2011

Cybercrime Victimization: An Examination of Individual and Situational Level Factors

Fawn T. Ngo
University of South Florida, fawnngo@usf.edu

Raymond Paternoster
University of Maryland

International Journal of Cyber Criminology
Vol 5 Issue 1 January - July 2011

Cybercrime Victimization: An examination of Individual and Situational level factors

Fawn T. Ngo[1]
University of South Florida-Sarasota/Manatee, USA

Raymond Paternoster[2]
University of Maryland, USA

Abstract

Using a sample of college students, we apply the general theory of crime and the lifestyle/routine activities framework to assess the effects of individual and situational factors on seven types of cybercrime victimization. The results indicate that neither individual nor situational characteristics consistently impacted the likelihood of being victimized in cyberspace. Self-control was significantly related to only two of the seven types of cybercrime victimizations and although five of the coefficients in the routine activity models were significant, all but one of these significant effects were in the opposite direction to that expected from the theory. At the very least, it would appear that other theoretical frameworks should be appealed to in order to explain victimization in cyberspace.

Keywords: General Theory of Crime; Routine Activities Theory; Lifestyles Theory; Cybercrime; Cybercrime Victimization.

Introduction

Over the past two decades, cybercrime has emerged as a salient area of inquiry for criminologists and a growing concern for public policy. Although there are many definitions of cybercrime, the term generally refers to crimes committed through the use of computers and computer networks, but it also includes crimes that do not rely heavily on computers (Britz, 2008). Extant research has explored the nature and extent of cybercrime (Cukier & Levin, 2009; Finley, 2009; Finn, 2004; Geis et al., 2009; Huang et al., 2009; Jaishankar, Halder, & Ramdoss, 2009; Ponte, 2009; Stroik & Huang, 2009), correlates of offending and victimization (Berg, 2009; Bossler & Holt, 2010; Buzzell et al., 2006; Choi, 2008; Higgins, 2005; 2006; Higgins, Fell & Wilson, 2007; Higgins & Makin, 2004; Higgins, Wolfe & Marcum, 2008; Holt & Bossler, 2009; Marcum, 2008; Skinner & Fream, 1997; Turgeman-Goldschmidt, 2009) and issues relating to investigating and

[1] Assistant Professor, University of South Florida-Sarasota/Manatee, College of Arts and Sciences,8350 North Tamiami Trail, C250,Sarasota, FL 34243 (941) 359-4727, United States of America. Email: fawnngo@sar.usf.edu

[2] Professor, Department of Criminology and Criminal Justice, 2220, Lefrak Hall, University of Maryland, College Park, Maryland 20742, United States of America. Email: rpaternoster@crim.umd.edu

prosecuting this type of crime (Roberson, 2009; Hinduja, 2009; Shoemaker & Kennedy, 2009). In spite of the considerable and growing scholarship on cybercrime, however, few studies have examined the theoretical causes and correlates of cybercrime victimization.

To date, there have been five studies that applied the lifestyles/routine activities perspective (Cohen & Felson, 1979; Hindelang, Gottfredson & Garafalo; 1978) and the general theory of crime (Gottfredson & Hirschi, 1990) to account for cybercrime victimization (Ashalan, 2006; Bossler & Holt, 2010; Choi, 2008; Holt & Bossler, 2009; Marcum, 2008). Overall, the findings generated from these studies underscore the importance of both situational and individual factors in understanding online victimization. However, whether both individual and situational factors predict all types of cybercrime victimization *equally* remains elusive. For instance, there is evidence that low self-control is a significant predictor of person-based cybercrime victimization (i.e., offenses where a specific person was the target) but not computer-based cybercrime victimization (i.e., offenses where computers and not the individuals were the targets; see Bossler & Holt, 2010). While the expectation would be that criminological theories such as the general theory of crime, routine activities, rational choice, and different versions of social control theory should be able to explain different types of crimes and different sub-types of cybercrimes equally because they claim to be *general theories*, our empirical knowledge on this matter is rather meager. Hence, assessing the role that individual and situational factors play in certain forms of cybercrime victimization will be pertinent not only to the development of a theoretical framework on cybercrime victimization but also on the advancement of the victimology scholarship and providing information for specific public policies.

To that end, the current study explores the effects of individual and situational factors on seven forms of cybercrime: computer virus, unwanted exposure to pornographic materials, sex solicitation, online harassment by a stranger, online harassment by a non-stranger, phishing and online defamation.[3] In particular, this study applies the general theory of crime (Gottfredson & Hirschi, 1990) and the lifestyles/routine activities perspective (Cohen & Felson, 1979; Hindelang, Gottfredson & Garofalo, 1978) to determine if low levels of self-control, and exposure to motivated offenders, online risky behaviors and activities, and capable guardianship affect the above seven forms of cybercrime crime *similarly*. In the following sections, we first review the lifestyles/routine activities perspective and the general theory of crime. We also discuss the empirical evidence among exposure to motivated offenders, online risky behaviors and activities, capable guardianship, low levels of self-control and cybercrime victimization. Next, we describe our methods and data. Finally, we discuss our findings and their implications.

Theoretical Background

Lifestyle/Routine Activities Perspective

Routine activity theory (hereafter RAT; Cohen & Felson, 1979) has been argued to be an expansion of the lifestyle exposure theory of victimization (Hindelang, Gottfredson &

[3] While these seven forms of cybercrime could be further categorized into legal classifications of cyberspace victimization such as cyber-trespass, cyber-pornographic/obscenity, cyber-theft/deception and cyber-violence (see Wall, 2001), due to a caution that collapsing cybercrime victimization types into various categories could mask important differences in findings (see Bossler & Holt, 2010), we opted against categorizing the offenses.

Garofalo, 1978). That is, although the goal of the lifestyle exposure theory is to account for demographic differences in risks of personal victimization and the focus of RAT is on the spatial and temporal order of criminal events, both perspectives focus on how daily routine activities or lifestyles of individuals create opportunities for them to be victimized by or to commit crime (see for example, Miethe & Meier, 1990; 1994; Miethe et al., 1990). Further, since the routine activities perspective was proposed *after* the introduction of the lifestyle exposure theory and it encompasses not only the theoretical element inherent in the lifestyle exposure theory (suitable target) but also two additional elements (motivated offender and capable guardianship), routine activities theory is thus perceived as an extension and more general expression of the lifestyle exposure theory (Choi, 2008). Within the victimology literature, these two theories tend to be applied together and are known as the lifestyles/routine activities theory (hereafter LRAT) and it is generally appreciated that they are theories of both victimization and crime.

According to RAT, crime results when three things converge in time and space: a motivated offender, a suitable target and the lack of a capable guardian (Cohen & Felson, 1979).[4] The theory predicts that crime occurs when a motivated offender comes into contact with a suitable target in the absence of a capable guardian that could potentially prevent the offender from committing crime. The theory also posits that variations in crime rates could be explained by the supply of suitable targets and capable guardians, and from our understanding the theory is somewhat agnostic about the role of the supply of motivated offenders.

