Routine Citizen Internet Practices and Cyber Victimization: A State-wide Study in Virginia

Randy R. Gainey,

Department of Sociology and Criminal Justice, Old Dominion University

Jay S. Albanese

Wilder School of Government & Public Affairs, Virginia Commonwealth University

Tancy Vandecar-Burdin

Social Science Research Center, Old Dominion University

James Hawdon

Department of Sociology and Center for Peace Studies and Violence Prevention, Virginia Tech

Thomas E. Dearden

Department of Sociology, Virginia Tech

Katalin Parti

Department of Sociology, Virginia Tech

THIS IS A PRE-PUBLICATION VERSION OF A PAPER PUBLISHED IN CRIMINAL JUSTICE STUDIES. PLEASE CITE AS: Gainey, Randy, Tancy Vandecar-Burdin, Jay Albanese, James Hawdon, Katalin Parti, and Thomas Dearden. 2023. "Routine Citizen Internet Practices and Cyber Victimization: A State-wide Study in Virginia." ***Criminal Justice Studies.*** **http://doi.org/10.1080/1478601X.2023.2254094.**

Routine Citizen Internet Practices and Cyber Victimization: A State-wide Study in Virginia

Abstract

Cybercrime is a major concern across the world, in the US and in the state of Virginia. A better understanding of cybercrime activity is needed to target and prevent it more effectively, minimize its consequences, and provide support for victims. Research on cybercrime victimization has exploded in the past few years, but much of it relies on convenience samples and is largely descriptive in nature. The research presented here involves the collection of data from a large sample of Virginia households in 2022 (n=1,206). The data are analyzed to provide a partial test of routine activity theory to better understand fraud and theft via the internet. The data provide a solid baseline for describing the extent of cyber victimization across the state. Bivariate and multivariate analyses (logistic regressions) show support for routine activity theory and provide important insights for future research. In particular, dark web exploration, posting personal information, buying and selling things online, among other activities seem to better predict unique forms of cybervictimization than other activities or simply the length of time spent on the internet. We conclude that to better assess cybercrime victimization and engagement, better measurement and longitudinal panel data will be needed.

Introduction

Victimization from cybercrime is a major concern across the world, in the US and in the state of Virginia. As individuals spend more time online, it becomes increasingly important to understand cybercrime and how to protect against it. Such an understanding is dependent on valid and reliable baseline data that identifies the specific nature, extent, and outcomes of cybercrime activity. A better understanding of cybercrime activity is needed to target and prevent it more effectively, minimize its

consequences, and provide support for both individual and corporate victims. A strong theoretical base will also promote better empirical models, interpretable results, and promote better policy and practice.

In this analysis, we focus on theft and fraud because they are the most frequent cybercrimes reported to authorities (FBI Internet Crime Report, 2022; Reep-van den Bergh & Junger, 2018). The high incidence of fraud illustrates that online shopping and commercial dealings are primary online activities, placing the exchange of funds for a large number of transactions globally at a higher risk of compromise or abuse (Button & Cross, 2017; Rungsrisawat, Sriyakul & Jermsittiparsert, 2019). The high cost of theft and fraud are not only financial (Brenner et al., 2020), but have personal and emotional consequences as well (Golladay and Holtfreter, 2017).

To gain a better understanding of the factors affecting cyber theft and fraud, we borrow from Cohen and Felson's (1979) routine activities theory that argues crime is likely to occur when there is a convergence of motivated offenders, suitable or attractive targets, and the absence of capable guardians. The theory has been advanced to apply to crimes where there is no face-to-face contact (Eck and Clark, 2003), and more specifically to cyber victimization (Hawdon et al., 2017; Reyns et al., 2011; Vakhitova et al., 2016). An important and growing empirical literature has examined the ability of the theory to explain various forms of cyber victimization including theft and fraud via the internet.

Review of the Literature

A growing body of theoretical thought and empirical research has emerged over the past 15-20 years and increased rapidly over the past 3-5 years, focused on the ability of routine activities theory to explain cyber victimization. Routine activities theory has been proffered to explain malware infection (Bossler and Holt, 2009;Leukfeldt et al., 2016; Holt and Bossler, 2013; Kigerl, 2021; Holt et al., 2020), cyberbullying (Holt et al., 2015; Navarro and Jasinski, 2012; Arntfield, 2015; Aizenkot, 2021; Kaluarachchi et al., 2020), cyberstalking (Nutter, 2021; Reyns et al., 2011), unwanted pornography and online sexual

conversations, sexual solicitations (Holt et al., 2016; Ngo and Paternoster, 2011; Ngo et al., 2020); self-protection on the internet (Dearden, 2021) and theft and fraud (Pratt, Holtfreter & Reisig, 2010; van de Weijer et al., 2019) among others (Hawdon et al., 2020; Costello, et al., 2021). Although most research focused on routine activities has been at the micro level focusing on individuals, it has also been employed at the macro level to explain cyber victimization across countries (Perkins et a., 2022; Kigerl, 2021; Williams, 2016) and states (Song et al., 2016; Hawdon et al., 2020).

A large body of empirical work on the routine activities of middle, high school, and college students as it related to cyber victimization has emerged (Bartlacci et al., 2014; Bossler and Holt, 2009; Choi, 2008; Holt et al., 2016; Ngo and Paternoster, 2011; Ngo et al., 2020; Kabiri et al., 2021; Tewksbury & Mustaine, 2003; Holt & Bossler, 2009). Convenience samples such as these are important (Payne and Chappell, 2008) but they tend to be limited in terms of generality. Fortunately, there have been large national representative samples of individuals discussed in the literature both in the United States (Navarro and Jasinski, 2012; Costello et al., 2021), Finland (Marttila et al., 2021), the Netherlands (Leukfeldt et al., 2016; Holt et al., 2020), China (Yao-Chung Chang, 2019; Yao-Chung, 2010), Vietnam (Nguyen, 2020) and studies that include multiple countries (Nasi, 2015). Few representative studies within states have been conducted; as we discuss below, Virginia offers a promising context to examine cyber victimization, especially fraud and theft.

Routine Activities and Cyber Crime Victimization

Routine activity theory (Cohen & Felson 1979) is the most widely used theory of victimization (Mirò, 2014). According to routine activity theory, the opportunity for criminal victimization is highest at the nexus of motivated offenders, suitable targets, and a lack of capable guardianship (Cohen & Felson, 1979). When all three components spatiotemporally converge, victimization is likely to increase. In addition, the likelihood of this convergence occurring is influenced by the ‘‘routine activities’’ in which

people engage. Although it was developed long before the advent of the Internet to explain direct predatory interpersonal crimes, routine activity theory has been applied to online spaces with only modest modifications since evidence suggests contact can occur in the virtual world asynchronously (see Eck & Clarke 2003; Reyns, Henson & Fisher. 2011; Miró, 2014).

