UNIVERSITY OF CALIFORNIA,
IRVINE

A Mixed Methods Approach to Understanding Undergraduate Students' Victimization, Perceptions, and Reporting of Cybercrimes

THESIS

submitted in partial satisfaction of the requirements for the degree of

Master of Science

in Information and Computer Science

with a concentration in Informatics

by

Morvareed Bidgoli

Thesis Committee:
Professor Gloria Mark, Chair
Professor Bonnie Nardi
Professor Teresa A. Dalton

2015

TABLE OF CONTENTS

	PAGE
LIST OF FIGURES	iii
LIST OF TABLES	iv
ACKNOWLEDGEMENTS	v
ABSTRACT OF THE THESIS	vi
INTRODUCTION	1
CHAPTER 1: Related Work	4
1.1 Cybercrime Victimization	4
1.2 Cybercrime Perceptions	6
CHAPTER 2: Semi-structured Interviews	9
2.1 Information Security Practices	10
2.2 Cybercrime Knowledge	11
2.3 Cybercrime Victimization	13
2.4 Cybercrime Perceptions	19
2.5 Cybercrime Reporting	23
CHAPTER 3: Online Survey	27
3.1 Model #1: Cybercrime Perceptions	29
3.2 Model #2: Preventative Measures	32
3.3 Model #3: Enablers	33
3.4 Model #4: Likelihood of Cybercrime Reporting	35
3.5 Cybercrime Victimization	36
3.6 Importance of Cybercrime Reporting and Cybercrime Victimization Statistics	37
CHAPTER 4: Discussion	40
CHAPTER 5: Conclusion	46
REFERENCES	49
APPENDIX A: Interview Artifact	51
APPENDIX B: Online Survey Questions	52

LIST OF FIGURES

		Page
Figure 1	I know how to and to whom I should report a cybercrime I have experienced.	37
Figure 2	I think it is important to report cybercrimes.	38
Figure 3	I think it is important to have access to cybercrime victimization statistics.	38

LIST OF TABLES

		Page
Table 1	Multiple Linear Regression Results (Dependent Variable: Cybercrime Perceptions)	31
Table 2	Multiple Linear Regression Results (Dependent Variable: Preventative Measures)	33
Table 3	Multiple Linear Regression Results (Dependent Variable: Enablers)	34
Table 4	Multiple Linear Regression Results (Dependent Variable: Cybercrime Reporting)	36
Table 5	Cybercrime Victimization Statistics	36

ACKNOWLEDGEMENTS

I would like to thank my committee chair, Professor Gloria Mark, for advising me for the past two years. I am grateful that she saw a passion in me and encouraged me to do my Master's thesis on this topic.

I would like to thank my committee members, Professor Bonnie Nardi and Professor Teresa A. Dalton, for their support and teaching me the methodology I employed in my study.

I am thankful for the friends I have made over these past two years who have not only supported me through my work, but have proven to be an invaluable asset for research advice.

I would like to dedicate this work to my parents, Hossein and Nooshin Bidgoli. It is with the utmost respect and gratitude that I have been blessed with such incredible parents. Thank you for believing in me and supporting me throughout my academic career. To my father, Dr. Hossein Bidgoli, you are my inspiration for why I want to acquire a Ph.D. and become an exceptional professor like you someday.

ABSTRACT OF THE THESIS

A Mixed Methods Approach to Understanding Undergraduate Students' Victimization, Perceptions, and Reporting of Cybercrimes

By

Morvareed Bidgoli

Master of Science in Information and Computer Science
with a concentration in Informatics

University of California, Irvine, 2015

Professor Gloria Mark, Chair

A mixed methods study was conducted to understand undergraduate students' victimization, perceptions, and reporting of cybercrimes. Semi-structured interviews were conducted with 10 participants that provided the groundwork for questions that would be asked in an online survey. A total of 222 survey responses were collected from which four linear regression models were built to predict for perceptions (i.e. fear and concern) of cybercrimes, preventative measures that can mitigate cybercrime victimization, enabling behaviors that can lead to cybercrime victimization, and the likelihood of cybercrime reporting. The results of the models were that: (1) media exposure, cybercrime knowledge, and the harmfulness of cybercrimes were associated with cybercrime perceptions; (2) self-control was associated with preventative measures and enabling behaviors; and (3) cybercrime perceptions were associated with enabling behaviors and the likelihood of cybercrime reporting. Participants reported acquiring their knowledge of cybercrimes predominantly through personally knowing someone

who had been victimized by a cybercrime (i.e. vicarious cybercrime experiences) and the media. The survey results show that undergraduate students reported being predominantly victimized by malware, hacking, and phishing. Despite the fact that both interviewees and survey participants expressed that they found reporting cybercrimes and having access to cybercrime victimization statistics to be important, the majority of participants did not know how to officially report a cybercrime. Cybercrime victimization can cause various kinds of harm (e.g. psychological, social, financial) to those affected. The focus on how cybercrimes affect a young subject group like undergraduate students who use technology frequently is motivated by the goal to bring more awareness to this issue and for preventative measures to be taken early on to help mitigate cybercrime risk.

Keywords: cybercrimes, undergraduate students, victimization, perceptions, reporting

Introduction

Cybercrimes have proven to be a pressing issue of today worth addressing. According to McAfee, a computer security software company, cybercrimes cost the U.S. $100 billion annually and $300 billion annually worldwide ("2013 – The Impact of Cybercrimes," 2013). Based on the 2013 Internet Crime Report compiled by the Internet Crime Complaint Center (IC3), the IC3 received 262,813 complaints with a total loss of $781,841,611; 45.5% of the complaints received reported financial loss ("2013 Internet Crime Report," 2013). In late 2013, one of the largest data breaches of consumer information occurred where approximately 40 million Target customer's credit and debit cards were stolen.

Despite the fact that there have been a number of studies focused on explaining undergraduate cybercrime victimization and cybercrime victimization in general, I found very little literature that has focused on computer users' perceptions of cybercrimes and aptitude in knowing how to appropriately report a cybercrime. I believe understanding computer users' perceptions of cybercrimes to be important because the perceived fear, concern, or severity of cybercrimes can influence whether preventative measures and risky online behaviors are taken, which would impact computer users' cybercrime risk. Many of the studies that focus on cybercrime victimization of undergraduate students focus on specific types of cybercrimes or a single individual cybercrime (e.g. cyberharassment) where as my study is more focused on providing a more holistic view of many cybercrimes and ones that have relevancy in nature to each other (e.g. breach of personal information). Lastly, I found very little literature focused on cybercrime victims' aptitude in knowing how to report

cybercrimes and whether cybercrimes are reported, which is a central point I unpack in my study.

The harmful consequences and prevalence of cybercrimes computer users are faced with today motivated me to research just how prevalent cybercrime victimization is among undergraduate students since they are an arguably active segment of the computer user population; in fact, the Pew Research Center found in 2010 that 98% of undergraduate students reported using the Internet (Smith et al., 2011). I present a mixed methods study conducted to understand undergraduate students' victimization, perceptions, and reporting of cybercrimes. My study looks to answer the following research questions:

RQ #1: How prevalent is cybercrime victimization among undergraduate students?

RQ #2: Where does undergraduate students' knowledge of cybercrimes come from?

RQ #3: What are undergraduate students' perceptions (i.e. severity, level of concern, fear) of cybercrimes?

RQ #4: Are cybercrimes reported and do undergraduate students know how to report cybercrimes?

Semi-structured interviews were conducted with 10 participants that provided the groundwork for questions that would be asked in an online survey. A total of 222 survey responses were collected from which four linear regression models were built to predict for perceptions (i.e. fear and concern) of cybercrimes, preventative measures that can mitigate cybercrime victimization, enabling behaviors that can lead to cybercrime victimization, and the likelihood of cybercrime reporting.

Participants reported acquiring their knowledge of cybercrimes predominantly through personally knowing someone who had been victimized by a cybercrime (i.e. vicarious cybercrime experiences) and the media. Media exposure, cybercrime knowledge, and the harmfulness of cybercrimes were found to be associated with cybercrime perceptions. Self-control was found to be associated with preventative measures and enabling behaviors. Cybercrime perceptions were associated with enabling behaviors and the likelihood of cybercrime reporting. The survey results show that undergraduate students reported being predominantly victimized by malware, hacking, and phishing. Despite the fact that both interviewees and survey participants expressed that they found reporting cybercrimes and having access to cybercrime victimization statistics to be important, the majority of participants did not know how to officially report a cybercrime.

Cybercrime victimization can cause various kinds of harm (e.g. psychological, social, financial) to those affected. The focus on how cybercrimes affect a young subject group like undergraduate students who use technology frequently is motivated by the goal to bring more awareness to this issue and for preventative measures to be taken early on to help mitigate cybercrime risk.

1 Related Work

I will now present some of the relevant literature that has been done on cybercrime victimization and cybercrime perceptions. The most work has been done on explaining the causes of cybercrime victimization while very little work has been done to explain what factors influence computer users' cybercrime perceptions. For the work that has been done on cybercrime victimization, I did not come across any that looked at cybercrime victims' reporting behavior nor did I find any literature that looked at how computer users' perceptions of cybercrimes affects their likelihood to report a cybercrime. Lastly, there is very little literature that particularly focuses on understanding how cybercrimes as a whole affect undergraduate students.

1.1 Cybercrime Victimization

In a cross-sectional survey of 15-74 year olds in Finland, Oksanen and Keipi (2013) found that cybercrime victimization is more prevalent among the younger age group of 15-24 year olds than to the older age groups. Based on multinomial logistic regression analysis, the study found that age, participation in online communities (i.e. discussion, gaming, etc.), and prior violent victimization (i.e. violent assaults, robbery) were strongly associated with cybercrime victimization (Oksanen and Keipi, 2013). The study also found that previous cybercrime victims expressed being concerned about being victimized again within the next year (Oksanen and Keipi, 2013).

Routine Activity Theory proposed by Cohen and Felson (1979) suggests that crime is likely to occur when there is a motivated offender, suitable target, and lack of a capable guardian. Marcum et al. (2010) conducted a study that tested the three components of

Routine Activity Theory to explain three different types of cybercrime victimization: the receipt of sexually explicit material, non-sexual harassment, and sexual solicitation experienced by a sample of undergraduate students during their freshman year of college and senior year of high school. The results of the study found that Internet and computer mediated communications (CMCs) (e.g. email, chat rooms, social networking sites) usage increased the likelihood of victimization, providing personal information and communicating with people met online were also found to be good predictors and increased the likelihood of victimization, while protective measures (i.e. anti-virus software) had somewhat of an effect on victimization and did not prove to mitigate victimization from occurring (Marcum et al., 2010).