Relating to the element of a motivated offender, RAT takes criminal inclination as a given. It is noteworthy that routine activity theorists do not deny the importance of understanding the offenders' motivation and the circumstances under which individuals become criminals. Instead, they argue that understanding the characteristics of situations that produce crime is more pertinent for crime prevention as these characteristics can be altered and crime, thus, could be prevented (Clarke & Felson, 1993) without appealing to offender's motivations. Regarding the element of a suitable target, RAT posits that an individual's lifestyles reflects their routine activities and these activities, in turn, create the level of target suitability that a motivated offender assigns to that particular target. As for the element of a capable guardian, RAT distinguishes two forms of guardianship with physical guardianship denoting factors such as having an alarm system installed on one's home or having lighting on the street and social guardianship including factors such as having a roommate or a next door neighbor.

With regard to *offline* (for example, street crimes) victimization, RAT has been applied to explain offenses such as burglary (Cohen & Felson, 1979; Coupe & Blake, 2006), larceny (Mustaine & Tewksbury, 1998), vandalism (Tewksbury & Mustaine, 2000), physical assault (Stewart et al., 2004), robbery (Spano & Nagy, 2005), general violence (Kennedy & Forde 19990, and fraud (Holtfreter et al., 2008). Further, although the theory has received a great deal of empirical support, it has been criticized for doing a better job in accounting for property crimes than violent crimes (Miethe et al., 1987; Miethe & Meier, 1994).

[4] It is noteworthy that since its introduction in 1979, Felson has elaborated and refined the RAT framework by introducing additional mediating variables (see for example, Felson, 1986; 1998; 2000). However, in accordance with previous research on cybercrime victimization, we examine RAT in terms of its original formulation.

Online Lifestyle, Capable Guardianship and Cybercrime Victimization

Notwithstanding the recent contention regarding the applicability of the LRAT framework to the study of crime and criminals in cyberspace (see Yar, 2005; also see Grabosky, 2001; Newman & Clarke, 2003; Taylor et al., 2006), several studies have applied LRAT to account for *online* victimization (Choi, 2008; Bossler & Holt, 2009; Holt & Bossler, 2009; Marcum, 2008). These studies have all employed samples of students (college and high school) and overall, they provide modest though not always consistent support for the utility of LRAT in understanding the risks of victimization in cyber space. In particular, in accordance with the research on offline victimization, these studies reveal that engaging in online risky behaviors and activities such as downloading free games and free music at unknown websites, opening unknown email attachments and clicking on pop-up messages significantly increase the likelihood of online victimization (Choi, 2008; Marcum, 2008). In other words, the routine activities of one's computer usage put one at varying risk of being a cyber victim.

As for the element of exposure to motivated offenders, previous research has examined whether daily computer activities, both legal and illegal, place individuals in differential proximity to motivated offenders. The evidence reveals that simply spending more time on the computer does not increase victimization risks. Rather, it is participating in certain activities while online and spending more time with others in a specific context that significantly increased the odds of being victimized. Much like being in the street may not be a general risk factor for victimization but being on certain streets or being on the street alone or at certain hours of the day are differentially consequential. For instance, using a sample of college students and applying RAT to account for online harassment, Holt and Bossler (2009) found that while respondents' general computer use and activities such as playing video games, shopping, or checking e-mail did not have a significant impact on the likelihood of experiencing online harassment, the number of hours respondents spent in chat rooms and using instant message (IM) chat did.

With regard to the association between capable guardianship and cybercrime victimization, previous research has distinguished two forms of guardianship with physical guardianship denoting computer software developed to help protect computer system from computer criminals (e.g., antivirus, anti-spyware and firewall programs) and personal guardianship referring to respondents' skill level with computers and technology. Relating to the association between physical guardianship and cybercrime victimization, the evidence is mixed with some studies reporting a significant negative association between computer security (i.e., having antivirus, anti-spyware and firewall software) and the probability of experiencing online victimization (Choi, 2008) while other studies indicating that computer security (i.e., antivirus, firewall, filtering and blocking software) had no effect on the likelihood of cybercrime victimization (Holt & Bossler, 2009; Marcum, 2008). As for the relationships between personal guardianship and cybercrime victimization, personal guardianship has been found to have no effect on the likelihood of being victimized in cyberspace (Holt & Bossler, 2009; Marcum, 2008).

The General Theory of Crime and Victimization

Known as a general theoretical perspective that could explain all individual differences in the propensity to refrain or commit crime, including all acts of crime and deviance, at all ages and under all circumstances, the general theory of crime was crafted by Michael Gottfredson and Travis Hirschi (1990). According to the theory, the main individual

factor in causing crime and deviance is low self-control, which is defined as the inability by an individual to exercise personal restraint in the face of tempting immediate and easy gratification both in the short and long-term (Hirschi, 2004). Gottfredson and Hirschi also maintained that an individual's level of self-control is established early in life, between the ages of 8 and 10, is a product of ineffective child rearing, and has many diverse manifestations that reverberate throughout the life cycle (bullying, bad grades, delinquency, dropping out of school, divorce, alcoholism, obesity, crime and unemployment).

While the general theory of crime was developed to explain criminal offending, Gottfredson and Hirschi do acknowledge the similarities in victimization and offending (Wolfgang, Figlio & Sellin, 1972) and accept that many of the elements of their theory could be logically extended to predict victimization. As a result, scholars have explored the link between low levels of self-control and various forms of victimization (Forde & Kennedy, 1997; Piquero et al., 2005; Schreck 1999; Schreck et al., 2006). There are few research studies applying the general theory to victimization but the overall findings appear to support the theory's usefulness in understanding victim experiences. In particular, low levels of self-control have been found to be related to homicide (Piquero et al., 2005), property victimization and violence (Schreck, 1999; Schreck et al., 2006), fraud (Holtfreter et al., 2008) and cybercrime victimization (Bossler & Holt, 2010).

Self-Control and Cybercrime Victimization

To our best knowledge, to date there is only one study that has explored the relationship between levels of self-control and cybercrime victimization. Using a sample of college students enrolled at a southeastern university in the U.S. and attitudinal measures of self-control (Grasmick et al., 1993), Bossler and Holt (2010) assessed the effects of self-control on the probability of experiencing five forms of cybercrime victimization: unauthorized access to one's computer, having information added, deleted or changed on one's computer without knowledge or permission, data loss due to malware infection, having one's credit card information electronically obtained without knowledge or permission, and online harassment.

The authors found low levels of self-control were significantly related to the likelihood of experiencing three of the five forms of cybercrime victimization – unauthorized access to one's computer, having information added, deleted or changed on one's computer without knowledge or permission, and online harassment. However, when the effects of respondent and peer offending were controlled for, the direct effect of self-control on the probability of experiencing the above three forms of online offenses disappeared. Notably, the authors performed a subsequent factor analysis in which the five forms of cybercrime were sorted into two categories, person-based victimization (i.e., offenses where the individual was the specific target) and computer-based victimization (i.e., offenses where the individual was not the target but computers were). Additionally, when these two categories were treated as dichotomous dependent variables, the authors found low levels of self-control predicted person-based cybercrime victimization but not computer-based victimization. The authors recommended that future research examine whether individual and situational factors predict all types of cybercrime *equally* as this task is crucial toward a better understanding regarding the connections between individual and situational factors and victimization, both on- and off-line (Bossler & Holt, 2010).

