9-5-2016

Cybercrime and Facebook: An Examination of Lifestyle Routine Activity Theory

Kristina E. Morales

CYERCRIME AND FACEBOOK: AN EXAMINATION OF LIFESTYLE-ROUTINE ACTIVITY THEORY

A Thesis

by

KRISTINA EDITH MORALES

Submitted to Texas A&M International University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

December 2016

Major Subject: Criminal Justice

Cybercrime and Facebook: An Examination of Lifestyle-Routine Activity Theory

CYBERCRIME AND FACEBOOK: AN EXAMINATION OF LIFESTYLE-ROUTINE ACTIVITY THEORY

A Thesis

by

KRISTINA EDITH MORALES

Submitted to Texas A&M International University
in partial fulfillment of the requirements
for the degree of

MASTER OF SCIENCE

Approved as to style and content by:

Chair of Committee,	Dr. Claudia San Miguel
Committee Members,	Dr. Marcus Ynalvez
	Dr. Thomas Zawisza
	Dr. Kate Houston
Head of Department,	Dr. John Kilburn

December 2016

Major Subject: Criminal Justice

DEDICATION

I dedicate this thesis to my loved ones for always supporting me and encouraging me to do better.

ABSTRACT

Cybercrime and Facebook: An Examination of Lifestyle-Routine Activity Theory
(December 2016)

Master of Science in Criminal Justice, Texas A&M International University, 2016;

Chair of Committee: Dr. Claudia San Miguel

The purpose of this study is to determine if Facebook® utilization impacts online victimization experience, and if prevention measures moderate such impact. This study primarily focuses on Facebook® users due to this social media outlet being considered the most prominent online networking site today (Milanovic, 2015). It will focus on an understudied population—Hispanic college students. Additionally, this study argues that lifestyle-routine activity theory is appropriate in the attempt of explaining cybercrime. Overall, this study will explain and define: online victimization, types of cybercrimes, prevention measures, Facebook® utilization, Hispanic and college student statistics, and studies on the application of lifestyle-routine activity theory in the explanation of cybercrime victimization.

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Dr. Claudia San Miguel, and my committee members, Dr. Ynalvez, Dr. Houston, and Dr. Zawisza, for their guidance and support throughout the course of this research.

Thanks also, to my friends and colleagues and the faculty and staff of the Department of Social Sciences and the University Police Department for making my time at Texas A&M International University a great experience.

Finally, I want to thank my mother, father, brothers, sister, sister-in-law, grandparents, aunts, uncles, and my partner's family for their encouragement and support throughout my journey. I would also like to thank my partner for her patience, love, and support during the process of obtaining a master's degree. I do not know what I would have done without the love and support of my family. Thank you.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

In our modern society, the use of social media is rapidly taking the place of regular person-to-person communication (Keller, 2013). The burgeoning use of social media has created distinct implications for the criminal justice system, such as the corruption of evidence by the general public, and ensuring the right to a fair trial (Milivojevic & McGovern, 2014). Although various leading and contemporary criminological theories can be used to explain crime, the habitual use of social media has led to new forms of criminal activity and victimization (Federal Bureau of Investigations, 2014) which do not fit nearly into traditional criminological theory. Therefore, in order to cope with the new domain of cybercrime, traditional theories may require broadening or re-envisioning. As the Internet has become an important facet of everyday life, particularly for social interactions and means of communication, many individuals have fallen victims to cybercrime on social media sites (Federal Bureau of Investigations, 2014; Reyns, Henson, & Fisher, 2011). Peer-to-peer networks, such as Facebook®, Twitter, and Instagram, are examples of social media sites and are often abused by online motivated offenders who engage in a variety of cybercrimes (Federal Bureau of Investigations, 2014). In 2014 alone, the Federal Bureau of Investigations (hereafter FBI) concluded that 9,833 individuals were victims of cybercrimes on social media outlets.

Victimization is defined as a person is suffering or has experienced physical, emotional, mental, or financial harm committed by another. Victimization is often related to actions or inactions taken by users of social media sites. Most often, inactions are associated

---

This thesis follows the style of *Adult Education Quarterly*.

with privacy or security settings and/or the oversharing of information which create prime opportunities for motivated offenders. For instance, Facebook®, which is the most commonly used social media site with a worldwide average of 1.01 billion active users a day (Milanovic, 2015), offers users two privacy/security options. Users may either set their profiles to public or private; a public profile means that others can view all of the information posted on the user's profile (Henson, Reyns, & Fisher, 2011). Users who want a more private profile may pick and choose the information they would like to share with people who are considered to be their "friends" on the networking site (Henson et al., 2011). Furthermore, the security feature known as "user control", affords users the ability to accept or decline a friend request(s) to be associated with another user's profile page (Henson et al., 2011). The precautions and/or prevention measures, or a distinct lack thereof, in an online environment may create ample opportunities for cybercriminals. In essence, an individual's cyber lifestyle and online routines may increase the likelihood of victimization.

Research on victimization in cyberspace is still in its infancy, and the majority of available studies have been: (1) exploratory in nature, (2) focused on adolescent samples, and (3) generally limited to analyzing the sole cybercrime of—bullying due to its prevalence in cyberspace (Gilkerson, 2012). Additionally, little empirical attention has been devoted to the correlation between a user's Facebook® utilization (i.e., victimization prevention measures) and victimization (Henson et al., 2011). A user's privacy/security settings are critical factors to analyze since they may create opportunities for motivated offenders. More importantly, this study will advance research by focusing on an understudied population—Hispanic college students. Although there are a number of studies on Hispanic victimization that are unrelated to cyber activity (see FBI, 2014; Sugarmann, 2014; FBI Law Enforcement Bulletin,

2015), little is known about the prevalence of cybercrimes committed on Hispanic college students. Therefore, this research serves to address this gap in the literature on victimization of Hispanics.

While cyber victimization can occur on any social media site such as Twitter and Instagram, this study will focus its attention on Facebook® because it is the most commonly used social media site worldwide (Milanovic, 2015). The core hypothesis of this study is that Facebook® utilization (measured as online activity and/or number of hours spent online) will impact online victimization but, such experience will be moderated by the type of prevention measure used (e.g., the number of mutual friends and the recognition of friend requests, and the degree of user control pertaining to what type of information they allow to be public or private). Thus, victimization experience will be the dependent variable and Facebook® utilization, personal characteristics, and prevention measures will be independent variables. This study will then be able to determine if personal characteristics, prevention measures, and Facebook® utilization are significant in determining victimization experience.

This study will further advance the application of a theoretical framework by analyzing two theories—routine activity theory and lifestyle theory. When considering criminological theoretical perspectives, Cohen and Felson's routine activity theory (1979) has been used in an attempt to explain cybercrime (Reyns et al., 2011). Routine activity theory accounts for how opportunities of criminal victimization are produced or increased by analyzing and examining an individual's behavior and routines of everyday life (Reyns et al., 2011). Additionally, even though space and time are requirements for criminal victimization to occur in a physical environment, when considering routine activity theory, such elements may not be applicable to online victimization (Reyns et al., 2011). According to Reyns et al.

(2011), the latter elements of the theory may not apply because individuals do not physically come into contact with the offender. However, in an online setting, space and time may arise as factors, when the potential victim and the offender connect in some form using an Internet connection (Reyns et al., 2011). For instance, an offender and a victim can be roaming a chat room, the same shopping website, or on the same social media site (Gordon & Ford, 2006). Therefore, there may be convincing arguments for the application of routine activity theory to the explanation of victimization in an online environment (Reyns et al., 2011) and this study will explore such applications.

Lifestyle theory, is considered to be a personal victimization theory first developed by Michael Hindelang, Michael Gottfredson, and James Garafalo in 1979 (Jenson & Brownfield, 1986). Lifestyle theory first posits that an individual's patterns and daily activities play a major role in the likelihood of increasing or decreasing chances of victimization (Myrstol & Chermak, 2005). Hindelang, Gottfredson, and Garafalo (as cited in Jenson & Brownfield, 1986) indicate that the degree, extent, and/or severity of victimization depends on their exposure to motivated offenders and guardianship in accordance to their lifestyle(s). Because routine activity theory and lifestyle theory are intertwined in the explanation of how victimization occurs as a result of an individual's routines or lifestyles, both theories will be combined into lifestyle-routine activity theory which we will refer to as LRAT for the purpose of this study. Combining these theories has been reported in previous research of cybercrime and online victimization (see Holt & Bossler, 2009; Reyns, Henson, & Fisher, 2011; Yar, 2005; Taylor et al., 2006; Choi, 2008; Bossler & Holt, 2009; Ngo & Patermaster, 2011).

Summary

In sum, this study aims to provide an overall understanding of cybercrimes, specifically in relation to: (1) types of cybercrimes committed against college students, (2) different precautions or actions taken by students in a cyber-environment, and (3) the user's adoption of security settings on social networking sites in pertinence to the number of mutual friends, recognition of the individuals who send friend requests, and the degree of user control. Most importantly, this study will explore these factors with a Hispanic student population—an understudied population in relation to cyber victimization.

This research study is important to the criminal justice system because it acknowledges the prevalence of cybercrimes occurring on social networking sites. The study will explore the pervasiveness of crimes occurring online as the result of lifestyle choices and routines taken in cyberspace. The study will also identify types of cybercrimes being committed amongst the Hispanic college student population. Moreover, this study advances research in the criminal justice field by providing an overall understanding of cybercrimes, analyzing how prevention measures differ in an online environment, and by adopting an analytical approach where LRAT is incorporated in explaining cybercrime victimization. Additionally, when referring to cybercrime victimization throughout this proposal, such term will be used to define the different types of cybercrimes that will be studied (e.g. hacking, online-romance scams/catfish, cyber-impersonation, online/internet fraud, and identity theft). The reason for this clarification is due to a majority of literature focusing on the form of cyberbullying victimization and online victimization is broader than pure cyberbullying victimization.

The following chapters of this thesis will discuss and analyze cybercrime and online victimization on social networking sites, particularly on Facebook®. Additionally, the sections will present and discuss the issue of risk pre-cautions individuals may take in a physical and online environment in regards to privacy/security settings. The study sections and subsections will: define social networking sites, cybercrimes, online victimization/cybercrime victimization, types of cybercrime (cyberbullying/harassment, hacking/cyber warfare, online romance scams/catfish, cyber impersonation, online/internet fraud, and identity theft), Facebook® utilization (online activity), prevention measures (i.e., number of mutual friends, the recognition of friend requests, and the degree of user control), Hispanic victimization statistics, college students victimization statistics, and lifestyle-routine activity theory applied to cybercrime victimization. Finally, the theoretical framework will be discussed followed by the methodology section which includes the study location, target population, sampling technique and sample information, the instrument used, the conduct of study, hypothesis, measurements (dependent and independent variables), and limitations of the research study.

CHAPTER 2

LITERATURE REVIEW

The Internet has provided people all over the world with an infinite number of opportunities, including criminal opportunities (Reyns et al., 2011). Not only does the Internet allow individuals to interact with others, communicate with family and friends, develop new personal relationships and build professional networks, but it also gives an individual the chance of not having to leave his/her home nor having to meet others in the physical world (Bossler & Holt, 2009). The Internet has altered how individuals communicate and interact with others so much so that it has modified routines and lifestyles (Bossler & Holt, 2009; Bossler et al., 2012). As of 2013, Internet usage has grown to having approximately 657 million users worldwide (Marcum, Higgins, Freiburger, & Ricketts, 2013). While the Internet has created many beneficial impacts to daily interactions, it has also increased opportunities for crime (Marcum et al., 2013). Undoubtedly, the Internet has created new prospects for criminal activities (cybercrimes) such as cyberbullying, identity theft, and cyber impersonation which will be discussed in a subsequent section. The prospects can occur in cyber-venues or social networking sites such as Twitter, Instagram, and Facebook® (Reyns et al., 2012).

Social Networking Sites and Privacy/Security Settings

As of April 2015, the top three social networking sites listed as the world's most important were: Twitter, Instagram, and Facebook® (Milanovic, 2015). Twitter is considered to be one of the simplest and easiest social media platforms to learn and use (Milanovic, 2015). Users can send messages but they are limited to only 140 words. Setting up an account is fast and easy (Milanovic, 2015). Instagram, on the other hand, simply allows an

individual to take a picture, choose a filter of their liking, add comments, and share photos with those who are following them if their account is private or allows everyone to view their photos if the account settings are set to public (Instagram, 2013; Milanovic, 2015). Facebook® allows individuals to become connected online (called "friends" in Facebook® terminology) with colleagues, relatives, and even strangers (Milanovic, 2015). Facebook® focuses on sharing pictures, thoughts, links, and the opportunity of supporting and liking pages of organizations and brands (Milanovic, 2015). Of the three, Facebook® has the most users—an average of 1.01 billion active users a day (Milanovic, 2015).

When discussing the topic of online victimization on social networking sites, privacy settings are of great importance due to the amount of personal data shared in the world of social media (Liu, Gummadi, Krishnamurthy, & Mislove, 2011). Oftentimes, users believe their information is private when in reality desired settings are rarely present (Liu et al., 2011). Users desired settings are continuously more open to exposing content such as their phone numbers, addresses, pictures of their family members, the cars they drive, how much money they make, drug usage, and other supplementary personal information (Barnes, 2006). Most users do not understand or are not aware of the dangers that may occur due to revealing personal information on social networking sites (Barnes, 2006). As a result, if an individual is not cognizant of his/her privacy settings, they may become a victim of a cybercrime. To avoid becoming an online victim from any form of cybercrime, the National Cyber Security Alliance (2015) suggests that users learn and review the privacy and security settings that exists for the social networking site they associate with. The organization states individuals should be cautious as to how much personal information they are providing criminals with and to be aware of what individuals they are adding on their profiles. Additionally, every

online social networking site provides a security or privacy setting to where the user may change the settings to what best makes them comfortable (Trend Micro, 2015).

Facebook®, for example, offers users two options: basic privacy settings or advanced privacy control settings (Facebook Help Center, 2015). Basic privacy settings allows a user to select who can view his/her information, how he/she can connect with friends, who can add him/her, who can see his/her profile, and remove posts he/she does not want to be linked/tagged to his/her profile page (Facebook Help Center, 2015). Alternatively, the advanced privacy controls allow users to remove posts he/she was tagged in, approve tags before allowing his/her friends to view the post(s), stop a user from posting on their timeline, make finding him/her more difficult, and allow certain posts to be hidden from others (Facebook Help Center, 2015). With Instagram, this social networking site allows its users to block a person, delete or report comments, make their posts private or public, and report a post (Instagram, 2013). The Instagram community is dedicated to using powerful tools that will help users obtain a supportive, safe, and private account (Instagram, 2013). On the other hand, when an Internet user creates a Twitter account, that user's profile is automatically public (Twitter Help Center, 2015). The user will then have the option of setting his/her Twitter account to private to protect his/her Tweets (Twitter Help Center, 2015). On a positive note, Tweets that had been public once a user decides to set his/her account to private, will no longer be available to the public when they search for his/her account; only approved Twitter followers will have access to a user's Tweets (Twitter Help Center, 2015). As can be surmised, most cybercrimes are association with privacy/security settings on social media sites.

This study will solely focus on one social networking site— Facebook®, due to the enormous amount of daily users. On average, there are over 1.5 billion active users a month plus Facebook® has one of the most featured-rich and widely-used platforms (Smith, 2016). Additionally, Facebook® is constantly evolving to allow users more flexibility to add photos, friends, videos, applications, games, and to review their security and privacy settings online (Facebook Product/Service, 2012). Overall, the focus on Facebook® in this study is due to its history, popularity, and growth compared to other top social networking sites mentioned above.

Cybercrimes

A cybercrime is defined by Halder and Jaishankar (2011) as an offense committed against an individual or a group of individuals through the use of technology such as the Internet, emails, and chat rooms with the criminal intent of purposefully causing physical, mental, or emotional harm as cited in Oluga, Ahmad, Alnagrat, Oluwatosin, Sawad, and Muktar (2014). The use of computer-based technologies is the principal means of committing an offense through cyberspace (Kshetri, 2013; Oluga et al., 2014). Various kinds of cybercrimes exist such as cyberbullying, cyber extortion, hacking, copyright infringement, online romance scams, identity theft, online fraud. (Oluga et al., 2014). Additionally, it is important to note that cybercrimes may occur in a variety of facets or scenarios such as online shopping websites, emails, and social networking sites (Gordon & Ford, 2006).

Cybercrime has become a growing concern for public policy and has been examined through the use of various criminological theories, individual factors, and situational factors (Ngo & Paternoster, 2011). Furthermore, since the Internet does not solely provide Internet connection for computers, it is important to consider other objects or devices that connect to

the Internet which send or receive data such as cellular devices, as cyber threats (Federal Bureau of Investigation, 2015). Palmiotto (2015) mentions that any electronic device or object that has the capability of connecting to the Internet or that is able to receive or transmit data should be categorized as a computer when discussing cybercrime.

