When Cybercrimes Strike Undergraduates

Morvareed Bidgoli
College of Information Sciences and Technology
The Pennsylvania State University
University Park, PA, United States
mbidgoli@psu.edu

Bart P. Knijnenburg
School of Computing
Clemson University
Clemson, SC, United States
bartk@clemson.edu

Jens Grossklags
College of Information Sciences and Technology
The Pennsylvania State University
University Park, PA, United States
jensg@ist.psu.edu

***Abstract*— Cybercrimes can cause various kinds of harm to those affected. This paper focuses on how cybercrimes impact undergraduate students, a group particularly vulnerable to cybercrimes due to their extensive use of technology and their recently gained financial responsibility and social independence. We present a mixed methods study to understand students' knowledge, perceptions, and behaviors regarding cybercrimes. 10 semi-structured interviews provided the groundwork for a theoretical model, which was subsequently tested on a sample of 222 survey responses. We found that roughly half of the undergraduate students in our studies have experienced one or more cybercrimes while in college, with malware, hacking, and phishing being the most prominently experienced cybercrimes. Furthermore, we found that students acquire their knowledge of cybercrimes predominantly through people they personally know who have been victimized by a cybercrime and the media. Our model shows how students' knowledge of cybercrimes and their self-control in using the Internet influences their perceived cybercrime self-efficacy and their fear of cybercrimes. Self-efficacy and fear, in turn, influence their tendency to take preventative measures to avoid enabling behaviors and to report cybercrimes to the appropriate entities. We also find that despite the reported importance of adequate cybercrime reporting and access to comprehensive cybercrime statistics, the majority of students do not know how to officially report a cybercrime.**

Keywords—interview study; survey study; cybercrimes; undergraduate students; victimization; perceptions; reporting

I. INTRODUCTION

Cybercrimes are a pressing issue worth addressing. In 2014, the Internet Crime Complaint Center (IC3) received 269,422 complaints with a total loss of approximately $800 million; 45.9% of the complaints received reported financial loss [1]. Beyond the scope of cybercrimes officially reported, McAfee estimates that cybercrimes cost the United States $100 billion annually with worldwide costs estimated at $300 billion annually [2]. Additionally, in 2014, the largest consumer data breach to date occurred when credit and debit card information of approximately 56 million customers of the home improvement retail chain, Home Depot, were stolen [3].

Despite existing behavioral work on specific cybercrimes [4]–[8] we found no literature investigating more generally how computer users' knowledge of cybercrimes influences their perceptions, and, in turn, their intentions to mitigate cybercrime victimization. We believe understanding computer users' perceptions to be important because their fear of cybercrimes and their perceived ability to mitigate cybercrime victimization (i.e., self-efficacy) can influence whether preventative measures will be taken, risky online behaviors will be avoided, and eventual victimizations will be reported to the appropriate entities.

In this paper, we focus on cybercrime victimization among undergraduate students since they are a highly active segment of the computer user population (in 2010, the Pew Research Center reported that 98% of undergraduate students use the Internet [9]) who have usually just recently gained financial responsibility and social independence, making them a likely target for cybercriminals. Since cybercrime is a topic that is not necessarily taught at school, we were particularly interested in understanding where students' cybercrime knowledge comes from, so we can better explain how they perceive cybercrimes and how they deal with cybercrime victimization. Finally, we were interested in understanding whether undergraduate students report any of the cybercrimes they experience and whether they are familiar with the appropriate procedures for doing so.

Since this is arguably the first systematic investigation of undergraduate students' knowledge, perceptions, and behaviors regarding cybercrimes, we take a mixed methods approach, employing:

- Semi-structured interviews with 10 participants to qualitatively explore the topic and help inform the development of a theoretical model.
- An online survey with 222 participants to quantitatively test the theoretical model.

With these two studies we attempt to answer the following research questions:

RQ #1: How prevalent is cybercrime victimization among undergraduate students and how do past victimizations affect their perceptions of cybercrimes?

RQ #2: Where does undergraduate students' knowledge of cybercrimes come from, and how does this knowledge affect their perceptions of cybercrimes?

RQ #3: What are undergraduate students' perceptions (i.e., fear, self-efficacy) of cybercrimes, and how are these perceptions related to each other?

978-1-5090-2922-8/16/$31.00 ©2016 IEEE

RQ #4: What is the effect of undergraduate students' perceptions of cybercrimes on their subsequent behavior (i.e., taking preventative measures, avoiding enabling behaviors, and reporting cybercrimes)?

This paper is structured as follows: After discussing relevant related work, we present the results of semi-structured interviews conducted with 10 participants that provided the groundwork for a theoretical framework surrounding our research questions. Subsequently, we present the results of an online survey with 222 participants that was employed to test this theoretical model. Finally, we discuss our findings and conclude with suggestions for future work.

II. Related Work

A. Past Cybercrime Victimizations

In a cross-sectional survey of 15-74 year-olds in Finland, Oksanen and Keipi [10] found that cybercrime victimization is more prevalent in the age group of 15-24 year-olds than in older age groups. 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. The study also found that previous cybercrime victims expressed being concerned about being victimized again within the next year.

B. Cybercrime Perceptions

Henson et al. [5] conducted an online survey of 838 undergraduate students at a large public university that looked at the effect of perceived risk of direct, indirect, and previous Online Interpersonal Victimization (OIPV) on the fear of OIPV by an intimate partner, friend/acquaintance, and stranger. The study found that perceived risk of OIPV had positive effects on all three types of victim-offender relationships, previous direct online victimization had a positive effect on fear of OIPV by an intimate partner, previous indirect online victimization had a 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) did not have a statistically significant effect on any of the types of victim-offender relationships.

Graves et al. [11] 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 study found that the scope (i.e., number of records downloaded) and the motivation of the cybercriminal (particularly for a monetary gain) had significant effects on the perceived seriousness of the cybercrime.

