research methods in international marketing* (pp. 195-218). Emerald Group Publishing Limited.

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.

Schneider, T. R., Salovey, P., Pallonen, U., Mundorf, N., Smith, N. F., & Steward, W. T. (2001). Visual and auditory message framing effects on tobacco smoking. *Journal of Applied Social Psychology*, *31*(4), 667-682.

Schneier, B. (2001). Managed security monitoring: Network security for the 21st

century. *Computers & Security*, *20*(6), 491-503.

Schneier, B. (2009). *Schneier on security*. John Wiley & Sons.

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Schrader, P. G., & Lawless, K. A. (2004). The knowledge, attitudes, & behaviors approach how to evaluate performance and learning in complex environments. *Performance Improvement*, *43*(9), 8-15.

Schumacher, M., Fernandez-Buglioni, E., Hybertson, D., Buschmann, F., & Sommerlad, P. (2013). *Security Patterns: Integrating security and systems engineering*. John Wiley & Sons.

Scott, W. R., & Davis, G. F. (2015). *Organizations and organizing: Rational, natural and open systems perspectives*. Routledge.

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.

Shackman, J. D. (2013). The use of partial least squares path modeling and generalized structured component analysis in international business research: A literature review. *International Journal of Management*, *30*(3), 78.

Shariff, A. F., Greene, J. D., Karremans, J. C., Luguri, J. B., Clark, C. J., Schooler, J. W., ... & Vohs, K. D. (2014). Free will and punishment: A mechanistic view of human nature reduces retribution. *Psychological science*, *25*(8), 1563-1570.

Sherer, M., & Rogers, R. W. (1984). The role of vivid information in fear appeals and attitude change. *Journal of Research in Personality*, *18*(3), 321-334.

Shneiderman, B. (2005). Human-Computer Interaction Opportunities for Improving Security/Privacy.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31-41.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database*, *38*(1), 60-80.

Siponen, M., Pahnila, S., & Mahmood, A. (2007, May). Employees' adherence to information security policies: an empirical study. In *IFIP International Information Security Conference* (pp. 133-144). Springer, Boston, MA.

Siponen, M., Pahnila, S., & Mahmood, A. (2007, May). Employees' adherence to information security policies: an empirical study. In *IFIP International*

Information Security Conference (pp. 133-144). Springer, Boston, MA.

Skoudis, E., & Zeltser, L. (2004). *Malware: Fighting malicious code*. Prentice Hall Professional.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness.Journal of Information Privacy and Security, 8(4), 3-26.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: a systematic review of quantitative studies. *Information Management & Computer Security*, *22*(1), 42-75.

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215-225.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & security*, *24*(2), 124-133.

Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). Sp 800-30. risk management guide for information technology systems.

Subrahmanian, V. S., Ovelgönne, M., Dumitras, T., & Prakash, B. A. (2015). Human Behavior and Susceptibility to Cyber-Attacks. In *The Global Cyber-Vulnerability Report* (pp. 69-92). Springer International Publishing

Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of electronic commerce*, *7*(3), 135-161.

Szor, P. (2005). *The art of computer virus research and defense*. Pearson Education.

Talib, S., Clarke, N. L., & Furnell, S. M. (2010, February). An analysis of information security awareness within home and work environments. InAvailability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 196-203). IEEE.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

Telecommunications Regulatory Authority, (2017). *Cybersecurity in Lebanon*. *TRA – Telecommunications Regulatory Authority*. Retrieved 2 March 2017, from http://www.tra.gov.lb/Cybersecurity-in-Lebanon

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. *Computers &*

Security, *24*(6), 472-484.

Thomson, M. E., & von Solms, R. (1998). Information security awareness: educating your users effectively. *Information management & computer security*, *6*(4), 167-173.

Thornburgh, T. (2004, October). Social engineering: the dark art. In *Proceedings of the 1st annual conference on Information security curriculum development* (pp. 133-135). ACM.

Trevino, L. K. (1992). The social effects of punishment in organizations: A justice perspective. *Academy of Management Review*, *17*(4), 647-676.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & security*, *52*, 128-141.

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24*(1), 38-58.

Tu, Z., & Yuan, Y. (2012, January). Understanding user's behaviors in coping with security threat of mobile devices Loss and theft. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 1393-1402). IEEE.

Urban, G. L., Amyx, C., & Lorenzon, A. (2009). Online trust: state of the art, new frontiers, and research potential. *Journal of Interactive Marketing*, *23*(2), 179-190.

Van der Molen, F. (2012). *Get ready for cloud computing*. Van Haren.

Van Niekerk, J. F. (2005). *Establishing an information security culture in organizations: an outcomes based education approach*(Doctoral dissertation, Nelson Mandela Metropolitan University).

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190-198.

Vasudevan, A., & Yerraballi, R. (2006, May). Cobra: Fine-grained malware analysis using stealth localized-executions. In *Security and Privacy, 2006 IEEE Symposium on* (pp. 15-pp). IEEE.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information systems research*, *11*(4), 342-365.