Self-control theory (also known as the General Theory of Crime) proposed by Gottfredson and Hirschi (1990) posits that individuals with low self-control (i.e. impulsive, short-sighted, engage in risk-taking behavior) are more likely to commit crime. Despite the fact that this theory is predominantly used to explain why a crime occurs, the theory has also been used to explain victimization. Bossler and Hold (2010) conducted a study with a sample of 573 undergraduate students and found low-self control to increase the likelihood of three types of cybercrime victimization: password access, having computer information changed, and cyberharassment. The study also found that individual cyber deviance (i.e. looking at pornographic material, accessing someone's computer without permission) had a statistically significant positive effect on cyberharassment while peer offending (i.e. having friends who looked at pornographic material, accessed someone's account without permission) was shown to have statistically significant positive effects on the likelihood of victimization of

password access, having computer information changed, malware, credit card theft, and cyberharassment (Bossler and Hold, 2010).

1.2 Cybercrime Perceptions

Henson et al. (2013) conducted an online survey of 838 undergraduate students at a large public university that looked at the effect perceived risk of previous online victimization (direct, indirect, and previous online interpersonal victimization (OIPV)) had on the fear of OIPV by an intimate partner, friend/acquaintance, and stranger. Based on the OLS regression results, the study found that perceived risk of OIPV had statistically significant positive effects on all three types of victim-offender relationships, previous direct online victimization had a statistically significant positive effect on fear of OIPV by an intimate partner, previous indirect online victimization had a statistically significant negative effect on fear of OIPV by intimate partners and friends/acquaintances, while online exposure (i.e. Internet usage, usage of dating sites, online groups, instant messengers, and YouTube) was not found to have a statistically significant effect on any of the types of victim-offender relationships (Henson et al., 2013).

Graves et al. (2014) conducted six between-subjects survey experiments to examine the effects that the type of data, scope, motivation of the offender, consequences of the crime, co-responsibility, and context had on survey participants' perceptions of the seriousness of cybercrimes. Participants were presented with a vignette of a hypothetical consumer data breach where the previously mentioned variables were manipulated. The results of the study found that the scope (i.e. number of records downloaded) and the

motivation of the cybercriminal (particularly for a monetary gain) in particular had significant effects on the perceived seriousness of the cybercrime (Graves et al., 2014).

Rader et al. (2012) conducted a survey with a sample of 301 undergraduate students to see how non-expert computer users use the stories they hear from other people to make security decisions. Six different types of security stories emerged from the survey responses, which were having issues with a PC due to a security problem (i.e. loss of information, slow performance), having a computer broken into due to hacking or viruses, theft (i.e. through phishing, monetary or personal information taken), spam, phishing, and other stories that did not fit a particular category (Rader et al., 2012). Many respondents mentioned hearing stories from a family member or friend and hearing stories led to a change in a little over half of respondents' security behavior and the way in which virtually all respondents thought about security (Rader et al., 2012). Autobiographical stories, stories told by more knowledgeable people, and stories producing emotion (particularly anxiety and anger) were more likely to lead to a change in security behaviors (Rader et al., 2012). Lastly, nearly half of respondents reported retelling a story to others (Rader et al., 2012).

Wiederhold (2014) makes the point that psychology can play an important role in minimizing cybercrime risk by providing insights into what end users' perceptions are in terms of what the tradeoffs of the risks and rewards are when making online privacy decisions particularly in the face of socially engineered cybercrimes. She also makes the suggestion that psychologists can help raise awareness through outlets like the media about the cybersecurity risks that are out there to help "…adjust people's perception and, subsequently, their behavior toward privacy" (Wiederhold, 2014, p. 131).

Yar (2013) emphasizes the role that media plays in our understanding of cybercrimes. He mentions that media (e.g. films, print media, broadcast media, the Internet) have fueled "moral panics" and a dystopic view at the hands of technology. Yar warns that such representations of technology can "…obscure the realities of criminal activity and its impacts, hindering rather than facilitating a balanced understanding" (Yar, 2013, p. 4). Yar also provides a number of reasons for why underreporting of cybercrimes can occur. One of the reasons Yar cites is that a victim may consider the cybercrime he/she experienced to lack enough seriousness to contact the authorities (Yar, 2013). Thus, the perceived severity of a cybercrime plays a crucial role in whether it will be reported, which would in turn affect the likelihood that a potential resolution (e.g. finding the cybercriminal) can be achieved.

2 Semi-structured Interviews

The first method of data collection involved semi-structured interviews. The only requirements to participate in an interview was that a participant was a current UCI undergraduate student, 18 years or older, and had either been a victim of a cybercrime while in college or had some knowledge about cybercrimes. Recruitment for participants was done through a variety of ways such as social media (i.e. Facebook), brief in class announcements, class emails sent out to students by professors, and flyers posted around campus (e.g. building bulletin boards, bridges, etc.). All interviews were conducted in person on an on campus UCI location, scheduled at a time that worked for the researcher and interviewee, and audio recorded with the interviewee's consent. On average, the interviews lasted between 30 minutes to an hour. A total of 10 participants were interviewed.

The objectives of the interviews were to gain a deeper understanding of what practices (i.e. security measures) undergraduate students employ, the level of cybercrime knowledge they have, the perceptions they have of cybercrimes specifically in terms of severity, whether a cybercrime incident was reported if a student was victimized, and how much they know about reporting cybercrimes. Once all interviews were concluded and subsequently transcribed, grounded theory (Strauss and Corbin, 1998) was used to analyze the data. The important themes that emerged from the interview data provided the groundwork for questions to be formulated for an online survey that would help provide more insight on this research topic.

2.1 Information Security Practices

I asked interviewees what security measures they employ when using technology, which would provide insight about the extent to which undergraduate students are able to protect themselves and minimize their cybercrime risk. The majority of interviewees stated that they use anti-virus software as a security measure. Participant #4, who was not a cybercrime victim, mentioned she did not really use security measures. Upon being asked why she did not use anti-virus software she stated, “Because Macs don’t get viruses.” This statement provides some insight as to why some undergraduate students may not be as concerned about their online security or not feel compelled to employ online security measures since they never were victims before. Many interviewees also mentioned looking for SSL (Secure Socket Layer) or HTTPS as an indication of a secure online connection before entering in sensitive personal information (i.e. social security number, credit/debit card numbers). Other online security measures interviewees stated they employ included: password protected computers, creating unique and complex passwords, and providing fake or very little private information about themselves online. Interviewees #2 and #6 mentioned providing fake information about themselves online, which is an interesting and rather unconventional online security measure to employ. Interviewee #2 stated that he uses an alias and uses completely fake information (i.e. email, Google phone number, address) for online sign ups and sites he does not really care about. Interviewee #6 also mentioned providing fake information about himself (i.e. an inaccurate current city location on Facebook) and simply being less concerned about his online security since he does not post a lot of private information about himself online.

Interviewees #5 and #8 invested in obtaining certain security measures after experiencing cybercrimes. Interviewee #5 bought an e-key after experiencing an online scam, but not falling victim to it within a Chinese online game she plays. She uses the e-key whenever she plays online games. She described the e-key as a security measure that gives an end user a number that needs to be inputted whenever a user uses his/her account. Once that number is used no one else can use it. A unique number is given each time the end user uses his/her account; this number changes every 10 seconds. Interviewee #8 bought anti-virus software after being a victim of adware.

2.2 Cybercrime Knowledge

Cybercrimes is a topic that is not necessarily taught through school; thus, this motivated me to inquire about what the exact sources of cybercrime knowledge are for undergraduate students. Additionally, it is important to understand where undergraduate students' cybercrime knowledge comes from so we can better understand how undergraduate students perceive cybercrimes and in turn know how to effectively deal with cybercrime victimization. Based on interview data, I found that interviewees predominantly acquire cybercrime knowledge from someone they personally know who has been victimized in the past (i.e. vicarious cybercrime experience), a family or friend who has technical expertise on cybercrimes or computers, or through a media source (i.e. online news article, TV show, etc.).

A majority of interviewees expressed that they personally knew either a friend or family member who had been a victim of a cybercrime, which in turn informed them about certain cybercrimes. Among some of the cybercrimes interviewees' friends or family

members have been previous victims of included hacking (via gaming and social media), phishing, identity theft, and credit card fraud. A few interviewees also expressed that they acquired cybercrime knowledge through the computer or cybercrime expertise a friend or family member had. Interviewee #1 has an uncle who works in security at Microsoft that shared cybercrime stories with him while interviewees #2 and #3 learned about cybercrimes through a friend and brother who both are studying Computer Science, respectively.

Most interviewees expressed they gained their cybercrime knowledge from media sources like online news articles, TV shows, or films. Interviewees #2, #7, #8, and #10 stated they learned about cybercrimes through the news or by reading online news articles. Interviewees #6, #7, and #9 mentioned that they had learned about cybercrimes through either films that cover cybercrimes such as hacking and online fraud or through detective TV shows.

Other means in which interviewees stated they acquired their cybercrime knowledge from included their own personal exposure to cybercrimes (i.e. past cybercrime victimization and encountering a cybercrime, but not falling victim to it), school, and doing personal research on cybercrimes. Interviewees #2, #6, and #7 all mentioned that they learned about phishing by encountering it, but not falling victim to it. Interviewees #7, #8, and #10 acquired cybercrime knowledge by previously being victims of cybercrimes prior to college (i.e. hacking, malware, and malware, respectively). Interviewees #1, #8, and #9 mentioned they learned about some cybercrimes (i.e. hacking and phishing) through a course they took. However, it was particularly interesting to hear from interviewees #3 and #5 that they both attended school assemblies (middle school, high school, respectively) that covered the issue

of cyberbullying since cyberbullying is not considered a cybercrime, but rather a civil law violation. In fact, interviewee #5 stated that she recalled cyberbullying being mentioned as a cybercrime, which is not the case. Interviewees #1 and #5 did personal research online to learn about cybercrimes.

