Not Everyone Is a Target: An Analysis of Online Identity Crime Victimization Using Routine Activities Theory

By

Zinaida Zaslawski

A thesis submitted to the Graduate Program in Sociology

In conformity with the requirements for the degree of Master of Arts

Queen's University Kingston, Ontario, Canada

April, 2017

ABSTRACT

This study examines online identity theft, consumer fraud and phishing victimization using data from a national survey of Canadians. The goal is to answer the following questions: (1) Is everyone equally likely to be a target of online crime? and (2) What factors might lead to online victimization? This research utilizes Routine Activity Theory (Cohen and Felson 1979) and an extension proposed by Eck and Clarke (2003). This approach specifies that crime is facilitated by an offender's motivation, the absence of effective guardians, and the availability of suitable targets online.

This research draws on the 2009 General Social Survey (GSS). Logistic regression is used to analyze the relationships between demographic variables, perceptions of risk and online routine activities on identity theft, consumer fraud, and phishing victimization.

Findings reveal that education has a consistent effect on all three types of victimization when taking into account routine activities. Men are less likely to change passwords regularly and to delete emails on a regular basis compared with women. Men, compared with women, are also more likely to be victims of consumer fraud and phishing. Results show that perceptions of risk are correlated with victimization. Several forms of routine activities (using the internet for banking, making reservations or bookings, and belonging to online social network websites) increase all three types of victimization. In addition, using the internet for purchasing goods or services or using online chat services increases victimization for consumer fraud and phishing. The results also reveal that those who deal with known websites, enter misleading information online, regularly change their passwords and delete emails are more likely to be victims of online

consumer fraud and phishing. This could be explained by other 'risky' online activities that moderate relationships.

Findings provide support for Routine Activities Theory as an explanation for online identity theft, consumer fraud, and phishing victimization. Further research should explore additional causes, such as 'risky' online activities that lead to online victimization. Research should also focus on prevention measures aimed at those most at risk of victimization.

ACKNOWLEDGEMENTS

I would like to start by extending my thanks to Dr. Fiona Kay, who has been invaluable to my progress on this thesis. Her endless help and support throughout the process of writing this thesis is greatly appreciated, as well as her patience and countless edits of my drafts. I am also very appreciative for the insight given by committee member Dr. Victoria Sytsma, and external examiner Dr. Vincent Sacco. I also would like to appreciate the help of Mr. Jeff Moon at the Queen's University Data Library who assisted me with access to data and with weighting procedures.

Of course, these last two years would not have been the same without my office mates: Brandon, Kyle, Jade, and (honorary office mates) Megha and Tom. Their endless support was what kept me motivated during this stressful time. Finally, I would like to extend a special thanks to my wonderful boyfriend, Mike, my extremely supportive parents, Elena and Alex, and my brother, Michael, and my dear friends, Melissa and Zlata, who always encouraged me all through this journey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE: INTRODUCTION

Identity theft is a crime that grew dramatically with the rise of the information society. The internet has made it easier to access personal information and crimes related to identity theft are more profitable to perpetrators (Newman 2008). The Canadian Competition Bureau (2017) estimates that in 2016 out of the 90,000 received fraud complaints, more than 20,000 were online scams. The reported online crimes account for more than $40 million in losses.[1] The Canadian Competition Bureau (2017) reports that "scam artists continue to use traditional techniques by telephone, emails and in person, but have also latched on to social media platforms to target a new demographic: millennials and generation Z. Despite being tech-savvy, this demographic has such a strong presence on social media that they have become natural targets for fraudsters."[2]

Although there is an increase in online identity crime, the reality is that only about 5% of fraud gets reported in Canada (Competition Bureau 2017).[3] Similarly, the Australian Bureau of Statistics (ABS) found that only 43% of victims of crimes of credit and debit card theft were prepared to report their victimization to the police (Holm 2012: 69). There is a significant gap in the knowledge of incidence, offenders, and potential fraud threats. It is important to research online fraud crimes and victimization in order to improve upon existing policies and to develop new programs that will reduce the frequency of fraud in Canada.

In this chapter I will discuss the various definitions of identity crime to better conceptualize the problem of victimization. I will discuss online identity crimes, specifically: online identity theft, online consumer fraud, and phishing. I will also explain the importance of

[1] Retrieved March 15, 2017 (http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04201.html)
[2] Ibid.
[3] Ibid.

this research in terms of prevalence and harm. Finally, I will identify the research question that this thesis aims to address.

Definitions of Identity

In order to properly explore identity crime it is important to understand what researchers regard as identity and what elements of a person's identity are vulnerable to victimization. Newman (2008) suggests that there are two primary components of identity: what we are biologically and who we are based on our life history. He asserts that "our meager attempts in the marketplace that link what we are to who we are is typically a photograph of the individual attached to a piece of paper or plastic, issued by an authoritative body that depends on documents issued by other authoritative bodies that issue documents pertaining to the applicant's life history" (Newman 2008: 12). Having a disconnect between the biological and life history identities creates multiple opportunities for theft because verifying one's identity can be done without the actual presence of the person to whom the identity documentation belongs.

Another way to conceptualize identity is discussed by Finch (2007). She argues that identity is composed of three parts: personal, social, and legal. First, personal identity is experienced and internalized by the individual. It is a self-perception that evolves with interactions. Second, social identity is concerned with how the individual is perceived by others. This identify can be different from that of personal identity. Third, and probably the most relevant component of identity for this study, legal identity provides "the ability to substantiate claims to be a particular person" (Finch 2007: 30). This is the information that differentiates individuals objectively. Its purpose is to authenticate a person at any point in time and provide historical continuity and to associate with this person's events from the past, such as education

and financial records. The end goal is to create a strong association between information and the individual to whom the information relates.

Unlike personal and social identity, legal identity does not change with interactions. It is permanent. With time the legal identity becomes more detailed and comprehensive, but once the facts exist (connected to the legal identity) theft of those facts are possible (Finch 2007). Finch (2007) asserts that it is important to explore if this misappropriation of identity is a crime that deserves to carry a criminal liability. In the next section, I will discuss the challenges to defining identity theft. I will also examine what constitutes consumer fraud and phishing victimization.

Definitions of Identity Crime

In the past *identity fraud* referred to crimes against an agency, such as the government or financial institution, that received fraudulent information. In contrast, *identity theft* referred to a crime against the individual—the person who had their information stolen and used (McNelly and Newman 2008).

Presently, there are many terms used to describe the misappropriation of personal information. These include: identity crime, identity theft, identity fraud, identity fabrication, and identity manipulation, among others (Smith 2010). In 2006 the Australian Center for Policing Research (ACPR), the Australian Transaction Reports (ATP) and the Analysis Center's Proof of Identity Steering Committee (ACPISC) developed definitions of specific types of fraud. They define identity manipulation as alterations which are done to one's own identity. Identity theft is when one assumes a pre-existing identity—with or without consent. Identity fraud is when there is a monetary or other kind of gain or the avoidance of punishment by using another's identity (Smith 2010).

The Canadian Anti-Fraud Centre and the Royal Canadian Mounted Police (RCMP) define identity theft and identity fraud similarly to the definitions used by ACPR, ACPISC and ATP. Identity theft in Canada is defined as the collection of someone else's personal information for criminal purposes. Identity fraud is the actual use of another person's information, which includes impersonation and the misuse of debit or credit card data for financial gain (Canadian Anti-Fraud Centre 2017; RCMP 2015).

According to Finch (2007), identity fraud is defined as the use of another person's identity for various purposes. However, identity theft is defined as the permanent appropriation of another person's identity. The main distinction is that after *identity fraud* is committed the offender reassumes their own identity; whereas the offender that commits *identity theft* continues to live their life under the assumed identity (Finch 2007).

Holm (2012) describes what identity fraud and identity theft entail based on similar definitions. The former is when the offender assumes part of victim's identity to commit crimes with already open bank accounts. The latter is when the offender assumes the whole identity to open new accounts. According to this definition of the two offences, a person who commits identity theft is not committing a crime under the law. It is only after the use of an identity to commit an offence that the action is considered criminal (Finch 2007; Smith 2010).

Koops and Leenes (2006) make a similar argument. They argue that identity theft is primarily defined as a subsidiary crime—when one's identity is used to commit an actual crime. They suggest that since one will not be able to commit identity fraud without committing identity theft first, then identity fraud can be a more encompassing term. On the contrary, Milne, Rohm and Bahl's (2004) argue that identity theft is the more general term because theft is the appropriation of someone else's personal or financial identity to commit fraud or theft. McNelly

and Newman (2008) argue that identity fraud and theft refer to the same thing and can be used interchangeably. Smith (2010) takes this one step further and suggests using 'identity crime' as a general category for these types of crimes. There are several conflicting definitions. For the purpose of this thesis, I will refer to identity theft and identity fraud as identity theft for ease and consistency. Using one term to include both types of crime is consistent with work by McNelly and Newman (2008).

Definitions of Online Identity Crime

Recently, with the increasing use of technology and the internet, research has found that identity crime offenders are now using the internet as a means to reach targets and collect personal information (Holtfreter, van Slyke, and Blomberg 2005; Koops and Leenes 2006; Reyns 2013). This changes how scholars and policy-makers understand victimization because "not only does the default position of trust render potential victims vulnerable to deception, their unwary acceptance of others at 'face value' (despite the absence of a face) leads to lack of caution in sharing personal information that facilitates access to their legal identity, making it vulnerable to misuse by the fraudster" (Finch 2007: 38).

Grabosky and Smith (2001) claim that online identity crime is not a new phenomenon. Rather, the medium where the crime takes place is new. The internet created unlimited opportunities for fraud by providing access to numerous possible victims at a minimal cost. Grabosky and Smith (2001) further assert that cyberspace makes it extremely hard to detect offenders. Individuals who want to conceal their identity can do so by "weaving" through multiple international sites. This helps offenders remain anonymous and undetected (Grabosky and Smith 2001). Smith (2010) also comments on this issue by stating that identity crime is

greatly increased by the numerous information and communications technologies. The internet has provided a rich source of personal information to steal, fabricate and use for criminal purposes.

Scholars argue that with technological advances the main target of internet crime is information (Newman and Clarke 2008; Pratt, Holtfreter, and Reisig 2010). Offenders look for two types of information: life history and financial information. First, life history is the personal information such as name, age, and address. Second, financial information is the bank name, bank account number, and passwords (Smith 2010). There are many means to obtain this information. For example, information can be obtained by committing computer crimes such as spam and phishing.[4] Additionally, Holm (2012) discusses how information can be easily stolen through interpersonal exchanges on social networking sites.

I will now turn to the other types of victimization that will be analyzed in this thesis: consumer fraud and phishing. Consumer fraud is not a form of identity crime like identity theft—it is a form of economic crime. Titus (2001:57) defined this crime as "intentional deception or attempted deception of a victim with the promise of goods, services, or other benefits that are nonexistent, unnecessary, were never intended to be provided, or were grossly misrepresented."

Despite the fact that consumer fraud is not specifically regarded as an identity crime, there are still similarities to identity theft. These similarities make it important to explore both forms of crime. There is great monitory loss and psychological harm (I will discuss these in detail in the 'Prevalence of Online Crime' section on page 8). Both crimes take place in cyberspace as a medium to victimization.

[4] Spam involves the promotion of fraud through unsolicited or junk emails (Competition Bureau 2012).

The last victimization this thesis will examine is phishing. Also known as "brand spoofing," it is the attempt to deceive the targeted person to provide personal information by posing as a legitimate organization (The Canadian Anti-Fraud Centre 2017; Reyns 2015). The Canadian Anti-Fraud Centre explains that the term, phishing, comes from the analogy that the offenders are sending mass emails to 'fish' for personal or financial information. Consumer fraud and phishing definitions are a lot more straight-forward than identity theft. I will turn next to discuss why victimization by these crimes is an important subject to research.

Prevalence of Online Crime

Online crime, and more specifically identify theft, has reached the level of international crisis. In the United Kingdom the financial losses were estimated at 2.75£ billion in 2005, which is about CAN$4.5 billion. During the same year there was a loss of $8.5 billion in Australia (Smith 2010: 291). In addition, the Australian Bureau of Statistics (ABS) estimated that in 2012 about 3% of Australian residents were victims of identity theft (Holm 2012). In the U.S. in 2008, 8.1 million people reported being victims of identity fraud with a reported loss of US$45 billion. In addition, in 2002 an estimated loss of CAN$2.5 billion was reported in Canada (Smith 2010: 292). Mazowita and Vézina (2014) reported that fraud accounted for 54% of the reported cybercrime in Canada in 2012. They also report that 5% of fraud and 3% of identity theft is cleared by a charge or cleared otherwise by the police, leaving most incidents unresolved.

Berg (2009: 226) cited the 2007 U.S. Federal Trade commission (FTC) report to describe the victimization rates of various identity fraud related crimes. Credit card fraud, which is when the offender uses the victim's identity to obtain new or used cards, accounts for 25% of the reported identity crimes. Bank fraud involves opening new accounts using the victim's

information and then making fraudulent withdrawals and writing bad cheques. It accounts for 16% of the reported identity crimes. And lastly, attempted identity theft is when the personal information is stolen but not used. This crime accounts for 6% of the reported identity-related crimes (Berg 2009: 226).