The Present Study

Following Bossler and Holt's (2010) recommendation, we apply the general theory of crime and the LRAT framework to assess the effects of individual and situational factors on cybercrime victimization. It is noteworthy that our project extends previous research on cybercrime victimization in three ways. First, our study incorporates both individual and situational factors in predicting the likelihood of being victimized in cyber space. Second, unlike previous research that encompasses a limited set of outcome variables, our study involves seven forms of cybercrime. Finally, to improve upon previous research, our study contains extensive measures pertaining to risky online behaviors/activities and capable guardianship.

Methods

Data for the current study came from an online self-report survey administered at a southeastern university campus in the U.S. between October and December 2010. The university is an upper-division campus that offers junior, senior and graduate course work leading to bachelor and master degrees as well as certificate programs. It is noteworthy that due to the university's commitment to the 2+2 Program (i.e., the 2+2 Program is designed to assist students who have completed an AA degree at a community college to have the opportunity to enroll in and earn a bachelor's degree at a state university), its student body is very diverse and unique in that it encompasses individuals who have recently graduated from high school to retired senior citizens returning to school in hope of attaining their degrees or program certificates.

During the first week of October, an initial email was sent by the Office of Student Activities to 1,533 registered undergraduate students and students seeking program certificates informing them about the study and encouraging them to participate in it. This email also contained information regarding the purpose of the study, the study's principal investigator along with her contact information, and the anonymous nature of the study. In November and December, bi-weekly reminder emails were sent to the students through the Office of Student Activities. Additionally, throughout the month of December, the principal investigator selected all large courses (i.e., courses with more than 35 students) and conducted class visits to further promote the study and encourage students to go online and participate.

Sample

Of the 1,533 registered undergraduate students, 295 students completed the online survey. This yielded an overall response rate of 19% of the total number of registered undergraduate students at the university, and these 295 individuals comprise the sample for the current study. This response rate is not atypical of that found in other studies that have used web-based data collection surveys (Porter & Whitcomb, 2003, 2007; Ranchhod & Zhou, 2001). Table 1 shows the demographic and other characteristics of the study sample as well as the larger student population. As shown in Table 1, the study sample consists of mostly females and the mean age of the sample was 40. At first glance, the mean age of our sample is higher than the mean age in other samples involving college students. However, as we explained previously, the student body at large at the university where our sample was drawn is very diverse and includes individuals who just recently graduated from high school to retired senior citizens returning to school to attain their degrees or program certificates. Table 1 also reveals that the majority of our sample were white and

about an equal number of the sample was married or never been married. Further, slightly over one-third of our sample was not employed and about one-third of the sample had full-time employment.

Compared to the large student population, the demographic characteristics of our sample appear to be similar to the characteristics of the student body at large with regard to sex, race, and employment status (see Table 1). For instance, both our sample and the student body at large consist of mostly females (66% and 66% respectively) as well as the majority of our sample and the student body at large were white (84% and 87% respectively). Similarly, slightly over one third of respondents in our sample and approximately one third of the student body at large had full-time employment (33.8% and 33% respectively). On the other hand, with regard to age and marital status, respondents in our sample tend to be older than the student body at large (the mean age of our sample is 40 while the mean age of the student body at large is 30) and more respondents in our sample are married relative to the student body at large (36.5% and 24% respectively).[5]

We recognize that the university that we sampled from is not representative of a typical U.S. university. We also acknowledge that our selected sample is not completely representative of the university. However, it needs to be emphasized that our work is but a preliminary study that can at least determine the extent to which self-control and rational choice theories are relevant to cyber victimization within our sample, and thus, providing some understanding of the matter to be exploited and developed in future research. Also, in accordance with prior research on cybercrime that utilize samples of college students (see for example, Choi, 2010; Bossler & Holt, 2009; 2010; Holt & Bossler, 2009; Skinner & Fream, 1997), we too rely on a segment of the population who are in an educational environment that not only uses the computer on a daily basis but also very likely to own a computer.

Dependent Variables

Respondents were asked if they experienced each of the following seven forms of cybercrime victimization in the past 12 months: getting a computer virus, receiving unwanted exposure to pornographic materials, being solicited for sex, encountering phishing, experiencing online harassment by a stranger and by a non-stranger, and experiencing online defamation. These items were coded as dichotomous variables with 1= the respondent reported that he/she experienced each of the above seven forms of cybercrime at least once in the past year and 0 = the respondent indicated that he/she did not experience it. Appendix A displays the exact wording of the above seven items as well as their descriptive statistic.

Independent Variables

Self-Control Theory

Our measure of self-control consists of a scale based on the 24 items first used by Grasmick et al. (1993) in their study of self-control and used by many others thereafter. The response options for each of the twenty-four items ranged on a five-point scale from strongly agree to strongly disagree with higher scores on this scale indicate lower levels of self-control. To minimize the loss of observations due to missing data on scale items,

[5] The demographic statistics for the student body at large were obtained through InfoCenter, the university's online data platform.

respondents who completed at least 80% of the scale's items were retained in the analysis. Specifically, for respondents with missing data on this scale but who completed at least 80% of the scale, scale scores were based on the items they did complete. Conversely, respondents who completed less than 80% of the scale were coded as missing on that scale. The scale (Self-Control) was constructed by averaging the responses to each provided item. The Cronbach alpha's for the self-control scale is .86 and the exact wording of the original twenty-four items along with their descriptive statistics are listed in Appendix A.

Routine Activity Theory

We measure three theoretical constructs from routine activities theory: exposure to motivated offenders, target suitability, and capable guardianship. To assess potential exposure to motivated offenders, respondents were asked to report the number of hours they spent per week engaging in the following four activities on the computer: (1) purchasing goods and merchandises, doing research, or gathering information, etc. (Internet Hours), (2) using e-mail (Email Hours), (3) using instant messaging (IM Hours); and (4) participating in chat rooms/IRC/IM (Chat Room Hours). It is noteworthy that our measures of exposure to motivated offenders were designed to capture both the participation in certain activities while online as well as the amount of time one spends with others online in a specific context. The exact wording of these items and their descriptive statistics are listed in Appendix A.

For the measure of target suitability, respondents were asked about their online activities that indicate attractiveness as a suitable target for victimization. From their responses three separate measures were created. Respondents were asked if in the past 12 months, they: (1) communicated with strangers online, (Communicate with Strangers) (2) provided personal information to person(s) online (Provide Personal Info), and, (3) frequently opened any unfamiliar attachments to e-mails that they received, clicked on any of the web-links in the emails that they received, opened any file or attachment they received through their instant messengers, or clicked on a pop-up message that interested them (Click/Open Links). The response options for the above items were 1 = yes and 0 = no. Responses to the four items in the Click/Open Links measure combined into a summated scale with higher scores indicating riskier online behaviors. The exact wording of these items along with their descriptive statistics is listed in Appendix A.

Finally, to measure capable guardianship, two forms of guardianship, physical and personal, were created. Physical guardianship was measured using respondents' report on whether they had anti-virus, spyware, and firewall software on their computers in the past 12 months (Security Software).[6] The response options for these three items were 1= yes and 0 = no and the responses were combined with higher scores indicate greater physical guardianship. Personal guardianship was measured using three items. The first item asked respondents about their computer knowledge and skills and the response options for this item included, 1 = I am afraid of computers and don't use them unless I absolutely have to, 2 = I can surf the net, use some common software but not fix my own computer, 3 =

[6] Although we attempted to increase the precision of our computer security measures by describing each type of software and providing examples for each type, an anonymous reviewer noted that our measures of computer security may lack content validity. We concur with the reviewer that it is possible that not all of the study participants understood the differences among the three types of computer securities, as well as the study participants may not remember exactly when they had the computer securities installed on their computers.