Lastly, every interviewee was provided with an artifact with a list of cybercrimes (see Appendix A). This artifact was provided to interviewees for two reasons: (1) to inquire about how many of the listed cybercrimes they were familiar with, and (2) to specify which cybercrime(s) they may have been a victim of while in college. Overall, interviewees claimed that they were familiar with most of the cybercrimes outlined in the artifact; however, there were certain cybercrimes that many interviewees were not familiar. Many interviewees mentioned not being familiar with pharming and a romance scam. Other cybercrimes interviewees mentioned not being familiar with included: phishing, a Distributed Denial of Service (DDoS) attack, and certain types of malware (i.e. backdoors, rootkits, ransomware). Most interviewees mentioned that they were familiar with the following cybercrimes: most types of malware (i.e. viruses, worms), identity theft, keylogging, cyberharassment, and cyberstalking.

2.3 Cybercrime Victimization

When initially beginning my study, one of the major research questions I wanted to answer was “how prevalent is cybercrime victimization among undergraduate students?” Therefore, I was particularly interested in interviewing undergraduate students who had previously been victimized by a cybercrime while in college. I later decided to remove this requirement when I realized it might be difficult to not only gather the number of

interviewees we needed, but also became interested in knowing how undergraduate students perceive cybercrimes. In the end, five interviewees identified as being cybercrime victims while in college. The cybercrimes the five interviewees were victims of were commercial fraud, cyberstalking, a virus, online fraud, and adware.

Interviewee #1 was a victim of commercial fraud during the end of his sophomore year of college. He was trying to assist his aunt in buying merchandise from Abercrombie & Fitch's website. After searching for the website through Google, he claimed he was redirected to another website that looked legitimately like the one belonging to Abercrombie & Fitch; this website's URL was: www.abercrombieoutletsale.us/. He claimed that everything about the website he was directed to looked exactly like Abercrombie & Fitch's in terms of the layout and merchandise sold, but it was not until after he had purchased the merchandise for his aunt that he realized the website was a fraud. He arrived to this conclusion after seeing that the website claimed his package was still being prepared after three days, never received an email notification about his order, and subsequently checked his bank statement to see that he was charged by a place in Beijing, China. In order to resolve the matter, he decided to contact Abercrombie & Fitch's customer service who advised that nothing could be done for him on their end and suggested he cancel his card as soon as possible. Therefore, he decided to report the fraudulent charge to his bank and canceled his card. In the end, he did receive the items he purchased from the fraudulent Abercrombie & Fitch website, which turned out to be fake merchandise. He was unable to recover this money since he received the fake merchandise and the merchandise totaled to $220. The fraudulent Abercrombie & Fitch website the interviewee visited no longer exists and when

visiting the website it states that a lawsuit is underway. Experiencing such an incident has led him to be more careful about making online purchases. In order to have trust in making an online purchase on a website, he stated that he will consult the website's policies and ensure the website is legitimate by checking the website's domain or contacting the website's customer service before making an online purchase.

Interviewee #2 was a victim of cyberstalking over the course of many months during his 4th year of college. The incident involved an ex-girlfriend who he had a very close relationship with; thus, his ex-girlfriend knew a lot of information about him such as his Facebook password and was able to gain access to his online accounts by answering security questions to create new passwords. His ex-girlfriend was only about to obtain access to his social media accounts and email accounts not his banking account. He did not immediately change his passwords explaining that it would be difficult to have to change everything and keep track of the changes, but eventually changed his passwords a few months later creating a password system where each online account's password was different. His ex-girlfriend was able to stalk him through having access to his online accounts. Even when he unfriended her on Facebook she would use her friends' Facebook profiles to stalk him since they both had mutual friends in common. She would even stalk him on Spotify and based on his activity make conclusions of what activities he was doing. The stalking even persisted offline for some time where she would track his whereabouts on campus and his work schedule as a UCI Anteater Express shuttle driver. He claims the stalking persisted for so long because he would continue talking to her having still cared about her and was concerned about her well being since she had a history of mental issues and became suicidal. Over time the stalking subsided,

but when his ex-girlfriend and him were in a five week research program together, the stalking persisted for a few weeks after the program ended. He then began to receive text messages from his ex-girlfriend for a little over a month claiming she was pregnant. Upon seriously following up on this, he was able to conclude that his ex-girlfriend was lying to him about being pregnant. After this incident, he stopped talking to his ex-girlfriend entirely. He never reported the incident, but considered it. He did not want to report it to the police because he did not want her to have a criminal record and due to her mental issues. However, he did consider reporting the incident to the Office of Student Conduct on campus. Experiencing such an incident made him create a password system where all his passwords are unique, which would mitigate his ex-girlfriend's ability to stalk him online. He also added that he would now know how to react if he were ever in a similar situation again by simply blocking someone, being careful about giving out information to others, and contacting the Office of Student Conduct.

Interviewee #3 was a victim of a virus while she was taking a leave of absence at the end of her first year as a transfer student. She described having overheating issues with her laptop for quite some time, but once the overheating became more frequent (i.e. every five minutes) and her computer would just shut down without warning, she started to become more concerned. She tried to see if her brother who studies Computer Science could help her figure out what was wrong with her computer, but he was unable to figure out what was wrong with her computer. She then decided to contact Dell customer service to see if they could resolve the issue and they were able to confirm through remote login that her computer had a virus. She had to purchase a new version of Windows that cost $25. The only

damage the virus caused was that she lost a few files she was not able to save in time, which she claimed were not very important. She did not report the incident to the police since she claims the virus did not do any real damage; however, if it was able to take her personal information or hack into her account saying hurtful things to others then she would consider reporting it. Experiencing such an incident made her a little more cautious about what websites she visits since she does not exactly know where the virus came from.

Interviewee #7 was a victim of online fraud during his junior year of college. A buyer who was interested in purchasing some of his dodgecoins contacted him. He explained that dodgecoins are a joke crypotocurrency (Bitcoin) based off a dog. The person who was interested in doing an exchange with him sent a fake link to a platform that looked very similar to the standard service everyone uses to do Bitcoin exchanges. The interviewee ended up sending 250,000 dodgecoins to the address he was provided by the interested buyer and stated that as soon as the dodgecoins were sent he could no longer see the transaction and the coins were gone. He lost 250,000 dogecoins, which amounts to $250 (1000 dogecoins/dollar). He did not report the incident to the police claiming it would be difficult for the police to track an anonymous connection especially with a type of currency many people are probably unfamiliar with. However, he decided to report the incident to the legitimate platform that many use to exchange Bitcoin warning them about the scam that he experienced. He also reported the incident to Reddit, which was where the scammer contacted him. Reddit banned the scammer's account. The scammer's wallet address was also tracked, which would warn other Bitcoin users to be mindful of doing future exchanges with the user. Experiencing such an incident made him create unique passwords across his

online accounts (i.e. Facebook, Reddit, email) and become more watchful of scammers on Bitcoin to the extent that he would even warn other people to watch out for suspicious transactions or parties who were interested in doing exchanges. Ultimately, the incident made him learn about cybersecurity and to be more careful about buying and selling things on the Internet.

Interviewee #8 was a victim of adware while he was in community college. While surfing the web and reading online articles, he came across an advertisement regarding a PC optimizer. The advertisement for the PC optimizer looked legitimate showing the speed of his computer was slow and itemized the viruses along with all the infected computer files his computer had. Upon clicking on the advertisement, his computer became messed up and he lost computer files (i.e. work and school related files, digital media). He resolved the issue by doing a system restore on his computer. He claimed that despite not reporting the incident, he probably would have, but does not know how to report it. Experiencing such an incident made him more mindful of clicking online advertisements and to employ security measures (i.e. buying anti-virus software).

Three interviewees experienced cybercrimes, but did not fall victim to them. Interviewee #2 described an incident resembling the components of phishing, which he experienced during his 4th year of college. He was personally messaged by a female on Facebook and was asked for his email. Upon posting about receiving the message on Twitter, he found out that some of his other friends who also attend UCI had also received the same message. As a result of finding out this information, he concluded that the message was probably geared towards UCI students. He decided to block the user who messaged him. He

claims he knew it was phishing immediately based on the language of the message (i.e. poor grammar) and the fact that his email was asked for. He did not report the incident. Interviewee #5 described an online scam she experienced within an online Chinese game she plays. She was trying to buy a piece of equipment from someone else within the game. After chatting with the seller of the item on a Chinese voice chat platform, she was sent a document by the seller to confirm the item she was interested in buying. Upon clicking on the file, she hesitated to download the file upon noticing that the file format was different to ones she was familiar with (i.e. .jpg, .gif). Thus, she decided not to download the file and deleted it. She also logged off the game and restarted her Internet connection as safety measures. She reported two people: the person who personally emailed her referring her to the seller and the seller who tried to scam her to the respective administrators of the places she was contacted by them in. Lastly, interviewee #6 has been continually cyberharassed by the same person for the past two years. He has received an email every week from someone who used to be a friend of his. The person who has been sending him the emails he claims is schizophrenic and has formed an obsession. Despite this being a case resembling cyberharassment, he claimed he does not feel bothered or threatened by the contact in any way. Every email he has received from the person has been deleted and never opened. He did not consider reporting the person because he did not feel bothered or threatened by the communication and never told the person to stop contacting him.

2.4 Cybercrime Perceptions

Interviewees were asked to comment on the severity of cybercrimes specifically in relation to offline crimes. To make the comparison easier, interviewees were asked if they

had been a victim of an offline crime before or to simply choose an offline crime to juxtaposition it to a cybercrime they have experienced or been victimized by. A number of interviewees mentioned that they believe cybercrimes are more severe than offline crimes. Interviewee #1 commented on the fact that since cybercrimes are intangible and typically more on a globalized scale, it makes it difficult to always know whether you have been victimized. He states, “In an offline crime, if someone steals your wallet you know it’s gone, but if you are a victim of a cybercrime you won’t even know your information has been stolen.” Interviewee #2 stated that cybercrimes should be punished and policed more because “[cybercrimes are] more long term or can even be instantaneous like someone robs your whole bank account like that. There goes your thing as opposed to getting mugged on the street and someone takes $20 from your wallet or all the cash in your wallet you know?” For him cybercrimes are more severe than even severe offline crimes like murder because the likelihood of being victimized by a cybercrime is higher. Interviewee #4 stated that she finds both cybercrimes and offline crimes to be severe, but what makes cybercrimes particularly severe is the fact that you cannot always put a name to a face of the cybercriminal.