Riek et al. [12] used Structural Equation Modeling (SEM) to investigate the effects of media awareness, cybercrime experience, and perceived cybercrime risk on the avoidance of three online services: online banking, online shopping, and online social networking. The authors found that cybercrime experience and media awareness increase perceived cybercrime risk, which in turn increases the intention to avoid all three online services.

C. Exposure via Others and Media

Rader et al. [13] conducted a survey among 301 undergraduate students to see how non-expert computer users use the stories they hear from others to make security decisions. Six different types of security stories emerged: 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. 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 behaviors and the way in which virtually all respondents thought about security. 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. Lastly, nearly half of respondents reported retelling a story to others.

Yar [14] 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 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" (p. 4).

D. Self-control

Self-control Theory (also known as the General Theory of Crime) posits that individuals with low self-control (i.e., impulsive, short-sighted, engage in risk-taking behavior) are more likely to commit crime [15]. Although the original theory focuses on the offender, the theory has also been used to explain victimization. For example, Bossler and Holt [4] conducted a study with a sample of 573 undergraduate students and found that low self-control increases the likelihood of three types of cybercrime victimization: password access, having computer information changed, and cyberharassment.

Similarly, van Wilsem found that individuals with low self-control had a higher likelihood of being victims of hacking, cyberharassment, and "diversified victimization" (both hacking and cyberharassment) [7], and that individuals with low self-control who engage in risky online activities (i.e., impulsive online purchasing, online forums) are at increased risk of being victims of online consumer fraud [8]. Van Wilsem [8] predicted that a 20 year-old individual with an academic education who is both an active online shopper and forum participant, but has low self-control, is 43.1% more likely to be a victim of online consumer fraud; thus, engagement in risky online activities (i.e. impulsive online purchasing) increases the likelihood of online consumer fraud victimization.

A behavioral economic perspective that helps to explain the prominent effect of self-control on cybercrime victimization is *hyperbolic discounting*. Hyperbolic discounting describes the notion that when a consumer can achieve a short-term gain (e.g., a disregard of safe Internet usage practices to use a service) at a potential long-term cost (e.g., victimization of a

cybercrime), the short-term benefits can disproportionally outweigh the long-term costs. This leaves computer users—particularly those with low self-control—to underappreciate "long-term risks and losses while acting in privacy-sensitive [or security-sensitive situations]" [16].

E. Enabling Behaviors

Van Wilsem [7] found that personal guardianship (i.e., computer knowledge) had an unforeseen effect on the likelihood that an individual would be at risk of being hacked finding that individuals who lacked computer security software knowledge actually had less of a likelihood of being hacked. However, computer "illiteracy" also has the consequence of preventing individuals from being able to effectively recognize whether they are victims of hacking. Van Wilsem also found that online deviance (i.e., looking at pornographic material, accessing someone's computer without permission) was shown to increase the likelihood that an individual would be at risk of being harassed online, while long-time usage of Internet communication activities was shown to increase the risk of being harassed online as well as diversified victimization.

Bossler and Holt [4] found that online deviance had a 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 positive effects on the likelihood of victimization of password access, having computer information changed, malware, credit card theft, and cyberharassment.

Marcum et al. [6] conducted a study among undergraduate students to investigate three different types of cybercrime victimization: the receipt of sexually explicit material, non-sexual harassment, and sexual solicitation. They found that Internet and Computer Mediated Communications usage (e.g., email, chat rooms, social networking sites) increased the likelihood of victimization. They also found that providing personal information and communicating with people met online increase the likelihood of victimization.

F. Preventative Measures

Not enough is known about the protective measures that users take to mitigate cybercrimes. Interestingly, Marcum et al. [6] found that protective measures (i.e., anti-virus software) did not prove to mitigate cybercrime victimization (see also [17]–[19]).

Wash and Rader's [20] survey may give an explanation for this finding; their study looked at the specific behaviors users undertook to protect themselves against viruses and hackers. The three behaviors that were employed by users to protect against viruses and hackers were trust-in-software (i.e., use of anti-virus, firewall), trust-in-self (i.e., use of good passwords, blocking popups), and expert security settings (i.e., updating software patches, backing up information). Interestingly, the study found that users who utilized anti-virus software and avoided downloads to ward off risk of being a victim of a virus, were actually shown to be more likely to engage in risky behaviors, since such individuals were shown to be less likely to employ trust-in-software and trust-in-self actions. Lastly, the study also found that older individuals engage in more careful behaviors to protect themselves from viruses and hackers.

G. Reporting Cybercrimes

Similar to protective measures, very little is known about users' cybercrime reporting behaviors. Van Wilsem [7] found that people with little knowledge of computer security software had lower chances of reporting hacking victimization.

Yar [14] provides a number of reasons for why under-reporting of cybercrimes can occur, including the suggestion that victims may consider the cybercrime they experienced to lack enough seriousness to contact the authorities. 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 cyber-criminal) can be achieved.

Both Yar [14] and Wall [21] state that a cybercrime victim may be unaware that they experienced a cybercrime. Fafinski et al. [22] further note that this may be due to a lack of expertise in understanding the nature of cybercrimes. Al-Nemrat et al. [23] elaborate on this point by stating that "cybercrime" is a term people are familiar with, but that no specific definition exists, and that there are many interpretations as to what a cybercrime constitutes. They explain that this definitional issue can greatly affect the process of investigation and reporting.

H. Gaps in the Literature

Most of the discussed work focuses on explaining the causes of cybercrime victimization, while only limited work has been done to explain what factors influence computer users' cybercrime *perceptions* (a notable exception is Riek et al. [12], who focus on an EU sample of users that extends beyond college students). Moreover, not enough is known about cybercrime victims' reporting behavior, for example, we came across very little literature that looked at how computer users' perceptions of cybercrimes (i.e., fear, self-efficacy) affect their likelihood to report a cybercrime. Lastly, while existing studies on undergraduate student samples focus on specific cybercrimes, there is very little literature that focuses on understanding how cybercrimes as a whole affect the undergraduate student population (not focusing on college students, Riek et al. [12], is again a notable exception).