Motivated Offenders: Like the physical world there is no lack of the supply of motivated offenders on the internet. Cybercrime research influenced by routine activities theory generally focuses on the routine cyber activities of potential victims that increases exposure to motivated offenders—equipment owned or used, how much time they spend on the internet and what sorts of activities they engage in (banking, socializing, shopping) (Holt and Bossler, 2009; Holt and Bossler, 2013; Navarro & Jasinski, 2012; Ngo et al., 2020).

Suitable Targets: Some research has utilized demographic variables such as income, employment, and gender as indirect measures of target suitability (see Nasi et al., 2015). Other researchers have focused on the types of personal information people put out on the internet. Marcum and colleagues (2010), for example, collected data from college freshmen about their sex related online victimization experiences and internet practices currently and while in high school. They developed an index based on posting "age, gender, descriptive characteristics, picture…goals, sexual information…" (Marcum, 2010: 418) and found it related to various forms of sexually related victimization, especially among females. In addition, Reynes and colleagues (2011) included in their study of 974 college students nine items that asked if respondents posted their full name, email addresses, relationship status, interests, among other personal information. They formed a composite index with these items that significantly predicted cyberstalking victimization controlling for other measures derived from routine activities theory.

Capable Guardians as a Protective Factor: Several studies have developed unique measures of "online guardianship on the internet" (Reynes et al., 2011: 1158). Sometimes researchers make a distinction between physical guardianship (e.g., security programs, firewalls) and social guardianship (e.g., parental supervision, deviant peer associations). Other times they have emphasized the protective factors internet users employ and their skills in terms of computers and navigating the internet to measure guardianship on the internet. Holt and Bossler (2013) found that self-reported skill level and those with a hardware firewall were less likely to report malware infection, but that those with antivirus software reported higher levels of malware victimization. The latter result may occur because those who experience malware infection purchase antivirus software in response to malware victimization.

Context of the Study

Virginia presents a unique intersection of cyber-physical systems with a large workforce in the maritime, defense, technology, and transportation sectors, combined with an educated and mobile workforce making it a uniquely targeted area. As one of the 50 states of the USA, Virginia is the 12th most populous state and ranks high on several indicators related to quality of life (World Population Review, 2022). For example, Virginia ranked 7th across 8 desirable outcomes. The rankings are based on more than 70 metrics (Callahan, 2021). Virginia has the fourth-best public schools overall in the United States, ranking fourth for quality and third for safety (World Population Review, 2022a).

Alternatively, Virginia closely matches the remainder of the US on other attributes. For example, Virginia is in the middle quintile in both per capita income growth and per capita personal consumption expenditures (U.S. Department of Commerce, 2021; 2022). Growth in GDP in Virginia closely matches the USA as a whole (-1.7% versus -1.6%, comparing the last quarter of 2021 with the first quarter of 2022) (U.S. Department of Commerce, 2022).

The US population is highly urbanized, with 82.3% of the population residing in cities and suburbs. Virginia is similar with 88% living in cities and suburbs (Virginia Rural Health Plan, 2022). Virginia also ranks in the middle of the pack on other attributes, such as 24th in the United States for its economic outlook, and 30th for its economic performance (American Legislative Exchange Council Center for State Fiscal Reform, 2022; Virginia Employment Commission, 2022). Two-thirds of Virginia residents have at least some college experiences, similar to the percentage nationwide (69%) (Ryan & Bauman, 2016). The median age in the US is 38.8 years. In Virginia, it is 38.4, and life expectancy is the same at 78 years (World Population Review, 2022c). There exists a number of interesting similarities and differences between Virginia and the rest of the United States overall making it a suitable context to study cyber victimization.

Methods

This study was conducted using accepted techniques of survey research that involve telephone interviews (Daikeler, Bošnjak & Lozar, 2020; Evans & Mathur, 2018; Kalton, 2019) and web-based surveys. Telephone and web surveys were conducted with a sample of 1,206 adults, ages 18 or older, living in Virginia. Telephone interviews were conducted by landline (n=256) and cell phone (n=449) as well as via an on-line survey panel (n=501) provided by CINT, a company providing sampling and survey panels to researchers. The telephone interviews and web surveys were conducted in English from February to June, 2022.

A combination sample was used consisting of listed and random digit dial (RDD) numbers for both landline and cellular numbers to reach adults in Virginia who have access to either a listed or unlisted landline or cellular telephone number. As many as seven attempts were made to contact landline telephone numbers, and as many as five attempts were made to contact cell phone numbers. Calls were made at different times of day and different days of the week to maximize the chance of contacting potential respondents. The introductory language directed the interviewer to speak with the

member of the household who was 18 years of age or older with the most recent birthday. Selecting respondents in this manner has been shown to result in data that closely mirror the population in terms of age. Combining the different data sources resulted in a total of 1,206 household responses.

Dependent Measures

Cyber fraud and theft suffered ever and in the past year

The dependent variables related to cyber fraud and theft were measured through a series of nine items. To set up this question batteria, we utilized the Identity Theft Supplement to the National Crime Victimization Survey (NCVS, 2018). Questions had been updated to reflect development in modus operandi of, as well as the latest trends in identity theft and fraud (see FTC, 2021a; 2021b). Answer options had been aggregated in order to maintain survey conciseness and avoid survey fatigue. Respondents were first asked if they or anyone in their households had experienced any of nine types of cybercrimes. Specifically, respondents were asked, "Has anyone in your household ever…

1. Been tricked or deceived out of money or goods by email, text, or online via the internet
2. Bought a product or service via the internet, after which the product or service was never delivered because the seller was deceptive
3. Ever sold a product or service via the internet, and delivered it, but never received any money from the buyer because the buyer was deceptive
4. Had someone without permission, use or attempt to use their personal information to open any NEW accounts such as cellphone accounts, credit cards, etc.
5. Had someone claim an income tax refund or unemployment benefits in your name without your knowledge or permission
6. Had their credit card been used to obtain money or buy goods or services without their permission or knowledge
7. Had their bank account illegally or fraudulently debited
8. Experienced fraud or theft because someone used their social security number
9. Transferred money to someone who contacted them via email or the internet with a false story about earning money through an inheritance, investments, etc.

These items were then repeated but referencing victimization experiences in the past year. Two dichotomous variables were created indicating whether or not anyone in the respondents' households

had ever had any of these victimization experiences, and whether any had occurred in the past year (1=victim, 0=not a victim).