Interviewees #5, #8, and #10 stated that they found offline crimes to be more severe than cybercrimes because someone can be physically harmed in an offline crime. Interviewee #7 also pointed out the physicality present in an offline crime would affect his reaction to being a victim of an offline crime versus a cybercrime. He makes the comparison between being robbed and having your money being taken online (i.e. online fraud) as both being

severe, but states that he would be more scared if he was robbed rather than online scammed since it is a physical taking versus a virtual taking of someone's money.

Other interviewees pointed out that the severity of cybercrimes depends on context. Interviewee #3 explained that she did not find the virus she was a victim of to be too severe, but believes that "[an] online crime has the potential to be equal if not more severe" than an offline crime. One example of such an instance would be cyberbullying in which she referenced a girl she knew who killed herself because she was cyberbullied by a group of people from her high school. Again, it is worth noting that despite cyberbullying not being considered a cybercrime, but rather a civil law violation, interviewee #3 makes the important point that online offenses that spill into the physical world where physical harm can occur can be particularly severe. Interviewee #6 seconded Interviewee #3's comments about cybercrimes being severe based on context. He states that they have the potential to be severe and it depends on the cybercrime. He specifically stated cyberstalking for example has potential to be extremely severe when it leads to physical violence. Interviewee #9 also points to context when comparing the severity of offline crimes to cybercrimes stating that the extent to which someone is physically harmed affects the degree of severity of an offline crime. Generally speaking, he finds a cybercrime like the hacking of a bank account is more severe than being robbed on the basis that more money can be taken, which can be socially debilitating for a person. He finds cybercrimes to have far reaching consequences.

It is also important to note that the perceived degree of severity of a cybercrime experience can greatly impact whether someone will feel compelled to consider reporting a cybercrime. Interviewee #3 did not consider reporting her cybercrime victimization because

she claimed that the virus did not do any real damage that she perceived to be severe; however, if a cybercrime had the ability to take her personal information she would take reporting into consideration. Similarly, interviewee #6 did not consider reporting the person who has been sending him harassing emails for the past few years because he did not feel bothered or threatened by it and never told the person to stop contacting him. On the other hand, interviewees #1 and #7 who experienced financial loss as a result of their cybercrime victimizations were particularly interested in reporting their victimizations. It is evident that the degree to which a person is harmed (i.e. financially, the loss of private data, psychologically, emotionally) plays a key role in not only determining the perceived severity of a cybercrime, but also whether a cybercrime will be reported.

The definitive distinction to make between the severity of offline crimes and cybercrimes seems to be the presence of a physical component for many of the interviewees. If someone is physically harmed than an offline crime is generally considered to be more severe than a cybercrime. Some reasons interviewees gave for why cybercrimes were seen as more severe than offline crimes were due to the global impact they have, the anonymity or difficulty in being able to always identify who is perpetrating a cybercrime, and the higher likelihood of being a cybercrime victim than an offline victim. It is evident that many interviewees find cybercrimes to be severe such as cybercrimes that can cause a person a great deal of financial harm (e.g. a hacked bank account). Lastly, for a few interviewees context was exceptionally important when considering the juxtaposition of offline crimes to cybercrimes in terms of severity.

2.5 Cybercrime Reporting

Every interviewee was asked whether they knew how to officially report a cybercrime. There was not a single interviewee who knew how to officially report a cybercrime. However, there were some interviewees who did mention that they knew how to report credit card fraud, which would entail calling a person's respective bank to cancel his/her debit and/or credit cards. Interviewee #6 mentioned he knew how to report identity theft, which would entail contacting entities such as the police, the bank, and the credit bureaus. Some interviewees mentioned the possibility of reporting their cybercrime victimizations to the police, but only if they had the appropriate evidence amount of evidence to present to the police or if a cybercrime happened where money was stolen. Other interviewees expressed that contacting the police was not even a viable option for reporting on the basis that cybercrimes are not physical crimes and that it would be extremely difficult for the police to track down the cybercriminals involved even if the appropriate evidence was collected. Despite not knowing how to officially report a cybercrime, an overwhelming majority of interviewees expressed that they believed if would be useful to know how to officially report cybercrimes and have access to annual reports on cybercrime victimization statistics.

Among the five interviewees who were cybercrime victims, every interviewee either informally reported the cybercrime they experienced or tried to reach out to entities that could help resolve the issues they experienced. It is important to note that none of the five interviewees reported their cybercrime victimizations to the police. It was particularly common for interviewees to reach out to the entities involved within the space in which the cybercrime took place. In a few instances, the interviewees resolved their issues on their

own. Interviewee #1 reported the commercial fraud he experienced to not only his bank to cancel his card, but to Abercrombie & Fitch since the fraudulent website was impersonating the brand. Interviewee #2 did not report his ex-girlfriend for cyberstalking to any entity either formally or informally, but considered reporting her to the Office of Student Conduct on campus. Interviewee #3 contacted Dell customer service to help resolve the virus on her computer. Interviewee #7 reported the online scam of his dogecoins to the legitimate platform that many use for Bitcoin exchanges and reported the incident to Reddit, which was where the scammer contacted him. Lastly, interviewee #8 did not report the adware he experienced and resolved the issue on his own by doing a system restore on his computer.

Interviewee #2 who experienced an incident resembling the components of phishing, but did not fall victim to it gave the following reasoning for why he did not report the incident,

> "…honestly I feel like reporting on social media doesn't really do anything to them [cybercriminals] or to solve the issue…I always assumed it's just a numbers game that the more people that report them it works and I should report them, but I didn't even think about it to report them. I kind of wish I did."

He adds,

> "the only closure in terms of reporting it would be the person gets caught and punished in some form like fined or I don't know what the punishment is for phishing, but I don't think that would happen through this…"

Interviewee #5 experienced a scam within an online game she plays. She reported the person who referred her to the seller to the game administrator and reported the seller who tried to

scam her to the administrator of the Chinese voice chat. She went on to explain that it did not particularly bother her that an actual result did not come out of reporting the two individuals giving the following reasoning,

> "I feel like they [game administrators] have other stuff to deal with and since I know that there are too many that they just can't deal with them one by one. If they actually had a way to deal with it once and for all then I'm probably going to be happy now, but probably no. Banning one account doesn't really make any difference."

Upon asking her who she would report the incident to if she fell for the scam and downloaded the bad attachment she was sent, she stated, "Probably no one because it's actually your own fault." Based on interviewees #2 and #5's responses, we see that there is a sense of hopelessness that the interviewees feel towards the potential of a cybercrime experience being resolved and that cybercrime reporting is viewed as ineffective when done. It is also particularly interesting that interviewee #5 adds that if she were to have fallen for the scam and downloaded the bad attachment, the aftermath of her actions was something she had to resolve rather than the people running the space in which the cybercrime occurred in.

Despite knowing who perpetrated the cybercrimes they experienced, interviewees #2 and #6 did not report the incidences for personal reasons. As previously mentioned, interviewee #2 did not want to report his ex-girlfriend to the police because he did not want her to have a criminal record and due to the fact that she had a history of mental issues. However, he did consider reporting her to the Dean of Conduct on campus. Interviewee #6 did not report a former friend of his to the police because he never told her to stop sending

him emails and did not find the behavior to be bothersome or threatening. From these two examples, it is evident that a lack of severity of the cybercrime experienced or even personally knowing someone can impact the likelihood that a cybercrime will be reported.

Despite the fact that none of the interviewees knew how to officially report a cybercrime, an overwhelming majority of interviewees expressed that they believed it would be useful to know how to officially report cybercrimes. Interviewees also expressed that it would be useful to have access to annual reports on cybercrime victimization statistics. A number of interviewees expressed that they would find it useful for the UCI police department to post cybercrime victimization statistics of online offences that occur on campus; currently, there are only statistics for offline crimes (i.e. murder, robbery, rape, stalking, etc.) that students report in a given year. Interviewee #9 expressed that cybercrime victimization statistics that specifically focus on the undergraduate student population would be more useful for undergraduate students to have than general cybercrime statistics for society at large. He explains that such statistics would "…be more pertinent to the people viewing it because it's their neighbors, their classmates rather than just statistic #4. I think the locality makes it easier for people to internalize."

3 Online Survey

After all the interview data was coded and analyzed, questions were formulated for an online survey. The survey questions cover eleven constructs that I wanted to unpack further, which are primarily motivated by the themes that emerged from the interview data. The constructs are: cybercrime victimization, vicarious cybercrime experiences, media exposure, cybercrime knowledge, information security knowledge, the harmfulness of cybercrimes, cybercrime perceptions, self-control, preventative measures, enablers, and cybercrime reporting. I consulted www.inn.theorizeit.org, which provides a database of survey items researchers can consult to reuse in their own studies. Some survey items were taken or modified from searches I made on the website for the information security knowledge and self-control constructs (Anderson & Agarwal, 2010; Fennis et al., 2009). The respective questions and the measurement scales used for each construct are outlined in Appendix B. A total of 67 items were asked.

The online survey was constructed through Google Forms. A brief explanation about the online survey and study along with an online link to the study information sheet was provided at the beginning of the online survey. The only requirements to participate in the online survey was that a participant had to be 18 years or older and a current UCI undergraduate student. Every item was required to be answered on the survey or the survey could not be submitted. At the end of the survey's completion, each participant was given the option to provide his/her email address to be entered into a raffle to win one of ten $10 Starbucks gift cards. Recruitment for participants was done through convenience sampling through three channels: emailing professors and/or TAs to share the online survey link with their students, contacting people I

personally knew who were well connected with undergraduate students to encourage participation, and sharing the online survey via social media (i.e. Facebook, Twitter). Participation for the online survey began on April 8, 2015 and closed on April 20, 2015. A total of 222 survey responses were collected.

The gender of the survey participants comprised of 154 female students (69.4%), 67 male students (30.2%), and 1 student identifying as other (0.5%). The majority of survey participants were between the ages of 18 and 22 with some exceptions of students who were older. Given the fact that I had a previous affiliation with the School of Social Ecology and a current affiliation with the School of Information and Computer Sciences, it is unsurprising that the majority of participants came from these two schools; however, there was at least one student from each school. There was a fairly representative mixture of each academic class represented in the survey results, which comprised of 33 Freshmen (14.9%), 57 Sophomores (25.7%), 58 Juniors (26.1%), and 74 Seniors (33.3%).