III. Interviews

A. Procedures

Ten semi-structured interviews were conducted to gain a deeper understanding of what practices (i.e., security measures) undergraduate students employ to mitigate cybercrime victimization, their level of cybercrime knowledge, the extent to which they have been victims of cybercrimes, whether they had ever reported a cybercrime incident, and how much they know about reporting procedures. Participants were recruited among undergraduate students, 18 years or older, and who had either been a victim of a cybercrime while in college or had some knowledge about cybercrimes. Since at the outset of the interview study we had no knowledge of exactly what cybercrimes undergraduate students were most susceptible to being victims of, we left the definition of cybercrimes to be generally broad—ranging from socially engineered crimes (i.e., phishing) to technically oriented crimes (i.e., malware, hacking)—because we did not want to limit participation to

victims of a preconceived list of cybercrimes. Recruitment was done through social media (i.e., Facebook), brief in-class announcements, class emails sent out by various professors from different departments, and flyers posted around campus. All interviews were conducted in person on campus at a time convenient for both the researcher and interviewee. Interviews were audio recorded with the interviewee's consent. Interviews were subsequently transcribed and coded. The important themes that emerged from the interview data provided the groundwork for the questions asked in the online survey study. No incentives were given for participation.

The main themes are described in the remainder of this section. In general, we found that even for a relatively homogenous sample of college students, the interviewees showed a surprisingly large variation in their level of *Cybercrime Self-efficacy* (i.e., their perceived ability to mitigate cybercrime victimization). Most interviews revolved around two antecedents of fear and self-efficacy (i.e., *Past Victimizations and Exposure*) and two consequences (i.e., *Reporting* and *Preventative Measures*). We describe these four main themes below.

B. Cybercrime Victimization

Five of our ten interviewees indicated having been victims of a cybercrime while in college. These cybercrimes included commercial fraud, cyberstalking, a virus, online fraud, and adware.

Interviewee #1 was a victim of commercial fraud during the end of his sophomore year. He was trying to assist his aunt in buying merchandise from Abercrombie & Fitch's website. After searching for the website through Google, he was redirected to another website: www.abercrombieoutletsale.us. He claimed that everything about the website looked exactly like Abercrombie & Fitch's in terms of the layout and merchandise sold, but it was not until after he made a purchase 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, that he never received an email notification regarding his order, and when he subsequently checked his bank statement he found that he was charged by a place in Beijing, China. To resolve the matter, he contacted Abercrombie & Fitch's customer service, who advised that nothing could be done for him and suggested he cancel his card as soon as possible. Subsequently, he reported the fraudulent charge to his bank and canceled his card. In the end, he did receive the items, which turned out to be fake merchandise and as a result he was unable to recover his money ($220). The fraudulent website no longer exists, and it now states that a lawsuit is underway. Experiencing this incident has led interviewee #1 to be more careful about making online purchases by consulting the website's policies and ensuring the website is legitimate by checking its domain or contacting its customer service before making an online purchase.

Interviewee #2 was a victim of cyberstalking during his 4th year of college. The incident involved an ex-girlfriend who knew his Facebook password and was able to gain access to other online accounts by answering security questions. He did not immediately change his passwords explaining that it would be difficult to have to change everything and keep track of the changes. He eventually changed his passwords a few months later, creating a system with different passwords for different accounts. Even after unfriending his ex-girlfriend on Facebook, she would continue to stalk him using the Facebook profiles of mutual friends. She would even stalk him on Spotify, and draw conclusions about his activities based on his music listening activity. The stalking also persisted offline, where she would track his whereabouts on campus using his work schedule as a campus shuttle driver. After an incident where his ex-girlfriend lied about being pregnant, he stopped talking to her altogether. Interviewee #2 never reported the incident to the police, because he did not want her to have a criminal record. However, he did consider reporting the incident to the Office of Student Conduct on campus.

Interviewee #3 was a victim of a virus 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. After her brother, a Computer Science student, was unable to figure out what was wrong with her computer, she decided to contact Dell customer service to see if they could resolve the issue. They were able to confirm through remote login that her computer had a virus, and offered her a solution to purchase a new version of Windows that cost $25. The overall resulting damage 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 the virus did not do any substantial damage. However, if the virus would have been able to take her personal information or hack into her online accounts saying hurtful things to others then she would have considered reporting it. Experiencing the 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. He was contacted by someone on Reddit, who was interested in purchasing some of his dogecoins (i.e., a joke minor cryptocurrency based on a dog). The person sent a fake link to a platform that looked similar to a standard cryptocurrency exchange service for Bitcoin exchanges. The interviewee ended up sending 250,000 dogecoins ($250) to the interested buyer. As soon as the dogecoins were sent, he could no longer see the transaction and the coins were gone. 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 unfamiliar with. Instead, he reported the incident to the legitimate Bitcoin exchange platform, warning them about the scam. He also reported the incident to Reddit, the platform on which he came into contact with the scammer and which subsequently banned the scammer's account. The scammer's wallet address was also flagged, which would warn other Bitcoin users to be mindful of doing future exchanges with the scammer. Experiencing this incident made interviewee #7 create unique passwords across his accounts (i.e., Facebook, Reddit, email) and become more watchful of cryptocurrency scammers on Bitcoin to the extent that he would even warn others to watch out for suspicious

transactions and to carefully evaluate 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, he came across an advertisement for a PC optimizer. The advertisement claimed that his computer was slow and showed a list of viruses along with the purportedly infected files on his computer. Upon clicking on the advertisement, his computer lost several files (i.e., work and school related files, and digital media). He resolved the issue by doing a system restore. He claimed that he wanted to report the incident, but did not know how. Experiencing the incident made him more mindful of clicking on online advertisements and motivated him to buy and install anti-virus software.