More recent data show that about 7% of U.S. residents of the age of 16 were victims of identity theft in 2014. Out of those estimated 17.6 million residents, 86% were victims of fraud where the offender misused existing credit and debit cards and bank accounts. Approximately 4% had their personal information stolen and new accounts were opened using that information for fraudulent activities. Seven percent of the victims experienced multiple types of identity theft crime (Harrell 2015: 2). The same data source shows that about 90% of the victims did not know the offender or how the offender obtained the information.

Phishing prevalence is also high according to Turner et al. (2013). Phishing offenders send a copious number of fraudulent emails which provide increased opportunities to commit crime. Turner et al. (2013: 83) state that "there is a substantial 'dark figure' associated with any type of fraud" but to exemplify how much can be lost, they suggest that even if 1% of the targeted people who received a fraudulent email and would pay an initial fee of 19.95$, this would result in a loss of 8.5$ million (Turner et al. 2013: 83).

According to the Federal Trade Commission (FTC) report 11.2% of the U.S. population experienced consumer fraud victimization in 2003 (Anderson 2004: 28). Based on a later FTC survey (2005), Anderson (2007: 45) suggests that the estimate loss per person for those who said they never received goods they paid for is $60. In the most recent FTC report (2011) Anderson (2013: 17) states that 7.9 million of U.S. adults experience identity theft or consumer fraud. Other research suggests that consumer fraud victimization costs a victim on average about $220

and the annual financial loss from those consumer fraud crimes result in approximately $690 million (Holtfreter, Reisig and, Pratt 2008; Pratt et al. 2010 :268). Based on the International Crime Victims Survey data, van Dijk, van Kesteren and Smit (2007: 86) assert that the online consumer fraud victimization rate is about 1 to 3% among Western European countries and the United States.

The most recent Canadian data were released by the Canadian Anti-Fraud Centre in collaboration with the "Better Business Bureau" (BBB) of Mainland British Columbia in 2017 to raise awareness to the occurrence of online fraud and to reveal theft crimes and how damaging these crimes are. In the report “Top 10 Scams” it is shown that $11 million was lost due to identity fraud, $8.6 million lost due to online purchase scams and $13 million lost due to phishing (The BBB 2017).[5]

Beyond the money lost, there is also significant harm done to the victims of identity theft, consumer fraud, and phishing. It is found that about 14% of identity theft victims in the U.S. experienced an out-of-pocket loss of $1 or more. Of those, about half suffered losses of less than $100 and 14% lost $1,000 or more (Harrell 2015: 9). Moreover, scholars assert that the number of victims and the costs of fraud exceed those who have been victimized by serious street crime (Moore and Mills 1990; Pratt et al. 2010; Titus 2001).

Milne (2003) highlights four more harms that victims experience: (1) invasion of privacy, (2) psychological trauma due to destroyed reputation, (3) financial liabilities due to money loss, and (4) costs associated with restoration of name and reputation. Harrell (2015) asserts that those victims who spend more time trying to resolve problems associated with the victimization experience emotional distress and problems with work and personal relationships. Among those who spend more than 6 months to resolve their financial problems, 29% experienced severe

[5] Retrieved on March 15, 2017 (http://www.bbb.org/mbc/programs-services/top-10-scams/top-10-scams-in-detail/)

emotional distress compared with 4% who spent a day or less resolving financial issues (Harrell 2015: 9). Of course, some of those damages are impossible to quantify due to their subjective nature and the psychological harms are ignored in the statistics that pertain to identity crime (Holm 2012).

Research Problem

There are several difficulties with attempting to research online crime in an effort to draw conclusions in an effort to improve policies. First, there is a lack of official data. In Canada the General Social Survey only recently (2009) surveyed online crime victimization. Second, in a lot of the cases the crimes go underreported due to various reasons such as victim embarrassment or not being aware of victimization. Third, it is suggested that the offenders are "fairly atypical in terms of criminological expectations" (Wall 2001: 8). In other words, anonymity and wide access to targets on the internet has made it possible for anyone to be an offender of online crime. Fourth, enforcing the law is particularly challenging with trans-jurisdictional issues. It is difficult to determine whether the harm falls within civil (tort) or criminal law (Wall 2001). Fifth, the media construct online fraud crimes as a certain "social problem" and give credibility to the claims about the prevalence, incidence, and harm and in a way creating a moral panic (Levi 2001). The media shapes people's understanding of online crime and creates a disconnection between the perception of "potential" harm and the "actual" harm (Wall 2001).

Despite all these challenges, it is extremely important to study online identity crime victimization in order to be able to suggest new policies and prevention programs that might educate those who are most at risk of victimization and reduce victimization rates. In this thesis I aim to do exactly that. I will investigate what attracts an offender to a potential victim. In other

words, I seek to answer the following questions: (1) Is everyone equally likely to be a target of online crime? and (2) What factors might lead to online victimization? Based on Routine Activities Theory and previous research I will suggest possible factors that put individuals at higher risk of targeting and victimization of online identity crime.

This chapter has provided an overview to research on victimization through online identity theft, consumer fraud, and phishing. The next chapter will start with a discussion of Life-Style Exposure Theory, followed by a discussion of Routine Activities Theory. Routine Activities Theory is the framework that guides this study's effort to understand online crime victimization. Moreover, an extension of the Routine Activities Theory will be introduced as a way to explain online victimization. Additionally, I will review the relevant literature on demographics, perceptions of risk, and online routine activities as those relate to online identity theft, consumer fraud, and phishing victimization.

The third chapter presents the methodology used in this project. In this chapter I discuss how concepts are operationalized. I also outline the analytical procedures used in this thesis. In Chapter Four, I discuss the results from the statistical analyses. In the last chapter, Chapter Five, I discuss the study's main findings and relate these to prior studies. I also suggest directions for future research and I explore how the findings of this study can improve policies and programs to target online victimization.

CHAPTER TWO: THEORY AND LITERATURE REVIEW

Online identify theft victimization is a serious problem that merits further study. Previous research has suggested several theories that could be used to explain this victimization (Holtfreter et al. 2010; Reyns 2013; Reisig, Pratt, and Holtfreter 2009; van Wilsem 2011). This chapter will focus on two theories: Life-Exposure theory and Routine Activity theory. I argue that the risk of victimization is due to the different exposure levels of different online routine activities. Certain activities put people at higher risk of victimization online.

Life-Exposure Theory

Life-Exposure Theory was first proposed by Michael Hindelang, Michael Gottfredson and James Garofalo in 1978. The main assertion of the theory is that daily activities can increase the likelihood of victimization. Those activities are vocational, such as work and school, and leisure, such as shopping and exercising. Further, Hindelang et al. (1978) claim that personal and demographic characteristics are antecedent to lifestyle (Reyns 2013). In other words, demographic factors affect the decision to engage in certain activities, which in turn affect exposure to victimization. For example, a person with a higher income is likely to shop online more frequently because they have the means to do so, and this in turn exposes them to victimization.

It is argued that age and gender are substantially associated with role expectations. Different individuals of different ages and genders are expected to follow normative rules of society that correspond to cultural norms and ascribed statuses. These role expectations and other social structures create constraints (Choi 2010; Choi, Choo, and Sung 2016). For example, Vold, Bernad and Snipes (2002) suggest that individuals who are young, male, unmarried, poor and

African American have higher risks of victimization of traditional street crimes because they have an "increased tendency to be away from home, especially at night, to engage in public activities while away from home, and to associate with people who are likely to be offenders" (205).

In regards to online fraud, research has shown that young people and people with some college education were targeted more often because of their online daily activities (Berg 2009). Online lifestyle activities such as shopping, socializing and seeking information are becoming a prominent part of individuals' everyday life. All these activities lend high exposure to victimization.

Life-Exposure Theory is the basis for Routine Activities Theory. Choi (2010) argues that Routine Activity Theory (RAT) developed by Lawrence Cohen and Marcus Felson (1979) is an extension of Life-Exposure theory. He claims that RAT adds the concepts of motivated offender and capable guardianship to the Life-Exposure Theory. The strength of incorporating the two theories is a more complete understanding of the 'suitable target' concept found in RAT (Choi 2010).

Routine Activity Theory

Cohen and Felson (1979) introduced Routine Activities Theory to fill a gap in criminological theory. They claim that most theories of crime neglect social structures and they propose that emphasis on the circumstances in which the crime occurs is necessary. RAT posits that a crime will occur in the presence of motivated offenders, the absence of effective guardians, and the availability of suitable targets in the same time and space (Choi et al. 2016; Cohen and Felson 1979; Jackson et al. 2006; Reyns 2015). Simply put, an individual's daily activities in a social

situation create certain conditions or opportunities for motivated offenders to commit criminal acts (Choi et al. 2016). The following is a discussion of the three requirements presented by Cohen and Felson (1979).

Motivated Offender

The first requirement for a crime to take place according to the theory is a motivated offender. Choi (2010) argues that there is always going to be a motivated offender waiting for the opportunity to commit a criminal act. Because I am examining victimization I will not test the assumption that there will always be motivated offenders. I simply accept this assumption. As suggested by Cohen and Felson (1979), motivation is assumed in victimization studies, therefore it does not pose a challenge for this research.

The growth of online communications has created mass opportunities for prospective offenders and also elevated risks for prospective victims (Grabosky and Smith 2001). Today's society is highly dependent on information technology and a vast volume of personal information is stored online. This creates opportunity and motivation for criminals to commit crime online. In order to reduce crime, the best way would be to reduce opportunity "given that much digital crime depends upon unauthorized access to information systems, access control and authentication technologies have become essential" (Grabosky and Smith 2001: 36). Technologies that encrypt credit card information or biometric devices that authenticate users are examples of systems that help to reduce opportunities for crime. These technologies are designed to make it harder to access private information and reduce motivation (Choi 2010; Grabosky and Smith 2001; Smith 2010).

A Suitable Target

RAT further suggests that individuals' lifestyles or behavioral patterns provide others with the opportunity to offend by increasing contact with potential victims (Jackson et al. 2006; Reyns 2015). This leads to the second requirement of the theory: a suitable target. An in-depth discussion of suitable target was offered by Felson (1998). He provided an extension to RAT by examining target suitability in terms of VIVA: Value, inertia, visibility, and access.

First, targets are more valuable when the offender has more to gain from them, usually economically. Second, lower levels of inertia resistance will most likely attract offenders and straighten levels of target suitability. However, it is suggested that in cyberspace inertia is relatively weaker than in the physical world (Choi 2010). Third, visibility increases the target suitability. Choi (2010: 17) stated that "Computer crime targets are 'globally visible' to computer criminals in cyberspace," which makes them very attractive targets. Lastly, Felson (1998) described accessibility as the ability to get to the offender and get away from the crime scene without getting caught. Due to the internet not having boundaries and borders, criminals are able to locate victims at a minimum risk and cost and they are likely to use encryption devices and third party systems to avoid detection (Choi 2010).

Cohen and Felson (1979) asserted that lifestyles reflect individuals' routine activities such as social interaction, social activities and other activities such as school, work and leisure. These activities, in turn, create the level of target suitability that a motivated offender assigns to that particular target (Choi 2008; Choi et al. 2016). One strategy to avoid victimization is target hardening. This refers to the ability to limit access to personal information posted online, thus weakening visibility and accessibility. Examples in the physical world are alarms and locks. In cyberspace, examples of computer security include passwords and anti-hacking software (Choi 2010).

Capable Guardianship

The third element of the theory that has to be present in order for a crime to occur is a lack of capable guardianship. This component functions as the deterrent for the offender to commit the crime (Cox, Johnson, and Richards 2009). Choi (2010) described capable guardianship in terms of formal and informal social controls. Formal social controls are formal agents like the criminal justice system; in particular, the police, courts, and correctional system. In cyberspace there is a lack of formal social control because prosecuting computer criminals is incongruent with the traditional system due to the fact that some of the property involved is intangible. For example, bank accounts do not have a physical substance but they still have value which makes them easy and appealing to steal. There is also a deficit of specialized forces to patrol cyberspace. While there have been new guides for law enforcement procedures, most state and local departments lack the knowledge and training to properly process data as evidence. These factors further limit the conduct of effective investigations (Choi 2010). Further limiting formal agencies are new technologies that make it difficult to identify criminals. Informal social controls in the physical world are agents such as parents, friends, and teachers. In cyberspace informal social control agents are network administrators and other online users. Similar to formal social control agents, informal social control agents are not very successful in deterring crime online because self-regulation, cooperative measures, and codes of conduct are not followed by the offenders (Choi 2010). Yar (2005: 423) suggests that the offenders have gained "the ease of offender mobility and the temporal irregularity of cyber-spatial activities."