Independent variables

Exposure to Motivated offender

Several measures of exposure to motivated offenders were included in the survey. All indirect measures increase the likelihood of coming into virtual contact with a motivated offender. First, a three-item index was developed based on whether or not the respondent or someone in the household had a desktop computer, a laptop, or a tablet or other similar computing device. We also asked if they use social media sites or apps like Facebook, Twitter, Instagram, or LinkedIn and whether they use online methods for financial services (for example: paying bills, banking, transferring funds, etc.). Finally, we asked how often they used the internet with response options of: less than one hour per day, 1-2 hours per day, 3-5 hours per day, 6-7 hours per day, 8-9 hours per day, or 10 or more hours per day.

Protective Factors: Training, Protective Strategies, and Perceived Internet Skills

Respondents were asked about behaviors that should decrease their vulnerabilities or target suitability while online. Specifically, they were asked whether they had received training about how to safely use the internet or how to stay safe on the internet (1=yes, 0=no), and they were asked several behavioral questions about protective strategies against cyber victimization. There were a series of six items with the response options of: 1=always, 2=sometimes, and 3=never. We recoded appropriate items to reflect greater self-protective strategies:

1. I am careful when clicking links or attachments sent to me via email, text, or social media.
2. I use security alerts for my email and social media accounts.
3. I am able to tell if a website is legitimate.
4. I use personal information to create my passwords.
5. I update my passwords frequently.
6. I save my passwords in a digital/online password keeper.

In addition, respondents were also asked:

7. Thinking about all of the passwords you use to access your various online accounts, would you say that your passwords are very similar, somewhat similar, somewhat different, very different?
8. Have you ever shared a password to one of your online accounts with a friend or family member? (1=yes, 2=no)
9. Have you ever used your social media account (e.g. Facebook or Twitter) information to log into another website? (1=yes, 2=no)

A factor analysis with principal components and varimax rotation produced two factors with eigenvalues greater than 1.0. The first factor explains 19.79% of the variance across items and the second explains an additional 19.98% of the variance across the items. The first factor includes items 4 and 6 from the first set of items above and items 7-9 – all dealing with various issues surrounding passwords. The second factor included items 1, 2, 3, and 5 from the set of safety items above and focused on carefully navigating the web, using security alerts and updating passwords. Based on the results of the factor analysis, all items were first standardized and then summed into two scales labeled Password Caution and Careful Navigation, respectively.

A single item measure of perceived expertise with the internet, similar to other empirical investigations (see Holt and Bossler, 2013; Bossler and Holt, 2009; Leukfeldt and Yar, 2016; Nodeland and Morris, 2020; Hawdon et al., 2020; Ngo & Paternoster, 2011**)** asked respondents to assess their level of expertise with the internet. Response options included: 1= I am uncomfortable using a computer (uncomfortable), 2= I am able to go to specific web pages and use social media (Beginner), I am able to download applications, manage internet settings, fix some computer problems, and have knowledge of hardware (knowledgeable), I am a computer specialist, web developer, comfortable manipulating or writing computer programming (Expert).

Control Variables

Several studies have shown education to be positively related to cyber victimization (Breen, Henley & Redmiles, 2022; Whitty, 2020; Holtfreter et al., 2014). Of course, numerous studies of cyber

victimization have focused on college students where level of education (degree) is nearly a constant; however, Ngo and colleagues (2020) surveyed college students including senior citizens taking classes as non-degree seeking students (85% having a college degree) found that having a college degree was unrelated to 7 forms of cybercrime victimization. We included a dichotomous variable where 1 = a bachelor's or graduate/professional degree, and 0 = not having bachelor's or graduate/professional degree.

The notion that the elderly are attractive targets of cybercrime has become so commonly accepted that numerous programs have been developed to educate the elderly on best practices of computer and internet use (Quintana-Orts et al., 2022; Cross, 2017; Huey & Ferguson, 2021). Alternatively, the empirical research is less clear. For example, in the Ngo and colleagues study of college students referenced above that included senior citizens taking classes as nondegree seeking students (age range 18-87) found age to be negatively related to computer viruses, harassment by a nonstranger and defamation via the internet and unrelated to harassment by a stranger, unwanted pornography, sexual solicitations, and phishing (Ngo et al., 2020). In a study of residents of the Netherlands aged 15 and over, Leutfeldt and Yar (2016) found age to be negatively related to hacking but unrelated to malware victimization. Whitty (2020) examined a large sample of adult residents of the UK (mean age 48.5, s.d., 16.3) and found that age was unrelated to being cyber scammed. The relationship then, between age and cyber victimization, is certainly less than clear, and so we include age as a continuous variable in our models to further explore this variable.

Leukfeldt and Yar (2016: 270) have argued that motivated offenders may target victims with greater "value" as measured by financial characteristics such as personal and household income and suggest that these variables "are especially likely to play a role in fraud offenses". Their own analyses focus on hacking and malware and include personal income, household income, financial assets, financial possessions and savings as measures of "value" in a model with a host of other variables.

Among these variables only personal income is statistically associated with malware infection and the relationship is negative.

Results

Descriptive Statistics

Descriptive statistics comparing the sample to the commonwealth of Virginia are presented in Table 1. The sample represents the state in several respects but differs in ways common in survey research. Women, the elderly and college educated persons are more likely to respond to the survey than are males, younger persons and those without college degrees. However, the sample resembles the state in terms of racial/ethnic composition, marital status, owning computer equipment and, with the exception of the wealthiest residents, income.

_____

Insert Table 1 about here

_____

Bivariate Analyses

We first examine in an exploratory fashion the bivariate relationships between measures of target exposure, protective factors and the control variables to help develop the multivariate models that follow. We recoded (dichotomized or trichotomized) the independent variables to keep the statistical comparisons (chi-square) consistent. However, we were careful to make sure that the results presented in this section were confirmed with the full scale of the original variables that are used in the multivariate analyses. Results are presented in Table 2.

_____

Insert Table 2 about here

_____

First, we find the equipment index of households (e.g., having desktops, laptops and tablets or similar devices) is strongly related to ever experiencing a form of cybercrime. Only 37% of those responding that none of those devices were owned by a household member had experienced cyber fraud. Victimization increased in a linear fashion across the index with nearly twice the percentage of households with all three (71%) having been victimized. The relationship between household ownership of computer equipment and victimization in the past year was not as strong ($p<.10$), however, the percentages are telling, again increasing in a near linear fashion from 19% of those with no basic computer equipment experiencing theft or fraud increasing to 28% among both beginners and those being knowledgeable to 32% among those reporting to be experts.