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management science*, *46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.

Viega, J., & McGraw, G. R. (2001). *Building Secure Software: How to Avoid Security Problems the Right Way*, *Portable Documents*. Pearson Education.

Von Solms, B., & Von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

Wagner, D., & Disparte, D. (2016). Cyber Risk. In *Global Risk Agility and Decision Making* (pp. 199-220). Palgrave Macmillan UK.

Wallace, L. G., & Sheetz, S. D. (2014). The adoption of software measures: A technology acceptance model (TAM) perspective. *Information & Management*, *51*(2), 249-259.

Walters, R. (2014). Cyber attacks on US companies in 2014. *Heritage Foundation Issue Brief*, *4289*.

Walters, R. (2016). Cyber attacks on US companies in 2016. *Heritage Foundation Issue Brief*, 4636.

Wamala, F. (2011). ITU national cybersecurity strategy guide. *International Telecommunications Union*, *11*. (ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity)

Wang, H., Wu, S., Chen, M., & Wang, W. (2014). Security protection between users and the mobile media cloud. *IEEE Communications Magazine*, *52*(3), 73-79.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, *26*(1), 23-30.

Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer law & security review*, *26*(1), 23-30.

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the Ground Up*. Elsevier.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM*, *46*(8), 91-95.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.

Whitten, A., & Tygar, J. D. (1998). *Usability of security: A case study* (No. CMU-CS-98-155). CARNEGIE-MELLON UNIV PITTSBURGH PA DEPT OF COMPUTER SCIENCE.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, *59*(4), 329-349.

Wolmarans, A. (2003). *Implementing an effective information security awareness program* (Doctoral dissertation, University of Johannesburg).

Wood, C. C. (2004). Why information security is now multi-disciplinary, multi-departmental, and multi-organizational in nature. *Computer Fraud & Security*, *2004*(1), 16-17.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 proceedings*, 31.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662-674.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in human behavior*, *24*(6), 2799-2816.

Wu, F., Narang, H., & Clarke, D. (2014). An overview of mobile malware and solutions. *Journal of Computer and Communications*, *2*(12), 8.

Wu, X., Huang, X., Xu, R., & Yang, Q. (2013). An Experimental Method Study of User Error Classification in Human-computer Interface. *JSW*, *8*(11), 2890-2898.

Yeoh, P. (2017). The Fourth Industrial Revolution: Technological Impact and Privacy and Data Security Issues. *Business Law Review*, *38*(1), 9-13.

Yoon, C. (2011). Theory of planned behavior and ethics theory in digital piracy: An integrated model. *Journal of Business Ethics*, *100*(3), 405-417.

Zinatullin, L. (2016). *The Psychology of Information Security: Resolving conflicts between security compliance and human behaviour*. IT Governance Ltd.

Appendix I

Consent to participate in a Survey/Questionnaire

Information security Awareness Among University Students

I am Abir Sinno, I am an MBA student at LAU and I am conducting a study to investigate Information security awareness in University students in Lebanon
I would appreciate it if you can complete the following questionnaire as part of my Thesis . This questionnaire / survey aims to examine the level of information security awareness in university students and recommend ways to improve it.

The information you provide will be used to enhance and improve information security awareness in university students. Completing the survey will take 5 to 8 minutes of your time...

By continuing with the questionnaire, you agree with the following statements:

1. I have been given sufficient information about this research project.
2. I understand that my answers will not be released to anyone and my identity will remain anonymous. My name will not be written on the questionnaire nor be kept in any other records.
3. I understand that all responses I provide for this study will remain confidential. **When the results of the study are reported, I will not be identified by name or any other**

information that could be used to infer my identity. Only researchers will have access to view any data collected during this research however data cannot be linked to me.

4. I understand that I may withdraw from this research any time I wish and that I have the right to skip any question I don't want to answer.
5. I understand that my refusal to participate will not result in any penalty or loss of benefits to which I otherwise am entitled to.
6. I have been informed that the research abides by all commonly acknowledged ethical codes and that the research project has been reviewed and approved by the Institutional Review Board at the Lebanese American University
7. I understand that if I have any additional questions, I can ask the research team listed below.
8. I have read and understood all statements on this form.
9. I voluntarily agree to take part in this research project by completing the following survey.