The proposition that there needs to be exposure and proximity to a motivated offender and the victim is an attractive target with low guardianship has become a primary explanation of victimization risk (Reyns 2013). While this theory is a good explanation for traditional crimes that occurs in the physical world such as robbery, there needs to be a way to explain

victimization where the offender and victim are not in the same time and space, such as in the case of online identity theft and online consumer fraud (Eck and Clarke 2003; Holtfreter et al. 2008; Pratt et al. 2010; Reyns 2013).

An Extension of Routine Activities Theory

Cyberspace is not limited by distance, proximity, and physical separation. It is said to have a zero-distance dimension (Choi 2010). Yar (2005) claimed that cyberspace has a unique temporal structure. There are no time zones which make cyberspace available globally to anyone at any time. Activities that formerly required one to be physically present at a specific location, often at a specific time, can now be undertaken regardless of the individual's physical location or the time of day. This poses a challenge to routine activity theory. An adaptation of the theory to crimes in which the offender and target do not physically meet is necessary (Reyns 2013).

In 2003 Eck and Clarke proposed an extension by substituting geographical place to a network. They argued that changing of the setting of routine activities did not fundamentally change the theory, because the interaction of the victim and offender is still maintained online within a network. They state that it is the convergence of motivated offenders and suitable targets within unguarded systems or networks that creates circumstances conducive to victimization regardless of physical location or time (Eck and Clarke 2003; Reyns, Henson, and Fisher 2011; Reyns 2013). Reyns (2013) argued that criminal opportunities are evolving with technological advances, therefore, criminological theories to explain those crimes also must evolve. This is an important extension to the RAT theory because it provides the opportunity to apply RAT to internet crimes.

Individual Characteristics and Risk Perceptions

The relationship between personal factors and perceived risk is explained in terms of personal vulnerability. This is based on the work of Ferraro (1995) who claimed that people interpret the potential of victimization based on social interactions. Following that, it is suggested that personal characteristics influence the interpretations and in turn affect the risk of victimization. It is argued that there are two key dimensions that explain risk perception. The first is *physical* vulnerability: the belief that some people cannot adequately resist and struggle to deal with the traumatic consequences of victimization. It is suggested that women and older people are particularly influenced by physical vulnerability when considering risks (Reisig et al. 2009). The second factor is the *social* vulnerability which refers to the ability to deal with the economic consequences of victimization. Reisig et al. (2009) argue that this risk consideration especially influences lower income individuals. This is because individuals with low income struggle more to recover from monetary loss, and therefore, they are more likely to hold the perception that they are at high risk of victimization.

There are multiple studies that examine age and gender in relation to perception of risk of walking alone at night. This behavior was argued to be a good indicator of fear of traditional crime (Cossman and Rader 2011; Ferguson and Mindel 2007; Kanan and Pruitt 2002; Kruger et al. 2007; McGrath and Chananie-Hill 2011). However, there are only a handful of studies that examine online crimes. This means there is a gap in knowledge when exploring the relationship between gender and age and perception of risk in cyberspace. With regards to online crime, several studies found women have higher risk perceptions (Garbarino and Strahilevitz 2004; Liebermann and Stashevsky 2002; Smith and Torstensson 1997; Tomsich, Gover, and Jennings 2011). Two studies in particular examined the relationship between gender and risk associated

with certain online activities (Garbarino and Strahilevitz 2004; Liebermann and Stashevsky 2002). The first study was conducted by Garbarino and Strahilevit (2004) in the U.S., while the second study by Liebermann and Stashevsky (2002) was conducted in Israel.

Garbarino and Strahilevit (2004) based their hypothesis on previous research on risk perceptions, which suggested that gender differences in the perception of online shopping risks are likely. They suggested that women are generally more concerned with privacy and the loss of privacy than are men. There is evidence that this is the case with reference to internet privacy (Bartel-Sheehan 1999; Kehoe, Pitkow, and Morton 1998). To test their hypothesis, Garbarino and Strahilevit (2004) conducted a survey at a university in a major U.S. city in 1999. The study included 260 participants and received a response rate of over 60% (Garbarino and Strahilevit 2004:770). Based on the results the authors concluded that, even after controlling for amount of internet use, gender was still a significant predictor of risk perception. They stated that women perceived the loss of privacy to be a more prominent risk when shopping online compared with men (Garbarino and Strahilevit 2004).

The second study was aimed to test which demographic factors were associated with perception of risk online. Liebermann and Stashevsky (2002) surveyed 465 employed adults in Israel. The study received a response rate of 85%. They found that compared with men, women perceived significantly higher risks of online victimization. More specifically, they concluded that women had 3 significant elements of risk perception: (1) internet credit card stealing, (2) pornography and violence, and (3) missing the human side in purchases (Liebermann and Stashevsky 2002).

The two studies summarized above discuss the relationship between gender and risk perception. A study by Weitzer and Kubrin (2004) examines the relationship between age and

risk perception. Weitzer and Kubrin (2004) conducted a study in 2001 on risk perceptions of traditional crimes and how these perceptions are affected by media. To examine the effect of the media on crime they used a sub-sample of 480 participants from Washington, D.C. They suggested that older individuals have higher perceptions of risks. Their findings suggest that fear of crime initially decreases with age and then increases for older respondents. Similarly, Liebermann and Stashevsky (2002) found that older people perceived higher risks of computer use compared with younger people. However, Garbarino and Strahilevit's (2004) study did not find the same pattern as Liebermann and Stashevsky (2002). They discovered that age was not a significant factor influencing perceptions of risk. My research aims to further examine gender and age as possible attributes that may affect risk perceptions of online crime.

My research also aims to look at social vulnerability and test the argument that individuals with higher income and more education will have lower perceptions of risk. Several studies found support for this hypothesis with reference to traditional crime (Cossman and Rader 2011; Kanan and Pruitt 2002; McGarrell, Giacomazzi, and Thurman 1997; McGrath and Chananie-Hill 2011). Cossman and Rader (2011) provided support for this argument using a Canadian sample. Analyzing the General Social Survey (2009) they concluded that individuals with higher income and higher education reported lower perception of victimization risk.

Reisig et al. (2009) conducted a secondary analysis to test the hypothesis that individuals with lower socio-economic status (SES) will report higher levels of risk perception regarding online crime. The survey used by Reisig et al. was conducted between 2004 and 2005 with 1,000 participants in Florida and received a response rate of 44%. The authors used level of education, homeownership and income to conceptualize SES. The results showed that respondents with lower SES reported significantly higher levels of risk (Reisig et al. 2009). However, Reisig and

colleagues also found that the model only explained 5% of the variance in online crime victimization. They argue that other factors need to be identified to explain perceived risk in an online context. They suggest that further research should look at activities like adoption of self-protection measures and their association to perceptions of risk (Reisig at al. 2009).

Individual Characteristics and Routine Activity

Following the theoretical assumptions of Life-Exposure Theory presented above, I argue that personal characteristics such as gender, age and SES will have effects on the daily activities of individuals. Previous studies have established a relationship between personal demographics and routine activities in terms of traditional crime (Berg 2009; Hindelang et al. 1978; Sampson and Lauritsen 1990; Vold et al. 2002). My research will focus on how personal characteristics affect online routine activities.

Choi et al. (2016) conducted a secondary data analysis to understand how personal attributes affect routine activities online. They used a 2007 survey which was administered to 204 Pennsylvania State System of Higher Education students. They measured downloading of free games, music and movies as leisure activities. Their analysis found that men were more likely to engage in those leisure activities compared with women (Choi et al. 2016).

Bhatnagar, Misra and Rao (2000) examined whether age has an impact on online routine activities. Using an online survey in 1997, they found that older people were more likely to shop online. They suggested that older people have greater time constrains due to employment and family responsibilities which makes online stores more appealing. In contrast, Choi et al. (2016) observed the opposite relationship. They found that older participants were less likely to engage in online routine activities compared with younger participants. In regards to socio-

economic status (SES), Anderson (2006) found that individuals with higher incomes were more likely to engage in online banking. Anderson (2006) based his findings on data from a 2003 Federal Trade Commission survey on identify theft. This survey included more than 4,000 respondents in the U.S.

A study by Reyns (2013) found similar patterns. The data for this research were collected between 2008 and 2009 as part of the British Crime Survey (BCS). The sample size was 46,286 with a 76% response rate. The selection of cases for this article resulted in a sample of 5,985 participants. Reyns's analysis revealed a significant correlation between gender, age, and income and routine activities such as banking, shopping, social networking, and downloading. More specifically, men, younger people, and individuals with higher income all were more likely to engage in these routine activities (Reyns 2013).

Individual Characteristics and Victimization

Research on gender and victimization online is not consistent. For example, women were found to be at a greater risk of being victims of identity theft based on the 2003 Federal Trade Commission survey (Anderson 2006) and men reported higher levels of victimization in the 2004 Florida-based survey (Holtfreter, Reisig, and Blomberg 2006). But according to Reyns (2013), there is no relationship between gender and online victimization based on British Crime Survey (BSC) data and similar results were observed by Anderson (2007). In the U.S. some scholars suggest that gender victimization is crime-specific and therefore difficult to test (Holtfreter et al. 2006; Menard and Covey 2016). In other words, the relationship between gender and crime should not be generalized, because such an analysis should be contingent on the particular contexts of the crimes being studied.

Inconsistent relationships are also observed between age and online victimization. Previous research suggests that older individuals are at higher risk of victimization due to their increased vulnerability (Anderson 2006, 2007; Holtfreter et al. 2006; Reyns 2013, 2015). According to Reyns (2013), older persons are at an increased likelihood of experiencing online identity theft. Holtfreter et al. (2006) found that persons between the ages 25-34 and 45-54 are most likely to be victimized, suggesting that there might be a curvilinear relationship between age and victimization.

However, two Federal Trade Commission (FTC) reports found older persons were at lower risk of victimization. First, a 2003 FTC report found that individuals between the ages of 25 and 54 had the highest risk of any kind of identity fraud victimization (Anderson 2006).[6] A 2005 FTC study found elderly persons were significantly less likely to be victims of online fraud. Anderson (2007) reported that individuals over the age of 65 had the lowest risk of victimization. Holtfreter et al. (2006) also found that persons over the age of 65 are less likely to be victims of consumer online fraud in Florida. It is suggested that the time spent online decreases with age, and therefore also less likely to be victimized (Reyns 2013).

In terms of socio-economic status, income is consistently correlated with online victimization. Interestingly, this variable had the strongest correlation coefficient in Reyns's (2013) analysis. He found that people with an income of $75,000 or higher are at greater risk of identity theft. Anderson (2006:169) found that individuals with incomes in the $75,000 to $100,000 range were associated with a 49% increase in the risk of identity theft relative to the risk faced by those with an income of less than $25,000. Holtfreter et al. (2006) also found that individuals with higher incomes are at higher risks of consumer fraud victimization. Scholars

[6] Identity theft victimization was defined in the survey as: (1) a misuse of the person's existing credit card accounts, (2) misuse of other existing accounts, and (3) misusing personal information to open new accounts or commit other frauds (Anderson 2006).

have argued that the study of online victimization needs to move beyond demographic attributes to better understand victimization patterns (Holtfreter et al. 2006). I turn next to examine factors beyond demographic characteristics.

Risk Perceptions and Routine Activities

It is argued by Yar (2010: 106) that "one of the most significant issues related to public perceptions of crime concerns the ways in which fear of crime and associated understanding of victimization risks effect individuals and impact upon their subsequent social behaviour." Therefore, it is not surprising that perceived risk of internet crime is a significant predictor of people's online activities. There is a negative correlation between risk perceptions and routine activities. That is to say, individuals who perceive the risks to be high, engage in fewer activities online such as shopping, banking, and browsing (Reisig et al. 2009; Yar 2010).

Risk perceptions rise when individuals feel that an interaction will not yield favorable results or when they are uncertain about the outcomes (Forsythe and Shi 2003; Murray 1991). More specifically, risk perception could be said to be composed of two elements: the combination of probability of victimization and the severity of the possible victimization, and the emotional feeling of being unsafe (Riek, Bohme, and Moore 2016). Privacy concerns were also found to have an effect on risk perception. Disclosing personal information voluntarily or involuntarily and it being used for other purposes, or it just being stored in the system might feel like an invasion of privacy (Hankun et al. 2016).

There are a few other factors that could shape perceived risk and therefore affect online activities. Bhatnagar et al. (2000) highlight product category risk which is associated with the

product itself. Consumers will perceive higher victimization risk if they believe that the product will not be up to their expectations (Bhatnagar et al. 2010).

Forsythe and Shi (2003) demonstrate how psychological risk might affect people's online activities. They argue that it is the fear that a certain activity will cause frustration or shame. This is related to privacy concerns, because violation of privacy online might cause some people psychological stress. To avoid the possibility of negative outcomes and associated negative feelings, consumers and internet users might avoid providing personal information online (Forsythe and Shi 2003).

Lastly, financial risk plays a big part in decision-making in regards with online activities. Bhatnagar et al. (2000) found that consumers are hesitant to provide personal information over the internet because of the fear of money loss, which includes the misuse of credit card information (Forsythe and Shi 2003). When consumers believe that there is a high probability that their credit card information will be stolen, they are less willing to provide that information online (Caswell 2000; Forsythe and Shi 2003)

Rengifo and Bolton (2012) suggested that all these different dimensions of fear can be referred to as 'threat of criminal victimization.' Riek et al. (2016) claimed that risk of cybercrime victimization changes patterns in behaviour among computer users. They found that internet users avoid online shopping, online banking and online social networking due to elevated perceptions of risk.