Use of social media (e.g., Facebook, Twitter, and Instagram) is linked to higher levels of ever being victimized and being victimized in the past year (risk was 17% and 9% higher than those who do not use social media, respectively). Similar results are found with online banking, which was associated with 21% and 14% greater risk, respectively. Finally, how often respondents report using the internet was also positively associated with cyber victimization. For the bivariate analyses, responses to this question were trichotomized (2 hours or less, 3-7 hours and 8 or more hours) and the biggest differences were between those spending two hours or less compared to those spending 3 or more hours (14% and 16%, respectively) and this was consistent with the original 6 category response scales (<1 hour, 1-2, 3-5, 6-7, 8-9, and 10 or more hours). Overall, the bivariate analyses suggest that these measures of exposure were all positively correlated with victimization experience overall and in the past year.

Protective Factors

Interestingly, training about how to safely use the internet or how to stay safe on the internet was associated with increased risk of ever being victimized by theft or fraud but unrelated to

victimization in the past year. It is unlikely that training about how to use the internet safely, or how to stay safe on the internet increases the risk of victimization. Instead, victimization experiences may have *resulted in* seeking training, thereby producing a positive correlation with the ever-victimized variable. The null relationship with past year victimization may be the result of countervailing forces with some respondents receiving training before and some after their victimization. Such reciprocal effects are unlikely to be disentangled with cross-sectional data.

In terms of protective factors or guardianship, precautionary password behavior was significantly and negatively related to ever being victimized and victimization in the past year (reducing risk by about 14% in both cases). The second measure reflecting careful navigation on the internet was not associated with risk of ever being victimized but associated with lower risk in the past year (a 5.4% difference, $p<.10$).

Self-perceived internet and computer skills were ironically positively associated with both ever being victimized and being victimized in the past year. In terms of ever being victimized, approximately 42% of those uncomfortable with computers and the internet report being victimized, while 57% of beginners report being victimized. Among those more experienced, 67% and 69% of those reporting to be knowledgeable and experts, report ever being victimized. Turning to victimization in the past year, only 12% of those uncomfortable with computers and the internet report past year victimization while more than twice that number (27%) and nearly three times that number (32%) of those reporting to be knowledgeable report such victimization. The risk of past year victimization drops among experts (23%) but that is still nearly twice the risk of those who are uncomfortable with computers.

These unexpected results, of course, may be related to the important differences in exposure to risk experienced by those knowledgeable and even experts who likely spend considerably more time on the computer and the internet than do those who are very inexperienced and beginners. Examining the

inter-item correlations, the data show that the ordinal novice-to-expert variable is positively related to the equipment index (Gamma=.392, p<.001), the use of social media (Cramer's V= .175; p<.001), and the use of the internet for financial services (Cramer's V= .267, p<.001). Although it is not associated with the password caution scale (p>.10), it is related to taking care when navigating the internet (Cramer's V=.228, p<.001). These findings are consistent with the notion that perceived skills come from active use of computers and the internet resulting in greater exposure to motivated offenders leading to greater victimization.

Control Variables and Summary

Consistent with prior research, education as measured by a four-year bachelor's or graduate/ professional degree is positively related to ever being victimized, increasing the risk by 13 percentage points. However, education was unrelated to victimization in the past year. Income was also positively related to risk of ever being victimized, ranging from 58% for those households with incomes less than $50,000, increasing to 68% for those earning between $50,000-100,000 dollars, and 74% of those households making more than $100,000.

Finally, and not consistent with the literature, age was negatively associated with ever being victimized and victimization in the past year. These results were confirmed with the full scale of age (t-tests) showing those ever being victimized were about 3 years younger than those not victimized, and those victimized in the past year were about 6 years younger than those not recently victimized. To better understand this relationship, we correlated age with measures of exposure to motivated offenders. Age is also negatively correlated with time spent on the internet as well as using the internet (Gamma = -.38, p<.001), use of social media such as Facebook, Twitter, Instagram or LinkedIn (Cramer's V= -.29, P<.001) and use of the internet for financial services (Cramer's V = .22, p<.22).

Several interesting findings emerge from this preliminary bivariate analysis, and the results also have implications for the multivariate analyses. First, target exposure is consistently positively related to victimization at the bivariate level. Second, protective factors appear to be, for the most part, negatively related to victimization. Third, self-perceived comfort/expertise with the internet is unexpectedly positively related to victimization, but the data suggest that this is likely due to the amount of exposure to motivated offenders among those with greater skills who likely spend both more time on the internet and use the internet as part of their lifestyle (shopping, banking, social media, etc.).

Multivariate Models: Logistic Regressions Predicting Cyber Fraud/theft.

Because our dependent measures are dichotomous, we built our multivariate models with logistic regressions. We built two models (victimized ever and victimized in the past year) in three blocks of independent variables beginning with three measures of exposure to motivated offenders, followed by training, self-protective behaviors, and self-perceived knowledge and expertise with computers and the internet. The final block introduces demographic variables found to be important in the literature—age, education, and income[1]. The results are presented in Table 3.

_____

Insert Table 3 about here

_____

Focusing on the first block predicting ever being victimized, all of the items except how often one is on the internet are statistically and positively related to victimization as would be predicted by routine activities theory. That is to say, three essential elements of crime converge to help explain the risk of victimization: a motivated offender, an attractive target, and the absence of capable

[1] Income was statistically significant and positive at the bivariate level and we first ran the model including income. Income was not statistically significant, and the other substantive parameters did not change. However, the sample size dropped by over an additional 100 cases (from 829 to 720) so this model is not presented in text. Results are available from the authors.

guardianship. Use of social media doubles the odds of victimization while each piece of equipment used and banking on the internet increase the odds by 22% and 51%, respectively

Adding the second block of variables shows that both measures of self-protective behaviors (password caution and careful navigation of the internet) reduce the odds of victimization. Perhaps more importantly, their inclusion (along with self-perceived level of expertise with the internet) reduces the influence of two of the exposure variables (use of social media and online banking) substantially—to the point that they are no longer statistically significant. Only having more computer equipment (i.e., desktop, laptop, a tablet or other similar computing device) remains a significant predictor of victimization. Consistent with the bivariate analyses, the relationship between perceived skills in internet use and victimization is positive and statistically significant even after controlling for how frequently and what types of activities are conducted on the computer.

The final model that includes demographic variables did not change the results substantially. Age, education and income, which were all significant at the bivariate level, are not statistically significant predictors of victimization at the $p<.05$ level and contribute little to the full model.

Moving to the model predicting victimization in the past year, the first model shows that only online banking predicts recent theft or fraud, increasing the odds of victimization by 63%. Equipment, social media use, and frequency of internet use are not statistically significant predictors of victimization. Caution in the use of passwords significantly reduces the odds of victimization and mediates the effect of online banking—the coefficient is reduced and is no longer statistically significant once this variable is entered into the model. As in predicting ever-victimization, self-perceived skill in use of the internet is significantly ($p<.10$) and positively related to victimization.