I can use a variety of software and fix some computer problems I have, and 4 = I can use Linux, most software, and fix most computer problems I have. Higher scores on this item indicate greater computer knowledge and skills. The second and third items asked respondents whether or not they have participated in workshops or visited websites aimed at educating the public about cybercrime in the past 12 months. The response options for these items were 1 = yes and 0 = no and the responses were combined into a summated scale (Computer Skills) with higher scores indicating greater personal guardianship. Appendix A displays the exact wording and descriptive statistics for the measures of physical and personal guardianships.

Control Variables

Several items were included as control variables (see Table 1). Sex was coded as a dichotomous variable with 1 = male and 0 = female and age was measured in years. Race was coded as a dichotomous variable where 1 = white and 0 = non-white and employment was also coded as a dichotomous variable with 1 = full-time/part-time and 0 = unemployed. Marital status was also coded as a dichotomous variable with 1 = married and 0 = not married.

Given the evidence on the association between virtual offending and victimization (see Holt & Bossler, 2009), a measure of computer deviance was created and included as a control variable. Computer deviance was measured using five questions that asked respondents to indicate how often in the past 12 months they have either used their computer or another person's to: 1) make or give another person a "pirated" copy of commercially sold computer software; 2) make or give to another person "pirated" media (music, television show, or movie); 3) access another person's account or files without his or her knowledge or permission to look at information or files; 4) add, delete, change or print any information in another person's computer files without the owner's knowledge or permission; and 5) look at pornographic or obscene material. The response options for the above five items were 1 = yes and 0 = no and the responses were combined into a summated scale with higher scores indicating higher levels of virtual offending (see Table 1).

Data analysis

Given the dichotomous dependent variables, logistic regression is used to assess the effects of individual and situational factors on the prevalence of seven forms of cybercrime – computer virus, unwanted exposure to pornographic materials, sexual solicitation, phishing, online harassment by a stranger, online harassment by a non-stranger, and online defamation. Two separate analyses were estimated. In the first analysis, each of the above seven forms of computer crime was regressed on levels of self-control while holding sex, age, race, marital status, employment and computer deviance constant. In the second analysis, each of the above seven forms of computer crime was regressed on the LRAT measures - internet use hour, email hour, IM hour, chat rooms hour, communicate with strangers, provide personal info, click/open links, computer skills, security software and computer crime education - while controlling for sex, age, race, marital status, employment and computer deviance.

TABLE 1. Demographic and Other Characteristics of Sample and University Students

Characteristics	Sample Students					University Students				
	N	Mean /(%)	SD	Min	Max	N	Mean/(%)	SD	Min	Max
Age	282	40	19.12	18	87	1,533	30	9.48	18	87
Sex	282					1,533				
Male		34.0%					34.0%			
Female		66.0%					66.0%			
Race	236					1487				
White		84.3%					87.0%			
Black		6.1%					6.0%			
Asian		3.6%					3.0%			
American		0.4%					0.3%			
Indian/Alaskan		5.7%					1.0%			
Mixed Races										
Marital Status	282					1,518				
Married		36.5%					24.0%			
Not married		63.4%					74.0%			
Employment	281					1,502				
Full-time		33.8%					33.0%			
Part-time		27.4%					32.0%			
Not working		38.8%					33.0%			
Computer Deviance		0.63	0.97	0	4		---------	--------	--------	---------

Results

The results of the analyses outlined above are presented in Table 2 and Table 3. Table 2 presents the results of the logistic regression when the seven forms of computer crime were regressed on the measure of low self-control and control variables (sex, age, race, marital status, employment, and computer deviance). According to Table 2, low levels of self-control are significantly related to the likelihood of experiencing online harassment by a stranger or non-stranger only (see columns 2 and 3 of Table 2). In particular, individuals with low levels of self-control had greater odds (over 180%) of experiencing online harassment by a stranger relative to respondents with high levels of self-control. Similarly, individuals with low levels of self-control had greater odds (over 170%) of experiencing online harassment by a non-stranger relative to respondents with high levels of self-control. Contrary to the expectations of the general theory of crime, therefore, lower levels of self-control were not significantly related to all forms of cyber crime victimization.

The results shown in Table 2 also reveal that whites had significantly lower odds of obtaining a computer virus, receiving unwanted pornographic materials, and being solicited for sex relative to non-whites (see columns 1, 4 and 5 of Table 2). Specifically, being white decreased the odds of getting a computer virus by approximately 55%, receiving unwanted pornographic materials by about 67%, and being solicited for sex by about 62%. Age is also a significant predictor of computer virus and online defamation. Specifically, each additional year in age decreased the odds of obtaining a computer virus by approximately 2% and experiencing online defamation by about 6% (see columns 1 and 7 of Table 2).

Table 2. Logistic Regression of Seven Forms of Cybercrime on Low Self-Control and Control Variables

	(1) Computer Virus (n=238)	(2) Harassment Stranger (n=237)	(3) Harassment Non-Stranger (n=236)	(4) Unwanted Pornography (n=236)	(5) Sex Solicitation (n=237)	(6) Phishing (n=238)	(7) Defamation (n=238)
Low Self-Control	.01 (1.01)	1.03* (2.81)	.99*(2.70)	-.01 (.99)	.07 (1.07)	-.21 (.81)	.51 (1.66)
Male	-.31 (.73)	.31 (1.36)	.94 (2.57)	.26 (1.29)	-.40 (.67)	.14 (1.15)	.05 (1.05)
Age	-.02* (.98)	-.02 (.98)	-.04 (.97)	.02 (1.02)	.01 (1.01)	-.00 (1.00)	-.06* (.94)
White	-.80* (.45)	.43 (1.54)	.45 (1.57)	-1.11* (.33)	-.97* (.38)	.46 (1.58)	.62 (1.85)
Employment	.07 (1.07)	-1.25** (.29)	-.03(.97)	-.43 (.65)	-.24 (.79)	-.49 (.61)	-1.05*(.35)
Married	.21 (1.24)	.20 (1.23)	-.35 (.70)	-.42 (.66)	-.40 (.67)	-.33 (.72)	.82 (2.26)
Computer Deviance	-.14 (.87)	-.03 (.97)	.57**(1.77)	.48**(1.61)	.36 (1.43)	.44** (1.55)	.14 (1.14)
Constant	1.76 (5.83)	-3.62 (.03)	-5.31** (.01)	-1.63 (.20)	-.94 (0.39)	.27 (1.32)	-2.06 (.13)
Model X^2	12.665	17.815	36.171	16.375	12.079	13.006	14.766
df	7.000	7.000	7.000	7.000	7.000	7.000	7.000
p	0.081	0.013	0.000	0.022	0.098	0.072	0.039
Pseudo-R^2	0.069	0.131	0.256	0.104	0.089	0.071	0.145

NOTE: Entries are unstandardized coefficients; odds ratio are in parentheses.
*p<.05; **p<.01; ***p<.001

In addition to race and age, employment is also significantly related to harassment by a stranger and online defamation. According to Table 2, having full- or part-time employment decreased the odds of being harassed by a stranger (by approximately 71%) and experiencing online defamation (by about 65%; see columns 2 and 7 of Table 2). On the other hand, engaging in virtual offending significantly increased the odds of experiencing online harassment by a non-stranger (by almost 80%), receiving unwanted pornography (by over 60%), and experiencing phishing (by over 55%; see columns 3, 4 and 6 of Table 2). It is noteworthy that sex and marital status were not statistically related to any of the seven forms of computer crime (see Table 2).