There are several studies that tested the relationship between perceived risk and online activities. Most agree that perceived risk negatively influences users' acceptance of online payments (Hankun et al. 2016). A national study conducted in 2015 with 196 responses from the U.S. found that privacy concerns were a big factor in the attitudes towards online payment

(Hankun et al. 2016). Interestingly, the results of the study indicated that perceived risk was not a significant factor shaping attitudes toward online payments. Hankun et al. (2016) suggest that this could be because the participants were familiar with making online payments and therefore had relatively low perceived risk.

Another study was also undertaken by Miyazaki and Fernandez (2001) on the risk associated with online shopping. This study involved 160 participants and participants were typical of the average internet users based on age, gender, income, and education. The study's results supported the claim that perceived risk toward online shopping is negatively correlated with online purchase rates (Miyazaki and Fernandez 2001). In other words, more online purchases are done by individuals who have low risk perceptions of online shopping. Bhatnagar et al. (2000) came to a similar conclusion based on their 1997 survey. They found that the probability of purchasing online deceases with increased perceived financial risk. Reisig et al.'s 2005 Florida survey produced similar results. Participants who reported high risk perception made fewer online purchases and spent less time online (Reisig et al. 2009).

Forsythe and Shi (2003) used the 1998 'GVU WWW User Survey' to investigate perception risk on online behaviour.[7] They found that 39% of the respondents reported that they perceived product risks, 32% indicated psychological risks, and 23% reported financial risks. They also found that perceived financial risk was the most consistent predictor of subsequent changing of online behaviours (Forsythe and Shi 2003). Risk perception was correlated with lower frequency of browsing shopping websites, online purchases, and time spent online.

Reyns (2013) suggests that there is also a negative relationship between risk perception and actual victimization. This could be because individuals who have higher perceptions of risk

[7] GVU was previously known as Graphics, Visualization, and Visibility.

will expose themselves to less online activities and in turn will reduce the probability of actual victimization (Reyns 2013; Yar 2010)

Routine Activity and Victimization

This thesis draws on two theories, Life-Exposure theory (LET) and Routine Activity theory (RAT). This chapter demonstrates that personal characteristics have important effects on routine activities, in accordance with LET. This next section is concerned with how these activities affect victimization, as discussed by RAT.

Pratt et al. (2010) put forward the idea that in cyberspace the activities that are considered 'risky' are context-specific. In other words, it is suggested that there is a shift from deviant to nondeviant behaviors to which are found to be correlated to online identity theft. Holtfreter et al. (2006) suggested that the use of internet increases exposure to online crime. They claim that the use of internet itself is enough to put one at risk and any added activities, such as shopping or banking online, increase the likelihood of online victimization. Others have found support to suggest that internet use, and shopping in particular, create opportunities for targeting and victimization (Newman and Clarke 2003; Pratt et al. 2010).

Milne et al. (2004) explain that the elevated risk online is due to the fact that attaining and disseminating information in cyberspace is fairly easy because the personal information that is shared electronically can be intercepted and used for criminal purposes. Privacy can also be compromised with "cookies" that allow others to track click stream history (Milne et al. 2004). Choi's argument is that "people do not realize how they are constructing their online lifestyles through the constant use of computer technology" (Choi 2010:1). He based his research on the works of Cohen and Felson (1979) and found empirical support for the claim that individuals

who spend more time online have a higher chance of victimization in the form of computer virus infections (Choi 2010).

There are several studies that have explored the relationship between online routine activities and victimization. As per Routine Activities theory, the studies have examined how exposure to motivated offenders, absence of guardianship and available suitable targets are useful to predict victimization (Holt and Bossler 2013; Reyns 2015). Anderson (2006) analyzed the 2003 Federal Trade Commission survey on identity theft. He found that internet users who purchased goods online had a higher risk of victimization. Moreover, more online transactions increased this risk of becoming a victim of identity theft. Choi (2008) suggests that different lifestyle patterns are directly linked to criminal victimization online. This is supported by Anderson's (2006) U.S. findings.

A different study by Holtfreter et al. (2008) suggested that there is a cumulative effect, meaning that the more online activities performed, the higher chance of fraud targeting and victimization. They found that nearly 4% of the full sample of 922 people had been victims of fraud. They suggest that making online purchases exposes unguarded victims to potentially motivated offenders online (Holtfreter et al. 2008). They found that fraud targeting and victimization were positively associated with remote purchasing. Based on the same survey, Pratt at al. (2010) found that buying something online increases the odds of internet fraud targeting by 377%. Holtfreter et al. (2008) concluded that online activities such as remote purchasing are a strong indicator of fraud targeting and victimization, making Routine Activities theory (RAT) a useful theory to understand victimization in cyberspace.

Reyns's (2013) findings also support RAT. First, his research showed that people who shopped online were more likely than those who did not shop online to be victimized. Second,

individuals who used online banking were more likely to experience identity theft than those who did not do any online banking. Third, e-mailing and using instant messengers (IM) increased individuals' risks of victimization. Fourth, respondents who indicated that they downloaded music, movies or other media while online were at increased victimization risk compared with those who did not download these materials (Reyns 2013).

A large scale Dutch study (N=6,201) from 2008 indicated that 2.5% of the respondents had been victims of online fraud within the last year (van Wilsem 2013: 172). The study found that internet shopping and active online forum participation increased vulnerability to victimization after controlling for self control, other activities such as using social networks websites, and demographic characteristics (van Wilsem 2013). Holt (2013) suggested that the increased use of banking and shopping allows personal and financial information over the internet to be transmitted, which puts people at an elevated risk of victimization.

Two studies have used the Canadian General Social Survey to test similar hypotheses. In the first study, Reyns (2015) looked at phishing as means of criminal victimization. He found that about 43% of the respondents received fraudulent emails from someone posing as a trustworthy and legitimate organization and requesting personal information. To see whether targeting and victimization were affected by routine activities, he operationalized all three components of Routine Activities theory. Reyns (2015) concluded that each routine activity concept significantly influenced the likelihood that individuals would be targeted by phishing attempts. More specifically, it was found that having one's personal information posted online and personally posting accurate information online increases phishing. While deleting e-mails and regularly changing passwords were found to significantly lower targeting by phishing (Reyns 2015).

The second study was conducted by Reyns and Henson (2016) and explored identity theft online. Similar to the results from the previous study, Reyns and Henson found that having personal information posted online was a significant predictor of identity theft (2016). Also consistent with past findings, online banking and shopping were positively associated with identity theft. However, Reyns and Henson (2016) did not find using anti-virus software and regularly changing passwords to be negatively correlated with identity theft, although this was found in prior studies (Holt and Bossler 2013; Holt and Turner 2012; Reyns et al. 2011).

This chapter has reviewed the literature to explore who is at a high risk of identity theft online. This chapter also answers the first research question "Is everyone equally likely to be a target of online crime?" Not everyone is at risk. As well, this type of victimization does not happen at random (Holtfreter et al. 2008). It is suggested that examining demographics or routine activities is not enough to properly understand victimization online (Reyns 2013). It is possible that certain characteristics are mediated by specific activities such as online shopping, banking and using social network websites, as well as levels of risk perception. These processes are central to my research study. Below I summarize the main hypotheses to be tested in this research study.

Hypotheses

Based on previous research ten testable hypotheses can be constructed. Some scholars have suggested that examining demographics and routine activities is not enough to properly understand victimization online (Reyns 2013). It is possible that certain demographics are mediated by specific activities such as online shopping, banking and using social network websites, and levels of risk perception.

This research will examine the direct effects of demographics on victimization. The following hypotheses are proposed:

$H1_a$: Older individuals have a higher likelihood of experiencing online fraud victimization than younger individuals (while some studies suggest that younger are more likely to victimized, recent relevant research found that it is actually older people who are more likely to experience online crime victimization) (Holtfreter et al. 2006; Holtfreter et al. 2008; Reyns 2013, 2015).

$H1_b$: Gender is associated with online fraud victimization (Studies are inconsistent in terms of whether men or women are at greater risk) (Anderson 2006; Holtfreter et al. 2006; Menard and Covey 2016).

$H1_c$: More highly educated people have a higher likelihood of online fraud victimization.

$H1_d$: Greater income is associated with a higher likelihood of online fraud victimization.

This research also explores the effects of perception of risk and online routine activities on victimization, as proposed by previous research (Newman and Clarke 2003; Reisig et al. 2009; Pratt et al. 2010; Yar 2010). Therefore, with reference to perceptions of risk, the following hypothesis is suggested:

H2: Those with higher risk perceptions of online crime are less likely to do online shopping, banking and networking, and therefore, they are less likely to experience online fraud victimization.

With reference to online routine activities I propose the following hypotheses:

$H3_a$: People who use the internet for online banking more frequently are at higher risk of online fraud victimization.

$H3_b$: People who frequently use the internet for booking or reservations are at higher risk of online fraud victimization.

$H3_c$: People who frequently use the internet to purchase goods or are at higher risk of online fraud victimization.

Two further hypotheses evaluate people's efforts to protect themselves from online victimization:

$H4_a$: People who protect their privacy by regularly changing passwords are at lower risk of online fraud victimization.

$H4_b$: People who protect their privacy by regularly deleting e-mails are at lower risk of online fraud victimization.

In this thesis I aim to explore the relationship between people's demographic characteristics, risk perceptions, online routine activities and identity theft victimization using a large scale social survey (General Social Survey) conducted in Canada in 2009. The next chapter will describe the survey and present the variables analysed in this thesis.

CHAPTER THREE: METHODOLOGY

As demonstrated in the literature review, online fraud victimization is a serious problem with various antecedent factors that merit further study. The research examining correlates of online fraud victimization has been conducted primarily with American populations, with the exception of a few studies that used the Canadian General Social Survey or surveys in England, the Netherlands, and Israel. The samples are limited in their generalizability. The proposed research seeks to fill the gap in knowledge on online fraud victimization using Canadian data. This thesis will analyze how demographics, risk perception and online routine activities affect online fraud victimization. This chapter discusses the research methodology employed in this study. Specifically, I outline sample characteristics, describe the measures, and present the techniques of statistical analysis.

Sample

This research uses data from the Canadian General Social Survey (GSS) Cycle 23. The survey was conducted between February and November of 2009 by Statistics Canada. The participants were persons 15 years of age and older residing in Canada at the time of the survey. The survey excluded residents of the Yukon, Northwest Territories and Nunavut, as well as full-time residents of institutions (Statistics Canada 2010).[8] Survey data were collected using a stratified sampling technique that treated the provinces as strata. Census Metropolitan Areas (CMAs) were considered as separate strata. The CMAs included St. John's, Halifax, Saint John, Montreal, Quebec City, Toronto, Ottawa, Hamilton, Winnipeg, Regina, Saskatoon, Calgary, Edmonton,

[8] The survey codebook does not specify which types of institutions (e.g., hospitals, retirement and nursing homes, prisons).

and Vancouver. Other CMAs were located in Quebec, Ontario, and British Columbia. CMAs were later assembled into three strata by grouping them by province. Finally, the non-CMA areas were formed into 10 strata, one for each province. This resulted in a total of 27 strata. A total usable sample of 19,422 households was obtained, resulting in a 61.6% response rate (Statistics Canada 2010).

Participants were surveyed using computer assisted telephone interviewing (CATI). Among the respondents who completed the survey, 55.1% are female and 44.9% are male. Ages range from 15 to 75 and older and the largest share of respondents indicate an income between $20,000 and $39,999 (28.1%). Twenty-eight percent reported having a diploma or a certificate from a college or trade school. Forty-eight percent reported that they are married, 21.9% reported being single and the rest of the respondents are common-law, widowed, or divorced (9.8%, 3.5%, and 8.0% respectively). Most of the participants (74.6%) are from an urban area or a CMA. Additionally, the largest proportion (27.2%) of respondents reside in Ontario, followed by 19.1% in Quebec, and 13.1% in Alberta (Statistics Canada 2010).

Non-response in surveys can cause over- and under-representation of some groups and these issues can reduce the reliability of the conclusions reached (Bethlehem 2009). To correct over- or under-representation, weighting adjustment is used. This means that in under-represented groups, each individual receives a weight larger than 1 and in over-represented groups each individual receives a weight smaller than 1. These weights adjust and balance the groups to be representative of the actual population (Bethlehem 2009). In the GSS two weighting factors were used. The first (WGHT_PER) is the weighting factor at the individual level. And second (WGHT_HSD) is used only for estimation of household characteristics (Statistics Canada 2010). Because this research is conducted at the individual level, the first weighting adjustment

will be used.[9] In order to conduct statistical tests of inference a calculation for proportional weights was undertake by dividing WGHT_PER by its mean. This converted the data set to reflect the sample size (N=19,422).