Each item within a given construct has a respective measurement scale. Before regression models were run, each item was coded numerically within Microsoft Excel. The coding scheme used is outlined in Appendix B. Cronbach's alpha (1951) was used to test the internal reliability of the items I asked before taking a summative score that would measure the constructs I wanted to explain in my regression models. Based on the results, a few items were omitted from the variables I created to test which models would explain the survey data best. Additionally, a few items were also reverse coded to maintain a consistent directional sign between the items in a given construct. Once these steps were taken, summative scores were taken and turned into variables representing each construct. Four linear regression models

were created that predicted for perceptions (i.e. fear and concern) of cybercrimes, preventative measures that can mitigate cybercrime victimization, enabling behaviors that can lead to cybercrime victimization, and the likelihood of cybercrime reporting.

The assumptions of linear regression were checked for each model. Since convenience sampling was used, caution should be taken when interpreting the results of the regression models as they can only be generalized for this particular population of undergraduate students at a similar type university. It is also important to note that model specification error (i.e. omitted variables) can be an issue when constructing linear regression models. Based on the results of the Ramsey RESET test, the models for cybercrime perceptions and enablers were found to have an omitted variables issue.

3.1 Model #1: Cybercrime Perceptions

A multiple linear regression analysis was conducted to determine if undergraduate students' perceptions (i.e. fear and concern) of cybercrimes could be predicted from vicarious cybercrime experiences, cybercrime knowledge, media exposure, and the degree to which undergraduate students find cybercrimes to be harmful. The null hypothesis tested was that all the regression coefficients (i.e. the slopes) were equal to 0. I hypothesized that vicarious cybercrime experiences, cybercrime knowledge, media exposure, and the harmfulness of cybercrimes would all have positive effects on cybercrime perceptions.

The results of the multiple linear regression suggest that a significant proportion of the total variation in undergraduate students' cybercrime perceptions was predicted from vicarious cybercrime experiences, cybercrime knowledge, media exposure, and the harmfulness of cybercrimes, $F(4, 217) = 21.24$, $p < .001$. In other words, cybercrime knowledge, media

exposure, and the harmfulness of cybercrimes were found to be good predictors of undergraduate students' cybercrime perceptions while vicarious cybercrime experiences was not found to be a good predictor. For vicarious cybercrime experiences, I found the following: the standardized slope (0.105) to not be statistically significantly different from 0 ($t = 1.76$, $df = 217$, $p > .05$). For cybercrime knowledge, I found the following: the standardized slope (-0.198) to be statistically significantly different from 0 ($t = -3.43$, $df = 217$, $p < .01$); this means that a one standard deviation increase in an undergraduate students' cybercrime knowledge will result in a 0.198 of a standard deviation decrease in undergraduate students' cybercrime perceptions. For media exposure, I found the following: the standardized slope (0.163) to be statistically significantly different from 0 ($t = 2.72$, $df = 217$, $p < .01$); this means that a one standard deviation increase in media exposure will result in a 0.163 of a standard deviation increase in undergraduate students' cybercrime perceptions. Lastly, for the harmfulness of cybercrimes, I found the following: the standardized slope (0.466) to be statistically significantly different from 0 ($t = 8.01$, $df = 217$, $p < .001$); this means that a one standard deviation increase in the harmfulness of cybercrimes will result in a 0.466 of a standard deviation increase in undergraduate students' cybercrime perceptions. The intercept of the model tells us the value of undergraduate students' cybercrime perceptions has when vicarious cybercrime experiences, cybercrime knowledge, media exposure, and the harmfulness of cybercrimes are 0 is 4.115. The results of the multiple linear regression model for cybercrime perceptions are summarized in Table 1. Two of my hypotheses were confirmed by the model's results. Media exposure and the harmfulness of cybercrimes were both found to have a positive effect on cybercrime perceptions; however, cybercrime knowledge was found to have a negative effect

on cybercrime perceptions. A potential explanation for why cybercrime knowledge was found to have a negative effect on cybercrime perceptions could be due to the fact that having sufficient knowledge about cybercrimes (i.e. effects, different types that exist) may actually appease a person's fear or concern of cybercrimes. Multiple R squared indicated that approximately 28% of the variation in undergraduate students' cybercrime perceptions was explained by vicarious cybercrime experiences, cybercrime knowledge, media exposure, and the harmfulness of cybercrimes.

Independent Variable	**Description**	**Estimated Standardized Coefficients followed by Standard Errors in Parentheses**
vicexp	Vicarious Cybercrime Experiences	0.105 (0.100)
ccknow	Cybercrime Knowledge	-0.198* (0.031)
media	Media Exposure	0.163* (0.030)
ccharm	Harmfulness of Cybercrimes	0.466** (0.057)
Constant		4.115 (1.779)
Observations		222
R-squared		0.28

* = p < .01, ** = p < .001

Table 1: Multiple Linear Regression Results (Dependent Variable: Cybercrime Perceptions)

3.2 Model #2: Preventative Measures

A multiple linear regression analysis was conducted to determine if preventative measures being taken that can mitigate cybercrime victimization could be predicted from cybercrime perceptions and self-control. The null hypothesis tested was that all the regression coefficients (i.e. the slopes) were equal to 0. I hypothesized that cybercrime perceptions and self-control would both have positive effects on preventative measures.

The results of the multiple linear regression suggest that a significant proportion of the total variation in preventative measures was predicted from cybercrime perceptions and self-control, $F(2, 219) = 3.94$, $p < .05$. In other words, self-control was found to be a good predictor of preventative measures while cybercrime perceptions was not found to be a good predictor. For cybercrime perceptions, I found the following: the standardized slope (-0.037) to not be statistically significantly different from 0 ($t = -0.56$, $df = 219$, $p > .05$). For self-control, I found the following: the standardized slope (0.181) to be statistically significantly different from 0 ($t = 2.72$, $df = 219$, $p < .01$); this means that a one standard deviation increase in self-control will result in a 0.181 of a standard deviation increase in preventative measures being taken that can mitigate cybercrime victimization. The intercept of the model tells us the value of preventative measures when cybercrime perceptions and self-control are 0 is 8.643. The results of the multiple linear regression model for preventative measures are summarized in Table 2. One of our hypotheses was confirmed by the model's results. Self-control was found to have a positive effect on preventative measures. Multiple R squared indicated that approximately 3.5% of the variation in preventative measures was explained by cybercrime perceptions and self-control.

Independent Variable	Description	Estimated Standardized Coefficients followed by Standard Errors in Parentheses
perceptions	Cybercrime Perceptions	-0.037 (0.078)
selfcontrol	Self-control	0.181* (0.071)
Constant		8.643 (1.708)
Observations		222
R-squared		0.035

* = p < .01

Table 2: Multiple Linear Regression Results (Dependent Variable: Preventative Measures)

3.3 Model #3: Enablers

A multiple linear regression analysis was conducted to determine if enabling behaviors that can lead to cybercrime victimization could be predicted from cybercrime perceptions and self-control. The null hypothesis tested was that all the regression coefficients (i.e. the slopes) were equal to 0. I hypothesized that cybercrime perceptions and self-control would both have negative effects on enabling behaviors.

The results of the multiple linear regression suggest that a significant proportion of the total variation in enabling behaviors was predicted from cybercrime perceptions and self-control, $F(2, 219) = 20.41$, $p < .001$. In other words, cybercrime perceptions and self-control were found to be good predictors of enabling behaviors. For cybercrime perceptions, I found the following: the standardized slope (-0.177) to be statistically significantly different from 0 ($t = -2.84$, $df = 219$, $p < .01$); this means that a one standard deviation increase in cybercrime perceptions will result in a 0.177 of a standard deviation decrease in enabling behaviors. For self-control, I found the following: the standardized slope (-0.363) to be statistically significantly

different from 0 (t = -5.85, df = 219, p < .001); this means that a one standard deviation increase in self-control will result in a 0.363 of a standard deviation decrease in enabling behaviors. The intercept of the model tells us the value of enabling behaviors when cybercrime perceptions and self-control are 0 is 21.398. The results of the multiple linear regression model for enablers are summarized in Table 3. Both of my hypotheses were confirmed by the model's results. Both cybercrime perceptions and self-control were found to have negative effects on enabling behaviors. Multiple R squared indicated that approximately 16% of the variation in enabling behaviors was explained by cybercrime perceptions and self-control

Independent Variable	**Description**	**Estimated Standardized Coefficients followed by Standard Errors in Parentheses**
perceptions	Cybercrime Perceptions	-0.177* (0.082)
selfcontrol	Self-control	-0.363** (0.074)
Constant		21.398 (1.781)
Observations		222
R-squared		0.16

* = p < .01, ** = p < .001

Table 3: Multiple Linear Regression Results (Dependent Variable: Enablers)

3.4 Model #4: Likelihood of Cybercrime Reporting

A simple linear regression analysis was conducted to determine if the likelihood of reporting cybercrimes could be predicted from cybercrime perceptions. The null hypothesis tested was that the regression coefficient (i.e. the slope) was equal to 0. I hypothesize that cybercrime perceptions will have a positive effect on cybercrime reporting.

The results of the simple linear regression suggest that a significant proportion of the total variation in the likelihood of reporting cybercrimes was predicted from cybercrime perceptions, $F(1, 220) = 7.94$, $p < .01$. In other words, cybercrime perceptions were found to be a good predictor of the likelihood of reporting cybercrimes. For cybercrime perceptions, I found the following: the standardized slope (0.187) to be statistically significantly different from 0 ($t = 2.82$, $df = 220$, $p < .01$); this means that a one standard deviation increase in cybercrime perceptions will result in a 0.187 of a standard deviation increase in the likelihood of reporting cybercrimes. The intercept of the model tells us the value of the likelihood of reporting cybercrimes when cybercrime perceptions are 0 is 31.095. The results of the simple linear regression model for cybercrime reporting are summarized in Table 4. My hypothesis was confirmed by the model's results. Cybercrime perceptions were found to have a positive effect on cybercrime reporting. Multiple R squared indicated that approximately 3.5% of the variation in the likelihood of reporting cybercrimes was explained by cybercrime perceptions.