Three interviewees experienced cybercrimes, but did not fall victim to them. Interviewee #2 described an incident of phishing, which he experienced during his 4th year of college. He was personally messaged by a female on Facebook. He immediately suspected that it was phishing, based on the poor grammar and the fact that the person asked for his email address. Upon posting about receiving the message on Twitter, he found out that some of his friends had also received the same message. As a result, he decided to block the user. He did not report the incident.

Interviewee #5 described a scam she experienced within an online Chinese game. She was trying to buy a piece of equipment from someone else within the game. After chatting with the seller on a Chinese voice chat platform, she was sent a document to confirm the item she was interested in buying. She hesitated to download the file upon noticing an unfamiliar file format. As a result, she decided not to download the file. She also logged off the game and restarted her Internet connection as safety measures. She reported both the person who referred her to the seller and the seller to the respective systems' administrators.

Lastly, interviewee #6 has been continually cyberharassed by the same person for the past two years. He has received an email every week from a former friend, who is schizophrenic and has formed an obsession. The interviewee claimed he does not feel bothered or threatened by the emails, and he deletes them unopened. He did not consider reporting the person because he did not feel bothered or threatened by the communication and has never told the person to stop contacting him.

C. Exposure

We found that interviewees predominantly acquire cybercrime knowledge from someone they personally know who has been victimized in the past (i.e., Exposure via Others) or through online news articles, TV shows, etc. (i.e., Exposure via Media).

1) Exposure via Others: Eight interviewees expressed that they personally know either a friend or family member who has been a victim of a cybercrime, such as hacking via an online gaming platform or social media, phishing, identity theft, and credit card fraud, which in turn informed participants about these cybercrimes.

2) Exposure via Media: Six interviewees mentioned that they gained some of their cybercrime knowledge from media sources like online news articles, TV shows, or films. In this category, there were four interviewees who had learned about cybercrimes through the news or by reading online news articles, and three who had learned about cybercrimes through either films about cybercrimes (such as hacking and online fraud) or through detective-type TV shows.

D. Cybercrime Reporting

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 while none of the five interviewees reported their cybercrime victimizations to law enforcement, it was particularly common for interviewees to resolve their issues on their own or by reaching out to the entities involved within the space in which the cybercrime took place. Specifically:

- Interviewee #1 reported the commercial fraud he experienced to not only his bank to cancel his card, but also to Abercrombie & Fitch since the fraudulent website was impersonating the brand.
- Interviewee #3 contacted Dell customer service to help remove the virus from her computer.
- Interviewee #7 reported the online scam resulting in the theft of his dogecoins to the legitimate platform that many use for Bitcoin exchanges and also reported the incident to Reddit, which was where the scammer had contacted him.
- Interviewee #8 did not report the adware he experienced and resolved the issue on his own by doing a system restore on his computer.

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 Office of Student 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. Given these two examples, either a lack of perceived severity or personally knowing the perpetrator of the cybercrime can decrease the likelihood that it will be reported.

E. Preventative Measures

Interviewees were asked what security measures they employ to protect themselves against cybercrimes. For example, the majority of interviewees stated that they use anti-virus software as a security measure, and many interviewees mentioned looking for SSL (Secure Socket Layer) or HTTPS as an indication of a secure online connection before entering

sensitive personal information (i.e., social security numbers, credit/debit card numbers) on online forms. Other online security measures interviewees stated they employ included: password protected computers (2 participants), creating unique and complex passwords (4 participants), and providing fake or very little private information about themselves online (2 participants).

Interviewees #2 and #6 mentioned providing fake information about themselves online. Interviewee #2 stated that he uses an alias and separate contact information (i.e., an alternate email address, a Google Voice phone number, and a fake 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), which, as a result, made him less concerned about his online security.

Interestingly, interviewee #4 who was not a cybercrime victim, mentioned that she did not 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 students may not be as concerned about their online security or not feel compelled to employ online security measures since they believe to have never been victims before.

As mentioned earlier, interviewees #5 and #8 invested in obtaining certain security measures after experiencing cybercrimes. Interviewee #5 bought an e-key after experiencing (but not falling victim to) an online scam within a Chinese online game she plays. She uses the e-key whenever she plays online games. She described the e-key as a device that provides the end user with a one-time pin that needs to be entered when logging into their account. A unique, single-use number is given each time the end user uses their account; this number changes every 10 seconds. Interviewee #8 bought anti-virus software after being a victim of adware.

IV. Theoretical Model

Based on the discussed related work and interview results[1], we constructed a theoretical model that integrates undergraduate students' knowledge, perceptions, and practices regarding cybercrimes. The model, displayed in Figure 1, shows how four key factors (*Past Victimizations, Exposure via Others* and *via Media*, and *Self-control*; the latter influencing self-efficacy but not fear) influence *Fear of Cybercrime* as well as *Cybercrime Self-efficacy*. Note that we hypothesize that users with self-efficacy (i.e., a higher perceived ability to mitigate cybercrimes) have a reduced fear of cybercrimes. Consequently, students' fear and self-efficacy influences their *Intention to Report* cybercrimes, their intention to take *Preventative Measures*, and their intention to reduce their *Enabling Behaviors*.

This model shows several similarities, but also several important differences to Riek et al.'s [12] model. Like Riek et al., we place cybercrime perceptions (in our model: *Fear of Cybercrime* and *Self-efficacy*) in the center of our model, and consider the effect of cybercrime victimization, and media exposure as antecedents of these perceptions. Based on findings from our interviews and related work, we measure *Exposure via Others* and *Self-control* as additional antecedents. Moreover, unlike Riek et al., we argue that the proposed antecedents may not only increase *Fear of Cybercrime*, but also *Self-efficacy*, thereby reducing their overall effect on fear (since *Self-efficacy* reduces fear). Finally, we go beyond avoidance behaviors (the opposite of our *Enabling Behaviors*) and also include users' employment of security measures (*Preventative Measures*) and their willingness to report a cybercrime (*Intention to Report*) as consequences of cybercrime perceptions.

We tested this model in our online survey study, on which we report below.