The following subsections will focus on the cybercrimes this thesis will focus on. Each type will be defined and outlined in further detail below:

Cyberbullying and harassment

Cyberbullying is defined as an individual or a group of individuals willfully using electronic technology to repeatedly harass or threaten another individual by posting disturbing photos, texts, or graphics or by sending such information to others (Dilmac, 2009). Studies have shown that when considering online victimization in reference to traditional bullying, there is no difference in an online setting (Brandl, 2014). Bullying victimization of any kind may lead to poor academic performance, engagement in antisocial/deviant behavior, and mental health consequences such as depression, depending on the severity of cyberbullying taking place (Brandl, 2014). These consequences are exacerbated when hundreds or thousands of people view or share such information with others thus contributing to the emotional harm bullying causes (Brandl, 2014). At times, the information is inaccurate or even false (Brandl, 2014). The following two cases illustrate the adverse consequences of online victimization:

> Jessica Logan was an 18 year old girl who graduated from Sycamore High School in Ohio, Cincinnati in 2008 (Huffington Post, 2010). She was known as being artistic, fun, and a vibrant individual (Cincinnati.com, 2009). Unfortunately, as a result of being humiliated, frightened, harassed, bullied, and ridiculed in both an online and on a face-to-face basis, she committed suicide a month after graduation (Huffington Post, 2010). The taunting began after Jessica sent a nude photo of herself via cell phone to her current boyfriend, when she was in high school. Shortly after, Jessica and her boyfriend broke up and the ex-boyfriend sent the picture to other high school

girls (NoBullying.com, 2015). The photo was then sent by the ex-boyfriend and others to hundreds of teenagers from seven Cincinnati high schools (Cincinnati.com, 2009). She then was taunted not only in school but through social media networking sites such as Facebook® and Myspace and via text messages (Cincinnati.com, 2009). She was called names such as: whore, slut, and other vulgar terms (Cinncinati.com, 2009; NoBullying.com, 2015). Her mother presented her with the decision of being home-schooled but Jessica wanted to finish school and speak about her story and experience to make others aware about the danger of sending explicit photographs through text messaging (Benotsch, Snipes, Martin, & Bull, 2013). Unfortunately, Jessica later hung herself.

Tyler Clementi was an 18 year old college student at Rutgers University. Clementi was a shy, sweet, and talented violinist (Foderaro, 2010). He had a passion for music and played in the Rutgers Symphony Orchestra (Foderaro, 2010). Before leaving for college, Clementi disclosed to his mom about being gay. Ridicule about being gay began when his college roommate at the time, Dharun Ravi, secretly streamed a sexual encounter he had with a man online (Tyler Clementi Foundation, 2014). Clementi was not aware that he had been video recorded by his roommate until the following day (Tyler Clementi Foundation, 2014). He became a topic of interest online on the social networking site, Twitter (CBS News, 2015). Ravi continued to post comments that may have caused Clementi emotional distress. He stated comments such as: “I saw him making out with a dude. Yay; anyone with iChat, I dare you to video chat me between the hours of 9:30 and 12. Yes, it’s happening again” (Parker, 2012). Ravi did not act alone, as he was accompanied by a classmate, Molly Wei (CBS News, 2015). As a result of the harassment, Clementi took his own life on September 22, 2010 (Tyler Clementi Foundation, 2014). Shortly, before committing suicide, Clementi posted on Facebook®: “Jumping off the G.W. Bridge-sorry.” (CBS News, 2015). Dharun Ravi and Molly Wei were charged with several crimes which included bias intimidation concerning hate crimes, and with invasion of privacy under the peeping tom statute (CBS News, 2015). Wei agreed to a please and avoided prosecution. Ravi was not charged with causing Tyler’s death but was convicted on fifteen counts serving 20 days out of 30, in jail (CBS News, 2015).

Hacking/cyber warfare

While there are different kinds of hacking, this study focuses on computer hacking. Computer hacking or intrusion has wide significance in the world of computer networking and online communities (Jordan & Taylor, 1998). In addition, computer hacking is similar to cyber warfare in which Dipert (2010) defines as an attack against a governmental or civilians’ information system (Oluga et al., 2014). Warfare does not mean causing physical damage, killing someone, or injuring anyone in anyway but rather that individuals may be

affected by a cybercriminal taking confidential information from him/her that may benefit the criminal (Oluga et al., 2014). Computer hacking or cyber warfare includes deceiving, downloading, or intruding into a person's communication and information systems (Oluga et al., 2014). Hacking poses a great threat to those whose information has entered the cyberspace world since then such information may get lost or into the possession of cybercriminals. Below are two examples.

> Sanford Wallace, a computer hacker who is known as the "Spam King" (Nichols, 2015). Wallace gained access into Facebook® accounts and hijacked those accounts to send spam that was associated with phishing sites, and linked commercial websites that pay spammers for referrals (Brodkin, 2010). Wallace allegedly obtained the login credentials to the Facebook® accounts and Facebook® resulted fighting back against Wallace through the legal system (Brodkin, 2010). He was charged with eleven charges with ranged from fraud to damaging a protected computer for spreading more than 30 million spam posts and messages on Facebook®. Wallace pleaded guilty and agreed to a plea deal and is to serve no more than three years (Munson, 2015; Nichols, 2015).
>
> A second computer hacking story revolving around social networking sites would be the case of Iranians hacking State Department officials Facebook® accounts in the United States (Sanger & Perlroth, 2015). Even though it is noted that Iran's cyber skills are not as advanced as China's and Russia's they believe cyber espionage is a tool they are beginning to use since the United States is less likely to respond to a cyber-threat (Sanger & Perlroth, 2015). The Iranian hackers in this event hacked into the Facebook® accounts and emails of individuals who are State Department officials who focus on Iran and the Middle East (Sanger & Perlroth, 2015). By attaining access to their accounts, they were able to search and find other members from the State Department who focus on the geographical area of Iran (Sanger & Perlroth, 2015). Thanks to Facebook® new alert system, they were able to notify the users that their accounts had been hijacked.

Overall, these examples illustrate that computer hacking is a risk on social networking sites to both civilians and governmental officials.

Online Romance Scam/Catfish

Online romance scams, which may be referred to as being cat-fished, are schemes whereby cyber criminals pretend to be someone else and may seek romance and

companionship from a potential victim (Internet Crime Complaint Center, 2014). Such criminals search for probable victims through the use of chat rooms, dating sites, and social networking sites and often use lies and manipulation to trick the victim (Internet Crime Complaint Center, 2014). Online romance scams are a new form of fraud that became apparent in 2008 (Whitty & Buchanan, 2012). In these types of scams, victims receive a double hit-- losing a relationship, and losing money (Whitty & Buchanan, 2012). Online romance scams do not only rob victims of large sums of money, but they are left to deal with the psychological aftermath of this form of cybercrime (Whitty & Buchanan, 2012). The following examples illustrate this form of cyber-crime:

> Jennifer, a woman from Buffalo, New York and a mother of two, had been single for 15 years and was ready to look for someone she could spend the rest of her life with; someone who could be her companion and partner. Unluckily, Jennifer became a victim of an online romance scam and lost her life's savings of $50,000. Jennifer met a man on a dating web site in which she believed was the man of her dreams. They tended to communicate through the use of emails, text messages, and by the phone. She liked that he was kind and loving and just fell in love with the man she thought he was. The relationship was so serious to the point that the man proposed to Jennifer. He presented himself as being a business man, and one day said he had to leave to take care of a job overseas. Jennifer by that point, was desperately waiting to meet him in person. Suddenly, the man began to ask for money giving a reason that since he was out of the country, he could not attain any of his funds. She was manipulated by hearing what it was she wanted to hear. Jennifer decided to speak up about her experience as a victim of an online romance scam to make persons aware that there are cyber criminals out there who will do anything in their power to attain what it is they need, such as money (Moretti & Ciotta, 2015).

> Manti Te'o, a college football player at the time, was a victim of an online romance scam that affected him more on the emotional and psychological spectrum. He became involved with a girl named, Lennay KeKua from Stanford University (ESPN, 2013). They met online, and eventually began speaking on the phone when they "met" sometime in 2009 (Burke & Dickey, 2013). Te'o and KeKua never met after that one time he mentioned. Te'o then began to fall in love with her, he stated in an interview that she was the love of his life (ESPN, 2013). On September 2013, Te'o announced to media outlets that his grandmother and girlfriend, Lennay, had passed away (ESPN, 2013). Shortly after, KeKua called Te'o to tell him it was not true, that she was alive. Sadly, Lennay was not the person he thought she was. He was hoaxed into believing it was her, and was a victim of a sick joke and experienced pain and

> humiliation (ESPN, 2013). Te'o was not the only one who was contacted by KeKua and "KeKua" resulted in being a male named Ronaiah Tuiasosopo (ESPN, 2013; Gutman & Tienabeso, 2013).

As evidenced in the examples above, online romance scams may lead to pain, ridicule, humiliation, and even the loss of money. While cases differ, the common denominator is that the victim is deceived when searching for love online. Due to shame and the distraught the individual may have experienced, that may have deterred him/her from reporting the scam committed against them (Whitty & Buchanan, 2012).

Cyber Impersonation

Cyber impersonation is defined by Mann (2015) as a cybercriminal hacking into someone's account, posing as them and updating their statuses, comments, or sending messages that will make the individual look bad for the purpose of ruining their reputation, friendships, and/or to get them in trouble or in danger. T & M Protection Resources (2014) states that cyber impersonation involves using the Internet to post malevolent, unapproved content that relates to a specific individual or establishment of a(n) personal profile that has been designed to give resemblance of an actual existing account (Oluga et al., 2014). Oftentimes, this cybercrime is committed against an individual without his/her knowledge because cyber criminals usually make such actions hard to discover (Oluga et al., 2014). They create false profiles with the use of another individual's pictures, information, etc. (Oluga et al., 2014). Below are two cases that involve cyber impersonation.

> Daven Lee Nielsen a 54-year old man from Norfolk, Virginia was charged with online impersonation which is punishable to 10 years in prison as it is a third-degree felony. Nielsen is not yet in custody but will be punished for impersonating his ex-girlfriend and her two daughters on Twitter. Police state that Nielsen created fake Twitter accounts in which he used to send false, explicit messages to others. He is punished through the legal system since under the law and the revision of state legislature, someone can be charged with impersonating someone through the means of creating a social media profile or other online account. When such a page or profile

> is created without consent from the person, and their information is used to ruin their self-image it is a crime. When Nielsen was interviewed, he stated he created the accounts because he was bored and he did not know what he did was illegal (George, 2012).
>
> A 31-year old woman from Austin, Texas was in an unhealthy relationship with Marcos Lujan for nine months. Shortly, after the relationship ended, Lujan began to impersonate her online and offered sex for groups of men. He solicited her on Craigslist, for group sex and investigators found about 1,000 emails between Lujan and other men. Margaret, the victim, had to face unwelcomed visits late at night from men Lujan had sent there. Not only did men show up at her home, but presented themselves at her work too. Lujan was convicted of online impersonation and served several months then was released. Margaret was diagnosed with Post Traumatic Stress Disorder (PTSD) as a result of her experience and wanted to make others aware that online impersonation can happen to anyone (Lee, 2015).

Online/internet fraud

Online fraud, often referred to as Internet fraud, is a criminal activity involving the use of a computer and/or an internet connection where a perpetrator may use sophisticated technological tools to obtain personal information that may result in consequences for a victim (Legal Information Institute, 2015). Online fraud may involve identity theft or financial fraud (National Crime Victim Law Institute, 2010). Fraud is an act of intentional deception for the means of obtaining personal gain and/or to cause a loss to a second party (Serious Fraud Office, 2015). Online fraud is similar to identity fraud or identity theft because the term “fraud” includes false statements, deceitful conduct, and/or misrepresentation (FindLaw, 2015). Two instances of online-fraud are illustrated by the following cases.

> Adrian Ghighnia was indicted on seven counts of wire fraud in the year of 2010 in Chicago (Department of Justice, 2014). Separately, he was to be indicted by federal grand juries in the District of Columbia, and Florida. Ghighina admitted to opening numerous bank accounts with false information (Chicago Tribune, 2011). He had co-conspirators that created fraudulent online auctions for expensive items that ranged from cars to motorcycles and held sales on websites such as eBay, and Craigslist. (Chicago Tribune, 2011). The money they obtained was sent to one of Ghighina’s accounts and buyers would never receive the items they purchased (Department of

> Justice, 2014). Ghighina was sentenced to four years in federal prison for his role in the Internet fraud conspiracy (Chicago Tribune, 2011).
>
> Cameron Harrison pleaded guilty to retaining 260 comprised credit card and debit card numbers (Mallonee, 2014). He purchased stolen credit card, debit card, and personal information through an Internet fraud ring known as Carder.su (U.S. Immigration and Customs Enforcement, 2014). Harrison admitted to being associated with the Carder.su internet-based, international criminal enterprise organization (U.S. Immigration and Customs Enforcement, 2014). The organization trafficked account information, credit/debit card account information, counterfeit identification and committed crimes such as money laundering, the selling of narcotics, and other computer crimes (U.S. Immigration and Customs Enforcement, 2014). The criminal organization was discovered when Harrison was identified by an undercover agent when he tried to purchase a counterfeit Georgia driver's license (Mallonee, 2014). Harrison admitted that the ring used various secure and encrypted emails, chat rooms, or forums in order to hide their criminal activities from law enforcement and other criminal internet-based organizations (U.S. Immigration and Customs Enforcement, 2014). As a result, 26 individuals have been convicted and there are individuals pending trial or are fugitives (U.S. Immigration and Customs Enforcement, 2014). Harrison was sentenced to 115 months in a federal prison and was ordered to pay a total of $50.8 million in restitution given that he stole about $50 million from innocent Americans (U.S. Immigration and Customs Enforcement, 2014).

Identity theft

Identity theft is a crime and it has become one of the fastest growing crimes in America (Social Security Administration, 2015). Identity theft is when someone unlawfully acquires an individual's personal data in order to use an individual's private information to commit theft or fraud (FBI, 2015). Identity theft is the gathering of personal information without having to break into someone's home or stealing physical information (Department of Justice, 2015). Recently, identity theft has become more appealing for criminals in an online setting (Department of Justice, 2015). They steal personal information by creating spams, emails, viruses, etc. Furthermore, identity theft includes stealing information such as passwords, social security numbers, date of birth, passport numbers, death certificates, and other personal identification information. (FBI, 2015). Stealing an innocent person's information can benefit a criminal by applying for loans, credit cards, bank accounts, or

purchasing expensive materials (Department of Justice, 2015). To further comprehend what elements may contribute to identity theft crimes, consider the following cases:

> Alexander Paul from North Miami stole identities to aid him in taking tax refunds from innocent people (Department of Justice, 2015). Paul claimed over $109,322 from federal tax refunds having a total of fifty-three tax returns filed (Department of Justice, 2015). He plead guilty to authorizing access devices, and for aggravated identity theft. When they searched Paul's residence, investigators found and seized evidence of personal identification information from other individuals in two cell phones, a notebook, and on his computer (Department of Justice, 2015). On August 26, 2015 Paul was sentenced to 31 months, three years supervised release, and was ordered to pay a total of $18, 469 in restitution (Internal Revenue Service (IRS), 2015).
>
> Michael Floyd White and Sasha Cher-Von Beckett stole identities of many innocent people. White was punished to 39 months, three years of supervised release, and was to pay a total of $112,362 in restitution for his role in mail fraud and aggravated identity theft (Department of Justice, 2014). Co-defendant, Sasha Cher-Von Beckett was sentenced to 51 months, and three years' supervised release. Beckett pleaded guilty to charges on identity theft, access device fraud, and mail fraud (IRS, 2015). Both, White and Beckett willingly used innocent people's names, date of birth, and social security numbers to file false income tax returns to collect refunds for personal gain (Department of Justice, 2014; IRS, 2015).

Online Victimization and its Consequences

In 2014 alone, the FBI concluded that 9,833 individuals were victims of cybercrimes on social media outlets (FBI, 2014). The most frequent crimes were online fraud, online impersonation, and online romance scams (FBI, 2014). Online fraud was ranked as the crime that caused the most monetary loss for victims followed by online impersonation, and online romance scams (FBI, 2014). Given that there are approximately 657 million users worldwide who incorporate some type of online device to use the Internet in their daily lives (Marcum et al., 2013), individuals tend to engage in activities such as: purchasing online products, e-mail(s), searching for entertainment, news, and managing their investments (Marcum et al., 2013; Reisig, Pratt, & Holtfreter, 2009; Reisig et al, 2009). Thus, the probability for victimization is high. In addition to the possibility of monetary loss, research has found that

victims' experiences have led some to suicidal ideation, suicide, depression, and other psychiatric symptoms (Aricak, 2009).

Zhang, Land, and Dick (2010) indicated that cyberbullying constitutes violence that can lead to physical injuries and/or psychological and/or emotional harm. Individuals often report suffering from depression, embarrassment, stress, and feeling afraid or emotionally distressed as a result of being victimized online (Zhang et al., 2010). Online victimization has correspondingly had reported offline repercussions such as school violence and/or victims engaging in delinquent acts (Hinduja & Patchin, 2007). Hinduja and Patchin (2007) studied potential offline consequences as a result of online victimization and found that in regards to cyberbullying, victims were at risk for "negative developmental and behavioral consequences" like those listed above (school violence and delinquency) (Hinduja & Patchin, 2007, p. 103). Hinduja and Patchin, (2007) pointed to support that there are psychological and emotional costs associated with victimization experience in an online environment (Hinduja & Patchin, 2007).