Independent Variable	Description	Estimated Coefficients followed by Standard Errors in Parentheses
perceptions	Cybercrime Perceptions	0.187* (0.195)
Constant		31.095 (3.140)
Observations		222
R-squared		0.035

* = p < .01

Table 4: Multiple Linear Regression Results (Dependent Variable: Cybercrime Reporting)

3.5 Cybercrime Victimization

Students were asked if they were victimized by six cybercrimes (i.e. malware, hacking, credit card fraud, online fraud/scam, identity theft, and phishing) while they were in college. These cybercrimes were specifically chosen as they are similar in nature and some were among the subset of cybercrimes interviewees either were victimized by or experienced and did not fall victim to. Table 1 provides a summary of the cybercrime victimization statistics of each of these six cybercrimes.

	Yes	No
Malware	75 (33.8%)	147 (66.2%)
Hacking	44 (19.8%)	178 (80.2%)
Credit Card Fraud	27 (12.2%)	195 (87.8%)
Online Fraud/Scam	12 (5.4%)	210 (94.6%)
Identity Theft	6 (2.7%)	216 (97.3%)
Phishing	43 (19.4%)	179 (80.6%)

Table 5: Cybercrime Victimization Statistics

Based on the survey results, it is evident that undergraduate students are more prone to be victims of certain cybercrimes than others. Malware, hacking, and phishing were among the top three cybercrimes undergraduate students were most likely to be a cybercrime victim of. Credit

card fraud, online fraud/scam, and identity theft were among the three cybercrimes undergraduate students were least likely to be a cybercrime victim of. It is important to note that I did not inquire about potential cybercrime victimization of other cybercrimes such as cyberharassment, cyberstalking, sexting, or hate speech. It is possible that undergraduate students may experience these cybercrimes as well.

3.6 Importance of Cybercrime Reporting and Cybercrime Victimization Statistics

The final items in the online survey asked participants to share their aptitude in reporting cybercrimes along with their feelings on both the importance of reporting cybercrimes and having access to cybercrime victimization statistics. Figure 1 shows the results to the self-efficacy item: "I know how to and to whom I should report a cybercrime I have experienced." Figure 2 shows the results to the self-efficacy item: "I think it is important to report cybercrimes."

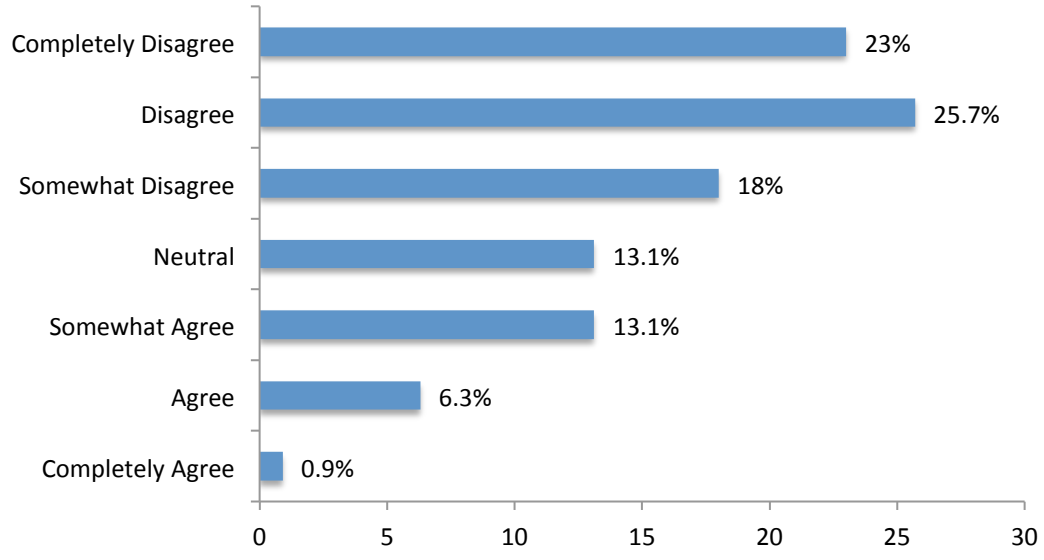

Figure 1: I know how to and to whom I should report a cybercrime I have experienced.

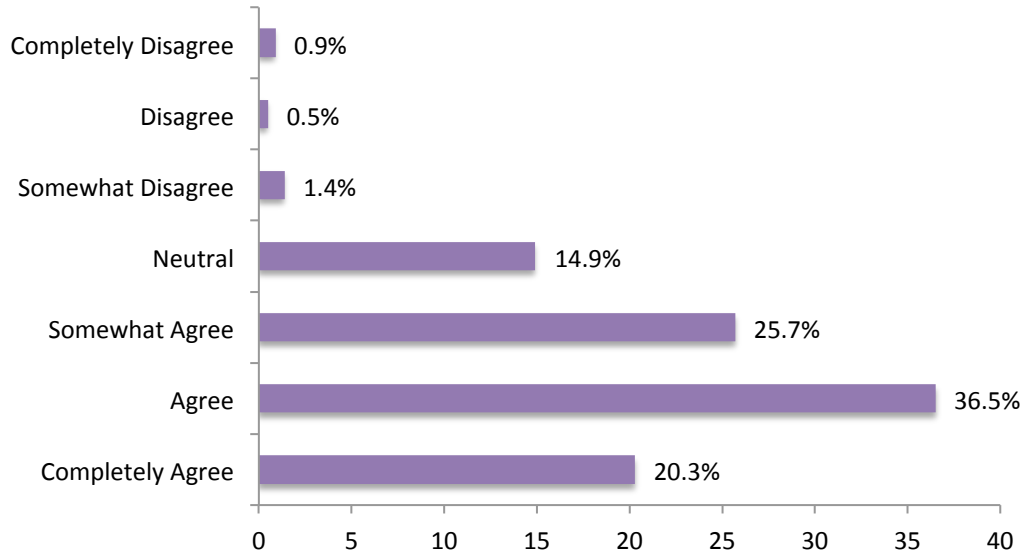

Figure 2: I think it is important to report cybercrimes.

Based on the results from these two survey items, it is evident that the majority of undergraduate students do not feel confident in knowing how to report a cybercrime, but believe that reporting cybercrimes is important. Figure 3 shows the results to the self-efficacy item: "I think it is important to have access to cybercrime victimization statistics."

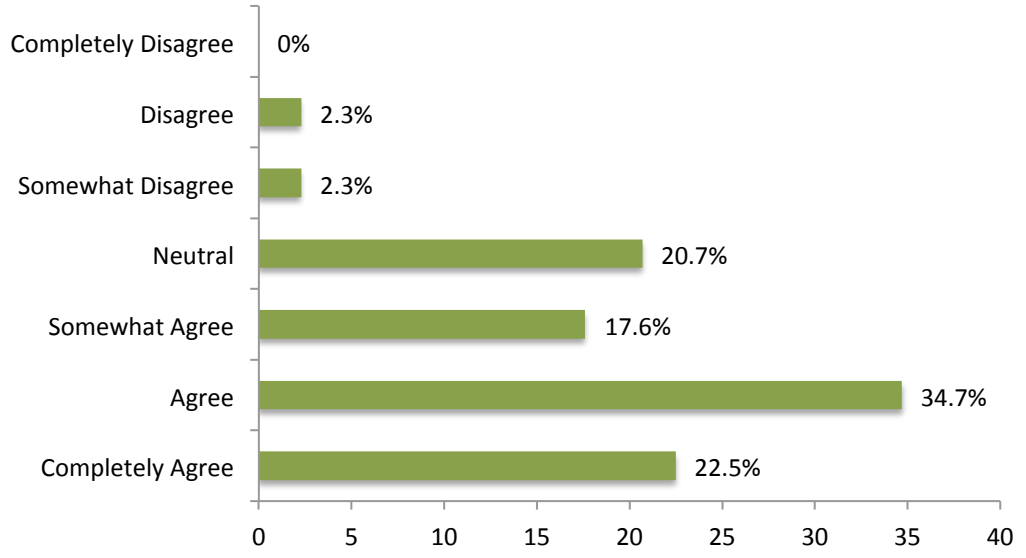

Figure 3: I think it is important to have access to cybercrime victimization statistics.

Based on the results of this item, it is evident the majority of participants find it important to have access to cybercrime victimization statistics. It is worth noting that the results of these three items were corroborated by my interview data where interviewees expressed that they found both the reporting of cybercrimes and having access to cybercrime victimization statistics to be important, but there was not a single interviewee that knew how to officially report a cybercrime.

Discussion

It is evident from the results of my study that undergraduate students are at risk of being victimized; therefore, I find it troubling that many do not know how to report a cybercrime. Fariborzi and Hajibaba (2012) provide a systematic review of what entities oversee Internet crime complaints in a number of countries including the United States. They point out that in the United States the FBI local offices, U.S. Secret Service, and the Internet Crime Complaint Center (IC3) handle the reporting of cybercrimes such as hacking, Internet fraud, and cyberharassment (Fariborzi and Hajibaba, 2012). The Internet Crime Complaint Center (IC3) provides cybercrime victims the opportunity to report their victimization officially and also provides access to annual reports of cybercrime victimization in the United States. Survey participants were asked about whether they had heard of the IC3. The results of this item showed that an overwhelming majority of participants had not heard of the IC3 (212 participants; 95.5%) and only a small percentage had heard of the IC3 (10 participants; 4.5%). Similarly, there was not a single interviewee who knew how to officially report a cybercrime. According to its website, the IC3 was created as

> "a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) to receive Internet related criminal complaints and to further research, develop, and refer the criminal complaints to federal, state, local, or international law enforcement and/or regulatory agencies for any investigation they deem to be appropriate" (www.ic3.gov/about/default.aspx).

Aside from being a referral mechanism for Internet crime complaints, the IC3 also provides annual reports of the crime complaints they have received since 2003. The IC3's latest annual

report was published in 2013. According to the 2013 IC3 Internet Crime Report, the IC3 received a total of 262,813 consumer complaints totaling $781,841,611 in loss. 45.5% of the complaints reported to the IC3 entailed financial loss ("2013 Internet Crime Report," 2013). Even though the IC3 encourages all types of Internet crimes to be reported despite whether a financial loss occurred, the report mainly consists of different types of Internet fraud that were reported. In 2013, California was the #1 ranked state in terms of the total number of complaints the IC3 received constituting for 12.13% of the total complaints ("2013 Internet Crime Report," 2013). The IC3 listed some of the Internet scams they received the most complaints about and some of these scams (i.e. romance scam, auto fraud, impersonation scam) were listed on the interview artifact that was presented to interviewees (see Appendix A). It was particularly interesting that despite these scams being among the most prevalent Internet crimes mentioned in the complaints the IC3 received, interviewees mentioned not being familiar or ever having heard of such scams (i.e. romance scam, auto fraud). This may in part be due to the fact that there is a wide age range of people (i.e. age 20 and older) who filed a complaint with the IC3 and are more likely to experience such scams than undergraduate students are. The IC3 also provides helpful Internet crime prevention tips on their website (www.ic3.gov) to protect Internet users from falling victim to common types of fraud (i.e. identity theft, credit card fraud). The IC3 also runs the website, www.lookstoogoodtobetrue.com, which provides a list of testimonials from people who either fell victim to or experienced a scam and how they avoided being a victim. The website also provides information about different types of fraud (i.e. financial fraud, identity theft, etc.) along with a list of respective avoidance tips.