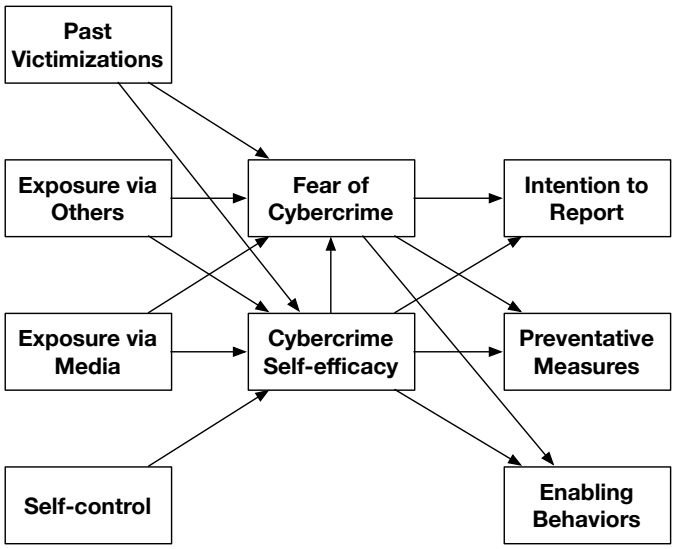

Fig. 1. A theoretical model of undergraduate students' knowledge, perceptions, and practices regarding cybercrimes.

V. Online Survey

A. Procedures

An online survey was conducted in April 2015 to formally evaluate our theoretical model. A sample of undergraduate students that were 18 years or older was recruited through a snowball sample via social media as well as class emails sent out by various professors from different departments. Participation was incentivized with a raffle of ten $10 Starbucks gift cards.

The survey contained 67 questions[2] (including demographics, yes/no questions, and Likert scale items), covering students' knowledge, perceptions and practices regarding cybercrimes.[3] The appendix details how these questions operationalize the theoretical model in Figure 1. A brief

[1] Not all modeled relationships follow directly from the interview data and/or the related work, but are inferred by the researchers on the basis of the interview data and related work.

[2] Not all survey items were used in our analyses. This is common practice for exploratory surveys [24].

[3] Based on the types of cybercrimes predominantly experienced by our interviewees, we made the decision to narrow our inquiry to cybercrimes that involved a breach of their online security or highly sensitive personal information.

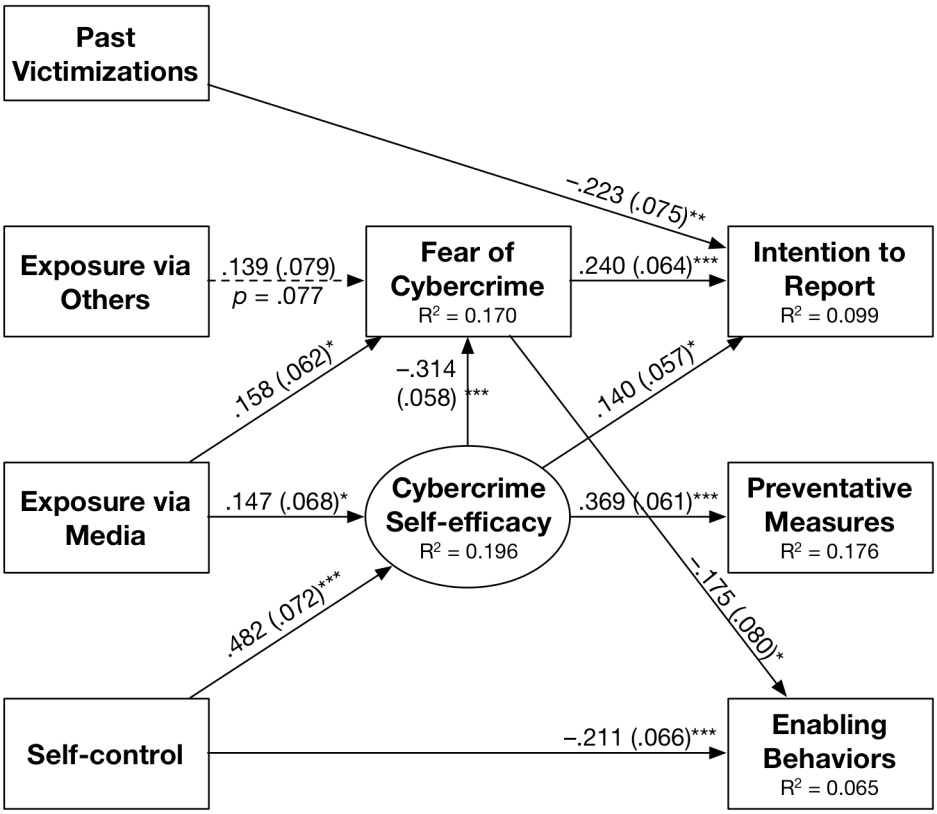

Fig. 2. Results of the online survey. Effects are standardized (with standard errors in parentheses). * $p < .05$, ** $p < .01$, *** $p < .001$.

explanation about the online survey and study along with an online link to the study information sheet (replacing the obtainment of informed consent as per IRB requirements) was provided at the beginning of the online survey.

A total of 222 survey responses were collected. The sample consisted of 154 females (69%), 67 males, and 1 student identifying as other. The majority of survey participants were between the ages of 18 and 22 with some exceptions of students who were older (15 participants). We observed a fairly representative mixture of each academic class represented in the survey results, which comprised of 33 Freshmen (15%), 57 Sophomores (26%), 58 Juniors (26%), and 74 Seniors (33%).

B. Descriptive Statistics

115 participants (52%) experienced at least one cybercrime while in college, a percentage that did not vary significantly with gender or age, but was (predictably) higher for students in higher classes, raising from 30% for freshmen to 59% for seniors. Malware was the most prominent cybercrime experienced by 75 participants (34%), followed by hacking and phishing with 44 and 43 victims (20% and 19%, respectively). Credit card fraud was the fourth most experienced cybercrime (27 participants, 12%), followed by online fraud/scams (12 participants, 5%), and finally identity theft (6 participants, 3%).