Measures

This following section will highlight the dependant and independent variables used in this analysis. Additionally, measurement and survey items will be discussed. See Table 1 for a full list of the variables and measurements used in this research.

Dependent variable

Victimization

The main focus of this research is to understand what factors effect online victimization. This thesis is focused on online identity crime, which is a general term that encompasses crimes such as identity theft, consumer fraud, and phishing. I therefore create three dependent variables to tap each of these offenses.

The first variable, *Phishing*, is measured with one item that asks, "Have you experienced any problems associated with receiving fraudulent e-mail from someone posing as a trustworthy and legitimate organization requesting personal information." The response is dichotomous (1, 2) and is recoded into a dummy variable (no=0, yes=1).

The second dependent variable, *Consumer fraud*, is measured with three dichotomous survey items which are combined into a single scale, ranging 0 to 3, which is then recoded into a dummy variable (no=0, yes=1). The survey items are: (1) "In the past 12 months, have you had

[9] When WGHT_PER is applied, the frequencies reflect the Canadian population estimates (N= 27,661,916).

problems with purchases over the Internet?"; (2) "In the past 12 months, have any of the following happened to you? The goods and services that arrived were not like the ones described on the website", and (3) "In the past 12 months, have any of the following happened to you? The goods or services were never delivered even though you had already paid for them." It is important to note that the first question might compromise construct validity. When answering the question "In the past 12 months, have you had problems with purchases over the Internet?" respondents might report problems that are not related to fraud, such as a delay in delivery time or that the products were not of good quality

The third variable, *Identity theft*, is also measured using two survey items: (1) "In the past 12 months, have any of the following happened to you? Extra funds were taken from your account without your permission" and (2) "In the past 12 months, has anyone used any of your credit or bank cards (or card details) from an Internet source, to purchase something or withdraw money from your account without your permission?" These questions also have yes and no responses and are combined into one scale ranging from 0 to 2, which was further recoded into a dummy variable (no=0, yes=1). This strategy, of converting the dependent variables into dummy variables, improves consistency by making the three types of victimization comparable.

Independent variables

Demographics

This research focuses on four characteristics which were found to be significantly correlated to online crime victimization (Anderson 2006, 2007; Holtfreter et al. 2006; Reyns 2013). First, age is measured with 7 categories coded from 1 to 7 (low to high age range). The first 6 categories employ 10-years intervals (15-24, 25-34...64-74) and the last category is 75 and above years.

Second, gender is measured as male and female, and for the purpose of this research it is recoded as a dummy variable with females=0 and males=1.

Third, education is measured using 5 categories that range from (1) no schooling/some schooling to (5) a post-secondary degree.

Fourth, income is measured using 12 categories. The first one is no income, then the category increase in increments of $5,000. There are 4 categories in these increments (less than $5,000, $5,000-9,999, $10,000-14,999, $15,000-19,000). There are then 4 increments of $10,000 between the range of $20,000 to 59,999 ($20,000-29,000 ..., $50,000-59,999). Next are 2 categories with increments of $20,000 ($60,000-79,999, $80,000-99,999). The last category is $100,000 or more.

Risk perception

Another independent variable that is analyzed in this research is risk perception. Studies have found that risk perception of online crime has an effect on routine activities and in turn influences online crime victimization (Newman and Clarke 2003; Pratt et al. 2010; Reisig et al. 2009; Yar 2010). In order to test these claims, risk perception is measured using two questions from the GSS. The questions are: "How concerned are you or would you be about security in relation to banking over the Internet?" and "How concerned are you or would you be about security in relation to ordering something or making purchases over the Internet?" These questions are measured on a 4-point scale ranging from 1 "being greatly concerned" to 4 "being not at all concerned." For the purpose of this research the responses are reverse-coded. Higher values indicate greater levels of concern. These questions have a respectable Cronbach alpha of .74, meaning that they are measuring the same constructs and have high scale reliability.

Online routine activities

This thesis employs Routine Activities Theory (RAT) to explore how online activities affect online victimization. Therefore, the measurements chosen in this research are representative of the three core concepts of RAT: 1) exposure to a motivated offender, 2) target suitability, and 3) lack of guardianship. Reyns (2015) used the same Canadian GSS in his research and operationalized RAT in a similar manner. This promotes reliability.

Consistent with Reyns (2015), the same three survey items were chosen to reflect possible activities that create opportunity for online victimization by increasing online visibility. The questions asked whether during the past month the respondent used the internet for certain activities. Those activities included electronic banking, making online booking or reservations, and purchasing goods or services. The responses are coded on a 5-point scale (1=at least once a day, 2=at least once a week, 3=at least once a month, 4=not in the past month, 5=never). The scale has a Cronbach alpha of .62. The responses are reverse-coded for this analysis. In addition, three more questions are used to measure exposure to motivated offenders. Reyns (2015) included only one survey item in his research: belonging to online social media groups. His research focused on phishing, hacking and malware infection victimization, whereas this research examines phishing, identity theft, and consumer fraud. Therefore, the following supplementary survey items are important for a complete analysis of phishing, identity theft, and consumer fraud victimization. The additional questions asked whether the participants belong to on-line social media groups and have connected to online chat (yes=1, no=2). These survey items are recoded into dummy variables, where no=0 and yes=1.

The second component of RAT is target suitability. It is measured with two survey items. The questions asked if “in order to protect your privacy, have you ever entered misleading

information about yourself over the internet" and "in order to protect your privacy, do you only deal with well-known organizations and business online." The responses are recoded into dummy variables, with no=0 and yes=1. It is important to note that is a potential threat to construct validity. These measures assume that dealing with well-known organizations lessens target suitability, but that might not always be the case. For example, in 2011 Sony Playstation network was compromised and personal information of about 77 million used have been stolen (Quinn and Arthur 2011).

Finally, two survey items are used to measure online guardianship. These questions were similar to the two previous ones. They ask about protecting the participants' security online. Respondents were asked whether they regularly change their passwords and if they regularly delete e-mails from unknown senders. The responses are recoded into dummy variables, with no=0 and yes=1. These measures carry the assumption that a target is more heavily guarded when passwords are changed and emails are deleted, but that might not always be the case. This raises construct validity concerns because respondents might be changing passwords frequently because they are compromised often. In the GSS other measures of guardianship were measured. For example respondents were asked if they use anti-virus software or if they use a firewall. These protection measures would not guard against phishing, consumer fraud, or identity theft. These measures would be a better fit to prevent malware or hacking victimization.

For his research, Reyns (2015) included the same four survey items in his operationalization of target suitability and guardianship (regularly deleting emails, regularly changing passwords, enter misleading information and dealing with well knows organizations). This helps to increase reliability of our measures. See Table 2 for percentage distributions, means and standard deviations of all the variables included in the analysis.

Analytical Procedure

Analysis

Once all the variables were recoded, frequency distributions were produced using Statistical Package for the Social Sciences (SPSS) version 20. A measurement table (see Table 1) and a descriptive table (see Table 2) were generated. Afterwards the bivariate relationships between the variables were analysed using a correlation table which included all the variables in this study to examine if there are problems of multicollinearity. Several cross-tabulations are analysed to supplement the regression analysis by exploring intervening effects in greater detail.

Logistic binary regression is used for prediction when the dependent variable is a dichotomous mutually exclusive criterion and when there are one or more independent variables (IV) of any level of measurement (Weinbach and Grinnell 2015). This analysis resembles a linear regression because it shows the odds change when a variable is changed by one unit, which is indicated by the β coefficient (Knoke and Bohrnstedt 1994). However, unlike linear regression, it does not assume that there is a constant amount of change between variables (Weinbach and Grinnell 2015).

Logistic regression can be interpreted similarly to linear regression, as long as there is the assumption that the dependent variable is not a probability, but rather a logarithm of the odds of two probabilities (Knoke and Bohrnstedt 1994). Kay and Hagan (1999: 537) further stated that "logistic regression coefficients are analogous in some ways to percentage difference measures or ordinary least squares regression coefficients, but they are more cumbersome to interpret. Specifically, logit coefficients represent the change in log of the odds of an outcome variable associated with a unit change in an independent variable." For the analysis a basic

exponentiation function will be used to interpret the results (Kay and Hagan 1999). This means that in order to present findings, a value of 1 will be deducted from the Exp β value and multiplied by 100. The new value can be interpreted as a percent change in the odds of the outcome.

Models

Figure 1 presents the causal model that guides the table building strategy for this analysis. There are three logistic binary regression tables, one for each dependent variable. The first table analyzes phishing, the second analyzes identity theft, and the third analyzes consumer fraud. For each dependent variable a three-step modeling strategy was created. The first model includes the first set of independent variables: demographics. This research examines four specific demographic characteristics: age, gender, income, and education. The second regression model includes the measures of risk of perception and demographics. The third and last model adds the ten measures of online routine activities into the multiple regression analysis while controlling for the previously tested demographics and perceptions of risk.

The three models reflect previous research. Demographic characteristics are the antecedent variables that are used as the baseline in the first model. Studies found that perceptions of risk mediate the relationship between demographic factors and routine activities. They are therefore added in the second model. The last model includes online routine activities as proposed by Routine Activities Theory, and are the prime theoretical focus of this thesis. Figure 1 presents the causal model for this research.