Furthermore, Wright and Li (2012) examined both face-to-face and cyber victimization in relevance to cyber-displaced aggression. They found that face-to-face and cyber victimization both play an important role in cyber-displaced aggression at least six months after the incidents (Wright & Li, 2012). Cyber-displaced aggression ranges from an individual feeling anxious to depressed, feeling lonely and performing poorly on given duties or academics (Wright & Li, 2012). Wright and Li (2012) conducted one of the first studies to indicate that victims may retaliate against other innocent persons and not necessarily against the perpetrator who victimized them. The findings of Wright and Li, (2012) are supported by other studies that state offenders have also experienced victimization (see Cunningham et al.,

2015; Hinduja & Patchin (2010). Wright and Li (2012) believe that their research can help future studies to acknowledge that cyber victimization and victimization in an offline setting may work interactively in producing delinquent behaviors such as aggression.

Not only does the duration and aftermath of a cybercrime experience adversely affect a victim, it could also impact the offender (Aricak, 2009). In a study conducted by Hinduja and Patchin (2010), it was found that perpetrators and victims both had suicidal thoughts as a result of experiencing cybercrime victimization (Schenk & Fremouw, 2012). Research shows that experiencing victimization such as bullying—both in an online and offline environment are linked with suicidal ideation for victims and offenders; suicidal ideation is higher for victims (Hinduja & Patchin, 2010; Schenk & Fremouw, 2012). Those who are bullied or those who bully tend to think, attempt, or complete suicide and research shows that victims and perpetrators often experience loneliness, hopelessness, and depression which are all significant in suicidal ideation (Hinduja & Patchin, 2010).

Victimization Experience

Victimization can vary in severity, intensity, frequency, and diversity (ever victimized) of victimization experienced. Depending on the cybercrime, victimization may require law enforcement, medical, and/or psychiatric or mental health assistance since victims may feel suicidal, depressed, nervous, anxious, or fearful and afraid (Zhang et al., 2010). With respect to the intensity of victimization, it is possible that individuals experience repeat victimizations (Ybarra et al., 2012). Thus, it is important to decipher how often an individual experienced victimization online in a typical week. Additionally, frequency is also important to understand and study as it is crucial to determine how long (i.e., duration) a user experienced being a victim or for current victims, how long they have been experiencing

online victimization. In this study, ever victimized, intensity, and frequency of victimization will be combined into one variable entitled victimization experience. Ever victimized will determine if users experienced being victims of cybercrime. It will include six main cybercrimes: cyber impersonation, online fraud, identity theft, romance scams/catfish, hacking cyber warfare, and cyberbullying/harassment.

Personal Characteristics

Personal characteristics are important to consider as they may alter an individual's severity, intensity, frequency, and the likelihood of being victimized. Therefore, factors such as—age, sex, educational level, sexual orientation, and ethnicity provide a basis of understanding cyber-victimization. With respect to ethnicity, there have been little to no studies that determine the prevalence of online victimization experience by different minority groups. This is peculiar since there are many studies on victimization of ethnic minority groups unrelated to cyber space. For instance, the FBI found that roughly 53% of Hispanic were targeted in a physical environment and 47% of Hispanics were victimized in 2013. The rate of violent crime involving Hispanic victims tripled from 0.6 per 1,000 persons to 2.0 per 1,000 individuals in 2012 (FBI Law Enforcement Bulletin, 2015). Homicide is determined to be the second leading cause of death for Hispanic individuals between the ages of 15 to 24 (Sugarmann, 2014). Hispanics are often victimized or killed by strangers rather than friends or family (Sugarmann, 2014). Overall, there are a number of studies showing the prevalence of crime in an offline environment being committed against the Hispanic/Latino population but limited to no statistics or literature on the amount of Hispanic cybercrime victimization.

When looking at the limited research on cybercrimes, Cunningham et al. (2015) found that men were more likely than women to be offenders of cybercrime or have

experienced both being a victim and being an offender of cybercrime (Aricak, 2009; Cunningham et al., 2015). Additionally, Reyns et al. (2011) found that females' likelihood of victimization is double to their male counterparts. Their chances of being stalked online and experiencing victimization were 1.8 times higher than males (Reyns et al., 2011). In another study conducted by MacDonald and Roberts-Pittman (2010), they found that male students reported bullying others at 11% and have experienced cyberbullying at 22%. On the other hand, females experienced cyberbullying at 22% and bullied someone else at 8% (McDonald & Roberts-Pittman (2010). But, MacDonald and Roberts-Pittman (2010) found that there is a slight difference in the percentage of males and females playing an important factor in cybercrime victimization. A second study found similar findings in which both males and females were more likely to cyberbully others on Facebook® if they themselves had experienced cyberbullying (Marcum et al., 2013). From the above research, one can conclude that there is little to no difference in the amount of students being victimized or cyberbullying others.

With respect to sexual orientation, Schwartz (2010) found that students had committed suicide as a result of being bullied over the Internet because of an individual's sexual orientation. The Campus Pride advocate group found that sexual orientation was related in one out of four reported harassments that led to negative consequences (Schwartz, 2010). Finn (2004) found that the LGBTQ community is likely to experience cyber stalking or cyberbullying twice as much as heterosexuals. In another study conducted by the Campus Pride advocate group, it was found that non-heterosexual students between 11 and 22 years of age had experienced online victimization (Schwartz, 2010). When considering the use of the Internet by age, the Pew Research Center (2015) found that young adults between the

ages of 18-29 use and adopt the Internet in their daily lives (Perrin & Duggan, 2015). The Pew Research Center also found that 95% of adults who are in college or in graduate school use the Internet more than other subpopulations (Perrin & Duggan, 2015). Educational attainment is considered to be one of the strongest indicators of determining Internet use for Americans (Perrin & Duggan, 2015). Since college students have a propensity to routinely use the internet or electronic media for various reasons ranging from educational purposes to staying socially connected to others through the use of text messages, chat rooms, social media outlets, etc. college students are an ideal study population and thus the focus on this study on cybercrime victimization.

It is noteworthy to discuss why this section focused mainly on cyberbullying. The reason for this, is due to the extensive attention cyberbullying has received in scholarly literature. Thus, because of the gap in literature with respect to studying other forms of cybercrime victimization, this study will help determine whether the information collected maps onto other forms of cybercrimes (i.e., online romance scams, online fraud, etc.).

Facebook® Utilization

Since there is no precise definition for online activity, for the sake of this study, online activity will be defined as individuals who use the Internet, primarily Facebook®, for the purpose of interacting, networking, and/or engaging with others who may be family, friends, or strangers. Online activity will determine if a person is active or inactive in an online setting. For instance, since the Internet has become a part of everyday life for many or all individuals, routinely accessing the Internet for information will be used to construct the variable Facebook® utilization in this study. While routinely accessing the Internet will likely lead to being considered as an active user for the purposes of this study, this variable will

also focus on the number of hours people use the Internet, primarily on Facebook® (Smith, 2016). Statistics show that 91% of millennials use Facebook® and that users tend to spend at least 20 minutes per day on Facebook® (Smith, 2016). There are limited statistics as to the number of time spent on Facebook® and the times in which people log onto Facebook®. Thus, in addition to this variable, participants will be asked at what times they are likely to log onto Facebook®, and if they log on during work, school, or both.

Research Participants

Research on victimization in cyberspace is still in its infancy –and the majority of available studies have been: (1) exploratory in nature and (2) focused on adolescent samples. However, there are reasons to pay closer attention to victimization of college students. First, 93% of college students use social networking sites at higher rates than adults (Lenhart et al., 2010; Lindsay & Krysik, 2012). The majority of college students fall under the millennials category which includes individuals who are between the ages of fifteen and thirty-four. Statistics show that 91% of millennials use Facebook® and that users tend to spend at least 20 minutes per day on Facebook® (Smith, 2016). Second, Identity Guard Resource Center (2015) stated that college students are disproportionately susceptible to being victims of identity theft, and they are slow at discovering they are victims of cybercrime. Also, there has only been a few studies conducted on the college student population in regards to cybercrime victimization. The majority of studies focus on adolescent or high school students (Marcum et al., 2010). While Marcum, Ricketts, and Higgins (2010) state that adolescents and younger adults are a population with one of the fastest growing rates of Internet use, it is equally if not more important to consider the college student population because they are also identified as an at-risk group for various experiences, especially cybercrime (Reyns et al., 2011). Their

risk is due to college students routinely connecting to the Internet to complete coursework requirements such as research papers, assignments, etc. (Reyns et al., 2011).

Admittedly, the knowledge of cybercrimes being committed worldwide is unknown. Such a lack of knowledge regarding the kinds and frequencies of cybercrime worldwide may be due to two fundamental difficulties that do not allow for accurate statistics (Kabay, 2013). The two problems preventing accurate statistics are detection and reporting (Kabay, 2013). Brandl (2014) states that online victimization when concerning college students may be anywhere between ten to forty-two percent. Since it is difficult to have precise statistics as to the number of individuals falling victims to cybercrimes, it is difficult to determine the severity, intensity, extensity, and diversity of victimization. Choi (2008), found that college students who neglect having computer-security software are more likely to be victimized than other students who do not neglect installing such software. When considering literature on the extant topic, research shows that numerous studies have been conducted in regards to college student's perceptions and attitudes of the Internet and their behaviors (Lindsay & Krysik, 2012). But, when taking Internet-related risk into consideration, little attention has been given to the dangers that college students may encounter on the Internet (Lindsay & Krysik, 2012).

Lifestyle-Routine Activity Theory (LRAT)

Lifestyle theory is considered to be a personal victimization theory that was first developed by theorists Michael Hindelang, Michael Gottfredson, and James Garafalo in 1979 (Jenson & Brownfield, 1986). Lifestyles, in relation to the theory, entails what people do on a daily basis: the patterns, routines, and activities they engage in during their daily lives including leisure, work, home, school, and evening recreational activities (Myrstol &

Chermak, 2005). According to theorists Hinelandg, Gottfredson, and Garafalo, an individual's "lifestyles" can predict the likelihood of victimization (Myrstol & Chermak, 2005). However, the centerpiece of the theory hinges on the time people spend in public places, their personal characteristics, and the interaction with offenders, which may be unknown to the individual (Jenson & Brownfield, 1986). Thus, lifestyles are of great importance because they can determine the degree to which individuals interact with motivated offenders in the absence of capable guardians (Jenson & Brownfield, 1986). In essence, the theory's focus is on the characteristics or personal characteristics of victims that can enable them to be vulnerable targets (Jenson & Brownfield, 1986).

Routine activity theory is best known for the expansion of lifestyle theory and will be discussed in more detail below. Routine activity theory was developed by criminologists Lawrence Cohen and Marcus Felson in 1979 (Frailing & Harper, 2013). Cohen and Felson (1979) state that people's daily routines may put an individual at higher risks of victimization than others. Three elements are required in order to produce a crime: a motivated offender, a potential target, and the lack of a capable guardian (Cohen & Felson, 1979). Crime occurs when a motivated offender encounters a suitable target in the absence of a capable guardian (Cohen & Felson, 1979). According to the theory, the probability of victimization decreases in the presence of a capable guardian (Cohen & Felson, 1979). When applied to cyber victimizations, a motivated offender may be found in a variety of cyber locales: chat rooms, shopping websites, social networks, etc. Potential targets or victims can be any individual who spends time using the Internet but, the more an individual spends time online the higher, the chances of them being victimized by potential offenders (Reyns et al, 2011). Reyns, Henson, and Fisher (2011) state that increase in internet usage increases target attractiveness.

Attractiveness also increases when an individual posts personal information such as their: relationship status, e-mail addresses, sexual orientation, activities, photos, height, and weight (Reyns et al., 2011).

In an online setting, capable guardianship can be measured as not having both a firewall or security program installed in a user's computer (Reyns et al., 2011). As stated previously, people who spend more time online have a greater chance of being victimized of cybercrime. Without having a degree of security measures possible, the chances of a user being victimized online increases (Frailing & Harper, 2013; Reyns et al., 2011). Additionally, there were physical and social characteristics said to influence the likelihood of victimization online, but it was not clear as to what this meant as a result of limited empirical research (Holt & Bossler, 2009). In addition, as cited earlier, anti-virus programs and firewalls serve as a physical component to computers and Internet connections (Holt & Bossler, 2009). These types of programs are used as physical guardians from computer bugs, malicious software, and system invasions that tend to threaten lines of communication (Holt & Bossler, 2009). In the social guardian spectrum, this includes owners updating their anti-virus programs, firewalls, and Internet browsers to reduce the likelihood of experiencing victimization (Anderson & Agarwal, 2010; Holt & Bossler, 2009; Wall, 2008).

In the current study, lifestyle theory and routine activity theory will be combined due to their similarities, and will be referred to as LRAT. Given that routine activity theory is an expansion of that of lifestyle theory, integrating both theories is beneficial in the examination of online victimization experience. Other researchers have also combined lifestyle-routine activity theory such as Holt and Bossler (2009) in their examination of applying LRAT to cybercrime victimization. A second study, along with many others includes Reyns et al.,

(2011) where they applied LRAT to cyber stalking victimization. Furthermore, since both theories intertwine, combining them in representing daily activities, patterns, and routines is beneficial for researchers.

Researchers posit that cybercrime may be explained by LRAT. For instance, Holt and Bossler (2008) found a positive correlation between the total number of hours an individual spends online and the likelihood of him/her being victimized. Holt and Bossler's, (2008) study focused on a particular form of cybercrime—online harassment and their study was used to test the LRAT in regards to online victimization. They examined computer usage, time spent online, social guardianship, motivated offenders, and potential targets (Holt & Bossler, 2008). Holt and Bossler (2008) found in their analysis that constructs of LRAT do apply to cybercrime. Additionally, they found it important to identify the association between victimization and delinquent acts, to include gender because females tend to be victimized at higher rates than males, and that online activity (i.e., regular use of computer-mediated communications) play an important role in cybercrime victimization (Holt & Bossler, 2008).

Results of another study suggest that when a motivated offender and a potential target intersect within a network, victimization is likely to take place (Reyns, 2013). Reyns (2013) aimed at applying the LRAT to crimes where an offender and a victim never come into direct contact. Reyns, (2013) examined victims of identity theft and an individual's daily routines while also considering their characteristics, and perceived risks of identity theft victimization. He states that there should be continuous research done on LRAT in order to expand its approach into considering offenses where a victim and an offender never come into physical contact with one another (Reyns, 2013). Reyns, (2013) did find support for the

application of LRAT to the explanation of online victimization given that his study proposes crimes do not only occur in direct contact but, may occur through internet connections.

But, there have been convincing arguments by other researchers that components of LRAT may not be suitable or adaptable to online victimization (Reyns et al., 2011). For instance, even though there are three basic tenets used in explaining conventional crime in a physical setting. Yar (2005) disputes that LRAT elements are not suitable for applying to cybercrimes (Reyns et al., 2011). Yar (2005) explains that one of the main elements LRAT holds is that time and space are central in explaining criminal activity (Reyns et al., 2011). As a result, because both space and time are essential in using the theory to explain crime, cybercrimes may not be explained by applying LRAT to an online environment (Reyns et al., 2011; Yar 2005). Since a victim and an offender must intersect for a crime to occur, in cyberspace an offender and a victim do not come together in the same physical environment which is the reason why many researchers believe LRAT may not be used to explain cybercrime (Reyns et al., 2011). Accordingly, researchers argue that LRAT is either limited to only place-based crimes or it simply needs revision to include other crimes where a victim and an offender do not have contact with one another in a physical environment (Reyns et al., 2011; Tillyer & Eck, 2009).

LRAT, however, can be revised to include contact between an offender and a victim, in an online setting. This may take place when the offender and the victim's network devices come into contact with one another (Reyns et al., 2011). Reyns (2013) states that some criminologists have recognized the advancements in the technological world, and as a result, they are now aware there has been a creation of new opportunities for crime and victimization to occur. Reyns (2013) positions that the Internet has created new opportunities

of crime to take place not only in a traditional environment but in a new environment—the online world. While the theory was created by Cohen and Felson in 1979 when the Internet was non-existent (Reyns, 2013), Cohen and Felson did note that technological and other structural advances would "influence the nature of criminal victimization" (Cohen & Felson, 1979, p. 591; Pratt, Holtfreter, & Reisig, 2010).

The applicability of LRAT to the online environment continues to be debated (Pratt et al., 2010) but arguments are tipping in favor of applying LRAT to cybercrimes. One of the primary arguments in favor of its applicability is the simple fact that people are using the Internet on a daily basis. File and Ryan (2014) found that 74.4% of U.S. households reported Internet use, and 83.3% reported owning a device that connects to the Internet. This comes to demonstrate how our world has become reliant on technology. Thus, the growth in remote activities has now shifted arguments in favor of the application of LRAT (Reyns, 2013) to cyberspace. Eck and Clarke (2003) suggest that LRAT could be modified to accommodate the necessity of space and time because there is contact of one network with another. Even though a motivated offender and a victim did not come to direct contact, the fact that one network overlapped with another is what allows an offender to victimize an individual (Reyns, 2013).

Also, the motivated offender component represented in this theory may be measured by considering the amount of time the user spends in an online environment (Bossler, Holt, & May, 2012). Additionally, asking various questions in regards to computer deviance and actions taken in an online environment may determine whether or not the users may be a motivated offender (Bossler et al., 2012). A suitable target may be measured by taking into consideration demographic characteristics since research shows that motivated offenders take

characteristics of an individual into consideration to determine who to victimize (Bossler et al., 2012). Lastly, the lack of a capable guardian element may be measured by determining whether or not the user had a security program installed in his/her computer, whether or not the user incorporated firewalls, and the amount of information provided online such as a user's address, or work place. It could also be measured by the extent to which users incorporate other prevention measures, which will be discussed below.