Table 3 presents the results of the logistic regression when the seven forms of computer crime were regressed on the LRAT measures (internet use hour, email hour, IM hour, chatrooms hour, communicate with strangers, provide personal info, click/open links, computer skills, security software and computer crime education) and control variables (sex, age, race, marital status, employment, and computer deviance). Pertaining to the element of motivated offenders, only one measure, IM Hour, is significantly related to harassment by a non-stranger. Specifically, each additional hour of instant messaging increased the odds of experiencing harassment by a non-stranger by about 6% (see column 3 of Table 3). Similar to the element of motivated offenders, only one suitable target measure, click/open links, is significantly related to computer virus. However, click/open links was related to computer virus in the opposite direction to that expected in that individuals who frequently opened any unfamiliar attachments to e-mails that they received, frequently clicked on any of the web-links in the emails that they received, frequently opened any file or attachment they received through their instant messengers, and frequently clicked on a pop-up message that interested them, had *lesser odds* (by about 35%) of obtaining a computer virus (see column 1 of Table 3).

With regard to the element of capable guardianship, the results indicate that the measure of security software (i.e., a measure of physical guardianship) is significantly related to computer virus and harassment by a stranger. However, security software was related to computer virus and harassment by a stranger in the opposite direction to that expected in that having security software such as anti-virus, spyware and firewall installed

on one's computer *increased* the odds of obtaining a computer virus by over 100% and experiencing online harassment by a stranger by approximately 70% (see columns 1 and 2 of Table 3). Similarly, the measure of computer crime education (i.e.., a measure of personal guardianship) is significantly related to unwanted pornography but the association was also opposite in direction to that which was expected. That is, individuals reporting that have participated in workshops or visited websites aimed at educating the public about cybercrime had greater odds of receiving unwanted pornographic materials (by over 120%) relative to individuals who did not participate in such workshops or visited such websites (see column 4 of Table 3).

Table 3. Logistic Regression of Seven Forms of Cybercrime on LRAT Measures and Control Variables

	(1) Computer Virus (n=231)	(2) Harassment Stranger (n=230)	(3) Harassment Non-Stranger (n=231)	(4) Unwanted Pornography (n=229)	(5) Sex Solicitation (n=231)	(6) Phishing (n=230)	(7) Defamation (n=231)
Exposure to Motivated Offender							
Internet Hours	-.01 (.99)	.00 (1.00)	-.01 (.99)	.02 (1.02)	.03 (1.03)	.00 (1.00)	.00 (1.00)
Email Hours	.01 (1.01)	.00 (1.00)	.00 (1.00)	.00 (1.00)	.04 (1.04)	-.01 (.99)	-.07 (.93)
IM Hours	.03 (1.03)	-.02 (.98)	.06* (1.06)	.02 (1.02)	-.01 (.99)	.01 (1.01)	.00 (1.00)
Chat Room Hours	-.01 (.99)	.05 (1.05)	-.03 (.97)	.02 (1.02)	-.04 (.96)	-.02 (.98)	.00 (1.00)
Target Suitability							
Communicate with Strangers	.49 (1.63)	.01 (1.01)	.85 (2.33)	.33 (1.39)	-.01 (.99)	.32 (1.38)	.88 (2.41)
Provide Personal Info	-.02 (.98)	.89 (2.43)	-.13 (.88)	-.88 (.41)	.51 (1.66)	-.55 (.57)	.77 (2.16)
Click/Open Links	-.43**(.65)	-.11 (.90)	-.20 (.82)	.10 (1.10)	.03 (1.03)	.00 (1.00)	-.18 (.83)
Capable Guardianship							
Computer Skills	.00 (1.00)	-.43 (.65)	-.38 (.69)	.16 (1.18)	-.53 (.59)	.05 (1.05)	.08 (1.09)
Security Software	.74***(2.10)	.53* (1.70)	.05 (1.05)	.49 (1.62)	.30 (1.35)	.35 (1.41)	-.06 (.95)
Computer Crime Info	.47 (1.59)	.61 (1.84)	-.41 (.66)	.80*(2.22)	.05 (1.05)	-.01 (.99)	-.24 (.78)
Control Variables							
Male	-.30 (.74)	-.05 (.96)	.59 (1.80)	.44 (1.55)	-.89 (.41)	.13 (1.14)	.30 (1.35)
Age	-.02 (.98)	-.03* (.97)	-.03 (.97)	.02 (1.02)	-.00 (1.00)	-.01 (.99)	-.05 (.95)
White	-.49 (.61)	- .48 (.62)	1.29 (3.62)	-.58 (.56)	-1.16 (.31)	.47 (1.61)	-.38 (.69)
Employment	.05 (1.05)	-1.67*** (.19)	-.06(.94)	-.77 (.46)	-.88 (.42)	-.51 (.60)	-.94 (.40)
Married	.30 (1.35)	.00 (1.00)	.06 (1.06)	-.43 (.65)	-.29 (.75)	-.16 (.85)	.63 (1.88)
Computer Deviance	-.11 (.89)	.01 (1.01)	.67**(1.95)	.50*(1.64)	.23 (1.26)	.37*(1.44)	.01 (1.01)
Constant	.15 (1.16)	.39 (1.48)	-2.48 (.08)	-4.49 (.01)	.87 (2.39)	-.84 (.43)	-.44 (.64)
Model X^2	41.111	27.045	36.381	32.664	27.318	18.536	20.259
df	16.000	16.000	16.000	16.000	16.000	16.000	16.000
p	0.000	0.041	0.003	0.008	0.038	0.293	0.209
Pseudo-R^2	0.232	0.196	0.267	0.207	0.197	0.104	0.194

NOTE: Entries are unstandardized coefficients; odds ratio are in parentheses.
*p<.05; **p<.01; ***p<.001

To put these results for routine activities theory in perspective, there are ten variables that measure the theory and seven distinct dependent variables. With 70 coefficients and a .05 alpha level we would expect 3.5 of them to be statistically significant by chance alone (70 x .05). What we observe in Table 3 is that five of the parameter estimates for the relationship between routine activities theory and the different forms of cyber victimization are statistically significant – not much of an improvement over chance. Moreover, recall that of the five parameter estimates that are statistically significant four of them are in the *opposite direction* to that expected by routine activities theory. Only the relationship between the number of hours doing instant messaging and harassment by a non-stranger was both statistically significant and in the expected theoretical direction. The magnitude of the effect is, moreover, quite modest (b = .06) with an odds ratio of only 1.06. It would appear from this that variables from routine activities theory are no

better than, and may indeed be less useful, those from the general theory of crime in explaining cyber crime victimization.