Figure 1: Causal Model of Online Crime Victimization

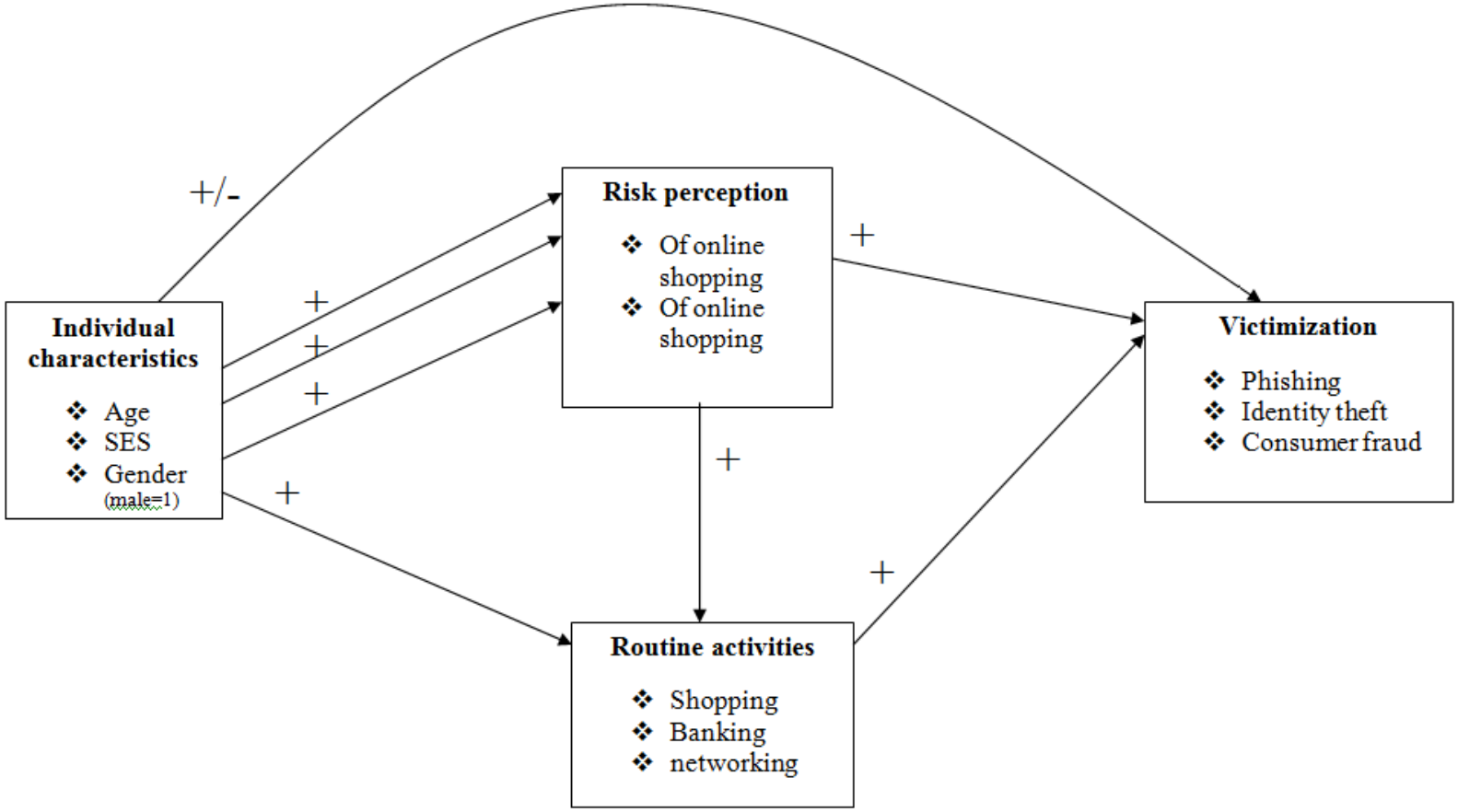

Table 1: Variables, Measurement, and Range

Variable	Measurement	Range
Dependent Variables		
Phishing	Have you experienced any of the following problems associated with security over the Internet? Received fraudulent e-mail from someone posing as a trustworthy and legitimate organization requesting personal information. Yes=1; No=0.	0-1
Consumer fraud	In the past 12 months, have any of the following things happened to you? The goods or services were never delivered even though you had already paid for them. Yes=1; No=0.	0-1
	In the past 12 months, have any of the following things happened to you? The goods or services that arrived were not like the ones described on the website. Yes=1; No=0.	0-1
	In the past 12 months, have you had problems with purchases over the Internet? Yes=1; No=0.	0-1
Identity theft	In the past 12 months, have any of the following things happened to you? Extra funds were taken from your account without your permission. Yes=1; No=0.	0-1
	In the past 12 months, has anyone used any of your credit or bank cards (or card details) from an Internet source, to purchase something or withdraw money from your account without your permission? Yes=1; No=0.	0-1
Independent Variables		
Demographics	Age of respondents was measured in groups of 10 years ranging from 15 to 75+	1-7
	Sex of respondents. Male=1; Female=0.	0-1
	What is the highest level of education that you attained? Answers were based on the following scale (1) doctorate/masters/bachelors degree, (2) diploma/certificate from community college/trade/technical, (3) some university/community college, (4) high school diploma and (5) some secondary/elementary/no schooling (reverse coded).	1-5
	What is your best estimate of your total personal income, before deductions, from all sources during the past 12 months?	1-12
Perception of risk	How concerned are you / would you be about security in relation to banking over the Internet? Would you say you are / you would be: measured using the following scale (1) greatly concerned, (2) somewhat concerned, (3) hardly concerned and (4) not at all concerned (Reverse coded).	1-4
	How concerned are you / would you be about security in relation to ordering something or making purchases over the Internet? Would you say you are / you would be: measured using the following scale (1) greatly concerned, (2) somewhat concerned, (3) hardly concerned and (4) not at all concerned (Reverse coded).	1-4
Online routine	During the past month, how often did you use the Internet: …for electronic banking? (1) At least once daily,	1-5

activities	(2) at least once a week, (3) at least once a month, (4) not in the past month, and (5) never (reverse coded).	
	During the past month, how often did you use the Internet: …to make an online booking or reservation? (1) At least once daily, (2) at least once a week, (3) at least once a month, (4) not in the past month, and (5) never (reverse coded).	1-5
	During the past month, how often did you use the Internet: …to purchase goods or services? (1) At least once daily, (2) at least once a week, (3) at least once a month, (4) not in the past month, and (5) never (reverse coded).	1-5
	Do you belong to an online social networking group such as Facebook or MySpace? Yes=1; No=0.	0-1
	Have you ever used the Internet to connect to an online chat service? Yes=1; No=0.	0-1
	To protect your privacy, have you ever entered misleading information about yourself over the Internet? Yes=1; No=0.	0-1
	To protect your security over the Internet, do you: only deal with well-known organizations and businesses online? Yes=1; No=0.	0-1
	To protect your security over the Internet, do you: regularly change your passwords? Yes=1; No=0.	0-1
	To protect your security over the Internet, do you: regularly delete e-mail from unknown senders? Yes=1; No=0.	0-1

Table 2: Percentages, Means and Standard Deviations of Variables Used in the Analysis

Variables	**Categories**	**Percentages**	**Mean**	**Standard deviation**	**Missing (%)**
Phishing					
Have you experienced any problems associated with receiving fraudulent e-mail from someone posing as a trustworthy and legitimate organization requesting personal information?	No Yes	58.0 42.0	.42	.49	30.0
Consumer fraud					
In the past 12 months, have any of the following things happened to you? The goods or services that arrived were not like the ones described on the website. Yes=1; No=0.	No Yes	96.2 3.8	1.96	.19	18.0
In the past 12 months, have you had problems with purchases over the Internet?	No Yes	87.2 12.8	.13	.33	59.8
In the past 12 months, have any of the following happened to you? The goods or services were never delivered even though you had already paid for them.	No Yes	94.9 5.1	.05	.22	59.8
Identity theft					
In the past 12 months, have any of the following happened to you? Extra funds were taken from your account without your permission.	No Yes	96.0 4.0	.04	.19	59.8
In the past 12 months, have any of the following things happened to you? The goods or services that arrived were not like the ones described on the website. Yes=1; No=0.	No Yes	93.4 6.6	1.93	.25	55.9
Demographics					
Age of respondents	1) 15 to 24 2) 25 to 34 3) 35 to 44 4) 45 to 54 5) 55 to 64 6) 64 to 74 7) 75+	9.6 13.5 17.2 19.3 19.1 12.4 9.0	3.98	1.75	0
What is the highest level of education that you attained?	1) Some secondary/ elementary/no schooling 2) High school diploma 3) Some university/ community college 4) Diploma/certificate from	19.0 14.6 13.3	3.24	1.45	1.1

	community college/trade/ technical 5) Doctorate/masters/ bachelors degree	28.0 24.0			
Sex of respondents	Female Male	55.1 44.9	.45	.50	0
What is your best estimate of your total personal income, before deductions, from all sources during the past 12 months?	1) No income 2) Less than $5,000 3) $5,000 to $9,999 4) $10,000 to $14,999 5) $15,000 to $19,999 6) $20,000 to $29,999 7) $30,000 to $39,999 8) $40,000 to $49,999 9) $50,000 to $59,999 10) $60,000 to $79,999 11) $80,000 to $99,999 12) $100,000 or more	5.3 3.8 5.6 7.3 7.3 13.8 14.3 11.4 8.2 11.4 5.1 6.6	6.92	2.64	14.2
Risk perceptions					
How concerned are you or would you be about security in relation to banking over the Internet?	1) Not at all concerned? 2) Hardly concerned? 3) Somewhat concerned? 4) Greatly concerned?	12.9 19.6 36.2 31.3	2.86	1.0	21.0
How concerned are you or would you be about security in relation to ordering something or making purchases over the Internet?	1) Not at all concerned? 2) Hardly concerned? 3) Somewhat concerned? 4) Greatly concerned?	9.0 17.9 43.3 29.8	2.94	.91	21.0
Online routine activities					
During the past month, how often did you use the Internet: for electronic banking? Was it:	1) Never 2) Not in the past month? 3) At least once a month (but not every week)? 4) At least once a week (but not every day)? 5) At least once a day?	31.6 7.0 16.6 34.7	2.84	1.43	25.9

		10.1			
During the past month, how often did you use the Internet: to make an online booking or reservation?	1) Never 2) Not in the past month? 3) At least once a month (but not every week)? 4) At least once a week (but not every day)? 5) At least once a day?	38.5 34.5 23.6 3.1 .3	1.92	.87	25.7
During the past month, how often did you use the Internet: to purchase goods or services?	1) Never 2) Not in the past month? 3) At least once a month (but not every week)? 4) At least once a week (but not every day)? 5) At least once a day?	38.5 31.5 25.6 4.1 .3	1.96	.91	25.7
Do you belong to an online social networking group such as Facebook or MySpace?	No Yes	53.6 46.6	.46	.50	23.1
Have you ever used the Internet to connect to an online chat service?	No Yes	73.5 26.5	.26	.44	20.2
To protect your privacy, have you ever entered misleading information about yourself over the Internet?	No Yes	83.1 16.9	.17	.37	20.4
To protect your security over the Internet, do you: deal with well-known organizations and businesses online?	No Yes	15.1 84.9	.85	.36	22.0
To protect your security over the Internet, do you: regularly change your passwords?	No Yes	66.6 33.4	.33	.47	21.1
To protect your security over the Internet, do you: regularly delete e-mail from unknown senders?	No Yes	8.2 91.8	.92	.27	29.4

CHAPTER FOUR: ANALYSIS OF RESULTS

This chapter presents the main results for this study. The results from the analyses will answer the research questions raised in Chapter One: (1) Is everyone equally likely to be a target of online crime? and (2) What factors might lead to online victimization? This chapter will also test the hypotheses I posed in Chapter Two. The main goal of this study is to explore whether certain personal characteristics, perceptions of risk, and online routine activities have effects on identity theft, consumer fraud, and phishing victimization.

In this chapter I will first present descriptive statistics related to overall reported victimization. A discussion of bivariate relationships will follow. The Pearson correlation analysis also allows us to assess whether multicollinearity is a concern for the multivariate regression analysis. Several cross-tabulation tables will be presented to explore further the relationships between the variables on a bivariate level. The main analyses are three binary logistic regression models—one for each type of victimization. All three dependent variables (identity theft, consumer fraud, and phishing) are dichotomous variables and the independent variables (demographics, perceptions of risk, and online routine activities) employ various measures (nominal, ordinal, and interval).

Table 2 presents a summary of descriptive statistics and also the reported victimization level for the individual scale items that compose the dependent variables. Table 3 presents the response rates for the recoded dependent variables. Those are the recoded victimization measures which are used in the multivariate analysis. Only one item measures phishing as a type of online victimization (Have you received fraudulent e-mail from someone posing as a trustworthy and legitimate organization requesting personal information?). Of the respondents who answered this

question (n=14,728), 42.4% reported that they had been victims of phishing. Identity theft is measured with 2 items that are recoded into a single dicotomous variable. Those items asked the respondents if in the past 12 months, if any of the following things happened: (1) “Extra funds were taken from your account without your permission”, (2) “Has anyone used any of your credit or bank cards (or card details) from an Internet source, to purchase something or withdraw money from your account without your permission?” Due to missing cases the number of respondents is significantly lower than the number of respondents to phishing (n=8,509). Out of those who did respond to this question, 7.8% reported being victims of identity theft. Lastly, consumer fraud is measured combining 3 items to create one victimization dependent variable. The items are: (1) “In the past 12 months, have the goods or services were never delivered even though you had already paid for them”, (2) “In the past 12 months, have the goods or services that arrived were not like the ones described on the website”, and (3) “In the past 12 months, have you had problems with purchases over the Internet?” Respondents who answered all three questions that composed consumer fraud are included in this analysis (n= 8,555). The univariate analysis shows that 14% of participants reported having been victims of consumer fraud.

Table 3: Reported Victimization Percentages

Dependent variable	Reported victimization categories	Reported victimization percentages
Phishing (n=14,728)	No Yes	57.6 42.4
Identity theft (n=8,509)	No Yes	92.2 7.8
Consumer fraud (n= 8,555)	No Yes	86.0 14.0

Bivariate Analyses

In this section I summarize the results from the correlation matrix and the cross-tabulation tables. The initial bivariate relationships suggest a few factors are significantly correlated with the three form of victimization.

Correlation Analysis

The aim of this section is to test for multicollinearity prior to the main analysis. The correlation matrix reveals that there are no issues of multicollinearity. Some initial results from the correlation analysis are presented in the following section.

Consumer Fraud

The first dependent variable examined is consumer fraud. This victimization refers to any incidents that involve problems with purchases over the internet, for example, goods that were paid for were not delivered or goods were delivered but they were not the ones described online. The table in Appendix A shows that age ($r=-.083$, $p\leq.01$), education ($r=-.022$, $p\leq.05$), and income ($r=-.047$, $p\leq.001$) were negatively correlated with consumer fraud. Individuals with less income and lower education and younger people are more likely to be victims of consumer fraud. On the other hand, gender was positively correlated with consumer fraud ($r=.083$, $p\leq.001$), indicating that men (who were coded as 1) are more likely to be victims of consumer fraud.

Interestingly, perception of risk associated with online shopping has a significant positive relationship with consumer fraud ($r=.036$, $p\leq.01$). This means that perceptions of higher risks associated with online shopping are correlated with higher victimization rates of consumer fraud.

In contrast, there is no statistically significant relationship between perception of risk associated with online banking and consumer fraud.

In regards to online routine activities, all but one of the independent variables were found be correlated with consumer fraud victimization. Dealing with known online organizations was negatively correlated with consumer fraud victimization ($r=-.063$, $p\leq.01$). That is, individuals who interact with well-known organization and businesses online are less likely to experience consumer fraud than those who get in contact via the internet with risky organizations or businesses. On the other hand, more frequent use of the internet for banking ($r=.065$, $p\leq.01$), booking, for example hotels and flights ($r=.036$, $p\leq.01$) and purchasing of goods and services ($r=.082$, $p\leq.01$), is correlated with increased consumer fraud victimization. Similarly, belonging to social network groups ($r=.085$, $p\leq.01$) and using online chats ($r=.085$, $p\leq.01$) are also positively correlated with consumer fraud victimization. Interestingly, entering misleading information ($r=.092$, $p\leq.01$) and regularly changing passwords ($r=.027$, $p\leq.05$) are also positively correlated with consumer fraud.

It is important to note that all the observed statistically significant relationships are very weak. The Pearson correlation values are as low as .022 and the highest is .092.

Identity Theft

The second dependent variable, identity theft victimization, looks at whether funds were taken from victims accounts without permission and unauthorised use of debit or credit cards online. In contrast to consumer fraud, only education and income are statistically significant. Moreover, the

positive correlation suggests that individuals with higher incomes (r=.030, p≤.01) and higher levels education (r=.063, p≤.01) are more likely to be victims of identity theft.