Since the 2013 IC3 annual report primarily focuses on providing a summary of different types of Internet fraud, I find it particularly troubling that the majority of survey participants have never heard of the IC3 since the survey also asked whether participants had been a victim of such related cybercrimes such as a fraud/scam, credit card fraud, identity theft, or phishing. For example, 43 survey participants (19.4%) stated that they were victims of phishing while in college; the third highest cybercrime survey participants reported being victims of. Moreover, interviewees #1 and #7 were both victims of online fraud and experienced financial loss; interviewee #1 lost $220 and interviewee #7 lost $250. Knowing about the IC3 could have been useful for not only these two interviewees, but also the survey participants who also reported being victims of online fraud. It is evident that a resource like the IC3 is needed for undergraduate students, but that there needs to be more awareness about its existence since it is evident that there are not many undergraduate students who have heard of it.

An interesting result I found from my study occurred when I was checking the significance of my hypothesized linear regression models. I hypothesized that the variable, cybercrime victimization, would have a statistically significant positive effect on cybercrime perceptions; this means that an increase in cybercrime victimization would also result in an increase in undergraduate students' perceived fear or concern of cybercrimes. In the end, I found the opposite to be true as cybercrime victimization was found to not be statistically significant in predicting for cybercrime perceptions. One potential explanation I have for why this result may have occurred can be related to the wording of the questions that were asked mainly revolving around the usage of the word "victim" to indicate that a participant was

victimized by the cybercrime inquired about. For example, it may be possible for a participant who experienced credit card fraud and received a proper resolution (i.e. called his/her bank, was absolved of the charges, and issued a new card) that he/she may no longer consider himself/herself as a victim since a resolution was given; however, for the purposes of my study I would still consider such a participant a victim despite a resolution being reached since the individual still experienced the full nature of the cybercrime. I made the decision to keep the usage of the word "victim" since I did not come across any issues using the label when conducting my interviews. One possible solution to minimizing the possibility of multiple interpretations of the usage of "victim" would be to simply provide a definition of what would constitute a person to be considered a victim.

One cause of underreporting of cybercrimes can be due to a computer user's lack of knowledge in knowing that what he/she experienced is indeed a cybercrime. It is evident from the results of my study that participants were not completely certain or accurate about their knowledge of cybercrimes. For example, 26.1% of survey participants agreed with the following statement: "Sometimes I doubt whether I know enough about cybercrimes." Interviewees were also not completely certain of all the cybercrimes listed on the artifact presented to them. An inaccurate perception of the extent to which a computer user believes he/she knows about cybercrimes can significantly impact the mere consideration of reporting a cybercrime. This is primarily why I was so interested in understanding where exactly participants acquired their cybercrime knowledge from. Very few interviewees mentioned learning about cybercrimes through an educational channel and as it stands only certain departments on campus provide courses that touch on the subject. Better awareness and

proper education about cybercrimes can not only minimize the confusion about cybercrimes, but also better prepare undergraduate students to mitigate their cybercrime risk. Given the interdisciplinary nature of cybercrimes, Stockman (2013) presents a case example of his efforts to create two separate undergraduate information technology courses at his university, which looked at how the social science disciplines of criminal justice and political science inform information technology. The objective of creating such course offerings was to help provide information technology students with "…a deeper understanding of cybersecurity problems and to present interdisciplinary methodological approaches to students who, in their careers, will be tasked with defending against cyberthreats" (Stockman, 2013, p. 121). Overall, the two courses were well received by the students (Stockman, 2013). At UCI, there are a few course offerings that relate to cybersecurity or cybercrimes, but are either offered by the Criminology, Law and Society department, Information and Computer Science department, or Computer Science department. These courses are offered on a limited basis and most give priority to major students when enrollment opens. It would be ideal if such interdisciplinary courses were open to all majors on campus to take so that students outside of technical departments like Computer Science can get exposure to the online threats that exist and to learn how they can better protect themselves online.

Having access to cybercrime victimization statistics was voiced as being important to both interviewees and survey participants. A number of interviewees expressed that they would find it useful for the UCI police department to post cybercrime victimization statistics of cybercrimes that affect their fellow peers on campus; currently, there are only statistics for

offline crimes (i.e. murder, robbery, rape, stalking, etc.) that students report in a given year. I believe that in the same way offline crime statistics are posted on the UCI police department website so should cybercrime statistics. On campus cybercrime statistics can act as a tool for which undergraduate students can not only see the prevalence of such activity affecting their fellow peers, but also promote more precaution to be taken when interacting online.

Conclusion

In this two-part study, qualitative and quantitative methods were employed. In the first part, semi-structured interviews were conducted to gain a deeper understanding of what practices (i.e. security measures) undergraduate students employ, the level of cybercrime knowledge they have, the perceptions they have of cybercrimes specifically in terms of severity, whether a cybercrime incident was reported if a student was victimized, and whether they know how to report cybercrimes. A total of 10 participants were interviewed. The results from the interviews set the groundwork for the questions that were asked in the second part of the study, which was an online survey. Based on the survey results, four linear regression models were created that predicted for perceptions (i.e. fear and concern) of cybercrimes, preventative measures that can mitigate cybercrime victimization, enabling behaviors that can lead to cybercrime victimization, and the likelihood of cybercrime reporting. A total of 222 survey responses were collected.

The results from the study show that undergraduate students are victimized by cybercrimes. Based on survey results, the top three cybercrimes participants were victims of were malware (33.8%), hacking (19.8%), and phishing (19.4%). Undergraduate students' cybercrime knowledge was shown to predominantly come from the media and through personally knowing someone who had been victimized by a cybercrime (i.e. vicarious cybercrime experiences). Survey participants reported personally knowing someone who had been victimized by malware the most (75.2%) while knowing someone who had been victimized by identity theft the least (31.1%). Survey participants reported hearing the most media stories about credit card fraud, online fraud/scams, identity theft, and hacking while hearing about

phishing and malware the least through media stories. These results were previously affirmed through the interviews that were conducted where a majority of interviewees shared that they personally knew a friend or family member who had been a victim of a cybercrime (i.e. vicarious cybercrime experiences), read online news articles, and watched TV shows or films, which informed their knowledge of cybercrimes. Despite the fact that survey participants expressed that they found reporting cybercrimes and having access to cybercrime victimization statistics to be important, the majority of participants reported not feeling confident in their ability to report a cybercrime. Similarly, interviewees found reporting cybercrimes and having access to cybercrime victimization statistics to be important, but there was not a single interviewee who knew who how officially report a cybercrime. An overwhelming majority of survey participants (95.5%) had not heard of the IC3, which provides a formal mechanism for people to report their cybercrime victimization. Lastly, four linear regression models were created based on the survey data collected. The models predicted for undergraduate students' perceptions (i.e. fear and concern) of cybercrimes, preventative measures that can mitigate cybercrime victimization, enabling behaviors that can lead to cybercrime victimization, and the likelihood of cybercrime reporting. All four models were shown to be statistically significant. As previously mentioned, some of my hypotheses of the kinds of effects some of the independent variables would have on the dependent variables were disproven. For instance, cybercrime perceptions and cybercrime knowledge were found to have a negative effect on preventative measures and cybercrime perceptions, respectively. Variables such as cybercrime victimization and information security knowledge were omitted from the model predicting for cybercrime perceptions. I hypothesized that both cybercrime victimization and information security

knowledge would be good predictors and have positive effects on cybercrime perceptions, but both variables ended up not being statistically significant. Future work should be done that looks at adding more items to the constructs tested in this study and using think aloud testing of the questions to see if the wording of the questions intended to be asked are not ambiguous.

References

2013 Internet Crime Report. (2013). Retrieved April 29, 2015, from https://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

2013 - The Impact of Cybercrime. (2013, November 1). Retrieved May 1, 2015, from http://resources.infosecinstitute.com/2013-impact-cybercrime/

Anderson, C., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly* *34*(3), 613-A15.

Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice*, *38*(3), 227, 236.

Fariborzi, E., & Hajibaba, M. (2012). Computer crimes, problems, Law enforcement for solving complaints and education. *International Proceedings of Computer Science & Information Technology*, *43*.

Fennis, B. M., Janssen, L., & Vohs, K.D. (2009). Acts of Benevolence: A Limited-Resource Account of Compliance with Charitable Requests. *Journal of Consumer Research*, *35*(6), 906-924

Graves, J., Acquisti, A., & Anderson, R. (2014). Experimental Measurement of Attitudes Regarding Cybercrime.

Henson, B., Reyns, B., & Fisher, B. (2013). Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization. *Journal of Contemporary Criminal Justice*. SAGE.

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.

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies*, *8*(4), 298-309.

Rader, E., Wash, R., & Brooks, B. (2012, July). Stories as informal lessons about security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 6). ACM.

Smith, A., Rainie, L., & Zickuhr, K. (2011, July 18). College students and technology. Retrieved May 1, 2015, from http://www.pewinternet.org/2011/07/19/college-students-and-technology/

Stockman, M. (2013, October). Infusing social science into cybersecurity education. In *Proceedings of the 14th annual ACM SIGITE conference on Information technology education* (pp. 121-124). ACM.

Wiederhold, B. K. (2014). The role of psychology in enhancing cybersecurity. *Cyberpsychology, Behavior, and Social Networking, 17*(3), 131-132.

Yar, M. (2013). *Cybercrime and Society* (2nd ed.). SAGE.