Other variables in the model were not strongly influenced by gender, age, or class level,[4] except that males had a significantly higher level of *Cybercrime Self-efficacy* and (consequently) a lower level of *Fear of Cybercrime* than females (both *p*s < .001). These effects do not significantly alter our model; hence we leave them out of subsequent analyses.

C. Structural Model

The initial model, a Structural Equation Model, was fit using a Weighted Least Squares estimator in Mplus.[5] In exploratory research, structural models can be trimmed or built based on theoretical and/or empirical standards [25]. The initial model had a few non-significant effects, which were removed from the model. Specifically, we found no effect from:

- Past Victimizations on Fear of Cybercrime
- Past Victimizations on Cybercrime Self-efficacy
- Exposure via Others on Cybercrime Self-efficacy
- Fear of Cybercrime on Preventative Measures
- Cybercrime Self-efficacy on Enabling Behaviors

Upon inspection of the model's modification indices, we also added two effects to the model, namely an effect from:

- Self-control on Enabling Behaviors
- Past Victimizations on Intention to Report

[4] We used p < .01 for these post-hoc tests.

[5] http://www.statmodel.com/

The resulting model (Figure 2) has an excellent model fit[6] ($\chi^2(42) = 49.38$, $p = .20$; *RMSEA* = .028, 90% CI: [.000, .056]; *CFI* = 0.997, *TLI* = 0.996). All effects in the model are standardized to aid the comparison of effects (i.e., a 1.00 standard deviation difference in participants' *Cybercrime Self-efficacy* is estimated to result in a 0.369 standard deviation difference in their tendency to employ *Preventative Measures*). The standard errors of the effects are displayed in parentheses with asterisks as *p*-value indicators.

D. Antecedents of Fear and Self-efficacy

There is very little that influences participants' *Cybercrime Self-efficacy*: *Past Victimizations* and *Exposure via Others* have no effect, and *Exposure via Media* has only a small significant positive effect. *Self-control* has the strongest (medium-large) effect on *Cybercrime Self-efficacy*, with those who exert more self-control reporting higher levels of self-efficacy.

Similarly, there is very little that influences participants' *Fear of Cybercrime*: *Past Victimizations* have no effect, and *Exposure via Others* and *via Media* both have small positive effects with only *Exposure via Media* being significant. *Cybercrime Self-efficacy* has the strongest (medium-sized) effect on *Fear of Cybercrime* with fear being lower for participants who report higher levels of self-efficacy.

E. Consequences of Fear and Self-efficacy

Both *Fear of Cybercrime* and *Cybercrime Self-efficacy* positively influence participants' *Intention to Report* cybercrimes, with fear having the stronger effect although both effects are small. Surprisingly, participants who experienced *Past Victimizations* reported a *lower* rather than higher *Intention to Report* cybercrimes.

Only *Cybercrime Self-efficacy* has a (medium-sized) significant positive effect on participants' tendency to take *Preventative Measures*, while *Fear of Cybercrime* has a (small) significant negative effect on participants' tendencies to engage in cybercrime *Enabling Behaviors*. *Self-control* also has a significant negative effect on *Enabling Behaviors*.

F. Total Effects

While we find several effects of the identified antecedents on *Fear of Cybercrime* and *Cybercrime Self-efficacy*, as well as several effects of these variables on behavioral consequences, we also find that an increase in *Cybercrime Self-efficacy* decreased participants' *Fear of Cybercrime*. Hence, antecedents that increase self-efficacy may consequently reduce fear, which in turn has an opposite effect on behavior. It is therefore useful to assess the *total effects* of the antecedents on the consequences. These effects are listed in Table I.

As previously mentioned, participants who experienced *Past Victimizations* had a lower *Intention to Report* cybercrimes. *Exposure via Others* has no significant effects on any of the antecedents. *Exposure via Media* has very small total effects on participants' *Intention to Report* and on their tendency to take *Preventative Measures*. Finally, *Self-control* has small total effects on both *Preventative Measures* and *Enabling Behaviors*.

TABLE I. TOTAL EFFECTS OF ANTECEDENTS ON CONSEQUENCES.

	Intention to Report	Preventative Measures	Enabling Behaviors
Exposure via Others	n.s.		n.s.
Exposure via Media	.047 (.020)*	.054 (.027)*	n.s.
Self-control	n.s.	.178 (.040)***	–.184 (.065)***

* $p < .05$, ** $p < .01$, *** $p < .001$.

VI. DISCUSSION

Our interview study showed a surprisingly large variation in interviewees' *Cybercrime Self-efficacy*. Our survey results demonstrate that to some extent *Exposure via Others* and *via Media*, and to a larger extent *Self-control* influence cybercrime perceptions. The survey results also show that these perceptions in turn influence students' *Intention to Report* cybercrimes, their tendency to take *Preventative Measures*, and their avoidance of *Enabling Behaviors*.

An interesting finding of our model involves *Cybercrime Self-efficacy*, which has to date only been regarded as a positive force in preventing cybercrimes (cf. [12]). Our results indicate that while *Cybercrime Self-efficacy* is an important requirement for participants to take control over their protection against cybercrimes, it inevitably leads to a *decrease* in *Fear of Cybercrime*. This may explain the finding by Wash and Rader [20] that users who are knowledgeable enough to mitigate cybercrime victimization are at the same time more likely to engage in risky behaviors; consequently, this may be due to their lack of fear. Similarly, Christin et al. [17] found that people were willing to install undocumented code in the face of direct incentive payments in turn ignoring commonly known security advice.