Identity theft is positively correlated with perceptions of risk associated with banking and shopping. This suggests that having higher perceptions of risk associated with online banking (r=.027, p≤.05) and online shopping (r=.065, p≤.01) are associated with increased victimization.

Contrary to the correlations found with consumer fraud, here only four online routine activities are correlated with identity theft. The positive correlations suggest that increased use of online banking (r=.064, p≤.01), booking for reservations online (r=.076, p≤.01) and online shopping (r=.026, p≤.01) and having social network account (r=.038, p≤.01) all increase the probability of identity fraud victimization.

Similar to the case of consumer fraud, the correlation coefficients are all below .08 which indicates weak, yet statistically significant relationships (p<.05).

Phishing

The last dependent variable is phishing as a form of victimization. This is where victims receive fraudulent emails from someone who is posing as a legitimate organization. From the correlation table (Table 3) we can see that three out of the four demographic factors are positively correlated to identity theft victimization. Men (coded as 1) are more likely than women (coded as 0) to be victims of phishing (r=.138, p≤.01). In addition, individuals with a higher level of education (r=.204, p≤.01) and higher income (r=.153, p≤.01) are more likely to be phishing victims.

Perceptions of risk associated with banking or shopping are not correlated with phishing victimization. This suggests that perceptions of risk are not a factor in phishing victimization.

However, all nine online routine activities are positively correlated with phishing victimization. Engaging in online banking ($r=.185$, $p\leq.01$), booking reservations ($r=.227$, $p\leq.01$), shopping ($r=.269$, $p\leq.01$), social networking ($r=.090$, $p\leq.01$) and online chatting ($r=.095$, $p\leq.01$) all increase the likelihood of phishing victimization. Entering misleading information ($r=.176$, $p\leq.01$), dealing with known online organizations ($r=.043$, $p\leq.01$), regularly changing passwords ($r=.059$, $p\leq.01$) and deleting emails ($r=.084$, $p\leq.01$) all are associated with an increase in phishing victimization.

For phishing victimization the relationships are considerably stronger than for consumer fraud and identity theft. The correlation coefficients range from .043 to .269.

Demographics

Interesting relationships are observed when looking at the correlations between demographic factors and perceptions of risk and certain online routine activities. There is a significant positive relationship between age and perception of risk. This indicates that older people perceive higher risks associated with online shopping ($r=.149$, $p\leq.01$) and banking ($r=.172$, $p\leq.01$). On the other hand, younger people are more likely to use social network sites ($r=-.471$, $p\leq.01$) and to use online chat forums ($r=-.372$, $p\leq.01$).

Higher education is positively correlated with higher occurrences of online banking ($r=.236$, $p\leq.01$), online shopping ($r=.234$, $p\leq.01$), and booking reservations online ($r=.309$, $p\leq.01$). Individuals with higher education are more likely to engage more often in these online activities. Similar correlations are observed with regards to income. This means that individuals with a higher income are more likely to use online banking ($r=.182$, $p\leq.01$), online shopping

(r=.195, p≤.01) and to book reservations online (r=.267, p≤.01), than do individuals with lower incomes.

Perceptions of Risk

There is a negative relationship between perceptions of risk and routine activities. This is not an unexpected correlation. This finding is consistent with previous research by Reising et al. (2009) and by Yar (2010). Higher perceptions of risk associated with online banking resulted in fewer online banking transactions (r=-.256, p≤.001). Additionally, higher perceptions of risk associated with online shopping resulted in fewer instances of online shopping (r=-.190, p≤.001).

Cross-Tabulations

For a more in-depth analysis at the bivariate level, specific correlations were chosen to be interpreted further using cross-tabulation tables. Firstly, the impact gender has on perceptions of risk is examined. Table 4 examines the relationship between gender and perception of risk associated with online banking. Women reported a higher concern associated with online banking compared with men. Fifteen percent of men reported that they are not at all concerned compared with 12.5% of women. While the difference is small, the Chi-Square test shows that this relationship is statistically significant (χ^2=24.238, p≤.001).

Table 5 demonstrates the relationship between gender and perceptions of risk associated with online shopping (χ^2=64.425, p≤.001). Almost 30% of women report being greatly concerned with making purchases online compared with 26% of men. These results suggest that men perceive lower risk associated with online shopping or banking compared with women. This

is consistent with past studies (Garbarino and Strahilevitz 2004; Liebermann and Stashevsky 2002) and proposed hypothesis (Hypothesis 2).

Research studies investigating the relationship between gender and victimization are not conclusive (Anderson 2006, 2007; Holtfreter et al. 2006). To examine this relationship three cross-tabulations are presented—one for each victimization variable. Interestingly, there are statistically significant relationships between gender and two forms of victimization. Based on these results, phishing has a statistically significant relationship with gender (χ^2=282.763, $p \leq .001$). There is a 13.7% difference between victimization rates among males and females. Table 6 shows that 35.6% of females reported victimization compared with 49.3% of men reported phishing victimization. While the Chi-Square test shows statistical significance (χ^2=7.662, $p \leq .01$), there is a small difference (2.1%) in consumer fraud victimization between men and women (see Table 7). Table 7 demonstrates that while 15% of men report consumer fraud victimization, 13% of women report consumer fraud victimization. Identity theft victimization is the only form of crime that does not have a statistically significant difference between male and female victimization. Table 8 presents these results (χ^2=.032, p=.857). This suggests that identity theft victimization occurs at similar rates among men and women.

Women perceive higher risks associated with online shopping and banking, however, they are less often victimized compared with men. On the other hand, men are victimized more often but have lower perceptions of risk. It could be that due to higher perceived risk women take more precautions online and adapt their behaviour, which results in lower victimization rates. These results also support previous claims that gender differences in victimization are crime-specific (Holtfreter et al. 2006; Menard and Covey 2016) because in this study gender differences are only significant in two of the three types of victimization.

To explore whether this might be the case, cross-tabulations between perceptions of risk and online routine activities are examined. Table 9 shows that 52% are very concerned with online banking and never use the internet to do online banking (χ^2=1709.883, p≤.001). The table also shows that 15.9% of those who are not at all concerned with its risks do online banking daily. In comparison, 7.7% of those who are very concerned with its risks but are nonetheless daily online banking users. There is further evidence that there is a significant relationship between perceptions of risk and online activities highlighted in Table 10. Out of those who are very concerned with risks associated with online shopping, 50.3% never made online purchases, compared with 42.4% of respondents who are not at all concerned with online shopping, but never made an online purchase. While the difference is not very large, it is still a statistically significant relationship (χ^2=473.163, p≤.001).

The findings suggest that those who have high perceptions of risks of online activities are less likely to engage in online activities. This could help explain the gender difference in victimization where perceptions and routine activities are mediating variables. It appears that women are victimized less because they have higher risk perceptions and in turn women adapt their behaviour. However, it is important to note that the directionality is not established. People who engaged in online banking or online shopping might have had bad experiences which in turn caused higher perceptions of risk and this led to less frequent online activities. In other words, it is possible that the online activities caused higher perceptions of risk as opposed to preconceived perceptions of risk caused a reduction of online activities.

Assuming that higher perceptions of risk lead to fewer online activities, it is logical that higher risk perceptions will in turn lead to reduced victimization. Four cross-tabulation tables are constructed to explore the relationship between perceptions of risk concerning potential

victimization when using online shopping and banking. The correlation matrix shows that perceptions of risk are not correlated with phishing. Therefore, I focus attention on identity theft and consumer fraud as the two types of victimization to analyze.

Consumer fraud victimization is affected by victims' perceptions of risk associated with online banking and online shopping. Table 11 shows that there is a small difference between those who have a higher perception of risk and low perceptions of risk of online banking (χ^2=16.180, p≤.001). Those who are very concerned with online banking are less likely to be consumer fraud victims compared with those who are not at all concerned with online banking (15.6% and 16.3%, respectively). Interestingly, an opposite relationship is observed between risk perceptions of online banking and identity theft. Table 12 shows that 9.2% of those who are very concerned about risk have been victimized compared with 8.4% of those who are not at all concerned about online banking (χ^2=21.153, p≤.001).

Tables 13 (χ^2=31.088, p≤.001) and 14 (χ^2=49.663 , p≤.001) explore perceptions of risk (associated with online shopping and consumer fraud) and phishing. Here we find similar results. Those with higher perceptions of risk are actually the ones who are at the greatest risk of identity theft and consumer fraud victimization. For example, 11.7% of those who reported being greatly concerned about risks when making online purchases also reported having been victimized, compared with 6.8% of those who reported that they are not concerned (with online shopping risks and consumer fraud victimization). These findings are contradictory to Hypothesis 2. Hypothesis 2 states that those with higher risk perceptions of online crime are less likely to do online shopping, banking and networking and therefore are less likely to experience online fraud victimization. Therefore, I reject this hypothesis. It could be the case that those who were victimized in the past now perceive online activities to be risky. However, it could be the case

that there are other factors that are involved. On the other hand, the reason also could be that the order of events is reversed and victimization increases fear. In the next section I will attempt to clarify the relationships between the different variables and examine whether there is support for the other hypotheses using a multivariate analysis.

Table 4: Cross-Tabulation for Gender and Perceptions of Risk Associated with Banking

		Gender		Total
		Female	Male	
Perceptions of risk associated with banking	1) Not at all concerned	1014 12.5%	1240 15.2%	2254 13.8%
	2) Hardly concerned	1749 21.6%	1704 20.8%	3453 21.2%
	3) Somewhat concerned	2961 36.5%	2880 35.2%	5841 35.9%
	4) Very concerned	2386 29.4%	2357 28.8%	4743 29.1%
Total		8110 100%	8181 100%	16291 100%

(χ^2= 24.238, P<.001)

Table 5: Cross-Tabulation for Gender and Perceptions of Risk Associated with Shopping

		Gender		Total
		Female	Male	
Perceptions of risk associated with shopping	1) Not at all concerned	658 8.1%	876 10.7%	1534 9.4%
	2) Hardly concerned	1479 18.3%	1695 20.7%	3174 19.5%
	3) Somewhat concerned	3546 43.8%	3497 42.7%	7043 43.2%
	4) Very concerned	2415 29.8%	2122 25.9%	4537 27.9%
Total		8098 100%	8190 100%	16288 100%

(χ^2= 64.425, P<.001)

Table 6: Cross-Tabulation for Gender and Phishing Victimization

		Gender		Total
		Female	Male	
Phishing victimization	No	4759 64.4%	3724 50.7%	8483 57.6%
	Yes	2628 35.6%	3617 49.3%	6245 42.4%
Total		7387 100%	7341 100%	14728 100%

(χ^2=282.763, P<.001)

Table 7: Cross-Tabulation for Gender and Online Consumer Fraud Victimization

		Gender		Total
		Female	Male	
Online consumer fraud Victimization	No	3405 87.1%	3952 85%	7357 86%
	Yes	503 12.9%	695 15%	1198 14%
Total		3908 100%	4647 100%	8555 100%

(χ^2=7.662, P<.01)

Table 8: Cross-Tabulation for Gender and Online Identity Theft Victimization

		Gender		Total
		Female	Male	
Online identity theft victimization	No	3581 92.2%	4265 92.3%	7846 92.2%
	Yes	305 7.8%	358 7.7%	663 7.8%
Total		3886 100%	4623 100%	8509 100%

(χ^2=.032, P= .857)

Table 9: Cross-Tabulation for Perceptions of Risk Associated with Online Banking and Frequency of Online Banking

		Perceptions of risk associated with online banking				Total
		1) Not At all concerned	2) Hardly concerned	3) Somewhat concerned	4) Very concerned	
Frequency of online banking	1) Never	448 21.1%	494 14.7%	1377 24.7%	2256 52.3%	4575 29.7%
	2) Not in the past month	160 7.5%	229 6.8%	416 7.4%	303 7%	1108 7.2%
	3) Monthly	304 14.3%	707 21%	1060 19%	504 11.7%	2575 16.7%
	4) Weekly	873 41.1%	1574 46.7%	2136 38.2%	920 21.3%	5503 35.8%
	5) Daily	338 15.9%	364 10.8%	596 10.7%	330 7.7%	1628 10.6%
Total		2123 100%	3368 100%	5585 100%	4313 100%	15389 100%

(χ^2=1709.883, P<.001)

Table 10: Cross-Tabulation for Perceptions of Risk Associated with Online Shopping and Frequency of Online Shopping

		Perceptions of risk associated with online shopping				Total
		1) Not At all concerned	2) Hardly concerned	3) Somewhat concerned	4) Very concerned	
Frequency of online shopping	1) Never	601 42.4%	986 32%	2158 32%	2085 50.3%	5830 37.9%
	2) Not in the past month	420 29.7%	1073 34.8%	2413 35.8%	1235 29.8%	5141 33.4%
	3) Monthly	337 23.8%	894 29%	1889 28%	718 17.3%	3838 24.9%
	4) Weekly	53 3.7%	114 3.7%	270 4%	98 2.4%	535 3.5%
	5) Daily	5 0.4%	18 0.6%	16 0.2%	13 0.3%	52 0.3%
Total		1416 100%	3085 100%	6746 100%	4149 100%	15396 100%