Discussion and Conclusions

This paper contributes to the literature on cyber victimization in several ways. First, we provide a largely representative sample of residents from the Commonwealth of Virginia, a state that is diverse and uniquely situated to study cyber victimization. The population is relatively highly educated, economically stable, and politically involved. Second, the survey contains a host of items focused on cybertheft and cyberfraud—very common forms of cyber victimization that can have serious economic costs and psychosocial consequences (Brenner et al., 2020; Golladay and Holtfreter, 2017). Third, although the survey was not developed with the sole goal to test routine activity theory, it includes a number of items drawn from our own and other research that allowed us to build statistical models that compares to and builds on a growing literature that uses routine activities to explain various forms of cybervictimization.

We included four measures linked to exposure to motivated offenders. Bivariate analyses show that owning more computer equipment, using the internet for social media (e.g., Facebook, Twitter Instagram or Linkedin), and using the internet for financial services (e.g., paying bills, banking, transferring funds, etc.) are significantly related to both ever experiencing cyber theft or cyber fraud and being a victim of these offenses in the past year. These factors have been found to be significant in some prior studies (Hutchings and Heyes, 2009; Reisig and Holtfreter, 2013; Pratt et al., 2010). Indeed, the majority of these effects disappeared once we entered the protective factors (capable guardianship) as a second block of variables into the models.

Our interpretation then is somewhat different from prior studies that discounted the importance of these factors. Our results suggest that the effects of exposure on victimization are not spurious or even weak; rather the effects are mediated by careful navigation on the internet and caution in the use of passwords that more directly affect fraud and theft victimization. We were surprised that a

single measure of time spent on the internet was not statistically significant at either the bivariate or multivariate level as some studies have found (Leufeldt and Yar, 2016; Marcum and Higgins, 2021). Alternatively, other studies have also had limited success with similar items (see Ngo et al., 2020; Ngo and Paternoster, 2011; Reyns et al., 2011). Some have argued that it is not so much the length of time spent online that puts people at heightened risk of victimization, but rather what people do while they are online (Ngo et al., 2020; Hawdon et al., 2020). In particular, dark web exploration, posting personal information, online chats and video, buying and selling things online, among other activities seem to better predict unique forms of cyber victimization than other activities or simply the length of time spent on the internet. Our limited measures are consistent in that using the internet for social media and financial services are both related to fraud and cyber victimization which is mediated by careful and cautious use of the internet.

Our measure of internet and computer skills had an unexpected positive effect on ever experiencing fraud/theft and being victimized in the past year. In their 2009 study, Bossler and Holt did not detect a significant relationship between self-reported skills and malware infection, but later research with a similarly sized but different data set of students found the same measure to be negatively related to malware victimization (Holt and Bossler, 2013). Hawdon and colleagues (2020) used a similar measure modeled after Nodeland and Morris (2020) who added to levels to the ordinal scale, in their study of cybercrime pre and post COVID and found it to be unrelated to a seven-item index of cybervictimization. Of course, perceived knowledge/comfort may result in letting one's guard down and not being as cautious or careful as those who feel less comfortable.

There are several limitations with this study that warrant attention. First, funding for the survey was limited and the survey instrument had to be kept reasonably short to get the necessary sample size promised in the proposal and cover the primary aims of the funding agency – baseline assessment of

cyber victimization and its consequences across Virginia. A shorter survey undoubtedly encouraged participation and helped keep respondent's attention, but it also meant that there was only a limited number of items to address theoretical interests. Thus, although we believe we have been able to provide a solid test of routine activity theory as it applies to cyber fraud and theft, it is not a complete test and some of our measures are weak.

Next, we used several strategies to obtain a representative sample and to a large extent we achieved that goal, however, as is common in survey research, especially that conducted by telephone, our sample included more females than males, more college graduates, and few respondents at the highest end of the income spectrum. Of course, there is always a concern that there are psychosocial correlates related to not responding to surveys, victimization experiences, and the theoretical variables of interest. Addressing this issue is beyond the scope of this article, but we note that our findings are consistent with other research using different data collection strategies. Nevertheless, the reader should interpret our results with these sampling issues in mind.

We also lost a considerable number of cases in the multivariate models because of missing data. Of course, there are techniques to minimize missing data and, in fact, we utilized one strategy for the income variable since it was missing from a considerable number of cases, as is common in survey research. But, once again, the reader is cautioned to interpret our results with this limitation in mind.

Directions for Future Research

One of the central goals of our research is to encourage the widespread collection of cybercrime data. It is imperative that we improve the quality of cybercrime data if we are to better understand its causes, consequences, and how to prevent it. Currently, we lack quality data that can be used to critically test theories of cybercrime. To do so, we need to collect longitudinal data and panel data as

well as to work toward better measurement of key concepts. Longitudinal data such as that provided from the National Crime Victimization Survey (NCVS) for offline crimes is needed to assess trends in cybercrime and cybercrime victimization. While cybercrime variables could be added to the NCVS, it is likely that a survey dedicated to cybercrime is needed so that nuanced data could be collected without making the instrument too burdensome for respondents. In addition, panel data are needed that follow the same individuals over time so that reciprocal effects such as those we postulate between victimization and the adoption of protective factors can be disentangled and better understood. In addition, these data are needed to devise critical tests of criminological theories and design strategies for reducing vulnerability. We currently rely primarily on target-hardening techniques to prevent victimization. While these strategies are undoubtedly important, they are only part of the equation. We must also account for human factors that motivate offenders, influence target suitability, and pattern the behavior and availability of capable guardians.

Conclusion

The early work of Cohen and Felson (1979:588) provided a powerful theoretical explanation of "an important sociological paradox" along with a rigorous empirical test of that explanation. They were able to show that important changes in routine activities over time accounted for the rise in violent crime in a decade where economic conditions were on the rise and most sociologists and criminologists would have expected stability or even decreases in violent crime. Subsequently a routine activity theory has provided a powerful theoretical tool to explain a wide variety of crimes at the micro, meso, and macro levels (see reviews by Pratt and Cullen, 2005; Engström, 2021; and Pusch and Holtfreter,2021).

While some researchers appear skeptical about the ability of routine activity theory to adequately explain criminal victimization in the in the virtual world, we are more optimistic. Here we have shown that that exposure to motivated offenders is relatively strongly related to fraud and theft

victimization and that exposure is mediated by protective guardianship. Demographic variables related to risk were also mediated by precautionary behaviors. Although the models did not explain a great proportion of the variance in fraud or theft victimization, we are hopeful that studies specifically designed to link routine activities to cyber victimization advance the field further. Specifically, greater conceptualization of key variables, more rigorous measurement, longitudinal designs, and sophisticated statistical modeling as well as qualitative endeavors will go a long way in advancing theory and practice.