Prevention Measures

There are certain safety precautions users can take in an online environment. Daily-life patterns and activities of an individual offline and online will determine the likelihood of an individual being victimized (Davis & Smith, 1994). Security measures or safety precautions can include: running and updating anti-virus programs they have installed in their computers, ensuring they have a running firewall, securing and using difficult passwords, and conducting updates needed in a user's computer (Anderson & Agarwal, 2010). Wall (2008) found that if a user had a reliable security program installed and updated Internet browsers, then those users reduced their likelihood of experiencing online victimization. Norton by Symantec (2015) provides prevention tips for online users such as: making sure a user's computer has the latest updates, using strong passwords that are also not shared with anyone, protecting and not distributing their personal information, protecting a computer with updated security software programs, and reviewing financial institution statements regularly to avoid becoming a victim of cybercrime. Since users are at a place where they can be vulnerable, securing devices that connect to the Internet is a serious factor that must be met by security policies to ensure a user's personal information is safe and secure from motivated offenders (Wall, 2008).

In this study, the importance of the prevention measures variable will be tested to determine whether such measures impact utilization and victimization experience. This will be done by analyzing the importance of having mutual friends, the number of mutual friends (mutuality), recognition of a user's profile name and user profile photo, and the degree of user control. Determining the number of users being victimized online, will be measured by the number of mutual friends a user has with a person attempting to add him/her on Facebook® and recognition (whether the user knows who is the person requesting a friend acceptance on their Facebook® profile). This variable will be measured by four different categories. The first level will involve a low number of mutual friends and the user knowing who is trying to add him/her. The second level will involve the user having a high number of mutual friends and knowing who is trying to add the user. The third category will involve a high number of mutual friends and the user not knowing the person. The last category will represent a low number of mutual friends and a user not knowing who the individual is. In accordance to prevention measures, the degree of user control will be evaluated to determine whether or not it correlates to cybercrime victimization. This variable will be analyzed by determining whether a user's Facebook® account/profile is set to private or public in reference to photos, videos, comments, posts, etc. and whether or not that impacts to probability of being victimized on Facebook®.

Being able to determine whether a respondent knows who sent them a friend request on Facebook®, will allow one to determine if a user's probability of being victimized is higher or lower based on friend mutuality and recognition. This measure will assist research by incorporating how an individual decides to add or delete a friend request. Moreover, since there has been noted research on who is more likely to engage in cybercrime—the mutuality

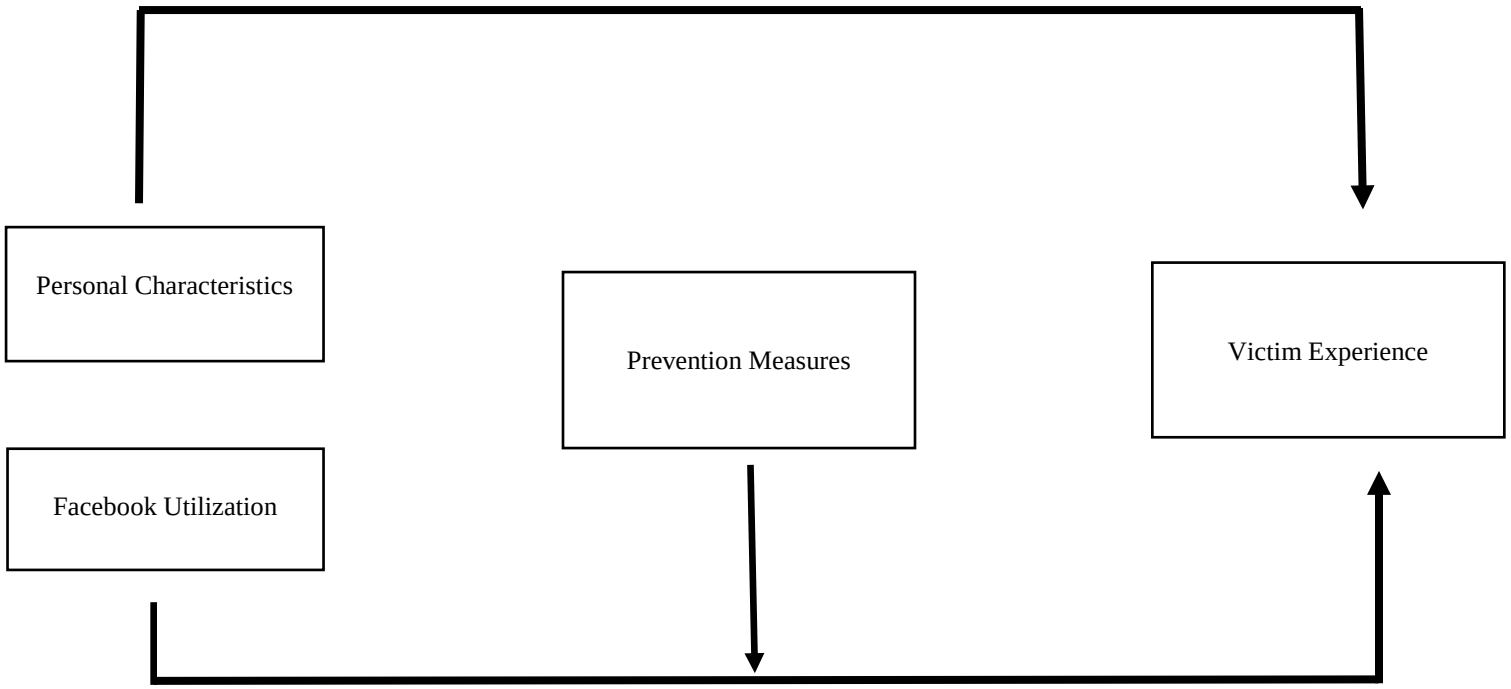
and recognition dimensions should aid in distinguishing who is more likely to partake in committing cybercrime. For example, Cunningham et al. (2015), found that a large percentage of students who reported being victims of cybercrime were committed by friends and/or acquaintances of the victims (Cunningham et al., 2015). Wolak, Mitchell, and Finkelhor (2007) piloted a study on online harassment which is known as cyberbullying and stated that cyberbullying tends to focus on offenders who are peers of a victim; but youth in the study also reported being victimized by people they only knew and met online (Wolak et al., 2007). Cyberbullying is now considered one of the most prominent types of cybercrimes, like online fraud, online impersonation, and identity theft (Hinduja & Patchin, 2007). Wolak et al. (2007) found that harassment incidents were being committed by peers more repeatedly than by individuals the victim only came into contact with online. A second study of students at the University of New Hampshire found that students received e-mails and messages from chat rooms that were harassing in nature from strangers they met online, acquaintances, and significant others (Finn, 2004). Thus, this measure will shed light on the decision-making process for adding or deleting a friend request.

Furthermore, focusing on the likelihood that a user decides to add or delete a friend request in pertinence to the number of mutual friends and recognition will aid in measuring whether or not this variable plays a key role in the probability of a Facebook® user becoming a victim of cybercrime. If so, this construct will be able to be used in the future when conducting additional research on cybercrime and prevention measures in regards to—Facebook®.

Below is a graphic depiction of the conceptual model that will be used in this study. While all constructs will be fully explained in forthcoming sections, the model tells us that

prevention measures will moderate or impact the strength of the relationship between Facebook® utilization and victimization experience. Additionally, the models tells us that personal characteristics directly affect victimization experience.

Figure 2.1 Conceptual Model



CHAPTER 3

METHODOLOGY

Study Location

The study was conducted in Laredo, Texas at Texas A&M International University (TAMIU). Laredo is located along the southwest border of Mexico. It has a population of approximately 255,473 people who are mainly of Hispanic origin (96%) (United States Census Bureau, 2015). Laredo has an average crime rate of 331 per 100,000 population, while the crime rate for the U.S. is an average of 257 per 100,000 population. Concerning cybercrime rates in Laredo, there are no statistics at this given time. However, Texas has been rated the third state out of ten top states for cybercrime as of 2014 in regards to the total number of complaints and money loss amounts in respects to cyber victimization (Internet Crime Complaint Center, 2014).

TAMIU is a 4-year public institution. TAMIU is predominantly an undergraduate institution, with 88.6% of its student population being undergraduate students. Current enrollment at TAMIU is approximately 7,400 students. In fall 2015, TAMIU's student population consisted of 59.4% female, 40.6% male, 92.7% Hispanic, 56% of all undergraduates are low income (eligible for Pell Grants) and 79% of freshman are low income, and 59.2% first-generation college students.

Sampling Technique and Sample

The study aimed at surveying two hundred to three hundred undergraduate, Hispanic college students currently enrolled at TAMIU in the criminal justice and psychology program—two of the largest undergraduate programs at the university. The primary goal of this study was to obtain a representative sample of students enrolled at TAMIU. However,

due to logistical challenges, a non-random or non-probability sample was obtained. Specifically, two separate sampling techniques were used. First, students who voluntarily enrolled in the SONA system, a cloud-based software environmental management system which aids universities in managing research studies and recruiting participants online (SONA Systems, 2016) was utilized to recruit students for the present study. The second sampling technique involved classroom visits to two criminal justice courses in the summer of 2016.

It is important to note that non-probability samples are commonly used in social science research and they are primarily used due to their accessibility and proximity to the researcher. Additionally, participants who volunteered and decided to participate in this study had to do so willingly. This is due to the SONA system allowing students who are interested in participating in the study to take the survey if they wish to do so and by professors providing extra credit if they would like to participate in the study. The reason for using such technique was because there was not enough time to use a random sampling technique and because there were no means to print over two-hundred copies the survey.

Instrument

The survey questionnaire asked questions regarding victimization experience, Facebook® utilization, personal characteristics, and prevention measures. Questions were based on various Likert-type scales ranging from 1= Always to 5= Never, 1= Not Important to 3= Very Important, and 1= Not at all severe to 10= Extremely severe. Additionally, questions were answerable by yes/no, time ranges, and fill in the box. Various techniques were used to gain meaningful information to test the hypothesis. A sample of the questionnaire is found in Appendix A.

The survey was created to focus solely on Facebook® users and most of it was based on previous research/survey instruments. Back (2016), for instance, assessed a survey instrument that concentrated on determining what social networking sites were mostly used, the time spend online, the reasons a user engaged online, and the experiences users had. Incorporating some of Back's ideas aided in creating a valuable survey instrument given that the goal of this study was to determine the time a user spends online, if they are active online, and the victimization experiences they have had. Back's (2016) survey was an important tool in the creation of my survey instrument.

Prior to data from respondents, this study and its survey instrument was submitted for IRB approval. IRB approval is needed for any study involving human subjects (American University, 2015). An IRB ensures that the privacy and safety of the respondents are not violated in any way. It also ensures that informed consent form participants, or human subjects, is sought and that participation is voluntary. Because the study involved human subjects, informed consent forms were required for this study.

Hypothesis

The study had one core hypothesis followed by several sub-hypotheses:

Core hypothesis: Facebook® utilization (i.e., online activity and/or number of hours spent online) will impact online victimization, but such experience is moderated by the type of prevention measure (e.g., the number of mutual friends and the recognition of friend requests, and the degree of user control pertaining to what type of information they allow to be public or private).

H2: Individuals who review their security settings to ensure the public does not have access to his/her profile are less likely to be victims of cybercrime unlike individuals who do not review their privacy/security settings (degree of user control).

H3: Users' who constantly spend time on Facebook® are more likely to have experienced online victimization compared to individuals who spend less time on the Facebook®.

H4: Facebook® users who do not take the number of mutual friends (mutuality) into consideration are more likely to experience victimization than users who do not accept friend requests if they have a low number of mutual friends.

H5: Participants who do not recognize a user's profile picture or username and accept a friend request are more likely to experience victimization than users who take those elements into consideration (recognition).

MEASUREMENT

Dependent variable

The construct of "victimization experience" was measured using four dimensions: intensity, frequency, severity, and ever victimized. The questions pertaining to this construct were either binary, nominal or ordinal level measurements. Each question was answerable by a yes (1) or no (0) or a list of five to nine answer choices in order to obtain a better understanding of how many times they have experienced a cyber-victimization and the frequency and severity of their experience. An example of a questions is: "How many times in the past 12 months have you experienced victimization on Facebook®?" The reason a time frame of twelve months is used here is because Neuman (2011) states that a researcher is to avoid false premises, distant future intention questions, and should avoid asking question

beyond a respondent's capabilities. Additionally, most questions are answerable by a number to determine how long ago they experienced cybercrime victimization, how long it lasted, how many times they experienced it, and how severe their experience was. For example, participants are asked, "How long did it last?" (Recall this question is a follow-up to a yes or no question) and the answer choices range from "0 to 1 year," "1 to 2 years," "2 to 3 years," and so forth. Six types of cybercrimes are examined and asked specific questions in regards to the type of crime. An illustration of the type of questions asked is: "Has anyone ever threatened you by sending you fearful messages, pictures, videos, or spreading rumors or untruthful facts about you on Facebook®? (Cyberbullying/Harassment)." Each question like the example provided above were answerable by yes (1) or no (0).

Cybercrime Victimization Experience

Experience was measured using a dichotomous variable that pertains to the question "Have you ever experienced cyber victimization on Facebook®?" A yes was coded as 1 and a no was coded as 0. Any respondent who answered yes to any one of the six listed crimes was scored as 1.

Ever Victimized

For ever victimized, this dimension was a derived variable consisting of six out regional variables answerable by yes= 1, no= 0. To measure this dimension of experience six different questions were used to determine whether a respondent had experienced being hacked, was a victim of cyber-impersonation, cyberbullying, identity theft, an online romance scam, and/or online fraud on Facebook®. For instance, I asked questions to the nature of: "Has anyone ever threatened you by sending you fearful messages, pictures, videos, or spreading rumors or untruthful facts about you on Facebook®?" Each question

pertaining to the type of victimization questions asked were coded as 1= Yes or 0= No. The sum of the responses to the six listed items were calculated. I added them and the maximum total was six. The maximum number of six (6) indicated high victimization experience, and a minimum of zero (0) designated no victimization. Given these values, the level of measurement for this measure is at the ratio level of measurement since an absolute zero is a possible score.

Frequency of Experience

To measure frequency of experience I used the question: "How many times did you experience this type of cyber-crime?" This question was used for all six types of cybercrimes being examined if the respondent answered 1= yes. However, I calculated the midpoints of the interval level questions and used this as my ultimate measure of frequency. For example, for question 30, referenced above (refer to Appendix A), had four different answer choices. Respondents were able to answer: (1) 1 to 2, (2) 3 to 4; (3) 5 to 6, (4) 7+. In this case, since the midpoints were used, each answered response was recoded as: (1) 1.5, (2) 3.5, (3) 5.5, (4) 7; this was done to obtain the midpoint value.

Severity of Experience

To measure the severity of cybercrime victimization, I used the question: "Which of the following describes the severity of your victimization experience?" This question had four subset questions that determined whether a respondent had to consult with a medical doctor, report the incident to Facebook® to deactivate the account, had to report the incident to law enforcement, and/or if the respondent had to consult with a psychologist. The question was answerable by a Likert-type scale ranging from 1= Not at all severe to 10= Extremely severe making it a nominal level measurement. Each response category were added to

determine which type of cybercrime victimization was more severe. This was done by creating a severity index which we added the numbers listed for all four sub-set questions regarding the severity of the participant's experience.

Intensity of Experience

To measure intensity of victimization experience, I used the question "For how many years have you been using Facebook®?" This question was used for all six types of cybercrimes being examined if the respondent answered 1= yes. The question was answerable by writing in the number of years in a text box—making it a ratio level measurement.

Independent Variables

Control variables

I measured the construct of cybercrime victimization on Facebook® by using three main concepts. The first concept, personal characteristics had five subset variables being: age, gender, ethnicity, sexual orientation, and classification. These variables were measured using a nominal level of measurement except for age being an interval-ratio level. Age was determined based on the year the respondent was born; for example, 1990. Gender was coded as: Male (0); Female (1). Ethnicity had two nominal categories being: Hispanic (1); Non-Hispanic (0). Sexual orientation was coded as Heterosexual (1); Homosexual (2); Bisexual (3); Questioning (4). Lastly, classification was coded as: freshman (1), sophomore (2), junior (3), senior (4).

Facebook® Utilization

The second independent variable, Facebook® utilization, was measured using nine to eleven questions which were answerable using an ordinal or interval level of measurement

which were recoded into a ratio level of measurement. This independent variable was answerable by one of the following: yes (1); no (0), single text box, Monday (1), Tuesday (2), Wednesday (3), Thursday (4), Friday (5), Saturday (6), Sunday (7), or 0 to <20 minutes (1), 30 minutes to <1 hour (2), 1 hour to <2 hours (3), 2 hours to <3 hours (4), 3 to <4 hours (5), 4 hours+ (6). For some questions, responses would continue to: 4 hours to <5 hours (6), 5 hours+ (7). Other responses ranged from: only friends (private) (1), just me (2), everyone (public) (3) or close friends (1) to everyone (strangers) (7). The construct of Facebook® utilization had two sub concepts that of intensity and extensity. I measured Facebook® extensity of use by asking the question "For how many years have you been using Facebook®?" Extensity is a ratio level of measurement. On the other hand, the intensity of Facebook® use was measured by asking, "On average, how many hours/minutes a day do you spend on Facebook®?" From the categories given, I calculated the midpoint of each category and made the response itself a midpoint, the original coding was not used in the survey. The recode gave a semblance to a ratio level variable.