Another interesting finding is that *Past Victimizations* had a *negative* effect on *Intention to Report* cybercrimes. This finding can be partially explained by undergraduate students' lack of knowledge on how to report cybercrimes to the appropriate entities (i.e., those who have been victimized in the past realize that they are not knowledgeable about this, and hence are also less likely to report cybercrimes). In the United States, the FBI, U.S. Secret Service, and the IC3 handle reports of cybercrimes such as hacking, Internet fraud, and cyberharassment [28]. The IC3 writes annual cybercrime reports and provides cybercrime victims the opportunity to report their victimizations officially. Additionally, the IC3 provides helpful Internet crime prevention tips on its website (www.ic3.gov) to protect Internet users from falling victim to common types of fraud (i.e., identity theft, credit card fraud). We asked survey participants whether they had heard of the IC3 to which an overwhelming majority of participants had not (212 participants; 95.5%). Similarly, there was not a single interviewee who knew how to officially report a cybercrime.

From a public policy perspective, we find it concerning that the majority of survey participants have never heard of the IC3,

[6] A good model has a χ^2 that is not statistically different from a saturated model ($p > .05$) [26]. Additionally, Hu and Bentler [27] propose cut-off values for other fit indices to be: *CFI* > .96, *TLI* > .95, and *RMSEA* < .05, with the upper bound of its 90% CI falling below 0.10.

given that roughly 50% of our survey respondents and interviewees had experienced at least one cybercrime. Reporting is a crucial step, not just for students, but for cybercrime victims in general. Without consistent reporting, statistics are downwardly biased. Moreover, adequate reporting can not only serve a pedagogical function for the general public through the use of cybercrime statistics, but can also help law enforcement to combat cybercrimes and even potentially reach a proper resolution for the victim by catching the cybercriminal [29].

We suggest that work needs to be done to make undergraduate students more aware of the services provided by the IC3. For example, interviewees and survey participants noted that they would like to have access to cybercrime statistics; a service provided by the IC3. A number of interviewees expressed that a more *localized* (on-campus) cybercrime reporting mechanism would be more useful to them as the victimization statistics would resonate better if they were coming from their own demographic. Currently, the campus police at most U.S. universities reports statistics for offline crimes (i.e., assault, robbery, rape, stalking, etc.). Given the prevalence of cybercrimes among undergraduate students, we believe that campus police should also report cybercrime statistics. On-campus statistics can show students the prevalence of such crimes and promote more caution to be taken when interacting online.

VII. Conclusion

Cybercrimes can cause various kinds of harm (e.g., psychological, social, financial) to those affected. We conducted a mixed methods study to understand how cybercrimes impact undergraduate students. Our literature review and interview study uncovered *Fear of Cybercrime* and *Cybercrime Self-efficacy* as key cybercrime perceptions, and set the groundwork for our theoretical model that integrates undergraduate students' knowledge, perceptions, and practices regarding cybercrimes. The results from our survey study subsequently showed that the top three cybercrimes experienced among undergraduate students were malware (34%), hacking (20%), and phishing (19%). We found that undergraduate students' cybercrime knowledge predominantly comes from the media and through personally knowing someone who has been victimized. These factors together with online self-control, influenced their perceptions of fear and self-efficacy. In turn, these perceptions influenced participants' behaviors in terms of reporting, preventative measures, and enabling behaviors.

Interestingly we find that past victimizations *decreased* participants' tendency to report cybercrimes. This is arguably related to the finding that not a single interviewee and very few survey participants knew how to officially report cybercrimes.

Our findings provide several opportunities for future work. First, our theoretical model can be tested on a general population to explore if our findings extend beyond undergraduate students. Moreover, we strongly encourage future work on increasing people's cybercrime self-efficacy *without disproportionately reducing their fear of cybercrimes*, as this would thwart the benefits of their newly gained confidence. We also suggest that cybercrime prevention should target users' online self-control, since this has a strong effect on their self-efficacy. Finally, more awareness should be created about how computer users can not only report cybercrimes, but also have access to cybercrime victimization statistics and vital prevention tips for mitigating cybercrime victimization.

Acknowledgment

We thank Gloria Mark for her guidance in developing the research studies conducted for this paper.

References

[1] Internet Crime Complaint Center, "2014 Internet Crime Report," http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf, 2015.

[2] P. Paganini, "2013 – The Impact of Cybercrime," *InfoSec Institute*, 01-Nov-2013.

[3] R. Sidel, "Home Depot's 56 Million Card Breach Bigger Than Target's," *Wall Street Journal*, 18-Sep-2014.

[4] A. M. Bossler and T. J. Holt, "The effect of self-control on victimization in the cyberworld," *J. Crim. Justice*, vol. 38, no. 3, pp. 227–236, 2010.

[5] B. Henson, B. W. Reyns, and B. S. Fisher, "Fear of Crime Online? Examining the Effect of Risk, Previous Victimization, and Exposure on Fear of Online Interpersonal Victimization," *J. Contemp. Crim. Justice*, vol. 29, no. 4, pp. 475-497, 2013.

[6] C. D. Marcum, G. E. Higgins, and M. L. Ricketts, "Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory," *Deviant Behav.*, vol. 31, no. 5, pp. 381–410, 2010.

[7] J. van Wilsem, "Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization," *J. Contemp. Crim. Justice*, vol. 29, no. 4, pp. 437–453, 2013.

[8] J. van Wilsem, "'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization," *Eur. Sociol. Rev.*, vol. 29, no. 2, pp. 168-178, 2013.

[9] A. Smith, L. Rainie, and K. Zickuhr, "College students and technology," *Pew Research Center*, 2010.

[10] A. Oksanen and T. Keipi, "Young people as victims of crime on the internet: A population-based study in Finland," *Vulnerable Child. Youth Stud.*, vol. 8, no. 4, pp. 298–309, 2013.

[11] J. Graves, A. Acquisti, and R. Anderson, "Experimental Measurement of Attitudes Regarding Cybercrime," in *13th Annual Workshop on the Economics of Information Security*, State College, PA, 2014.

[12] M. Riek, R. Bohme, and T. Moore, "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance," *IEEE Trans. Dependable Secure Comput.*, vol. 13, no. 2, pp. 261–273, 2015.

[13] E. Rader, R. Wash, and B. Brooks, "Stories As Informal Lessons About Security," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, Washington, DC, 2012, pp. 6:1–6:17.