APPENDIX A

List of Cybercrimes

- Malware ("computer contaminant"):
    - Viruses
    - Worms
    - Trojan horse
    - Spyware
    - Ransomware
    - Rootkits
    - Adware
    - Scareware
    - Backdoors
- Hacking
- Cracking
- Distributed Denial of Service (DDoS) Attack
- Keylogger/Keystroke Logger
- Fraud
    - Bank fraud
    - Identity theft
    - Extortion
    - Real estate fraud
    - Romance scam
    - Auto fraud
    - Impersonation scam (e.g. of a law enforcement agency such as the FBI)
- Phishing
- Cyberstalking
- Cyberharassment
- Pharming
- Spam
- Hate speech
- Sexting

APPENDIX B

Online Survey Questions

You are being asked to participate in a survey about undergraduate cybercrime victimization and undergraduate students' perceptions of cybercrimes as a part of a Master's thesis research project. Your feedback in this survey is vital in helping us better understand the extent to which undergraduate students are victimized online, how undergraduate students perceptions of cybercrimes are formed, and whether cybercrimes are reported. The following is a link that provides more information about the study: http://goo.gl/9SMhQx.

The only criteria to participate in the study is to be a current UCI undergraduate student and be 18 years or older. Once you have completed the survey, you will be asked to provide your email address to be entered in a raffle to win one of ten $10 Starbucks gift cards.

If you have any questions regarding this survey please contact Moury at mbidgoli@uci.edu. Thank you for your interest and participation in this research study!

Demographics

1. Gender:
   □ Male
   □ Female
   □ Other
2. How old are you? _____
3. What school does/do your major(s) reside in? *Note: if you are a double major check all the schools you are affiliated with.
   ☐ Arts
   ☐ Biological Sciences
   ☐ Business
   ☐ Education
   ☐ Engineering
   ☐ Humanities
   ☐ Information and Computer Sciences
   ☐ Nursing Science
   ☐ Pharmaceutical Sciences
   ☐ Physical Sciences
   ☐ Public Health
   ☐ Social Ecology
   ☐ Social Sciences
   ☐ Undecided/Undeclared

4. What is your current academic standing at UCI?
   □ Freshman
   □ Sophomore
   □ Junior
   □ Senior

Construct: Cybercrime Victimization

1. Have you been a victim of malware while in college?
   Examples of malware: virus, worm, trojan horse, spyware, adware, etc.
2. Have you been a victim of a hacked online account via any type of website (i.e. social media, e-commerce/online shopping, email, etc.) you have used while in college?
3. Have you been a victim of credit card fraud while in college?
4. Have you been a victim of any other type of online fraud/scam while in college?
   Online fraud/scam examples: commercial fraud, bank fraud, etc.
5. Have you been a victim of identity theft while in college?
   Identity theft: the illegal use of someone's private information that involves fraud or deception and is typically used for economic gain.
6. Have you been a victim of phishing while in college?
   Phishing: a legitimate looking email that frauds a person into giving out his/her private information.

   Measurement Scale:
   □ Yes = 1
   □ No = 0

Construct: Vicarious Cybercrime Experiences

1. Do you personally know anyone (i.e. a friend, family member, classmate, etc.) who has been a victim of malware?
   Examples of malware: virus, worm, trojan horse, spyware, adware, etc.
2. Do you personally know anyone who has been a victim of a hacked online account via any type of website?
3. Do you personally know anyone who has been a victim of credit card fraud?
4. Do you personally know anyone who has been a victim of any other type of an online fraud/scam?
   Online fraud/scam examples: commercial fraud, bank fraud, etc.
5. Do you personally know anyone who has been a victim of identity theft?
   Identity theft: the illegal use of someone's private information that involves fraud or deception and is typically used for economic gain.
6. Do you personally know anyone who has been a victim of phishing?
   Phishing: a legitimate looking email that frauds a person into giving out his/her private information

Measurement Scale:
□ Yes = 1
□ No = 0

Construct: Media Exposure

1. How often do you read/watch media stories (i.e. TV show, film, online news article, newspaper, etc.) about someone being a victim of malware?
   Malware examples: virus, worm, trojan horse, spyware, adware, etc.
2. How often do you read/watch media stories about someone being a victim of a hacked online account via any type of website?
3. How often do you read/watch media stories about someone being a victim of credit card fraud?
4. How often do you read/watch media stories about someone being a victim of any other type of online fraud/scam?
   Online fraud/scam examples: commercial fraud, bank fraud, real estate fraud, etc.
5. How often do you read/watch media stories about someone being a victim of an identity theft?
   Identity theft: the illegal use of someone's private information that involves fraud or deception and is typically used for economic gain.
6. How often do you read/watch media stories about someone being a victim of phishing?
   Phishing: a legitimate looking email that frauds a person into giving out his/her private information.

   Measurement Scale:
   □ Never = 1
   □ Very Rarely = 2
   □ Rarely = 3
   □ Occasionally = 4
   □ Frequently = 5
   □ Very Frequently = 6

Construct: Security Knowledge/Self-efficacy

1. Taking the necessary security measures is entirely under my control. **(Omitted)**
2. I am confident in my ability to protect myself from cybercrimes.
3. I have the knowledge to take the necessary security measures.
4. Taking the necessary security measures is easy. **(Omitted)**
5. I know how to protect myself against cybercrimes.

Measurement Scale:
□ Completely Disagree = 1
□ Disagree = 2
□ Somewhat Disagree = 3
□ Neutral = 4
□ Somewhat Agree = 5
□ Agree = 6
□ Completely Agree = 7

Construct: Cybercrime Knowledge/Self-efficacy

1. I feel that I am knowledgeable about cybercrimes.
2. I know the effects cybercrimes can have on my life.
3. I understand the differences between different types of cybercrimes.
4. Sometimes I doubt whether I know enough about cybercrimes. **Reverse coded 7 to 1**
5. I don't understand most cybercrimes. **Reverse coded 7 to 1**

Measurement Scale:
□ Completely Disagree = 1
□ Disagree = 2
□ Somewhat Disagree = 3
□ Neutral = 4
□ Somewhat Agree = 5
□ Agree = 6
□ Completely Agree = 7

Construct: Self-control

1. I feel like I make rational decisions when I am online.
2. I often act without thinking through all the consequences of my online actions. **Reverse coded 7 to 1**
3. I engage in risky online behavior. **Reverse coded 7 to 1**

Measurement Scale:
□ Completely Disagree =1
□ Disagree = 2
□ Somewhat Disagree = 3
□ Neutral = 4
□ Somewhat Agree = 5
□ Agree = 6
□ Completely Agree = 7

Construct: Harmfulness of Cybercrimes

1. How harmful do you find malware to be?
   Malware examples: virus, worm, trojan horse, spyware, adware, etc.
2. How harmful do you find hacking to be?
3. How harmful do you find credit fraud to be?
4. How harmful do you find online fraud/scams to be?
   Online fraud/scam examples: commercial fraud, bank fraud, etc.
5. How harmful do you find identity theft to be?
   Identity theft: the illegal use of someone's private information that involves fraud or deception and is typically used for economic gain.
6. How harmful do you find phishing to be?
   Phishing: a legitimate looking email that frauds a person into giving out his/her private information.

   Measurement Scale:
   □ Not Harmful at All = 1
   □ Minimally Harmful = 2
   □ Moderately Harmful = 3
   □ Very Harmful = 4
   □ Extremely Harmful = 5

Construct: Fear and Concern of Cybercrimes (Cybercrime Perceptions)

1. I believe cybercrimes can ruin someone's life.
2. I'm not concerned about being a victim of a cybercrime. **Reverse coded 7 to 1**
3. I am fearful of being a victim of a cybercrime.

   Measurement Scale:
   □ Completely Disagree = 1
   □ Disagree = 2
   □ Somewhat Disagree = 3
   □ Neutral = 4
   □ Somewhat Agree = 5
   □ Agree = 6
   □ Completely Agree = 7

Construct: Preventative measures

1. I use anti-virus software. **(Omitted)**
2. I delete spam emails without opening them. **(Omitted)**
3. I use unique passwords across all my online accounts.
4. I check to make sure an online connection is secure.
5. I check websites for privacy policies and privacy seals (e.g. TRUSTe, VeriSign).

6. I provide fake private information about myself online. **(Omitted)**

   Measurement Scale:
   □ Never = 1
   □ Very Rarely = 2
   □ Rarely = 3
   □ Occasionally = 4
   □ Frequently = 5
   □ Very Frequently = 6

Construct: Enablers

1. I provide payment information to unknown websites.
2. I interact with unknown individuals online.
3. I visit websites with illegal content.
4. I give out my private information online.
5. I open emails from senders I don't know.

   Measurement Scale:
   □ Never = 1
   □ Very Rarely = 2
   □ Rarely = 3
   □ Occasionally = 4
   □ Frequently = 5
   □ Very Frequently = 6

Construct: Likelihood of Reporting

1. If you were a victim of malware, how likely are you to report it to the appropriate entity?
   Malware examples: virus, worm, trojan horse, spyware, adware, etc.
2. If you were a victim of a hacked online account, how likely are you to report it to the appropriate entity?
3. If you were a victim of a credit card fraud, how likely are you to report it to the appropriate entity?
4. If you were a victim of any other type of online fraud/scam, how likely are you to report it to the appropriate entity?
   Online fraud/scam examples: commercial fraud, bank fraud, etc.
5. If you were a victim of identity theft, how likely are you to report it to the appropriate entity?
   Identity theft: the illegal use of someone's private information that involves fraud or deception and is typically used for economic gain.

6. If you were a victim of phishing, how likely are you to report it to the appropriate entity? Phishing: a legitimate looking email that frauds a person into giving out his/her private information.
7. How likely are you to report your cybercrime victimization to the local police?
8. How likely are you to report your cybercrime victimization to the FBI?

Measurement Scale:
□ Highly Unlikely = 1
□ Unlikely = 2
□ Somewhat Unlikely = 3
□ Neutral = 4
□ Somewhat Likely = 5
□ Likely = 6
□ Highly Likely = 7

General Reporting Self-Efficacy/Importance of Reporting

1. Have you heard of the IC3 (the Internet Crime Complaint Center)?

Measurement Scale:
□ Yes = 1
□ No = 0

1. I know how to and to whom I should report a cybercrime I have experienced.
2. I think it is important to report cybercrimes.
3. I think it is important to have access to cybercrime victimization statistics.

Measurement Scale:
□ Completely Disagree = 1
□ Disagree = 2
□ Somewhat Disagree = 3
□ Neutral = 4
□ Somewhat Agree = 5
□ Agree = 6
□ Completely Agree = 7