If you have any questions, you may contact:

Name (PI)	Phone number	Email address
Abir Sinno	03082407	Abir.sinno01@lau.edu

If you have any questions about your rights as a participant in this study, or you want to talk to someone outside the research, please contact the:

IRB Office,

Lebanese American University

3rd Floor, Dorm A, Byblos Campus

Tel: 00 961 1 786456 ext. (2546)

Information security Awareness among University Students

Questionnaire

Section 1 Demographics	
1. Gender : Female Male	2. I am Currently a : Undergraduate Student Postgraduate Student Employee
3. Age : 19 to 22 23 to 30 Above 30	4. Years of Work Experience if any: 1 to 3 years 3 to 5 years More than 5 years
5- What is your undergraduate major?	6. I studied my undergraduate degree at : AUB LAU BAU Other _____

The below questions are answered through a 5 Likert scale ranging from strongly

agree to strongly disagree

SA-Strongly Agree A-Agree N-Neutral DA-Disagree SDA-Strongly Disagree

Section 2: The Knowledge Attitude Behavior Model (KAB)					
	SA	**A**	**N**	**DA**	**SDA**
Knowledge					
I have the necessary knowledge to handle information security in my working situation.					
I know what information security is.					
I know what an information security incident is.					
. Internet access on the university's system is an academic resource and should be used for academic purposes only.					
. Phishing e-mail is the act of stealing users' sensitive and personal information.					
Attitude					
. My practice in handling sensitive information is appropriate and effective.					
. My practice in exercising care when opening a suspicious email is a wise move.					

. In my view, using a password protected computer is a crucial thing to do.					
. The thought of using an antivirus program is appealing to me.					
. Using the Firewall system at work is an important thing to do.					
	SA	**A**	**N**	**DA**	**SDA**
Behavior					
. I am aware that I should never give my password to somebody else					
. I do not open email attachments if the content of the email looks suspicious.					
. Before reading an email, I ~~will~~ first check if the subject and the sender make sense.					
. I never give my personal information (like home/email address, telephone number, etc.) to unknown websites.					
. I never download files (like documents, music, picture, software, etc.) from the Internet if the files are from unknown people.					
. I pay attention to anti-virus updates every time I use a computer.					

Section 3 Information Security CIA Triad					
Confidentiality					
. My university has well implemented security practices to protect important information from getting stolen by malicious intrusions (such as break-in, Trojans, and spy-wares).					
. Unauthorized personnel are prohibited from accessing university's information resources.					
. Information security measures are implemented in your university to prevent sensitive information from unauthorized disclosure.					
. Logging all access attempts of confidential files is mandatory.					
. Physical access control is always no.1 priority.					
Integrity					
. The database is periodically reconciled and regularly maintained in order to increase the accuracy and reliability of information.					
. When acquiring important information from the information sources, the information will be stored into the company's database.					
. Your university has security controls (such as change management procedures) in place to prevent					

unauthorized information changes (creation, alternation, and deletion).					
. Information should be protected or secured from unauthorized use.					
. The privacy of employees and students should be protected.					
. Integrity of the information on systems must be maintained.					
Availability					
. The probability of information system breakdown and information service disruption in my university is low.					
. A legitimate user with academic needs can access university information at any time and at any place.					
. The university should have redundancy in hardware to tolerate hardware failure.					
. All servers should be continuously available to their clients.					

Section 4 IS Awareness at my University

. Who is responsible for information security at your University? (Select all which apply) IT Services Deputy Registrar's Office Departments that use data Managers and Team Leaders Individual Employees	. I have read and understood the university's Information Security Policy and Regulation Governing Use of Computing Facilities * yes, I have No, I have not I am not aware that the university has an information security policy		
. I have received Information Security awareness training at the my university yes, I have No, I have not If yes was the training a: Classroom training Discussion-based training Web-based training Other_____	. I have received Data Protection awareness training at the University yes, I have No, I have not		
Technical knowledge			
Insert a	Yes	No	I Don't

			Know
. Have you ever found a virus or a Trojan on your computer?			
. Do you how to tell if your computer is hacked or infected?			
. Is the firewall on your computer enabled?			
. Is your computer configured to be automatically updated?			
. Is an anti-virus currently installed, updated and enabled on your computer?			
. Can you use your own personal devices, such as your mobile phone, to store or transfer confidential information?			
. If you format a hard drive or erase the files on it will you lose the information permanently?			
Do you understand the following term?	**Insert a**		
	I Understand It	**I Never Heard Of It**	
. Virus/Worm			

. Spam		
. Social engineering		
. Phishing		
. Pharming		
. Identity theft		
. Key loggers		
. Phlopping		
. Botnets		
. Denial of service		
. Packet sniffer		
. Hacker		
. Cracker		
. Whooping		

Trust /Perceived Threat

	SA	**A**	**N**	**DA**	**SDA**
. I feel that my computer is secure					
. My computer has no value to hackers, they do not target me.					
. I am careful when I open an attachment in an email					
. Online social networks that I use provide all necessary protection of my personal data					
. If my online account is protected then it is safe to use it from public computers (work, campus, WiFi zone)					

. Online social networks will purge data in my account after a few years of inactivity					
. I can give up some privacy of my personal data for increased convenience of public Web access					
. I am at risk that my laptop or flash drive with my data files can be lost or stolen on campus					
. Same passwords for several online accounts is safe					
. Sharing passwords with trusted college friends is safe					