References

Aizenkot, D. (2021). The predictability of routine activity theory for cyberbullying victimization among children and youth: Risk and protective factors. *Journal of Interpersonal Violence, 37*(13-14), 857-882. https://doi.org/10.1177/0886260521997433

American Legislative Exchange Council Center for State Fiscal Reform. (2022). *Rich States, Poor States: ALEC-Laffer State Economic Competitiveness Index*. https://www.richstatespoorstates.org/states/VA/

Arntfield, M. (2015). Toward a cybervictimology: Cyberbullying, routine activities theory, and the anti-sociality of social media. *Canadian Journal of Communication, 40*(3), 371–388.

Bartolacci, M. R., LeBlanc, L. J., & Podhradsky, A. (2014). Personal denial of service (PDOS) attacks: A discussion and exploration of a new category of cyber crime. *Journal of Digital Forensics, Security and Law*, *9*(1), 2.

Bossler, A. M., & Holt, T. J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology, 3*(1), 400–420.

Breen, C., Herley, C., & Remiles, E. M. (2022). A large-scale measurement of cybercrime against individuals. *CHI Conference on Human Factors in Computing Systems,* 1-41. https://doi.org/10.1145/3491102.3517613

Brenner, L., Meyll, T., Stolper, O., & Walter, A. (2020). Consumer fraud victimization and financial well-being. *Journal of Economic Psychology*, *76*, 1022-43.

Button, M., & Cross, C. (2017). Cyber Frauds, Scams and their Victims (1st ed.). Routledge. https://doi.org/10.4324/9781315679877

Callahan, E. (2021). *Virginia ranked as No. 7 for 'Best State,' according to U.S. News & World Report*. https://www.whsv.com/2021/03/09/virginia-ranked-as-no-7-for-best-state-according-to-us-news-world-report/

Choi, K-S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2*(1), 308–333.

Cohen, L.E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Costello, M., Restifo, S. J., & Hawdon, J. (2021). Viewing anti-immigrant hate online: An application of routine activity and Social Structure-Social Learning Theory. *Computers in Human Behavior*, *124*, 106927.

Cross, C. (2017). 'But I've never sent them any personal details apart from my driver's licence number …': Exploring seniors' attitudes towards identity crime. *Security Journal, 30*(1), 74–88.

Daikeler, J., Bošnjak, M., Manfreda, K. L. (2020). Web versus other survey modes: An updated and extended meta-analysis comparing response rates. *Journal of Survey Statistics and Methodology, 8*(3), 513-539. https://doi.org/10.1093/jssam/smz008

Dearden, T. E. (2021) Routine Activities and Self-Protection on the Internet: An analysis of Equifax. *Victims & Offenders, 16*(8), 1149-1160.

Eck, J. E., & Clarke, R. V. (2003). *Classifying common police problems: A routine activity theory approach*. In M. J. Smith & D. B. Cornish (Eds.), Theory and practice in situational crime prevention. Crime prevention studies (Vol. 16, pp. 7–39). Monsey, NY: Criminal Justice Press.

Engström, A. (2021). Conceptualizing Lifestyle and Routine Activities in the Early 21 st Century: A Systematic Review of Self-Report Measures in Studies on Direct-Contact Offenses in Young Populations. *Crime & Delinquency*, *67*(5), 737–782. https://doi.org/10.1177/0011128720937640

Evans, J. R. & Mathur, A. (2018). "The value of online surveys: A look back and a look ahead" *Internet Research, 28*(4), 845-887. https://doi.org/10.1108/IntR-03-2018-0089

FBI Internet Crime Report 2021. (2022). https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

FTC (2021a). *What to know about identity theft. Federal Trade Commission*. Retrieved August 30, 2022 from https://consumer.ftc.gov/sites/default/files/articles/pdf/677a_idt_what_to_know_wtd.pdf

FTC (2021b). *What to know about credit freezes and fraud alerts. Federal Trade Commission*. Retrieved August 30, 2022 from https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts

Golladay, K., & Holtfreter, K. (2017). The consequences of identity theft victimization: An examination of emotional and physical health outcomes. *Victims & Offenders*, *12*(5), 741-760.

Guerra, C., & Ingram, J. R. (2022). Assessing the Relationship between Lifestyle Routine Activities Theory and Online Victimization Using Panel Data. *Deviant Behavior, 43*(1), 44–60.

Hawdon, J., Parti, K., & Dearden, T. E. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment. *American Journal of Criminal Justice, 45*(4), 546–562.

Hawdon, J., Costello, M., Ratliff, T., Hall, L. and Middleton, J. (2017). Conflict Management Styles and Cybervictimization: An Extension of Routine Activity Theory. *Sociological Spectrum, 37*(4): 250-266.

Holt, T. J., Fitzgerald, S., Bossler, A. M., Chee, G., & Ng, E. (2016). Assessing the Risk Factors of Cyber and Mobile Phone Bullying Victimization in a Nationally Representative Sample of Singapore Youth. *International Journal of Offender Therapy & Comparative Criminology, 60*(5), 598–615.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime, 16*(2). https://doi.org/10.1080/17440572.2015.1013211

Holt, T., & Bossler, A. (2009). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior, 30*(1), 1–25.

Holt, T. J., & Bossler, A. M. (2013). Examining the Relationship Between Routine Activities and Malware Infection Indicators. *Journal of Contemporary Criminal Justice, 29*(4), 420–436.

Holt, T. J., Bossler, A. M., Malinski, R., & May, D. C. (2016). Identifying Predictors of Unwanted Online Sexual Conversations Among Youth Using a Low Self-Control and Routine Activity Framework. *Journal of Contemporary Criminal Justice, 32*(2), 108–128.

Holt, T.J., van Wilsem, J., van de Weijer, S., & Leukfeldt, E.R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review, 38*(2), 187-206. https://doi.org/10.1177/0894439318805067

Holtfreter, K., Reisig, M.D., Mears, D.P., & Wolfe, S.E. (2014). *Financial exploitation of the elderly in a consumer context.* Research report. Center for Victim Research. Retrieved August 29, 2022 from: https://ncvc.dspacedirect.org/bitstream/id/2044/Financial%20Exploitation%20of%20the%20Elderly_IR_508.pdf

Huey, L. & Ferguson, L. (2021). What do we know about senior citizens as cybervictims? A rapid evidence synthesis. *Sociology Publications,* https://doi.org/10.21428/cb6ab371.e6b80803

Hutchings, A. & Heyes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the 'net'?, *Current Issues in Criminal Justice, 20*(3), 433-451.