Prevention Measures

Prevention measures was measured by asking: How important are the following in accepting a Facebook® friend request? The questions were in regards to how important the number of mutual friends is, how many mutual friends must one have to accept a friend request, the importance of recognizing a user's profile and username, and what types of information they have set to private or public in regards to the degree of user control. The variable was answerable by: Not Important (1), Important (2), Very Important (3). If the number of mutual friends is important then participants were asked how many mutual friends they must have to accept a friend request. That questions were answerable by: 0 (1), 1-5 (2),

6-10 (3), 11+ (4). In regards to recognition, this construct was measured by asking a respondent: “How important is it to recognize a Facebook® user’s profile photo and username?” They were answerable by: Not Important (1), Important (2), Very Important (3). Lastly, the degree of user control was measured by asking respondents: “Who can view your: posts, videos, personal information, status updates, and photos?” These questions with the five categories were answerable by: Everyone (1) (Public), Only Friends (2) (Private). A copy of the survey questions is found in Appendix A.

Analytical Strategy

I used a generalized regression model meaning that I applied different types of regression link functions: binary logistic and normal error. For the binary dependent variable (1= Yes, 0= No), I used a binary, logistic regression approach. For the three sub-dependent variables (frequency, intensity, and severity) I applied a multiple linear regression analysis. For measurements of intensity, the response categories were recoded into midpoints, then a multiple linear regression model was applied. Using midpoints ensured that no valuable response data was lost as a result of the dichotomous variable.

Additionally, it is vital to mention that for the prevention measure of mutuality, I used a principal component analysis (PCA). A PCA is a statistical technique used to reduce the number of variables to a more parsimonious and trackable set of theoretical variables (PCs); these theoretical variables are linear combinations of the original variables. In other words, PCA is used to transform a large number of correlated variables into a smaller set of uncorrelated components (Alani, 2014). In this particular study, since the two dimensions of mutuality being number (1= 0, 2= 3, 3= 8, 4= 11+) and importance (1=Not important, 2=

Important, 3= Very Important) were fundamentally different in metrics, I could not use a simple average. Instead, PCA was used to combine both dimensions.

Chapter 4

Results

Overview

My conceptual framework casted four core constructs: (1) *personal characteristics*, (2) *prevention measures*, (3) *Facebook® utilization*, and (4) *online victimization experience*. Each of these constructs consisted of sub-dimensions. For instance, *personal characteristics* had the sub-dimensions of age, gender, ethnicity, sexual orientation, classification, and sex. *Prevention measures* had three sub-dimensions that of: (i) mutuality, (ii) recognition, and (iii) degree of user control. *Facebook® utilization* had the sub-dimensions of (i) intensity and (ii) extensity of utilization. Lastly, *victimization experience* had the sub-dimensions: ever victimized, and further conceptually split into intensity, frequency, and severity. The central hypothesis is: *Facebook® utilization* impacts *victimization experience* with the type of *prevention measure used* moderating the impact of Facebook® utilization on victimization experience. Put another way, it was predicted that prevention measures will condition the effect of Facebook® utilization on victimization experience.

Descriptive Statistics

My descriptive statistics results indicate that majority of respondents were female (74%), between ages 19 and 22, inclusive, and were mostly non-seniors in terms of student classification (53%). The reason that classification was recoded into a dummy variable 1= senior, 0= non-senior was a result of rather very uneven distribution among the classification's categories. In this recode, non-senior represents freshman, sophomores, and juniors, while the senior's category only represents seniors.

Although, it was initially imagined that there would be five sub-dimensions for *personal characteristics,* both data pertaining to ethnicity and sexual orientation could not be used in a meaningful way due to an empirical distribution that heavily represented Hispanic Americans, and heterosexuals. This is for the reason that 95% of respondents were Hispanics, and 94% were heterosexual which—in turn led to excluding both dimensions in the regression models. Excluding both ethnicity and sexual orientation was a necessary because if they would have been kept, the data would tilt more toward one category than other important measurements; thus, making estimates based on these variables unreliable due to the small sample sizes for these non-dominant categories.

In regards to Facebook® utilization, the majority of respondents stated they spent less than an hour a week on Facebook® (intensity; 34%) and had been using Facebook® for an average of six years (extensity; 23%). Focusing now on the moderating variables or prevention measures, in regards to the measurement of mutuality, most respondents found it very important (66%) to have mutual friends and indicated they needed to have between one and five friends 42%, in order to accept a friend request. When considering recognition, respondents found it to be not only important (46%) but, very important (46%) in being able to recognize a user's profile name. Additionally, respondents believed it was very important (56%) to recognize a user's profile photo to accept a friend request. Lastly, with respect to degree of user control, note that there were five items used to create the scale to measure user control: (i) posts, (ii) personal information, (iii) videos, (iv) photos, and (v) status updates. In examining the data further, only responses pertaining to posts and personal information could be used since there was a large number of missing values for the other three items. Most

respondents had their posts set to private (86%) and had their personal information set to public (68%). Descriptive statistics for variables of the study is given in Table 4.1.

Table 4.1 Descriptive Statistics

Independent Variables	Min.	Max.	M[1]	S.D.[2]
Age	20.50	27.0	23.3	2.63
Senior (1= Senior, 0= Non-Senior)	0.00	1.00	0.47	0.50
Male (1= Male, 0= Female)	0.00	1.00	0.26	0.44
Intensity (# of hours per week)	0.50	5.00	2.49	1.84
Extensity (# of years)	0.00	10.00	5.67	2.41
Importance of Mutual Friend (1= Not Imp, 2= Imp, 3= Very Imp)	1.00	3.00	2.56	0.67
Number of Mutual Friend (1=0, 2= 1-5, 3= 6-10, 4= 11+)	0.00	11.00	6.49	3.82
Recognition of User Name (1= Not Imp, 2= Imp, 3= Very Imp)	1.00	3.00	2.38	0.63
Recognition of User Profile Photo (1= Not Imp, 2= Imp, 3= Very Imp)	1.00	3.00	2.53	0.57
Posts (1= Public, 0= Private)	0.00	1.00	.142	0.35
Personal Information (1= Public, 0= Private)	0.00	1.00	.678	0.47

N= 209
[1] is the overall average.
[2] measures the amount of variation within the data values

Dependent Variable Overview

In exploring the dependent variable and its four sub-dimensions, it is best to begin by explaining what variables were used within the model. Examining the variables within the model will allow to determine whether or not there are predictors of victimization experience. The regression model used for all four sub-dimensions of victimization experience included the independent variables of age, sex, classification (personal characteristics), intensity, extensity (Facebook® utilization), degree of user control, mutuality, and recognition (prevention measures). These are used along with six interaction terms[1], namely: Intensity X Degree of user control, Intensity X Mutuality, Intensity X

Recognition, and Extensity X Degree of user control, Extensity X Mutuality, and Extensity X Recognition. These interaction terms represent the moderating effects of prevention measures on the relationships between Facebook® utilization and victimization experience.

In analyzing the dependent variable of ever victimized (Y_1), the entire sample size of n=209 respondents was used. For intensity (Y_2), severity (Y_3), and frequency (Y_4) of victimization only the n=95 respondents who have ever experienced online victimization were used. Beginning with ever victimized, (Y_1), a binary logistic regression analysis was performed because this dimension was answerable by 1=yes, 0=no (Table 4.2). For the remaining three dimensions frequency, intensity, and severity a multiple linear regression analyses was used (Appendix B).

Ever victimized (Y_1) revealed that the top three types of cybercrimes that Hispanic students at TAMIU experienced were cyber-bullying (27%), online romance scams (18%), and online fraud (10%). The 52% (n=95) who answered they have experienced online victimization will be applied to the multiple linear regression analysis models for intensity (Y_2), severity (Y_3), and frequency (Y_4).

Regression Results

Victimization Experience – For the outcome variable "ever victimized" (Y_1), the overall regression model was significant ($p<0.01$) (Table 4.2). The results associated with this model revealed no moderating effects. This means that there were no significant interaction terms. However, there were three significant variables: males ($p = 0.001$), intensity of Facebook® utilization (= 0.017), and degree of user control ($p = 0.019$). Since no interaction term was statistically significant, results mean that gender, intensity of Facebook® use, and degree of user control directly influence victimization experience. From the results,

the odds of males experiencing online victimization is 0.21 times [i.e, exp(B) = 0.21] that of females. Furthermore, results indicate that as the amount of time spent on Facebook® (intensity) increases by one hour per week, the odds of experiencing online victimization is magnified by 1.25 times [i.e., exp(B) =1.25].

For example, if one person spends 5 hours a day on Facebook® while another person only spends 4 hours a day engaging on Facebook®, the person who spends 1 hour more on Facebook® increases his/her odds of experiencing online victimization by 1.25x higher than the amount spent by the person who only uses Facebook® for 4 hours a day. Lastly, the model indicates that when considering degree of user control, the odds of individuals experiencing online victimization for those who have their privacy settings set to public, is almost 3X [exp(B) = 2.8] that of individuals who have their privacy settings set to private.

In Table 4.2, the terms that have to do with the moderation hypothesis (i.e. H2, H4, H5), were not significant at the 5% level. For example, the interaction between Facebook® intensity and prevention measure degree of user control, is not a significant term (Intensity X Degree of User Control: B = +.023; exp(B) = 1.023; p>.05). Additionally, the interaction between intensity and mutuality, is also not significant (Intensity X Mutuality: B = -0.272; exp(B) = .076; p>.05). The interaction term between Facebook® intensity and prevention measure recognition, is again not significant (B = -0.034; exp(B) = 0.967; p>.05). The remaining three interaction terms between Facebook® extensity and prevention measures degree of user control (Extensity X Degree of User Control: B = -0.202; exp(B) = 0.817; p>.05), mutuality (Extensity X Mutuality: B = +0.138; exp(B) = 1.148; p>.05), and recognition (Extensity X Recognition: B = -0.337; exp(B) = 0.714; p>.05) were not significant.

Table 4.2. Binary Logistic Regression for Ever Victimized				
independent variables	B	S.E.	exp(B)	p-value
	-2.667	1.625	0.069	.101
Age	-.096	.071	0.908	.176
Senior (1=senior, 0=not senior)	-.022	.374	0.978	.953
Male (1=male, 0=female)	-1.540	.459	0.214	.001**
Intensity of FB utilization (# in hours per week)	.228	.096	1.257	.017*
Extensity of FB utilization (# in years)	-.042	.094	0.959	.655
Degree of User Control (1= Public, 0= Private)	1.054	.448	2.868	.019*
Mutuality (PCA derived)[1]	-.071	.201	0.931	.724
Recognition (Mean derived)[2]	-.707	.487	0.493	.147
Intensity X Degree of User Control	.023	.112	1.023	.841
Intensity X Mutuality	-.272	.279	0.762	.330
Intensity X Recognition	-.034	.238	0.967	.887
Extensity X Degree of User Control	-.202	.235	0.817	.390
Extensity X Mutuality	.138	.093	1.148	.139
Extensity X Recognition	-.337	.238	0.714	.156
R^2	.207			
p-value	**.0100**			
df	152			
N=209				
[1] dervied by PCA of number (1= 0, 2= 3, 3= 8, 4= 11+; Midpoints) and importance (1,2,3).				
[2]derived by simple average; 1=Not Imp, 2=Imp, 3=Very Imp				

Frequency of Victimization Experience - On the other hand, when examining the frequency of victimization (Table 4.3), the model was found to be significant at the 5% type-I error rate (p = 0.0480). Findings tell us that in this particular model, there is a moderating variable and we will discuss this interaction term shortly. The unstandardized coefficients, B, indicates the change in the dependent variable per unit change of one independent variable holding all other independent variables in the model at constant value. The regression model for frequency of victimization experience indicates that (n = 95) respondents who stated they have experienced online victimization on Facebook®, males were 12.21 units higher to experience victimization experience than females (B=12.21; p =< .05). In addition, even though mutuality is significant (p =< .05), I take for granted and will focus instead on the

interaction term of Intensity X Mutuality (p =< .05) being that the interaction term—when significant—takes precedence over its component main effects (i.e., Intensity, and Mutuality) (see Table 4.2 and Figure 4.2).

In multiple linear regression analysis, the standardized coefficients are used to determine which independent variables are the most statistically important in determining the dependent variable (Nathan et al., 2012). A closer look at the results in Table 4.3, data indicates that gender (β= +0.268; p < .05) is a weaker predictor in determining whether an individual will experience online victimization compared to the main effect of mutuality (β= +0.299; p < .05) and the interaction term of intensity X mutuality (β= -0.299; p < .05).

Table 4.3. Multiple Linear Regression- Frequency

independent variables	Beta	B	S.E.	p-value
		37.071	17.654	.039
Age	-.168	-1.115	.797	.166
Senior (1=senior, 0=not senior)	.018	.591	4.042	.884
Male (1=male, 0=female)	.268	12.214	5.334	.025*
Intensity of FB utilization (# of hours per week)	-.168	-1.532	.959	.114
Extensity of FB utilization (# in years)	-.132	-1.065	.900	.240
Degree of User Control (1- Public, 0-Private)	.056	2.273	4.273	.596
Mutuality (PCA derived)[1]	.299	5.000	2.216	.027*
Recognition (Mean derived)[2]	-.012	-.447	4.683	.924
Intensity X Degree of User Control	-.086	-1.914	2.411	.430
Intensity X Mutuality	-.299	-2.807	1.143	.016*
Intensity X Recognition	.017	.394	2.809	.889
Extensity X Degree of User Control	.035	.742	2.290	.747
Extensity X Mutuality	-.075	-.550	.880	.534
Extensity X Recognition	.072	1.409	2.357	.552
R^2	.256			
Adjusted R^2	.117			
p-value of model	.0480			
df	89			
N=95				

[1] dervied by PCA of number (1= 0, 2= 3, 3= 8, 4= 11+; Midpoints) and importance (1,2,3).

[2] derived by simple average; 1=Not Imp, 2=Imp, 3=Very Imp

Figure 4.2 is a depiction of results found in Table 4.3 regarding the interaction term of intensity and mutuality. It shows that the lower an individual is in terms of mutuality, then the relationship between Facebook® utilization of intensity and the frequency of victimization experience gets ever stronger. By imagining the lines going counter clockwise, one can see that as the line moves from red to blue, meaning from high mutuality to low mutuality, then individuals who are low in mutuality (i.e. do not find it important to have mutual friends or do not have mutual friends before accepting a friend request) are more likely to experience a longer period of victimization. For those who are high in mutuality, that results show a weakening strength between Facebook® intensity of use and the frequency of victimization experience. This means that individuals who have a high number of friends, and believe that having mutual friends before accepting a friend request is important, will experience victimization for a shorter period of time. In other words, let's imagine a Facebook® user who does not take into consideration the number of friends he/she has with other friends on Facebook®. He/she receives a friend request, and accepts it. As a result of not finding it important to have mutual friends or finding the need of have a number of mutual friends before accepting a friend request, then the likelihood of a Facebook® user experiencing online victimization is longer whether it be in hours, days, weeks, months, or years.

Issues with Intensity and Severity Dimensions of Analysis

Directing focus to the intensity and severity dimensions, severity had to be eliminated due to the large amount of missing values. Since there was too many missing values, the analysis could not be completed without violating assumptions of the statistical test, thus rendering the results invalid as the threat to statistical conclusion validity is too high. The

dimension of intensity also could not be analyzed given none of the models were significant; therefore, it was not included in the regression analysis section.

Figure 4.2 will portray how the original conceptual framework resulted into the final theoretical model. The changes are due to empirical data findings.