[14] M. Yar, *Cybercrime and Society*, 2nd ed. Thousand Oaks, CA: SAGE Publications Ltd, 2013.

[15] M. Gottfredson and T. Hirschi, *A General Theory of Crime*, 1st ed. Stanford, CA: Stanford University Press, 1990.

[16] A. Acquisti and J. Grossklags, "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior," in *2nd Annual Workshop on Economics and Information Security*, College Park, MD, 2003.

[17] N. Christin, S. Egelman, T. Vidas, and J. Grossklags, "It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice," in *Financial Cryptography and Data Security*, G. Danezis, Ed. Springer Berlin Heidelberg, 2011, pp. 16–30.

[18] National Cyber Security Alliance, McAfee, and Zogby International, "2011 NCSA / McAfee Internet Home Users Survey," 2011.

[19] National Cyber Security Alliance, McAfee, and JZ Analytics, "2012 NCSA / McAfee Online Safety Survey," 2012.

[20] R. Wash and E. Rader, "Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users," in *Proceedings of the Eleventh Symposium on Usable Privacy and Security*, Ottawa, Canada, 2015, pp. 309–325.

[21] D. S. Wall, "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime," *Int. Rev. Law Comput. Technol.*, vol. 22, pp. 45–63, 2008.

[22] S. Fafinski, W. H. Dutton, and H. Z. Margetts, "Mapping and Measuring Cybercrime," Social Science Research Network, Oxford, United Kingdom, OII Forum Working Paper No. 18, 2010.

[23] A. Al-Nemrat, H. Jahankhani, and D. S. Preston, "Cybercrime Victimisations/Criminalisation and Punishment," in *Global Security, Safety, and Sustainability*, S. T. de Magalhães, H. Jahankhani, and A. G. Hessami, Eds. Springer Berlin Heidelberg, 2010, pp. 55–62.

[24] R. F. DeVellis, *Scale development: Theory and applications*. Thousand Oaks, CA.: SAGE, 2011.

[25] R. B. Kline, *Beyond significance testing: Reforming data analysis methods in behavioral research*. Washington, DC: American Psychological Association, 2004.

[26] P. M. Bentler and D. G. Bonett, "Significance Tests and Goodness of Fit in the Analysis of Covariance Structures," *Psychol. Bull.*, vol. 88, no. 3, pp. 588–606, 1980.

[27] L. Hu and P. M. Bentler, "Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives," *Struct. Equ. Model. Multidiscip. J.*, vol. 6, no. 1, pp. 1–55, 1999.

[28] E. Fariborzi and M. Hajibaba, "Computer crimes, problems, Law enforcement for solving complaints and education," in *2012 International Conference on Education Technology and Computer*, vol. 43, 2012.

[29] P. Swire, "No Cop on the Beat: Underenforcement in E-Commerce and Cybercrime," *J. Telecommun. High Technol. Law*, vol. 7, pp. 107–126, 2009.

APPENDIX: MEASUREMENTS

Our experimental questionnaire included 67 items including demographics questions. Some items did not fit their designated factors, and were therefore removed from the analysis. The concepts in the theoretical model (see Figure 1) were eventually operationalized as follows:

A. Past Victimizations

6 items, Cronbach's Alpha: 0.51: An index of six yes/no items with the format "Have you ever been a victim of _____ while in college?" covering the following cybercrimes:

- Malware*
- A hacked online account
- Credit card fraud
- Other types of online fraud/scams*
- Identity theft*
- Phishing*

Brief explanations were given for the starred cybercrimes.

B. Exposure via Others

6 items, Cronbach's Alpha: 0.73: An index of six yes/no items with the format "Do you personally know anyone (i.e. a friend, family member, classmate, etc.) who has been a victim of _____?" covering six cybercrimes (i.e., malware, hacking, credit card fraud, other types of online fraud/scams, identity theft, and phishing).

C. Exposure via Media

6 items, Cronbach's Alpha: 0.91: An index of six 6-point scale items (from never to very frequently) with the format "How often do you read/watch media stories (i.e. TV show, film, online news article, newspaper, etc.) about someone being a victim of _____?", covering the six cybercrimes previously mentioned.

D. Self-control

A single item measured on a 7-point scale (from completely disagree to completely agree): "I feel like I make rational decisions when I am online."

E. Fear of Cybercrime

A single item measured on a 7-point scale (from completely disagree to completely agree): "I am fearful of being a victim of a cybercrime."

F. Cybercrime Self-efficacy

4 items, Cronbach's Alpha: 0.91, AVE: 0.76: A latent factor consisting of four items, each measured on a 7-point scale (from completely disagree to completely agree):

- "I am confident in my ability to protect myself from cybercrimes."
- "I have the knowledge to take the necessary security measures."
- "I know how to protect myself against cybercrimes."
- "I feel that I am knowledgeable about cybercrimes."

G. Intention to Report

6 items, Cronbach's Alpha: 0.83: An index of six 7-point scale items (from highly unlikely to highly likely) with the format "If you were a victim of _____, how likely are you to report it to the appropriate entity?" covering six cybercrimes (i.e., malware, hacking, credit card fraud, other types of online fraud/scams, identity theft, and phishing).

H. Preventative Measures

6 items, Cronbach's Alpha: 0.61: An index of the following six 6-point scale items (from never to very frequently):

- "I use anti-virus software."
- "I delete spam emails without opening them."
- "I use unique passwords across all my online accounts."
- "I check to make sure an online connection is secure."
- "I check websites for privacy policies and privacy seals (e.g. TRUSTe, VeriSign)."
- "I provide fake private information about myself online."

I. Enabling Behaviors

5 items, Cronbach's Alpha: 0.68: An index of the following five 6-point scale items (from never to very frequently):

- "I provide payment information to unknown websites."
- "I interact with unknown individuals online."
- "I visit websites with illegal content."
- "I give out my private information online."
- "I open emails from senders I don't know."