Kabiri, S., Choi, J., Shadmanfaat, S. M. S., Lee, J. (2020). Using structural equations to test a multi-theoretical framework with data on cyberstalking victimization in Iran: Self-control, control deficit, peers' online deviant behaviors, and online deviant lifestyles. *Crime & Delinquency, 67.* https://doi.org/10.1177%2F0011128720968501

Kalton, G. (2019). Developments in survey research over the past 60 years: A personal perspective. *International Statistical Review, 87*(1), 10-30. https://doi.org/10.1111/insr.12287

Kaluarachchi, C., Sedera, D., & Warren, M. (2020). An intervention model for cyberbullying based on the general theory of crime and routine activity theory. *ACIS 2020 Proceedings, 8.* Retrieved Aug 29, 2022from https://aisel.aisnet.org/acis2020/8

Kigerl, A. (2021). Routine activity theory and malware, fraud, and spam at the national level. *Crime, Law & Social Change, 76*(2), 109–130. https://doi.org/10.1007/s10611-021-09957-y

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3), 263–280.

Marcum, C. D. & Higgins, G. E. (2021). A systematic review of cyberstalking victimization and offending behaviors. *American Journal of Criminal Justice,* 1-29. https://doi.org/10.1007/s12103-021-09653-6

Marcum, C. D., Ricketts, M. L., & Higgins, G. E. (2010). Assessing Sex Experiences of Online Victimization: An Examination of Adolescent Online Behaviors Using Routine Activity Theory. *Criminal Justice Review, 35*(4), 412–437.

Marcum, C. D. (2008). Identifying Potential Factors of Adolescent Online Victimization for High School Seniors. *International Journal of Cyber Criminology, 2*(2), 346–367.

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime Victimization and Problematic Social Media Use: Findings from a Nationally Representative Panel Study. *American Journal of Criminal Justice, 46*(6), 862–881.

Miró, F. (2014). Routine activity theory. *The encyclopedia of theoretical criminology* (pp. 1–7). London,England: Blackwell.

Näsi, M. J., Räsänen, P., Keipi, T., Oksanen, A. (2015). Perceived trust and victimization experiences in a four country study. *In Economic and Sociological Studies in Turbulent Times. Working Papers in Economic Sociology (VII).*

Navarro, J., & Jasinski, J. (2012). Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences. *Sociological Spectrum, 32*(1), 81–94.

NCVS (2018). *Identity Theft Supplement to the National Crime Victimization Survey*. Retrieved August 30, 2022 from https://bjs.ojp.gov/data-collection/identity-theft-supplement-its#surveys-0

Nguyen, T.V. (2020). Cybercrime in Vietnam: An analysis based on routine activity theory. *International Journal of Cyber Criminology, 14*(1), 156-173.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5*(1), 773–793.

Ngo, F. T., Piquero, A. R., LaPrade, J., & Duong, B. (2020). Victimization in Cyberspace: Is It How Long We Spend Online, What We Do Online, or What We Post Online? *Criminal Justice Review, 45*(4), 430–451. https://doi-org.proxy.lib.odu.edu/10.1177/0734016820934175

Nodeland, B., & Morris, R. (2020). The impact of low self-control on past and future cyber offending. *International Journal of Cyber Criminology, 14(1), 106-120.*

Nutter, K.J. (2021). Examining cyberstalking victimization using routine activities and lifestyle-routine activities theories: A critical literature review. *The Mid-Southern Journal of Criminal Justice, 2(*1), 1-24.

Payne, B. K., & Chappell, A. (2008). Using Student Samples in Criminological Research. *Journal of Criminal Justice Education, 19*(2). https://doi.org/10.1080/10511250802137226

Perkins, R. C., Howell, C. J., Dodge, C. E., Burruss, G. W., & Maimon, D. (2022). Malicious Spam Distribution: A Routine Activities Approach. *Deviant Behavior, 43*(2), 196–212.

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

Pratt, T. C., & Cullen, F. T. (2005). Assessing Macro-Level Predictors and Theories of Crime: A Meta-Analysis. *Crime & Justice*, *32*, 373–450. https://doi.org/10.1086/655357

Pusch, N., & Holtfreter, K. (2021). Sex-Based Differences in Criminal Victimization of Adolescents: A Meta-Analysis. *Journal of Youth & Adolescence*, *50*(1), 4–28. https://doi.org/10.1007/s10964-020-01321-y

Quintana-Ortz, C., Merida-Lopez, S., Chamizo-Nieto, M.T., Extremera, N., & Rey, L. (2022). Unraveling the links among cybervictimization, core self-evaluations, and suicidal ideation: A multi-study investigation. *Personality and Individual Differences, 186.* https://doi.org/10.1016/j.paid.2021.111337

Reisig, M.D. & Holtfreter, K. (2013). Shopping fraud victimization among the elderly. *Journal of Financial Crime, 20*(3), 324–337.

Reep-van den Bergh, C. M. M., & Junger, M. (2018). Victims of cybercrime in Europe: A review of victim surveys. *Crime Science, 7*(5). https://doi.org/10.1186/s40163-018-0079-3

Reyns, B.W., Henson, B., & Fisher, B.S. (2011). Being pursued online. Applying cyber lifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169. https://doi.org/10.1177/0093854811421448

Rungsrisawat, S., Sriyakul, T., & Jermsittiparsert, K. (2019). The era of e-commerce & online marketing: Risks associated with online shopping. *International Journal of Innovation, Creativity and Change, 8*(8).

Ryan, C. L., & Bauman, K. (2016). *Educational Attainment in the United States: 2015*. Retrieved from: https://vtechworks.lib.vt.edu/bitstream/handle/10919/83682/EducationalAttainment2015US.pdf?sequence=1&isAllowed=y

Song, H., Lynch, M., & Cochran, J. (2016). A Macro-Social Exploratory Analysis of the Rate of Interstate Cyber-Victimization. *American Journal of Criminal Justice*, *41*(3), 583–601.