Figure 4.1 Graph depicting the interaction between Intensity and Mutuality in relation to Frequency of Victimization

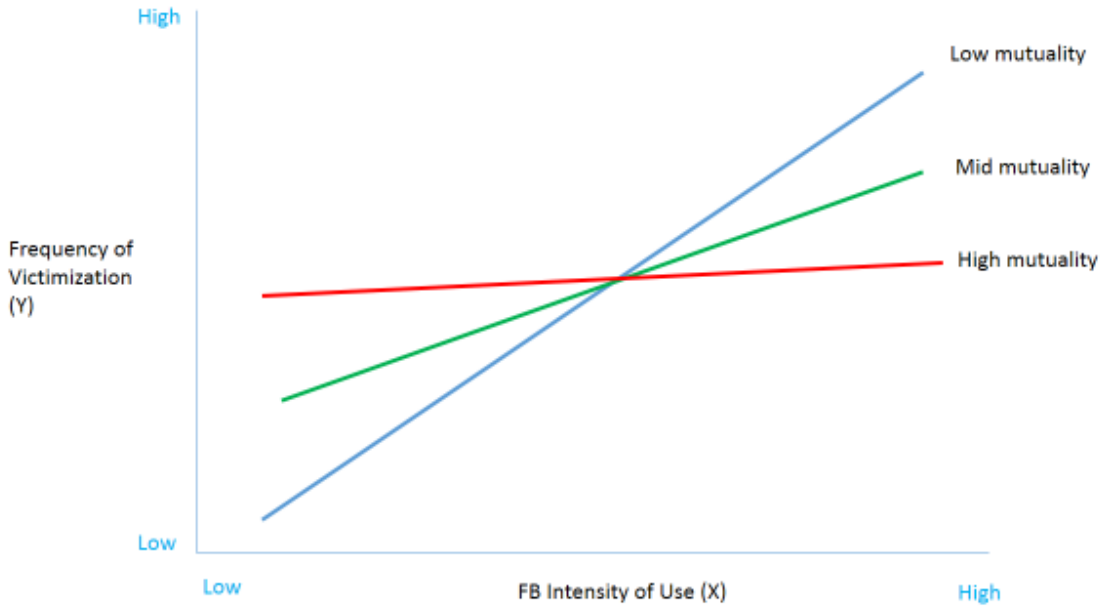
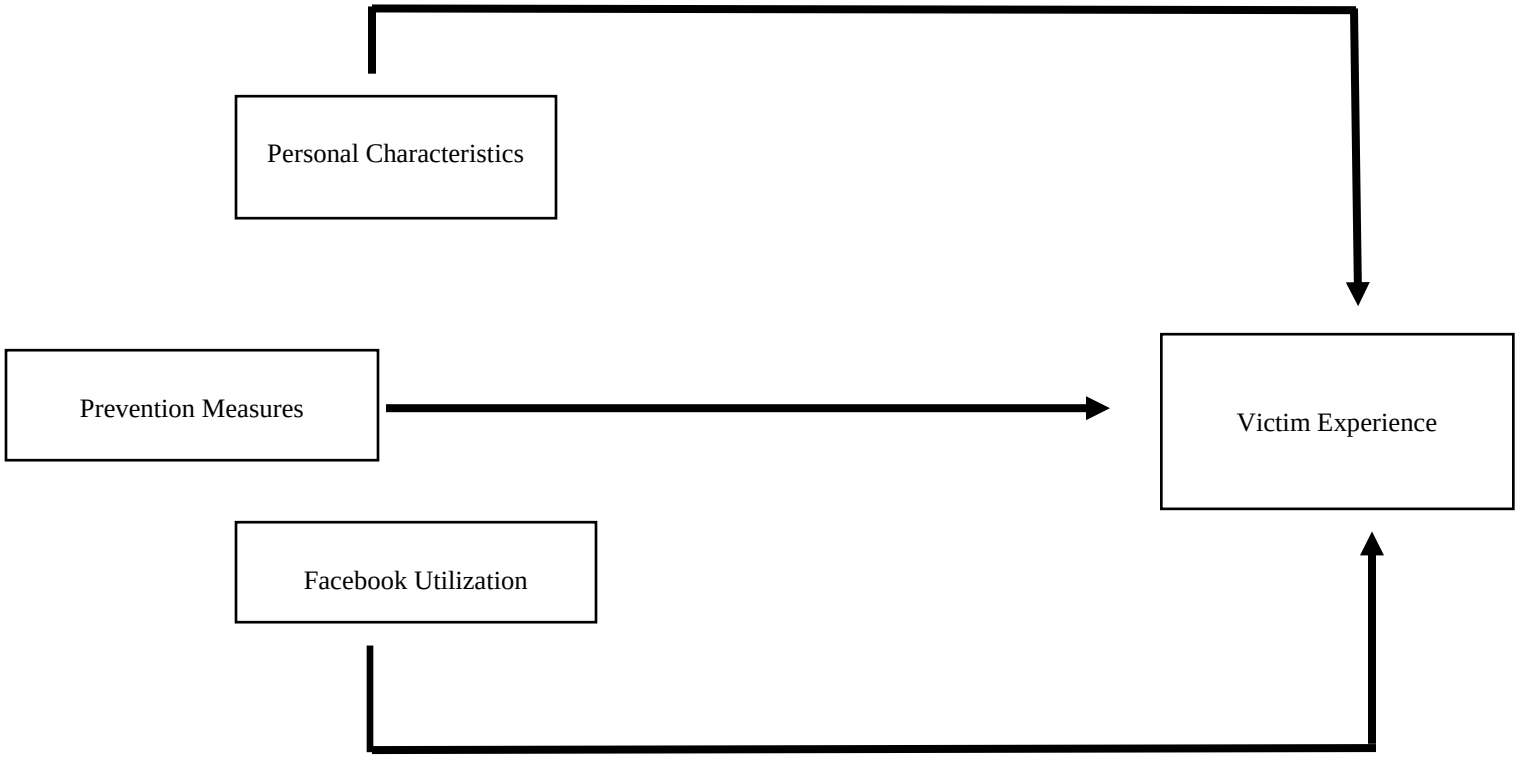


Figure 4.2 Recalibrated Theoretical Model



Chapter 5

Discussion

One of the main questions of this thesis was: "*does* Facebook® *utilization impact online victimization experience, and is such impact moderated by the type of prevention measure(s) used?*" With respect to the first part of this question, results suggest that the answer is yes. Results indicate that the amount of time a user spends online, increases the user's chances of experiencing online victimization. With respect to the second part of this question, the results suggest a more complicated picture. When "ever victimized" is considered, results suggest that there are no interaction/moderating terms that were significant. None of the prevention measures utilized had an influence on the relationship between Facebook® utilization and victimization experience. Furthermore, the findings show that Facebook® utilization directly affects victimization experience. In addition, prevention measures were also directly affecting victimization experience. This finding negated my core hypothesis, which posited that prevention measures would moderate the relationship between Facebook® utilization and victimization experience. Taking into account the measurement of extensity for the Facebook® utilization dimension, results suggest this not to be significant or important. Thus, the amount of time (e.g. years spent using Facebook®) is not important in predicting future victimization experience. While literature is silent on why this variable does not influence future victimization, one can surmise that this may be due to a fluctuation in use of Facebook® from one year to the next.

In regards to the frequency of victimization, the current data suggest that the most noteworthy finding was the interaction term of Intensity and Mutuality. Therefore, the prevention measure of mutuality moderated the relationship between Facebook® intensity of

utilization and the frequency of online victimization experience. Analysis indicated that as the importance of mutuality decreased, the positive relationship between intensity of Facebook® utilization and frequency of victimization became even stronger.

It can be concluded that individuals who spent more time online (Facebook®) are more likely to experience online victimization. The relationship between time spent online and victimization is consistent with the findings of of Marcum (2008) who found respondents who spent more time online increased their exposure to a motivated offender—then the greater the likelihood of experiencing online victimization. Thus, even though the internet and social media sites have had positive impacts on our daily lives, they have also increased the opportunities for crime to occur (Marcum, 2008). In considering gender, females were more likely than males to experience online victimization. The findings from the current research that females do in fact experience online victimization more than males is consistent with the extant literature (Marcum et al., 2012; Reyns et al., 2011).

In reflecting on degree of user control, previous research has not directly addressed the question of a relationship between privacy settings on social media and online victimization. The current research found that the odds of experiencing online victimization for individuals who have their privacy settings set to public are almost 3 times higher than those who have their privacy settings set to private, the study advances knowledge on this topic. Loong (2014) also found that in regards to Facebook® users, individuals who had their privacy settings set to public, were significantly related to cyber stalking. Additionally, Mathiyalakan, Heilman, and White (2012) and Williams et al., (2011) stated that individuals who had their privacy settings set to public were more vulnerable online as a result of disclosing information that could be harmful to the user.

Mutuality and recognition have never been applied to cybercrime victimization on Facebook®. Cruz-Cunha and Portela, (2015) examined the relationship between a person's privacy settings and the likelihood of accepting a friend request, but not the roles by which mutuality and recognition may play in determining the likelihood of experiencing online victimization. Cruz-Cunha and Portela, (2015) also found that individuals who did not have mutual friends, then the greater the chance they were to take risks online. The goal of Cruz-Cunha and Portela (2015) was to determine if users who take more risks were likely to share or reveal more information about themselves on Facebook®. The aim of the current research was to apply mutuality and recognition as a means to investigate whether these two dimensions have a relationship to that of victimization experience. The thought process behind deciding to create and use these two dimensions will be mentioned. For the measurements of mutuality and recognition, through personal experience of speaking with friends concerning who they tend to accept on Facebook® and why; I realized that it is of absolute importance to shed light upon what types of practices may lead to an increase in victimization experience. The prominence of defining whether or not mutuality and recognition play an important part in the likelihood of online victimization on Facebook® was due to determining what is considered before accepting or declining a friend request. Although there is no literature distinguishing why one accepts friend requests while others do not, research has focused on determining the risks users take online (Cruz-Cunha & Portela, 2015). Extant literature that focuses on what risks users take that lead to the type of information shared online brings forth wanting to know why one user may accept friend requests while others do not. As a result, that is why it was decided to incorporate the two new dimensions of—mutuality and recognition.

When applying these findings to LRAT, which contains three major elements: a motivated offender, a suitable target, and the lack of a capable guardian (Cohen & Felson, 1979), there are motivated offenders lurking social media—in this case, Facebook®; findings show that ninety-five respondents of the entire sample (n=209) experienced online victimization. When we take into account the potential target component, the findings supported literature because individuals who spent a large amount of time online, were more likely to experience online victimization (Reyns et al., 2011). The oversharing of personally identifiable information tends to also increased the likelihood of victimization experience since attractiveness increases when an individual posts personal information such as their: relationship status, e-mail addresses, sexual orientation, activities, photos, height, and weight (Reyns et al., 2011). The previous literature measures capable guardianship by acknowledging whether or not an individual has a firewall or a security program installed in their computer (Reyns et al., 2011). However, for the purposes of this study, the degree of use control dimension was used to measure the lack of a capable guardian element. The reason for this departure from the literature is because it is always the individual's decision to decide whether or not they want to install a firewall or a security program in their computer. So, applying the degree of user control dimension which also focuses on an individual *deciding* to set his/her privacy settings to public or private, it could be used to represent a lack of a capable guardian.

Finally, the results from the current study indicate that LRAT can be applied as an explanation of cybercrime victimization. Consistent with the extant research, this study shows that incorporating the three main elements of LRAT (a motivated offender, a suitable target, and the lack of a capable guardian) we can apply the theory to the explanation of

cybercrime victimization experience (see Holt & Bossler, 2009; Reyns, Henson, & Fisher, 2011; Yar, 2005; Taylor et al., 2006; Choi, 2008; Bossler & Holt, 2009; Ngo & Patermaster, 2011). Furthermore, the current findings offer support to a growing body of literature which suggests that when a motivated offender and a potential target intersect within a network, victimization is likely to take place (Reyns, 2013).

CHAPTER 6

CONCLUSION

Recap

In conclusion, cybercrime on social media sites is becoming more common (Illmer, 2016; George, 2014). As we enjoy the benefits of the advancements in technology, we must recognize that the opportunities of crime to occur increases online (Marcum, Higgins, Freiburger, & Ricketts, 2014). The research findings of the current research indicates that the core hypothesis (i.e. does Facebook® utilization impact online victimization experience and is such experience moderated by the type of prevention measure used) was found to be supported. But, when we consider the second part of the question: is victimization experience conditioned or moderated by the type of prevention measure used depends on the two different dimensions of ever victimized and frequency.

Considering the second hypothesis—it was indicated that individuals who review their privacy settings are less likely to become victims of cybercrime was found to be true for this population of Facebook® users. The dimension of prevention measures that has to do with degree of user control was found to be significant—stating that individuals who have their privacy settings set to public are more likely to experience online victimization than individuals who have their privacy settings set to private.

The third hypothesis stated that users' who constantly spend time on Facebook® are more likely to have experienced online victimization compared to individuals who spend less time on the Facebook®—this assumption too, was found to be supported. Considering the fourth statement that Facebook® users who do not take the number of mutual friends (mutuality) into consideration, are more likely to experience online victimization than users

who do not accept friend requests if they have a low number of mutual friends—this was found to be supported. Empirical data showed individuals who were low in mutuality did experience online victimization than individuals who had a high number of friends.

Lastly, the hypothesis that those who do not recognize a user's profile picture or a user's profile name and accept a friend request are more likely to experience victimization than users who take those elements into consideration—was found to be false or not supported. In addition, the recognition dimension was not found to be significant. Unfortunately, as stated previously, no literature determines why this may be the case, however, it may be linked to the fluctuations of use per year.

Moreover, the study along with other research found that LRAT can be applied in the attempt of explaining online victimization experience. The number of time one spends online, whether an individual has his/her privacy settings set to public, and being female all influence the likelihood of victimization experience. Taking into account a motivated offender, a suitable target based on attractiveness (oversharing of information and spending time online), and the lack of a capable guardian are important elements that determine the likelihood of victimization experience on Facebook®.

Policy Implications

As stated by literature, individuals who spend a great amount of time online tend to be the ones who experience online victimization (Bossler et al., 2012). Creating a solution to reduce the likelihood of individuals experiencing online victimization on social media outlets leads us to acknowledge campaigns and programs in place to reduce the likelihood of online victimization. As technology advances, so do the platforms of social media sites. Users should re-think how they engage with others in an online environment and how they are

keeping themselves safe from becoming victims of cybercrime. This study recommends users to become familiar with safe practices to reduce the likelihood of becoming victims. For instance, the Department of Homeland Security has a campaign blog titled *Stop.Think.Connect*. This blog assists online users to help them and their families stay safe while enjoying the benefits of technology (The Department of Homeland Security, 2016). In addition, there is a campaign named, *Take a Bite out of Cyber Crime*, which helps empower online users to protect themselves from online predators (CMO Council, 2016). These campaigns are implemented in the hope of increasing public awareness that cybercrime does exist and they should do everything in their power to battle against this growing criminal activity (CMO Council, 2016).

The focus of this research was online victimization experience on Facebook®. Therefore, a main recommendation from the findings of the current study is that, Facebook® users should become aware of a Facebook® prevention campaign that targets teenagers and their parents, but that could be beneficial to all. The resource is titled, the *Bullying Prevention Hub* which was developed by Facebook® in partnership with the Yale Center for Emotional Intelligence (Facebook®, 2016). This particular resource focuses mainly on cyberbullying and what teenagers, parents, and educators can do to prevent further victimization experience (Facebook®, 2016).

Incorporating various resources, becoming aware of different programs and campaigns with the goal of making users safe, this study recommends and encourages all users to become familiar with how one may continue to enjoy their time online while doing everything in their efforts to decrease the likelihood of experiencing online victimization. There are more programs, campaigns, and resources that online users can use and implement

in their daily lives. The social policy recommendations listed above are to assist users in the attempt of making them aware that there are ways to stay safe online, to avoid becoming victims of cybercrime.

Limitations

This study is not without limitations. The first limitation was the amount of missing values present within the data set for the dependent variable dimension of severity. The measurement could have been eliminated but after debating the pros and cons, I decided that it would be best to completely eliminate the variable. Briggs, Clark, Wolstenholme, and Clarke (2003) states that in cases of having a large amount of missing data for variables, then excluding them from the analysis is a beneficial option. Since, the dimension of severity would stand alone in the process of incorporating the multiple linear regression analysis approach, excluding this variable from the study did not affect further analysis for the study.

The second major detriment was that the external validity of this study is automatically threatened as a consequence of utilizing a non-probability convenience sampling technique. A convenience sampling technique is a method in which respondents are selected or voluntarily agree to partake in a research study due to their easy accessibility or proximity to the researcher (Etikan, Musa, & Alkassim, 2015). The fact that respondents who participated in this survey study were only either criminal justice or psychology students who volunteered to partake in this study—we cannot compare the results to that of other university findings. Results cannot be compared as a result of not having conducted a randomized, probability sampling technique that would include all students regardless of their field of study. Consequently, there are concerns with using a convenience sampling technique given that this type of sampling method is not to be representative of a populace,

and therefore, one is not to draw generalizations within a population or inferences about a population from a convenience sample (Etikan et al., 2015).

REFERENCES

Alani, A. S. A. (2014). Principal component analysis in statistics. Eastern Mediterranean University.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *Mis Quarterly*, *34*(3), 613-643.

Aricak, O. T. (2009). Psychiatric symptomatology as a predictor of cyberbullying among university students. *Eurasian Journal of Educational Research*, 34, 167-184.

Back, S. (2016). Empirical assessment of cyber harassment victimization via cyber-routine activities theory. *Master's Theses and Projects*. Bridgewater State University.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday Peer-Reviewed Journal on the Internet*, *11*(9). doi:10.5210/fm.v11i9.1394

Benotsch, E. G., Snipes, D. J., Martin, A. M., & Bull, S. S. (2013). Sexting, substance use, and sexual risk behavior in young adults. *Journal of Adolescent Health*, 52, 307-313.

Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, *3*(1), 400-420.

Bossler, A. M., Holt, T. J., May, D. C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, *44*(4), 500-523.

Brandl, S. G. (2014). Criminal investigation. SAGE Publications.

Briggs, A., Clark, T., Wolstenholme, J., & Clarke, P. (2003). Missing….presumed at random: Cost-analysis of incomplete data. *Health Economics*, *12*(5), 377-392.