With respect to the control variables, the results in Table 3 reveal that each additional year in age decreased the odds of experiencing online harassment by a stranger by about 3% (see column 2 of Table 3). Likewise, having a full- or part-time job decreased the odds of experiencing online harassment by a stranger by approximately 81% (see column 2 of Table 3). On the other hand, engaging in virtual offending increased the odds of experiencing online harassment by a non-stranger (by over 90%), receiving unwanted pornographic materials (by over 60%), and experiencing phishing (by over 40%; see columns 3, 4 and 6 of Table 3). Finally, sex, race and marital status were not related to any of the seven forms of computer crime (see Table 3).

Discussion

In this study, we examined whether an individual factor derived from the general theory of crime and situational factors drawn from routine activities theory affect seven forms of cybercrime victimization *similarly*. Overall, we found that self-control was only significantly related to two of the seven types of cyber crime victimization - the probability of experiencing online harassment by a stranger and non-stranger, while situational-level factors were only significantly related in the expected direction with one – the probability of harassment by an online stranger. We also found that of the control variables, age, race, employment status and computer deviance were significantly related to cybercrime victimization while sex and marital status had no effects on the likelihood of becoming a victim in cyberspace.

Our findings with respect to the general theory appears to be consistent with that reported in a previous study in which the authors found low levels of self-control predicted person-based cybercrime victimization (i.e., offenses where the individual was the specific target) but not computer-based victimization (i.e., offenses where computers were the targets; see Bossler & Holt; 2010). However, we did not find a significant association between levels of self-control and online defamation, an offense that could also be categorized as a person-based cybercrime. It is probable that this finding is due to a lack of variability in our outcome variable as less than 8% of our sample reported encountering this experience in the 12 months before completing the survey (see Appendix A).

We also did not find levels of self-control to be significantly related to any of the remaining offenses – computer virus, unwanted pornographic material, sex solicitation, and phishing. Perhaps in the virtual world, individual characteristics do not matter when crimes involving little or no direct interaction between offenders and victims are considered. For instance, given that computer viruses are malicious codes that attach themselves to host programs and then propagate when the host is executed, it is impossible to ascertain who the victim of a particular virus will be. As such, anyone who owns a computer could get a computer virus *regardless* of his or her level of self-control. Similarly, given the goal of phishers is to "fish" for account usernames, passwords, and other private information from the sea of Internet users in cyberspace, virtually anyone who uses the Internet is a potential victim of phishing *regardless* of his or her level of self-control. If corroborated this finding would put a small limit on the generality of the general theory of crime.

With regard to the situational-level factors (exposure to motivated offenders, target suitability, and capable guardianship), we found exposure to motivated offenders only

predicted online harassment by a non-stranger. None of the other measures of routine activity constructs significantly predicted any form of cyber victimization that was in the direction expected by the theory. Our finding that IM Hour predicted online harassment by a non-stranger appears to reflect previous research findings that suggest that it is the number of hours one spends partaking in *specific* activities on the computer that is salient in understanding cyberspace victimization (Bossler & Holt, 2009; Holt & Bossler, 2009; Marcum, 2008). This finding also appears to support the recommendation made in previous research on cybercrime and cyber victimization against collapsing cyber victimization types into various categories as doing so could mask notable differences (Bossler & Holt, 2010). Hence, future research should continue to examine distinct cybercrime and cyber victimization types as well as consider additional cybercrime and cyber victimization types that have not yet been examined. This one supportive finding notwithstanding, our generally null findings with respect to routine activities theory would suggest that it may not be the best theoretical platform to explain between individual variation in cyber victimization risk.

With respect to the observed negative association between having security software and obtaining a computer virus reflects the fact that having anti-viral or other protection on the computer provides a false sense of security for users. Alternatively, perhaps having security software would be more correctly operationalized as a lifestyle measure instead of as a guardianship measure. That is, having anti-viral or other protection provides a sense of security for users whom in turn engage in online activities that inopportunely dispose them as suitable targets for victimization. Further, it is noteworthy that similar to the measure of click/open links, we combined the items of having anti-virus, having anti-spyware and having firewall in creating the measure of security software. Accordingly, it is instructive that future research not only investigates the effect of security software on cybercrime and cyber victimization with security software operationalized as a lifestyle measure but also examine the effects of having specific security software on cybercrime and cyber victimization.

It is also possible that our measures of computer security lack content validity. In particular, although we attempted to increase the precision of our computer security measures by describing each type of software and providing examples for each type, perhaps not all of the study participants understood the differences among the three types of computer securities or they may not remember exactly when they had the computer security software installed on their computers. Hence, it is instructive that the results of the relationships between measures of computer security and the seven forms of cybercrime victimization be interpreted with caution. Future research should also be cognizant of the above issues and strive to attain more valid measures of these variables.

As for the negative association between the measure of computer crime info and receiving unwanted pornography, again, perhaps this measure would be more correctly operationalized as a lifestyle measure than a guardianship measure. That is, searching for online information relating to cybercrime requires using search engines and since not all search engines filter their links, information seekers could get redirected to fake or fraudulent websites (also known as web "spoofing" or "page-jacking") aimed at either extracting personal information or offering fake products and services or unwanted products such as pornography (Cukier & Levin, 2009). Also, similar to the measures of click/open links and security software, we combined the items of participating in workshops and visiting web sites aimed at educating the public about cybercrime to create

the measure of computer crime info. Accordingly, future research should investigate the effects of these two items on cybercrime victimization separately as well as consider operationalizing the measure of visiting web sites aimed at educating the public about cybercrime as a lifestyle instead of a guardianship measure.

With regard to the control variables, similar to the evidence on victimization in the physical world, we found several demographic variables were significantly related to the likelihood of becoming a victim in cyberspace. In particular, we found older individuals had *lesser* odds of getting a computer virus, experiencing online harassment by a stranger and defamation relative to younger individuals. This finding appears to reflect the evidence offline that suggests that older individuals have lesser risks of becoming crime victims relative to younger individuals (Hindelang et al., 1978). We also found whites were *less* likely to get a computer virus, receiving unwanted pornographic materials, and being solicited for sex relative to non-whites. Employment status was also significantly related to cybercrime victimization in that individuals with full- or part-time employment had *lesser* odds of experiencing defamation and online harassment by a stranger relative to individuals without employment. Notably, however, we found that sex and marital status had no effects on the likelihood of becoming a victim in cyberspace. These findings warrant further examination as they contradict the evidence offline that indicates that sex and marital status are the salient factors in accounting for the likelihood of becoming a crime victim. Finally, in accordance with the evidence offline on the association between offending and victimization, we found individuals engaging in virtual offending had *greater* risks of experiencing online harassment by a non-stranger, receiving unwanted pornographic materials and encountering online defamation relative to individuals who did not engage in virtual offending.

Conclusion

The results reported in this study indicate that an individual characteristic derived from the general theory of crime - low self-control - and situational factors drawn from the LRAT framework - exposure to motivated offenders, online risky behavior and activities and capable guardianship – are not particularly effective in explaining a diverse set of cyber victimizations. Traditional criminological theories such as the general theory of crime and the routine activities perspective seem to have limited utility in accounting for crime and victimization in a virtual environment. This would suggest that different theoretical traditions may need to be appealed to in understanding this form of criminal victimization. However, given the very sparse empirical record, more research on cybercrime and cybercrime victimization are warranted before a definite conclusion on this issue can be reached.