Tewksbury, R. & Mustaine, E.E. (2003). College students' lifestyles and self-protective behaviors. Further considerations of guardianship concept in routine activities theory. *Criminal Justice and Behavior, 30*(3), 302-327. https://doi.org/10.1177/0093854803252354

U.S. Department of Commerce. Bureau of Economic Analysis. (2021). *Personal Consumption Expenditures by State, 2020*. https://www.bea.gov/sites/default/files/2021-10/pce1021.pdf

U.S. Department of Commerce. Bureau of Economic Analysis. (2022). *Personal Income by State*. https://www.bea.gov/data/income-saving/personal-income-by-state

U.S. Department of Commerce. Bureau of Economic Analysis. (2022a). *Gross Domestic Product by State, 1st Quarter 2022*. https://www.bea.gov/news/2022/gross-domestic-product-state-1st-quarter-2022

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *Journal of Contemporary Criminal Justice, 32*(2), 169–188. https://doi-org.proxy.lib.odu.edu/10.1177/1043986215621379

Virginia Employment Commission. (2022). *Statewide Economic Analysis Report*. https://virginiaworks.com/_docs/Publications/LMI-Publications/Statewide-Economic-Analysis/PDF/SEA-2021.pdf

Virginia Rural Health Plan. (2022). *Defining Rurality in Virginia*. https://www.vdh.virginia.gov/content/uploads/sites/76/2022/01/Virginia-Rural-Health-Plan_2-Defining-Rurality.pdf

Walters, G. D. (2021). School-Age Bullying Victimization and Perpetration: A Meta-Analysis of Prospective Studies and Research. *Trauma, Violence & Abuse*, *22*(5), 1129–1139. https://doi.org/10.1177/1524838020906513

Weijer, van de, S.G.A., E.R. Leukfeldt, & W. Bernasco (2019) Reporting crime to the police: A comparison between traditional crime and cybercrime. *European Journal of Criminology, 16*(4), 486-508.

Whitty, M. T. (2020). Is there a scam for everyone? Psychologically profiling cyberscam victims. *European Journal on Criminal Policy and Research, 26,* 399-409. https://doi.org/10.1007/s10610-020-09458-z

Williams, M.L. (2016). Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *The British Journal of Criminology, 56,* 21–48. https://doi.org/10.1093/bjc/azv011

World Population Review. (2022a). *US States - Ranked by Population 2022*. https://worldpopulationreview.com/states

World Population Review. (2022b). *Public School Rankings by State 2022*. https://worldpopulationreview.com/state-rankings/public-school-rankings-by-state

World Population Review. (2022c). *Virginia Population 2022*. https://worldpopulationreview.com/states/virginia-population

Yao-Chung, C. (2010). *Cybercrime across the Taiwan Strait: Regulatory responses and crime prevention.* PhD Dissertation Series. Australian National University. Retrieved August 29, 2022 from https://openresearch-repository.anu.edu.au/handle/1885/150195

Yao-Chung Chang, L. (2019). Criminological perspectives on cybercrime: risk, routine activity, and cybercrime. In V. Mitsilegas, S. Hufnagel, & A. Moiseienko (eds.) *Research handbook on transnational crime* (pp. 327–343) Elgar Online Books.

Table 1. Descriptive Statistics

Sample Data Compared to Census (State Population 8,642,274, total sample size 1,206)				
		VA Census[a]		Sample
Age	% 65 +	16.3		27.6
Gender	% Female	50.5		60.0
Race/Ethnicity	% White	68.8		72.1
	% Black	20		17.7
	% Other	11.2		10.3
Education	% College Degree (25+)	39.5		48.8
HH Income	% <$75,000	62.1		59.1
	% $75-100,000	12.9		13.1
	% $100-150,000	17.2		13.5
	% $150,000 and over	20.7		14.3
Computer Equip.	% HH with Computers[c]	92.3		92.3
Marital Status	% Married[d]	49.92		50
a. Data from: https://www.census.gov/quickfacts/fact/table/VA,US/PST045221				
b. Data from: https://namecensus.com/demographics/virginia/				
c. Census data is base on 2016-2020 data, sample is 2022				
d. Census is % on those 15 year and older, sample base on 18 years and older				

Table 2. Bivariate Analyses Predicting Cyber Fraud and Theft, Ever and in the Past Year

Table 2.			Bivariate Analyses						
Ever Fraud Victim					Victimization Past year				
Exposure to Motivated Offenders									
Equipment (n=1206)									
None	One	Two	Three		None	One	Two	Three	
37.60%	58.40%	64.40%	70.80%	***	19.40%	27.80%	26.80%	31.60%	+
Use Social Media (n=1195)									
No	Yes				No	Yes			
49.30%	66.50%	***			20.60%	29.90%	**		
Online Banking (n=1185)									
No	Yes				No	Yes			
45.90%	67.30%	***			16.70%	30.80%	***		
Often Use Internet (n=1103)									
2 Hour of less	3-7 Hours	8+ Hours			2 Hour of less	3-7 Hours	8+ Hours		
52.00%	66.10%	66.30%	***		17.20%	31.20%	32.70%	***	
Protective Factors									
Training (n=1179)									
No	Yes				No	Yes			
58.40%	67.70%	***			27.90%	28.90%			
Precautionary Behavior (n=967 and 1122, respectively)									
	Low	High			Low	High			
Password Caution	72.30%	58.00%	***		37.60%	23.4%	***		
Careful Navigation	64.8%	63.2%			32.30%	26.9%	+		
Internet Skills (n=1187)									

Uncomfortable	Beginner	Knowlegeable	Expert		Uncomfortable	Beginner	Knowlegeable	Expert	
41.60%	57.00%	67.30%	69.10%	***	11.70%	27.40%	31.70%	22.80%	***
Control Variables									
Age (n=1185)									
18-34	35-54	55 and over			18-34	35-54	55 and over		
64.30%	68.80%	58.50%	**		32.00%	34.50%	21.80%	***	
College Degree (n=1181)									
No	Yes				No	Yes			
57.20%	69.80%	***			29.8%	26.40%			
Income (n=945)									
<50K	50-100K	>100K			<50K	50-100K	>100K		
58.10%	67.50%	74.10%	***		31.60%	30.50%	34.20%		

Table 3. Multivariate Models: Logistic Regression Predicting Cyber Theft and Fraud

Table 3. Multivariate Models: Logistic Regression Predicting Theft/Fraud													
Fraud Victimization Ever	(n=829)							Fraud Victimization Past year					
	Exp(B)		Exp(B)		Exp(B)			Exp(B)		Exp(B)		Exp(B)	
Exposure to Motivated Offenders													
Equipment	1.223	*	1.221	*	1.182	+		1.076		1.124		1.13	
Social Media	2.037	*	1.628		1.658			0.82		0.678		0.71	
Banking	1.511	*	1.289		1.21			1.633	*	1.44		1.355	
Often Use the Internet	1.059		1.003		1.014			1.071		1.04		1.027	
Protective Factors: Capable Guardians													
Received Training			1.297		1.242					1.034		1.03	
Password Caution			0.877	***	0.878	***				0.88	***	0.89	***
Careful Navigation			0.928	*	0.926	*				0.912	**	0.91	*
Internet Skills			1.422	**	1.378	**				1.24	+	1.29	*
Control Variables													
Age					1.002							0.996	
College Degree					1.34	+						0.784	
Income (missing = 0)					1.048							1.041	
Income Missing Adjustment					0.843							0.615	
Nagelkerke r-square	0.037		0.104		0.116			0.016		0.076		0.093	