Brodkin, J. (2010). Social networking hacks: Top 10 Facebook and Twitter security stories of 2009. Network World. Retrieved from: http://www.networkworld.com/article/224-1879/collaboration-social/social-networking-hacks--top-10-facebook-and-twitter-security-stories-of-2009.html

Burke, T., & Dickey, J. (2013). Manti Te'o's dead girlfriend, the most heartbreaking and inspirational story of the college football season, is a hoax. Deadspin.com. Retrieved from: http://deadspin.com/manti-teos-dead-girlfriend-the-most-heartbreaking-an-5976517

Cbsnews.com. (2015). Remembering Tyler Clementi. CBS Interactive Inc. Retrieved from: http://www.cbsnews.com/news/remembering-tyler-clementi/

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Chicago Tribune. (2011). Romanian man gets 4 years in Internet fraud case. Retrieved from: http://articles.chicagotribune.com/2011-06-29/news/chi-romanian-man-sentenced-in-internet-fraud-case-20110629_1_internet-fraud-adrian-ghighina-federal-prison-today

Cincinnati.com. (2009). Nude photo led to suicide: Family wants to educate teens about dangers of sexting. A Gannett Company. Retrieved from: http://archive.cincinnati.com/article/20090322/NEWS01/903220312/Nude-photo-led-suicide

CMO Council. (2016). Take a bite out of cybercrime campaign. The peer-powered network. Retrieved from: https://www.cmocouncil.org/media-center/press-releases/569

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, *44*(4), 588-608.

Cruz-Cunha, M. M., & Portela, I. M. (2015). *Handbook of research on digital crime, cyberspace security, and information assurance.* Advances in Digital Crime, Forensics, and Cyber Terrorism (ADCFCT) Book Series. IGI Global.

Cunningham, C. E., Chen, Y., Vaillancourt, T., Rimas, H., Deal, K., Cunningham, L. J., & Ratcliffe, J. (2015). Modeling the anti -cyberbullying prefer students: Adaptive choice *Aggressive behavior*, *41*(4), 369-385.

Davis, R. C., & Smith, B. (1994). Teaching victim's crime prevention skills: Can individuals lower their risk of crime. *Criminal Justice Review*, *19*(1), 56-68

Department of Homeland Security. (2016). Stop.Think.Connect. Campaign Blog. Retrieved from: https://www.dhs.gov/stopthinkconnect-campaign-blog

Department of Justice. (2014). San Antonio man sentenced to federal prison in aggravated identity theft and mail fraud scheme. The United States Attorney's Office. Western District of Texas. Retrieved from: http://www.justice.gov/usao-wdtx/pr/san-antonio-man-sentenced-federal-prison-aggravated-identity-theft-and-mail-fraud

Department of Justice. (2015). North Miami resident sentenced in stolen identity tax refund fraud scheme. The United States Attorney's Office. Southern District of Florida. Retrieved from: http://www.justice.gov/usao-sdfl/pr/north-miami-resident-sentenced-stolen-identity-tax-refund-fraud-scheme

Dilmac, B. (2009). Psychological needs as a predictor of cyber bullying: A preliminary report on college students. *Educational Sciences: Theory & Practice*, *9*(3), 1307-1325.

Dipert, R. R. (2010). The ethics of cyber warfare- Addressing new threats in the information age. Retrieved from: www.academia.edu/cyber_warfare

ESPN.com. (2013). Story of Manti Te'o girlfriend a hoax. College football, Notre Dame Fighting Irish. Retrieved from: http://espn.go.com/ncf/story/_/id/8851033/story-manti-teo-girlfriend-death-apparently-hoax

Eck, J. E., & Clarke, R. V. (2003). Classifying common police problems: A routine activity approach. *Crime prevention studies*, *16*, 7-40.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2015). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1-4.

Facebook. (2016). Bullying Prevention Hub. Retrieved from: https://www.facebook.com/safety/bullying/

Facebook Help Center. (2015). Advanced Privacy Controls. Retrieved from: https://www.facebook.com/help/466544860022370/?helpref=hc_fnav

Facebook Product/Service. (2012). Retrieved from: https://www.facebook.com/facebook/info/?tab=page_info

FBI Law Enforcement Bulletin. (2015). Bulletin report. Hate crime victimization statistics. Retrieved from: https://leb.fbi.gov/2015/april/bulletin-reports

Federal Bureau of Investigation. (2015). Identity theft. Retrieved from: https://www.fbi.gov/about-us/investigate/cyber/identity_theft

Federal Bureau of Investigation. (2015). Identity theft overview. Retrieved from: https://www.fbi.gov/about-us/investigate/cyber/identity_theft/identity-theft-overview

Federal Bureau of Investigation. (2014). Internet of things poses opportunities for cybercrime. Public Service Announcement. Retrieved from: http://www.ic3.gov/media/2015/150910.aspx

File, T., & Ryan, C. (2014). Computer and internet use in the United States: 2013. *American Community Survey Reports*. U.S. Department of Commerce. Economics and Statistics Administration.

Find Law. (2015). Fraud. Retrieved from: http://criminal.findlaw.com/criminal-charges/fraud.html

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal violence, 19*(4), 468-483.

Foderaro, L., W. (2010). Private moment made public, then a fatal jump. New York Times. Retrieved from: http://www.nytimes.com/2010/09/30/nyregion/30suicide.html?_r=0

Frailing, K., & Harper, D. W. (2013). *Fundamental of criminology: New dimensions.* Carolina Academic Press. Durham, N.C.

George, P. (2012). Men charged with impersonating Austin women online to damage their reputations. Statesman. Retrieved from: http://www.statesman.com/news/news/local-/men-charged-with-impersonating-austin-women-online/nRmGL/

George, T. (2014). The next big cybercrime vector: Social media. Retrieved from: http://-www.securityweek.com/next-big-cybercrime-vector-social-media

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*. *2*(1), 13-20.

Gutman, M., & Tienabeso, S. (2013). Timeline of Manti Te'o girlfriend hoax story. Abcnews.com. Retrieved from: http://abcnews.go.com/US/timeline-manti-teo-girlfriend-hoax-story/story?id=18268647

Halder, D., & Jaishankar, K. (2011). Cyber crime and the victimization of women: Laws, rights, and regulations. Hershey, PA, USA: IGI Global.

Henson, B., Reyns, B. W., & Fisher, B. S. (2011). Security in the 21st century: Examining the link between online social network activity, privacy, and interpersonal victimization. *Criminal Justice Review, 36*(3), 253-268.

Hindelang M. J., Gottfredson M. R., Garofalo J. (1978). Victims of personal crime: An empirical foundation for a theory of personal victimization. Cambridge, MA: Ballinger.

Hinduja, S., & Patchin, J. W. (2007). Personal information of adolescents on the internet: A quantitative content analysis of Myspace. *Journal of Adolescence*, 125-146.

Hinduja, S., & Patchin, J. W. (2007). Offline consequences of online victimization: School violence and delinquency. *Journal of School Violence, 6*(3), 89-112.

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior*, 29, 129-156.

Hinduja, S. & Patchin J. W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research, 14*(3), 206-221.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30, 1-25.

Huffingtonpost.com. (2010). Jessica Logan suicide: Parents of dead teen sue school, friends over sexting harassment. Retrieved from: http://www.huffingtonpost.com/2009/-12/07/jessica-logan-suicide-par_n_382825.html

Identity Guard Resource Center. (2015). Why your college student is especially vulnerable to identity theft. Retrieved from: http://www.identityguard.com/identity-theft-resources/articles/why-your-college-student-is-especially-vulnerable-to-identity-theft/

Illmer, A. (2016). Social media: A hunting ground for cybercriminals. BBC News. Retrieved from: http://www.bbc.com/news/business-36854285

Instagram. (2013). Retrieved from: https://www.instagram.com/about/legal/terms/api/

Internet Crime Complaint Center. (2014). Federal Bureau of Investigations. Retrieved from: https://www.fbi.gov/news/news_blog/2014-ic3-annual-report

Internal Revenue Service. (2015). Examples of identity theft investigations- Fiscal year 2015. IRS.gov. Retrieved from: https://www.irs.gov/uac/Examples-of-Identity-Theft-Investigations-Fiscal-Year-2015

Jensen, G. F., & Brownfield, D. (1986). Gender, lifestyles, and victimization: Beyond routine activity. *Violence and Victims*, *1*(2), 85-99.

Jordan, T., & Taylor, P. (1998). A sociology of hackers. *The Sociological Review*, *46*(4), 757-780.

Kabay, M. E. (2013). Understanding studies and surveys of computer crime. *Computer Security Handbook.*

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research*, *13*(1), 41-69.

Keller, M. (2013). Social media and interpersonal communication. *Social Work Today*, *13*(3), 10.

Lee, J. (2015). Woman shares ‘horrific’ online impersonation story. KHOU.com Retrieved from: http://www.khou.com/story/news/crime/2015/07/29/woman-shares-horrific-online-impersonation-story/30840047/

Legal Information Institute. (2015). Computer and internet fraud. Cornell University Law School. Retrieved from: https://www.law.cornell.edu/wex/computer_and_internet-_fraud#

Lenhart, A., Purcell, K., Smith, A., & Zichuhr, K. (2010). Social media & mobile internet use among teens and young adults. Retrieved from: http://www.pewinternet.org/files/old-media/Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report_Final_with_toplines.pdf

Lindsay, M., & Krysik, J. (2012). Online harassment among college students. *Information, Communication, & Society*, *15*(5), 703-719.

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. Retrieved from: http://www.ccs.neu-.edu/home/amislove/publications/Privacy-IMC.pdf

Loong, A. C. J. (2014). *Cyberstalking on Facebook: Examining the relationship between Facebook usage characteristics and cyber stalking victimization among young Malaysian Facebook users* (Doctoral dissertation, Department of Internet Engineering and Computer Science, Faculty of Engineering and Science, Universiti Tunku Abdul Rahman).

MacDonald, C. D., & Roberts-Pittman, B. (2010). Cyberbullying among college students: Prevalence and demographic differences. *Procedia-Social and Behavioral Sciences,* 9, 2003-2009.

Mallonee, M. K. (2014). Georgia man goes to prison in $50 million online fraud case. CNN.com. Retrieved from: http://www.cnn.com/2014/11/13/justice/georgia-man-prison-online-fraud/

Mann, B. L. (2015). Social networking websites- A concatenation of impersonation, denigration, sexual and aggressive solicitation, cyber-bullying and happy slapping videos. Privacy in the Information Society, 493-503. The Library of Essays on Law and Privacy. London, U.K. Ashgate Publishing. Retrieved from: http://www.ucs.mun-.ca/~bmann/0_ARTICLES/Mann_Social_Netg_PrivInfoSoc_15.pdf

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology*, 2(2), 346-367.

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381-410.

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2012). Battle of the sexes: An examination of male and female cyber bullying. *International Journal of Cyber Criminology*, *6*(1), 904.

Marcum, C. D., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2014). Exploration of the cyberbullying victim/offender overlap by sex. *American Journal of Criminal Justice*, *39*(3), 153-548.

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review*, *35*(4), 412-437.

Mathiyalakan, S., Heilman, G., & White, S. (2013). Gender differences in student attitude toward privacy in Facebook. *Communications of the IIMA, 13*(4), 35-44.

Milanovic, R. (2015). The world's 21 most important social media sites and apps in 2015. Social Media Today. Retrieved from: http://www.socialmediatoday.com/social-networks/2015-04-13/worlds-21-most-important-social-media-sites-and-apps-2015

Milivojevic, S., & McGovern, A. (2014). The death of Jill Meagher: Crime and punishment on social media. *Crime Justice Journal*, *3*(3), 22-39.

Moretti, L., & Ciotta, R. (2015). Local woman loses $50k in online romance scam. WIVB4.com. Retrieved from: http://wivb.com/investigative-story/local-woman-loses-50k-in-online-romance-scam/

Munson, L. (2015). Facebook spammer Sanford Wallace guilty of sending 27 million messages. Retrieved from: https://nakedsecurity.sophos.com/2015/08/26/facebook-spammer-sanford-wallace-guilty-of-sending-27-million-messages/

Myrstol, B. A., & Chermak, S. M. (2005). Victimology. Chapter 15. Retrieved from: http://wps.ablongman.com/wps/media/objects/1893/1938583/CH_15_web.pdf

National Crime Victim Law Institute (NCVLI). (2010). What is "online fraud"? Protecting, enforcing, & advancing victims' rights. Retrieved from: https://law.lclark.edu/live-/news/6855-what-is-online-fraud

National Cyber Security Alliance. (2015). Social networks. Staysafeonline.com. Retrieved from: https://www.staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks

Neuman, L. W. (2011). Social research methods: Qualitative and quantitative approaches. *Pearson*. 7th Edition.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Nichols, S. (2015). Spanking Spam King: Sanford Wallace faces jail for Facebook flood. Retrieved from: http://www.theregister.co.uk/2015/08/25/spammer_wallace_faces-_jail_facebook_scam/

NoBullying.com. (2015). Jessica Logan- The rest of the story. Retrieved from: http://nobu-llying.com/jessica-logan/

Norton by Symantec. (2015). What is cybercrime? Retrieved from: http://us.norton.com-/cybercrime-definition

Oluga, S. O., Ahmad, A. B. H., Alnagrat, A. J. A., Oluwatosin, H. S., Sawad, M. O. A., & Muktar, N. A. B. (2014). An overview of contemporary cyberspace activities and the challenging cyberspace Crimes/Threats. *International Journal of Computer Science and Information Security, 12*(3), 62-100. Retrieved from: http://search.proquest.com/-docview/1534315580?accountid=7081

Palmiotto, M. J. (2015). Combating human trafficking: A multidisciplinary approach. CRC Press. Taylor & Francis Group.

Parker, I. (2012). The story of a suicide: Two college roommates, a webcam, and a tragedy. The New Yorker. Retrieved from: http://www.newyorker.com/magazine/2012/02/06-/the-story-of-a-suicide

Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and self-esteem. *Journal of School Health, 80*(12), 614-621.

Perrin, A., & Duggan, M. (2015). Americans' internet access: 2000-2015. As internet use nears saturation for some groups, a look at patterns of adoption. *Pew Research Center*. Retrieved from: http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/

Pratt, T. C., Holfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267-296.

Reisig, M. D., Pratt, T. C., & Holtfreter, K. (2009). Perceived risk of internet theft victimization examining the effects of social vulnerability and financial impulsivity. *Criminal Justice and Behavior, 36*(4), 369-384.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyber lifestyle-routine activities theory to cyber stalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149-1169.

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior, 33*(1), 1-25.

Reyns, B. W. (2013). Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offenses. *Journal of Research in Crime & Delinquency*, *50*(2), 216-238. doi: 10.1177/0022427811425539

Sanger, D. E., & Perlroth, N. (2015). Iranian hackers attack state dept. via social media accounts. The New York Times. Retrieved from: http://www.nytimes.com/2015-/11/25/world/middleeast/iran-hackers-cyberespionage-state-department-social-media.html?_r=0

Schenk, A. M., & Fremouw, W. J. (2012). Prevalence, psychological impact, and coping of cyberbully victims among college students. *Journal of School Violence*, *11*(1), 21-37.

Schwartz, J. (2010). Bullying, suicide, punishment. *The New York Times*, 3.

Serious Fraud Office (SFO). (2015). What is fraud? Retrieved from: http://www.sfo.gov.uk-/fraud/what-is-fraud.aspx

Smith, C. (2016). By the numbers: 200+ amazing Facebook statistics. Digital Stats/Gadgets (DMR). Retrieved from: http://expandedramblings.com/index.php/by-the-numbers-17-amazing-facebook-stats/

Social Security Administration. (2015). Identity theft and your social security number. USA. Retrieved from: https://www.ssa.gov/pubs/EN-05-10064.pdf

Sona Systems. (2016). Retrieved from: https://www.sona-systems.com/about.aspx

Sugarmann, J. (2014). Murder rate for Hispanics is twice the murder rate for whites. Retrieved from: http://www.huffingtonpost.com/josh-sugarmann/murder-rate-for-hispanics_b_5309973.html

T&M Protection Resources (2014). Cyber identity theft and impersonation. Retrieved from: www.tmprotection.com

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., & Liederbach, J. (2006). Digital Crime and Digital Terrorism. Upper Saddle River, NJ: Pearson Prentice Hall.

Tillyer, M. S., & Eck, J. E. (2009). Routine activities. In J. M. Miller (Ed.), 21st century criminology: A reference handbook (pp. 279-287). Thousand Oaks, CA: Sage.

The Tyler Clementi Foundation. (2014). Tyler's story. Tylerclementi.org. Retrieved from: http://www.tylerclementi.org/tylers-story

The United States Department of Justice. (2015). Identity Theft. Retrieved from: http://-www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

Trend Micro.com. (2015). How to improve your privacy and security on social media. Security News. Retrieved from: http://www.trendmicro.com/vinfo/us/security-/news/online-privacy/how-to-improve-your-privacy-and-security-on-social-media

Twitter Help Center. (2015). Retrieved from: https://support.twitter.com/categories/282#

U.S. Immigration and Customs Enforcement. (2014). Cybercrime ring member responsible for $50 million in online identity theft sentenced. Financial Crimes. Retrieved from: https://www.ice.gov/news/releases/cybercrime-ring-member-responsible-50-million-online-identity-theft-sentenced

United States Census Bureau. (2015). QuickFacts. Laredo city, Texas. Retrieved from: https://www.census.gov/quickfacts/table/PST045216/4841464,00

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law Computers & Technology, 22*(1-2), 45-63.

Whitty, M. T., & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *CyberPsychology, Behavior, and Social Networking, 15*(3), 181-183.

Williams, J., Field, C., & James, K. (2011). The effects of a social media policy on pharmacy students' Facebook security settings. *American Journal of Pharmaceutical Education, 75*(9), 1-6, Article 177.

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2007). Does online harassment constitute bullying? An exploration of online harassment by known peers and online-only contacts. *Journal of Adolescent Health, 41*(6), S51-S58.