Lastly, we would be remiss if we did not acknowledge the limitations inherent in our study. In particular, since the university that we sampled from is not representative of a typical U.S. university as well as our selected sample is not completely representative of the large student population, our results may only be applied to this specific or similar sample. We encourage future research to employ more representative or other samples to further investigate cybercrime.

References

Alshalan, A. (2006). *Cyber-Crime Fear and Victimization: An Analysis of a National Survey*. Mississippi: Mississippi State University.

Berg, S. E. (2009). Identity theft causes, correlates, and factors: A content analysis. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp., 225-250). Upper Saddle River, NJ: Pearson Education, Inc.

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

——— (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Britz, M. T. (2008). *Computer Forensics and Cyber Crime: An Introduction*. Upper Saddle River, NJ: Prentice Hall.

Buzzell, T., Foss, D. & Middleton, Z. (2006). Explaining use of online pornography: A test of self-control theory and opportunity for deviance." *Journal of Criminal Justice and Popular Culture, 13*, 96-116.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308-33.

Clarke, R. V. & Felson, M. (1993). *Routine Activity and Rational Choice*. New Brunswick, NJ: Transaction Publishers.

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

Coupe, T. & Blake, L. (2006). Daylight and darkness targeting strategies and the risks of being seen at residential burglaries. *Criminology, 44*, 431-64.

Cukier, W. & Levin, A. (2009). Internet fraud and cybercrime. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp., 251-279). Upper Saddle River, NJ: Pearson Education, Inc.

Felson, M. (1998). *Crime and Everyday Life*. Thousand Oaks, CA: Pine Forge Press.

——— (1986). Routine activities, social controls, rational decisions and criminal outcomes. In D. Cornish and R. Clarke (Eds.), *The Reasoning Criminal* (pp. 119-128). New York: Springer Verlag.

——— (2000). The routine activity approach as a general social theory. In S. Simpson (Ed.), *Of Crime and Criminality: The Use of Theory in Everyday Life* (pp. 205-216). Thousand Oaks, CA: Sage.

Finley, L. (2009). Online pharmaceutical sales and the challenge for law enforcement. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 101-128). Upper Saddle River, NJ: Pearson Education, Inc.

Finn, J. (2004). A survey of online harassment at a university campus. *Journal of Interpersonal Violence,* 19, 468-83.

Forde, D. R., & Kennedy, L. W. (1997). Risky lifestyles, routine activities, and the general theory of crime. *Justice Quarterly,* 14, 265-294.

Grabosky, P. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies,* 10, 243-249.

Geis, G., Brown, G. C., & Pontell, H. N. (2009). Internet gambling. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 417-435). Upper Saddle River, NJ: Pearson Education, Inc.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Grasmick, H. G., Tittle, C. R., Bursik, R. J., Jr. & Arneklev, B. J. (1993). Testing the one empirical implication of Gottfredson and Hirschi's general theory of crime. *Journal of Research in Crime and Delinquency, 30*, 5-29.

Higgins, G. E. (2005). Can low self-control help with the understanding of the software piracy problem? *Deviant Behavior, 26*, 1-24.

——— (2006). Gender differences in software piracy: The mediating rules of self-control theory and social learning theory. *Journal of Economic Crime Management, 4*, 1-30.

Higgins, G. E., Fell, B. D., & Wilson, A. L. (2007). Low self-control and social learning in understanding students' intention to pirate movies in the United States. *Social Science Computer Review, 25*, 339-57.

Higgins, G. E., & Makin, D. A. (2004). Self-control, deviant peers, and software piracy. *Psychological Reports, 95*, 921-31.

Higgins, G. E., Wolfe, S. E., & Marcum, C. D. (2008). Music piracy and neutralization: A preliminary trajectory analysis from short-term longitudinal data. *International Journal of Cyber Criminology, 2*(2), 324-36.

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

Hinduja, S. (2009). Investigating computer crime. In F. Schmalleger and M. Pittaro (Eds.), *Crimes of the Internet*. Upper Saddle River, NJ: Pearson Education, Inc.

Hirschi, T. (2004). Self-control and crime. In R. F. Baumeister & K. D. Vohs (Eds.), *Handbook of self-regulation: Research, theory and applications* (pp. 537-552). New York: Guilford Press.

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

Holtfreter, K., Reisig, M. D., & Pratt, T.C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46*, 189-220.

Huang, W., Leopard, M. E. & Brockman, A. (2009). Internet child sexual exploitation: Offenses, offenders, and victims. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 43-65). Upper Saddle River, NJ: Pearson Education, Inc.

Jaishankar, K., Halder, D., & Ramdoss, S. (2009). Pedophilia, pornography, and stalking: Analyzing child victimization on the internet. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 28-42). Upper Saddle River, NJ: Pearson Education, Inc.

Kennedy, L. W. & Forde, D. R. (1999). *When Push Comes to Shove*. Albany: State University of New York Press.

Marcum, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology 2*(2), 346-67.

Miethe, T. D., Stafford, M. & Long, J. S. (1987). Social differentiation in criminal victimization: A test of routine activities/lifestyle theories. *American Sociological Review,* 52, 184-94.

Miethe, T. D., & Meier, R. F. (1990). *Crime and Its Social Context: Toward an Integrated Theory of Offenders, Victims, and Situations*. Albany, NY: State University of New York Press.

Miethe, T. D., & Meier, R. F. (1990). Opportunity, choice, and criminal victimization: A test of a theoretical model. *Journal of Research in Crime and Delinquency, 27*, 243-66.

Miethe, T. D., Stafford, M. C. & Sloane, D. (1990). Lifestyle changes and risks of criminal victimization. *Journal of Quantitative Criminology,* 6, 357-76.

Mustaine, E. E., & Tewksbury, R. (1998). Predicting risk of larceny theft victimization: A routine activity analysis using refined lifestyle measures. *Criminology,* 36, 829-57.

Newman, G., & Clarke, R. (2003). *Superhighway Robbery: Preventing E-Commerce Crime*. Cullompton: Willan Press.

Piquero, A. R., MacDonald, J., Dobrin, A., Diagle, L. E., & Cullen, F. T. (2005). Self-control, violent offending and homicide victimization: Assessing the general theory of crime. *Journal of Quantitative Criminology, 21*, 55-71.

Ponte, L. (2009). The warez scene: Digital piracy in the online world. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 384-407). Upper Saddle River, NJ: Pearson Education, Inc.

Porter, S. R., & Whitcomb, M. E. (2003). The impact of contact type on web survey response rates. *Public Opinion Quarterly, 67*, 577-588.

_____ (2007). E-mail Subject Lines and Their Effect on Web Survey Viewing and Response. *Social Science Computer Review, 25*, 99-110.

Ranchhod, A., & Zhou, F. (2001). Comparing respondents of e-mail and mail surveys: Understanding the implications of technology. *Marking Intelligence and Planning, 19*, 254-263.

Roberson, C. (2009). Evidence issues involved in prosecuting Internet crime. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 503-520). Upper Saddle River, NJ: Pearson Education, Inc.

Schreck, C. J. (1999). Criminal victimization and self-control: An extension and test of a general theory of crime. *Justice Quarterly,* 16, 633-54.