Wright, M. F., & Li, Y. (2012). Kicking the digital dog: A longitudinal investigation of young adults' victimization and cyber-displaced aggression. *Cyberpsychology, Behavior, and Social Networking*, *15*(9), 448-454.

Yar, M. (2005). The novelty of "cybercrime": An assessment in light of routine activity theory. *European Journal of Criminology*, *2*(4), 407-427.

Ybarra, M., Boyd, D., Korchmaros, J., & Oppenheim, J. (2012). Defining and measuring cyberbullying within the larger context of bullying victimization. *J Adolesc Health*, 51(1), 53-58.

Zhang, A. T., Land, L. P. W., & Dick, G. (2010). Key influences of cyberbullying for university students. *Pacific Asia Conference on Information Systems (PACIS)*, Paper 83, 1-12.

Appendix A: Survey

1. In what year were you born? (enter 4-digit birth year; for example, 1976)

2. What is your gender?
    - Female
    - Male
3. What is your sexual orientation?
    - Heterosexual
    - Homosexual (i.e. Gay; Lesbian)
    - Bisexual
    - Questioning
4. What is your ethnicity?
    - Hispanic
    - Non-Hispanic
5. What is your classification?
    - Freshman
    - Sophomore
    - Junior
    - Senior
6. Do you currently have a Facebook account?
    - Yes
    - No
7. Are you active on Facebook? (E.g. comment, post, share, like picture/videos/etc.)
    - Yes
    - No
8. How many friends do you have on Facebook?

9. For how many years have you been using Facebook?

10. One average, how many hours/minutes a day do you spend on Facebook?

    - 0 to <1 hour
    - 1 hour to <2 hours
    - 2 hours to <3 hours
    - 3 hours to <4 hours
    - 4 hours+
11. In a typical week, about how many hours/minutes do you actively engage (E.g. personal messaging, chatting, liking, and replying) on Facebook?
    - 0 to <1 hour
    - 1 hour to <2 hours

- 2 hours to <3 hours
- 3 hours to <4 hours
- 4 hours to <5 hours
- 5 hours+

12. The following questions will determine how often you use Facebook.

	Always	Most of the time	Sometimes	Once in a while	Never
How often do you log onto Facebook at work?	o	o	o	o	o
How often do you log onto Facebook at school?	o	o	o	o	o
How often do you log onto Facebook at home?	o	o	o	o	o

13. At what time of the day do you log onto Facebook?
    - 6:00 a.m. to 8:59 a.m.
    - 9:00 a.m. to 11:59 a.m.
    - 12:00 p.m. to 2:59 p.m.
    - 3:00 p.m. to 5:59 p.m.
    - 6:00 p.m. to 8:59 p.m.
    - 9:00 p.m. to 11:59 p.m.
    - 12 a.m. to 2:59 a.m.
    - 3:00 a.m. to 5:59 a.m.
14. These items will determine which days of the week you are most likely and less likely to be on Facebook.

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
Which day of the week are you most likely to be on Facebook?	o	o	o	o	o	o	o
Which day of the week are you second most likely to be on Facebook?	o	o	o	o	o	o	o
Which day of the week are you least likely to be on Facebook?	o	o	o	o	o	o	o
Which day of the week are you second least likely to be on Facebook?	o	o	o	o	o	o	o

15. In accepting a Facebook request, how important is having mutual friends?
    - Not Important
    - Important
    - Very Important
16. How many mutual friends do you have to have in order to accept a friend request?
    - 0
    - 1-5
    - 6-10
    - 11+

17. How important are the following in accepting a Facebook friend request?

	Not Important	Important	Very Important
In accepting a Facebook request, how important is having to recognize a user's profile name?	O	O	O
In accepting a Facebook request, how important is having to recognize a user's profile photo?	O	O	O

18. Whose friend request(s) do you tend to accept? (Please select all that apply).
    - o Close Friends
    - o Acquaintances
    - o Family members
    - o People you only met once
    - o Classmates
    - o Co-workers
    - o Everyone (strangers)
19. Who can view your:

	Only friends (Private)	Everyone (Public)
Posts	O	O
Videos		O
Photos	O	O
Status Updates	O	O
Personal Information (D.O.B., address, phone number, etc.)	O	O

20. Have you ever changed certain privacy/security setting on Facebook? Check all that apply in regards to changing such settings.
    - o Browse Facebook on a secure connection
    - o Set people who can look you up to only "friends"
    - o Enabled Login Notifications (to be alerted when you or someone else has logged on to your Facebook account from another device/laptop/etc., through text or e-mail)
    - o Have used one time passwords- Login Approvals (used when you have logged in from another device; a code will be sent to you via text)
    - o Changed who can see your timeline (e.g. only me; only friends)
    - o Have used remote sign out (Signed-out from another device you logged into in order to log out from another location)
    - o Set up a list of trusted contacts (e.g. you have approved certain friends to help you access your account when need be)
    - o You have changed your inbox filer from basic to strict filtering
    - o You have changed who can tag you on posts (e.g. only friends)
    - o You have blocked a certain user(s)
    - o You have added friends to your "restricted list"
21. Have you ever had your personal information stolen on Facebook? (Hacked)

- Yes
- No

22. How long ago did this take place?
    - 0 to 1 year
    - 1 to 2 years
    - 2 to 3 years
    - 3 to 4 years
    - 5+ years
23. How long did it last?
    - < than 2 weeks
    - < than 1 month
    - < than 3 months
    - < than 6 months
    - < than 10 months
    - < than 1 year
    - 1 to <2 years
    - 2 to <3 years
    - 3+ years
24. How many times did you experience this type of cyber-crime? (Hacking)
    - 1 to 2
    - 3 to 4
    - 5 to 6
    - 7+
25. Which of the following describes the severity of your victimization experience? (1 being not at all severe and 10 being extremely severe).

	1	2	3	4	5	6	7	8	9	10
You had to consult with a medical doctor.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to Facebook to deactivate the account.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to law enforcement.	O	O	O	O	O	O	O	O	O	O
You had to consult with a psychologist.	O	O	O	O	O	O	O	O	O	O

26. Has anyone ever used your pictures, videos, personal information, or etc. without your permission? (Cyber Impersonation)
    - Yes
    - No
27. How long ago did this take place?
    - 0 to 1 year
    - 1 to 2 years

- 2 to 3 years
- 3 to 4 years
- 5+ years

28. How long did it last?
    - < than 2 weeks
    - < than 1 month
    - < than 3 months
    - < than 6 months
    - < than 10 months
    - < than 1 year
    - 1 to <2 years
    - 2 to <3 years
    - 3+ years
29. How many times did you experience this type of cyber-crime? (Cyber Impersonation)
    - 1 to 2
    - 3 to 4
    - 5 to 6
    - 7+
30. Which of the following describes the severity of your victimization experience? (1 being not at all severe and 10 being extremely severe).

	1	2	3	4	5	6	7	8	9	10
You had to consult with a medical doctor.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to Facebook to deactivate the account.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to law enforcement.	O	O	O	O	O	O	O	O	O	O
You had to consult with a psychologist.	O	O	O	O	O	O	O	O	O	O

31. Has anyone ever threatened you by sending you fearful messages, pictures, videos, or spreading rumors or untruthful facts about you on Facebook? (Cyber-bullying/Harassment)
    - Yes
    - No
32. How long ago did this take place?
    - 0 to 1 year
    - 1 to 2 years
    - 2 to 3 years
    - 3 to 4 years
    - 5+ years
33. How long did it last?

- o < than 2 weeks
- o < than 1 month
- o < than 3 months
- o < than 6 months
- o < than 10 months
- o < than 1 year
- o 1 to <2 years
- o 2 to <3 years
- o 3+ years

34. How many times did you experience this type of cyber-crime? (Cyber-bullying/Harassment)
    - o 1 to 2
    - o 3 to 4
    - o 5 to 6
    - o 7+
35. Which of the following describes the severity of your victimization experience? (1 being not at all severe and 10 being extremely severe).

	1	2	3	4	5	6	7	8	9	10
You had to consult with a medical doctor.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to Facebook to deactivate the account.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to law enforcement.	O	O	O	O	O	O	O	O	O	O
You had to consult with a psychologist.	O	O	O	O	O	O	O	O	O	O

36. Has anyone deceived you into believing they were someone they were not, in order to get closer to you and to gain emotional feelings for him/her? (Online Romance Scam)
    - o Yes
    - o No
37. How long ago did this take place?
    - o 0 to 1 year
    - o 1 to 2 years
    - o 2 to 3 years
    - o 3 to 4 years
    - o 5+ years
38. How long did it last?
    - o < than 2 weeks
    - o < than 1 month
    - o < than 3 months
    - o < than 6 months

- o < than 10 months
- o < than 1 year
- o 1 to <2 years
- o 2 to <3 years
- o 3+ years

39. How many times did you experience this type of cyber-crime? (Online Romance Scam)
    - o 1 to 2
    - o 3 to 4
    - o 5 to 6
    - o 7+
40. Which of the following describes the severity of your victimization experience? (1 being not at all severe and 10 being extremely severe).

	1	2	3	4	5	6	7	8	9	10
You had to consult with a medical doctor.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to Facebook to deactivate the account.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to law enforcement.	O	O	O	O	O	O	O	O	O	O
You had to consult with a psychologist.	O	O	O	O	O	O	O	O	O	O

41. Has someone ever tried to steal your identity by making a fake profile on Facebook with accurate personal information? (Identity Theft)
    - o Yes
    - o No
42. How long ago did this take place?
    - o 0 to 1 year
    - o 1 to 2 years
    - o 2 to 3 years
    - o 3 to 4 years
    - o 5+ years
43. How long did it last?
    - o < than 2 weeks
    - o < than 1 month
    - o < than 3 months
    - o < than 6 months
    - o < than 10 months
    - o < than 1 year
    - o 1 to <2 years
    - o 2 to <3 years

- o 3+ years

44. How many times did you experience this type of cyber-crime? (Identity Theft)
    - o 1 to 2
    - o 3 to 4
    - o 5 to 6
    - o 7+
45. Which of the following describes the severity of your victimization experience? (1 being not at all severe and 10 being extremely severe).

	1	2	3	4	5	6	7	8	9	10
You had to consult with a medical doctor.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to Facebook to deactivate the account.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to law enforcement.	O	O	O	O	O	O	O	O	O	O
You had to consult with a psychologist.	O	O	O	O	O	O	O	O	O	O

46. Have you experienced fraud as a result of opening a link on Facebook, and purchasing something online? (Online Fraud)
    - o Yes
    - o No
47. How long ago did this take place?
    - o 0 to 1 year
    - o 1 to 2 years
    - o 2 to 3 years
    - o 3 to 4 years
    - o 5+ years
48. How long did it last?
    - o < than 2 weeks
    - o < than 1 month
    - o < than 3 months
    - o < than 6 months
    - o < than 10 months
    - o < than 1 year
    - o 1 to <2 years
    - o 2 to <3 years
    - o 3+ years
49. How many times did you experience this type of cyber-crime? (Online Fraud)
    - o 1 to 2
    - o 3 to 4
    - o 5 to 6

- o 7+

50. Which of the following describes the severity of your victimization experience? (1 being not at all severe and 10 being extremely severe).

	1	2	3	4	5	6	7	8	9	10
You had to consult with a medical doctor.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to Facebook to deactivate the account.	O	O	O	O	O	O	O	O	O	O
You had to report the incident to law enforcement.	O	O	O	O	O	O	O	O	O	O
You had to consult with a psychologist.	O	O	O	O	O	O	O	O	O	O

51. How many times in the past 12 months have you experienced victimization on Facebook?
    - o 1
    - o 2
    - o 3
    - o 4
    - o 5+
52. Did you change any online behavior on Facebook as a result of your victimization experience? If so, please select all that apply.
    - o Stopped using Facebook
    - o Deactivated Facebook account
    - o Changed privacy/security settings to private
    - o Made a new Facebook account
    - o Kept same Facebook account but changed password
    - o None.
53. The following questions focus on the aftermath of your victimization experience.

	Yes	No
Did you suffer from depression?	O	O
Did you feel lonely?	O	O
Did you suffer from anxiety?	O	O
Did you experience Post-traumatic Stress Disorder (PTSD)?	O	O
Did you experience headaches, nightmares, and/or insomnia?	O	O
Did you have difficulty having relationships with others in an online setting?	O	O
Do you fear being victimized again?	O	O
Did you seek medical attention?	O	O
Did you seek counseling?	O	O

54. The following questions will determine how confident you are that Facebook was the source of your victimization experience.

	Not at all confident	Somewhat confident	Very confident
How confident are you that Facebook was the source of your victimization experience?	○	○	○
If you are not confident, how confident are you that Facebook was a contributing factor to your victimization experience?	○	○	○

Appendix B: Frequency Tables

Table 1. Respondent's age group distribution

Age group	Count	%	Cumulative %
19-22 (1)	87	43.3	43.3
23-26 (2)	70	34.8	78.1
> 27 (3)	44	21.9	100.0
Total	201	100.0	

Table 2. Respondent's gender group distribution

Gender	Count	%	Cumulative %
Female-0	153	74.3	74.3
Male-1	53	25.7	100.0
Total	206	100.0	

Table 3. Respondent's classification group distribution

Classification	Count	%	Cumulative %
Not Senior-0	110	53.1	53.1
Senior-1	97	46.9	100.0
Total	207	100.0	

Table 4. Respondent's intensity (time spent online) group distribution

Intensity	Count	%	Cumulative %
0 to <1 hr	70	34.5	34.5
1 hr to 2 hr	32	15.8	50.2
2 hr to 3 hr	16	7.9	58.1
3 hr to 4 hr	22	10.8	69.0
4 hr to 5 hr	18	8.9	77.8
>5hr	45	22.2	100.0
Total	203	100.0	

Table 5. Respondent's extensity (# of years) group distribution

Extensity	Count	%	Cumulative %
0	13	6.4	6.4
1	4	2.0	8.4
2	4	2.0	10.4
3	9	4.5	14.9
4	16	7.9	22.8
5	37	18.3	41.1
6	46	22.8	63.9
7	34	16.8	80.7
8	19	9.4	90.1

9	8	4.0	94.1
>10	12	5.9	100.0
Total	202	100.0	

Table 6. Respondent's importance of having mutual friends group distribution

Importance Mutual Friend	Count	%	Cumulative %
Not Important-1	18	9.8	9.8
Important-2	45	24.6	34.4
Very Important-3	120	65.6	100.0
Total	183	100.0	

Table 7. Respondent's number of friends one must have to accept a friend request group distribution

Number of Friends	Count	%	Cumulative %
0 (1)	9	4.9	4.9
1-5 (2)	77	42.3	47.3
6-10 (3)	35	19.2	66.5
>11 (4)	61	33.5	100.0
Total	182	100.0	

Table 8. Respondent's recognition of profile name group distribution

Recognition of Profile Name	Count	%	Cumulative %
Not Important-1	10	7.7	7.7
Important-2	60	46.2	53.8
Very Important-3	60	46.2	100.0
Total	130	100.0	

Table 9. Respondent's recognition of user photo group distribution

Recognition of User Photo	Count	%	Cumulative %
Not Important-1	6	3.5	3.5
Important-2	69	40.1	43.6
Very Important-3	97	56.4	100.0
Total	172	100.0	

Table 10.1 Respondent's posts group distribution

Posts	Count	%	Cumulative %
Private-0	103	85.8	85.8
Public-1	17	14.2	100.0
Total	120	100.0	

Table 10.2 Respondent's personal information group distribution

Personal Information	Count	%	Cumulative %
Private-0	39	32.2	32.2
Public-1	82	67.8	100.0
Total	121	100.0	

Table 11.1 Hacked

N=209	Count	%	Cumulative %
No-0	160	87.4	87.4
Yes-1	23	12.6	100.0
Total	183	100.0	

Table 11.2 Cyber-Impersonation

N=209	Count	%	Cumulative %
No-0	163	88.6	88.6
Yes-1	21	11.4	100.0
Total	184	100.0	

Table 11.3 Cyber-Bullying

N=209	Count	%	Cumulative %
No-0	135	73.4	73.4
Yes-1	49	26.6	100.0
Total	184	100.0	

Table 11.4 Online Romance Scams

N=209	Count	%	Cumulative %
No-0	150	82.0	82.0
Yes-1	33	18.0	100.0
Total	183	100.0	

Table 11.5 Identity Theft

N=209	Count	%	Cumulative %
No-0	173	94.0	94.0
Yes-1	11	6.0	100.0
Total	184	100.0	

Table 11.6 Online Fraud

N=209	Count	%	Cumulative %
No-0	165	90.2	90.2
Yes-1	18	9.8	100.0
Total	183	100.0	

Table 12 Ever Victimized

N=209	Count	%	Cumulative %
No-0	89	48.4	48.4
Yes-1	95	51.6	100.0
Total			

VITA

Kristina E. Morales received her Bachelor of Science degree in Criminal Justice from Texas A&M International University in 2013. She entered the Criminal Justice Master's program at Texas A&M International University in the summer of 2014 and received her Master of Science degree in December 2016. Her research interests include human trafficking, the death penalty, prostitution and fracking, and cybercrime related topics. She plans to publish this thesis to advance research focused on cybercrime and social media sites. Ms. Morales may be reached through email at kristinamorales@dusty.tamiu.edu.