Schreck, C. J., Stewart, E. A. & Fisher, B. S. (2006). Self-control, victimization, and the influence on risky lifestyle: A longitudinal analysis using panel data. *Journal of Quantitative Criminology,* 22, 319-40.

Shoemaker, D., & Kennedy, D. B. (2009). Criminal profiling and cyber criminal investigations. In F. Schmalleger and M. Pittaro (Eds.), *Crimes of the Internet* (pp. 439-455). Upper Saddle River, NJ: Pearson Education, Inc.

Skinner, W. F. & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency, 34*,495-518.

Spano, R., & Nagy, S. (2005). Social guardianship and social isolation: An application and extension of lifestyle/routine activities theory to rural adolescents. *Rural Sociology 70*, 414-37.

Stewart, E. A., Elifson, K. W., & Sterk, C. E. (2004). Integrating the general theory of crime into an explanation of violent victimization among female offenders. *Justice Quarterly, 21*,159-81.

Stroik, A., & Huang, W. (2009). Nature and distribution of phishing. In F. Schmalleger and M. Pittaro (Eds.), *Crimes of the Internet* (pp. 191-205). Upper Saddle River, NJ: Pearson Education, Inc.

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

Tewksbury, R., & Mustaine, E. E. (2000). Routine activities and vandalism: A theoretical and empirical study. *Journal of Crime & Justice, 23*, 81-110.

Thornberry, T. P., Krohn, M. D., Lizotte, A. J., Smith, C. A., & Tobin, K. (2003). *Gangs and Delinquency in Developmental Perspective*. New York: Cambridge University Press.

Turgeman-Goldschmidt, O. (2009). The rhetoric of hackers' neutralizations. In F. Schmalleger & M. Pittaro (Eds.), *Crimes of the Internet* (pp. 317-335). Upper Saddle River, NJ: Pearson Education, Inc.

Wall, D. (Ed.), (2001). *Crime and the Internet: Cybercrimes and Cyber Fears*. New York: Routledge.

Wolfgang, M., Figlio, R. M., & Sellin, T. (1972). *Delinquency in a Birth Cohort*. Chicago:

University of Chicago Press.
Yar, M. (2005). The novelty of 'cybercrime': An assessment of light of routine activity theory. *European Journal of Criminology, 2*, 407-27.

Appendix A. Variables

Cybercrime Victimization	**Yes N (%)**	**No N (%)**
Computer Virus		
In the past 12 months, did you have computer virus infection incidents?	128 (46.0)	150 (54.0)
Online Harassment by a Stranger		
In the past 12 months, have you received messages from someone you don't know or barely know that threatened, insulted, or harassed you?	39 (14.1)	238 (85.9)
Online Harassment by a Non-Stranger		
In the past 12 months, have you received messages from an acquaintance, friend or "significant other" ((boy/girlfriend, spouse, etc.) that threatened, insulted, or harassed you?	37 (13.4)	240 (86.6)
Unwanted Exposure to Pornographic Materials		
In the past 12 months, have you received unwanted pornographic messages or pictures?	58 (20.9)	219 (79.1)
Sexual Solicitation		
In the past 12 months, have you received solicitation for sex over the Internet?	41 (14.7)	237 (85.3)
Phishing		
In the past 12 months, have you received emails that look like those coming from legitimate businesses including financial institutions or government agencies asking for personal data such as usernames and passwords?	153 (54.8)	126 (45.2)
Online Defamation		
In the past 12 months, has anyone posted false information or allegations about you on websites, chat rooms, blogs, or user pages for the purpose of damaging your reputation?	21 (7.6)	257 (92.4)

Self-Control Scale* (alpha = 0.86)	**Mean**	**SD**	**Min**	**Max**
I often act on the spur of the moment without stopping to think	1.92	1.07	1	5
I don't devote much thought and effort to preparing for the crime	1.87	1.07	1	5
I often do whatever brings me pleasure here and now, even at the cost of some distant goal	1.87	1.03	1	5
I'm more concerned with what happens to me in the short run than in the long run	1.86	1.07	1	5
I frequently try to avoid projects that I know will be difficult	2.00	0.99	1	5
When things get complicated, I tend to quit or withdraw	1.71	0.92	1	5

	Mean	SD	Min	Max
The things in life that are easiest to do bring me the most pleasure	2.23	1.01	1	5
I dislike really hard tasks that stretch my abilities to the limit	1.82	0.93	1	5
I like to test myself every now and then by doing something a little risky	3.13	1.21	1	5
Sometimes I will take a risk just for the fun of it.	2.52	1.20	1	5
I sometimes find it exciting to do things for which I might get in trouble	1.75	1.06	1	5
Excitement and adventure are more important to me than security	1.75	0.97	1	5
If I had a choice, I would almost always rather do something physical than something mental	2.44	1.09	1	5
I almost always feel better when I am on the go more than when I am sitting and thinking	2.93	1.19	1	5
I like to get out and do things more than I like to read or contemplate ideas	2.93	1.19	1	5
I seem to have more energy and a greater need for activity than most other people my age	2.96	1.17	1	5
I try to look out for myself first, even if it means making things difficult for other people	1.82	0.95	1	5
I'm not very sympathetic to other people when they are having problems	1.80	1.17	1	5
If things I do upset people, it's their problem not mine	1.72	0.86	1	5
I will try to get the things I want even when I know it's causing problems for other people	1.52	0.80	1	5
I lose my temper pretty easily	2.02	1.10	1	5
Often, when I'm angry at people I feel more like hurting them than talking to them about why I am angry.	1.58	0.93	1	5
When I'm really angry, other people better stay away from me	2.05	1.16	1	5
When I have a serious disagreement with someone, it's usually hard for me to talk calmly about it without getting upset.	2.42	1.25	1	5
Exposure to Motivated Offenders	**Mean**	**SD**	**Min**	**Max**
Internet Hours Please indicate the number of hours you spend per week on the Internet (to purchase goods and merchandises, do research, gather information, etc.)	18.75	15.12	0	85

Email Hours				
Please indicate the number of hours you spend per week using Email	7.29	9.64	0	63
IM Hours				
Please indicate the number of hours you spend per week using instant messaging	2.31	7.37	0	60
Chat Room Hours				
Please indicate the number of hours you spend per week in the chat rooms/IRC/IM	0.62	3.28	0	40

Target Suitability	**Yes N (%)**	**No N (%)**
Communicate with Strangers		
Do you communicate with strangers online?	59 (21.5)	216 (78.5)
Provide Personal Info		
Have you provided your personal information to person(s) online in the past 12 months?	55 (21.1)	219 (78.9)

	Mean	**SD**	**Min**	**Max**
Click/Open Links	1.33	1.02	0	4
Physical Guardianship				
Security Software	2.26	0.97	0	3
Personal Guardianship				
Computer Skills**	2.7	.60	1	4
Computer Crime Education	0.26	.51	0	2

* 1 = strongly disagree, 2 = disagree, 3 = neither agree nor disagree, 4 = agree
**1= I am afraid of computers and don't use them unless I absolutely have to; 2= I can surf the net, use some common software but not fix my own computer; 3= I can use a variety of software and fix some computer problems I have; 4= I can use Linux, most software, and fix most computer problems I have