(χ^2=473.163, P<.001)

Table 11: Cross-Tabulation for Perceptions of Risk Associated with Banking and Online Consumer Fraud Victimization

		Perceptions of risk associated with banking				Total
		1) Not At all concerned	2) Hardly concerned	3) Somewhat concerned	4) Very concerned	
Online consumer fraud victimization	No	993 83.4%	1886 87.5%	2891 86.7%	1562 84.4%	7332 86%
	Yes	198 16.3%	269 12.5%	442 13.3%	288 15.6%	1197 14%
Total		1191 100%	2155 100%	3333 100%	1850 100%	8529 100%

(χ^2=16.180, P<.001)

Table 12: Cross-Tabulation for Perceptions of Risk Associated with Banking and Online Identity Theft Victimization

		Perceptions of risk associated with banking				Total
		1) Not At all concerned	2) Hardly concerned	3) Somewhat concerned	4) Very concerned	
Online identity theft victimization	No	1092 91.6%	2027 94.4%	3033 91.8%	1670 90.8%	7822 92.2%
	Yes	100 8.4%	120 5.6%	270 8.2%	170 9.2%	660 7.8%
Total		1192 100%	2147 100%	3303 100%	1840 100%	8482 100%

(χ^2=21.153, P<.001)

Table 13: Cross-Tabulation for Perceptions of Risk Associated with Shopping and Online Consumer Fraud Victimization

		Perceptions of risk associated with shopping				Total
		1) Not At all concerned	2) Hardly concerned	3) Somewhat concerned	4) Very concerned	
Online consumer fraud victimization	No	672 85.4%	1899 87.6%	3624 86.8%	1149 81.4%	7344 86%
	Yes	115 14.6%	270 12.4%	552 13.2%	262 18.6%	1199 14%
Total		787 100%	2169 100%	4176 100%	1411 100%	8543 100%

(χ^2=31.088, P<.001)

Table 14: Cross-Tabulation for Perceptions of Risk Associated with Shopping and Online Identity Theft Victimization

		Perceptions of risk associated with shopping				Total
		1) Not At all concerned	2) Hardly concerned	3)Somewhat concerned	4) Very concerned	
Online identity theft victimization	No	731 93.2%	2049 94.7%	3817 92%	1237 88.3%	7834 92.2%
	Yes	53 6.8%	115 5.3%	331 8%	164 11.7%	663 7.8%
Total		784 100%	2164 100%	4148 100%	1401 100%	8497 100%

(χ^2=49.663, P<.001)

Multivariate Analyses

Examining the bivariate relationships from the correlation table and cross-tabulation tables revealed some interesting patterns. For example, some relationships are crime-specific such as gender. The relationship between gender and online victimization is statistically significant for phishing and consumer fraud, but not for identity theft. Also, the bivariate analysis led us to reject Hypothesis 2 (Those with higher risk perceptions of online crime are less likely to do online shopping, banking and networking, and therefore are less likely to experience online fraud victimization). In this next section, I will further explore whether online routine activities, perceptions of risk and demographics have impacts on online victimization. To do so, the next step is to conduct multivariate regression analyses. Each table presents three models and each table focuses on one form of victimization.

Identity Theft

The results of the first model of Table 15 indicate that of the four demographic variables (gender, age, education, and income) only education (Exp(B)=1.178, $p \leq .001$) is a risk factor associated with identity theft. The significant positive relationship suggests that those with higher education have increased odds of being a victim by almost 18%. However, the Nagelkerke R^2 of .008 indicates that the set of demographic variables explains less than 1% of the variance in victimization.

The second model adds to the demographic baseline model perceptions of risk. Education remains statistically significant (Exp(B)=1.174, $p \leq .001$) and increases the likelihood of victimization by 17%. Perception of risk associated with banking is not statistically significant, while risk perception associated with online shopping (Exp(B)=1.377, $p \leq .001$) is statistically significant and positive. This finding suggests that having higher perceptions of risk associated with online shopping increases the chances of being a victim of identity theft by 38%. This is a strong effect. This model accounts for 1.6% of the variance.

The third model includes the online routine activities in addition to demographic characteristics and perceptions of risk. The nine online routine activities include: (1) online banking, (2) making online bookings and reservations, (3) purchasing online goods and services, (4) using social network websites, (5) using online chat services, (6) entering misleading information, (7) dealing with well-known organizations online, (8) regularly changing passwords, and (9) regularly deleting e-mails. Interestingly, education still remains significant in this model but the coefficient is lower than in the previous two models (Exp(B)=1.098, $p \leq .05$), suggesting that the strength of the relationship is reduced once online routine activities are introduced. This could mean that those with higher education engage in more online activities

that lead to victimization. Perception of risk associated with online shopping (Exp(B)=1.295, p≤.001) continue to be a significant risk factor. As perception of risk associated with online shopping increases, the likelihood of victimization increases by thirty percent.

In this model, the three routine activities have a positive significant relationship with identity theft victimization after controlling for other predictors: (1) using the internet for banking (Exp(B)=1.186, p≤.001), (2) using the internet for booking reservations (Exp(B)=1.257, p≤.001), and (3) belonging to an online social networking site (Exp(B)=1.397, p≤.001). The results show that using the internet for booking reservations and banking increases the probability of victimization by approximately 26% and 19%, respectively. In addition, these results imply that belonging to a social network site has the largest effect on the odds of being an identity theft victim, increasing the possibility by almost forty percent. However, the addition of the nine online routine activities variables to the analysis increased the R^2 from .016 to .034, indicating that this model still only accounts for 3.4% of the variance in online identity theft victimization. In other words, this model is not a complete representation of the risk factors that might lead to online identity theft.

It was previously argued that some relationships are crime-specific. Therefore, it is important to see if the proposed hypotheses are supported or rejected for each form of victimization. Hypotheses 1_a (older individuals have a higher likelihood of experiencing online fraud victimization than younger individuals), 1_b (gender is associated with online fraud victimization), 1_c (more highly educated people have a higher likelihood of online fraud victimization) and 1_d (greater income is associated with a higher likelihood of online fraud victimization) suggest that there are associations between various demographic variables and victimization. Of these three hypotheses, only $H1_c$ is supported. The results show that more

highly educated people have a higher likelihood of identity theft victimization while controlling for the other variables in the model. The other three hypotheses anticipating relationships between gender, age and income and subsequent victimization are rejected.

Hypotheses 3_a (people who use the internet for online banking more frequently are at higher risk of identity theft victimization) and 3_b (people who frequently use the internet for booking or reservations are at higher risk of identity theft victimization) are supported by the results presented in Table 15, while the remaining hypotheses ($H3_c$: people who frequently use the internet to purchase goods or are at higher risk of online fraud victimization, $H4_a$: people who protect their privacy by regularly changing passwords are at lower risk of online fraud victimization, and $H4_b$: people who protect their privacy by regularly deleting e-mails are at lower risk of online fraud victimization) are rejected.

Consumer Fraud

Slightly more promising results are revealed in Table 16. This table examines consumer fraud as the dependent variable. In the first model, two of the demographic characteristics are found to be statistically significant. Gender predicts victimization (Exp(B)=1.275, $p \leq .001$). Men are more likely to be victims of online consumer fraud than are woman by approximately twenty-eight percent. Additionally, age has a negative and statistically significant relationship (Exp(B)=.851, $p \leq .001$). This relationship means that as each age group increased by 5 years the probability of victimization is reduced by 15%. This first model explains 1.8 percent of the variance in online consumer fraud victimization ($R^2 = .018$).

In the second model, a positive statistically significant relationship between age (Exp(B)=1.286, p≤.001) and victimization is observed. Also, as in the previous model gender is a predictor of consumer fraud (Exp(B)=.851, p≤.001). Two new relationships are found to be significant. Perception of risk associated with online shopping (Exp(B)=1.227, p≤.001) has a statistically significant positive relationship with consumer fraud victimization, indicating that as risk perceptions increase the likelihood of consumer fraud victimization increases by almost twenty-three percent. Perception of risk associated with online banking (Exp(B)=.917, p≤.05) has a statistically significant negative relationship with consumer fraud victimization, indicating that as risk perceptions increase the likelihood of consumer fraud victimization decreases by nine percent. This result is consistent with Hypothesis 2 (victimization is reduced with higher perceptions of risk). This model accounts for 2.1% of the variance in online consumer fraud, only 0.3% higher than the first model.

The third model shows some interesting results. Age, which was statistically significant in the previous two models, is not significant in this model. This leads to the rejection of $H1_a$ (older individuals have a higher likelihood of experiencing online fraud victimization than younger individuals). It is possible that it is a spurious relationship and the online routine activities younger people engage in could explain away this relationship. Gender remains significant and has a similar effect on victimization as in the previous two models (Exp(B)=1.235, p≤.01). Men are more likely to be victims of online consumer fraud compared with women. This provides support for $H1_b$ (gender is associated with online fraud victimization). The most interesting finding is that in this model when routine activities are introduced, education and income gained statistical significance, suggesting suppression effects. As education level increases victimization decreased by 7% (Exp(B)=.930, p≤.05). Higher

income brackets also reduce the probability of victimization by four percent. These two findings are contradictory to hypotheses 1_c (more highly educated people have a higher likelihood of online fraud victimization) and 1_d (greater income is associated with a higher likelihood of online fraud victimization) and therefore they are rejected.

Perception of risk associated with online shopping remained significant (Exp(B)=1.240, $p \leq .001$) in the final model. This means that with each increase in the risk perceptions of online shopping the probability of victimization increases by twenty four percent. On the other hand, perceptions of risk associated with online banking are not statistically significant in the final model.

For consumer fraud, seven routine activities are found to be significant while controlling for other predictors. First, greater use of the internet for banking (Exp(B)=1.149, $p \leq .001$) increases the likelihood of victimization by fifteen percent. Second, people who use the internet more often for making online reservations (for example, those who make online reservations at least once a month compared with those who make online reservations at least once a week) are nearly 10% more likely to be victims of consumer fraud (Exp(B)=1.099, $p \leq .05$). Third, using the internet to purchase goods and services also increases the probability of consumer fraud victimization by approximately 31% (Exp(B)=1.305, $p \leq .001$). These three statistically significant relationships are evidence in support of Hypotheses 3_a (people who use the internet for online banking more frequently are at higher risk of online fraud victimization), 3_b (people who frequently use the internet for booking or reservations are at higher risk of online fraud victimization), and 3_c (people who frequently use the internet to purchase goods or are at higher risk of online fraud victimization).

The other four noteworthy relationships are as follows. Dealing with well-known organizations (Exp(B)=.677, p≤.001) reduces the probability of being victimized by thirty-two percent. It is interesting to note that entering misleading information online (Exp(B)=1.342, p≤.001) leads to a 34% increase in consumer fraud victimization. Visiting social media websites increases the probability of victimization by 28% (Exp(B)=1.280, p≤.01). Individuals who use online chat services are more likely to be victimized by nearly 21% (Exp(B)=1.206, p≤.05). Hypotheses 4_a (people who protect their privacy by regularly changing passwords are at lower risk of online fraud victimization) and 4_b (people who protect their privacy by regularly deleting e-mails are at lower risk of online fraud victimization) are rejected because neither changing passwords nor deleting e-mails are found to effect consumer fraud victimization. This model explains only 6% of the variance in online consumer fraud victimization, suggesting that there are other risk factors that need to be further studied.

Phishing

Table 17 examines phishing victimization and the associated risk factors. In the first model all four demographics factors are statistically significant. Each increase in the age category increases phishing victimization decreased by approximately 9% (Exp(B)=.912, p≤.001). Men are 71% more likely to be victimized compared with women. There is a positive statistically significant relationships between education (Exp(B)=1.369, p≤.001) and phishing victimization. Similarly, a positive statistically significant relationship is observed between income and phishing victimization (Exp(B)=1.044, p≤.001). As education level increases so does the likelihood of phishing victimization by about 37%. Also, as income increases, the probability of victimization increases by four percent. This model already is a better fit for phishing than for

either identity theft and consumer fraud. The R^2 is .089. This model explains almost 9% of the variance in phishing victimization.

The second model is very similar to the first one because the demographic risk factors are statistically significant, but neither of the risk perceptions are statistically significant. In other words, as education (Exp(B)=1.376, p≤.001) and income (Exp(B)=1.042, p≤.001) increase so does phishing victimization. Men (Exp(B)=1.722, p≤.001) and younger people (Exp(B)=.915, p≤.001) are also at higher risk of victimization in this model. However, having higher perceptions of risk associated with shopping or banking does not appear to be related to victimization. This model explains 9% of the variance in phishing victimization.

The last model suggests that the effect of income on victimization is explained away by routine activities (it is no longer significant in this model). Nonetheless, age (Exp(B)=1.097, p≤.001), gender (Exp(B)=1.766, p≤.001) and education (Exp(B)=1.247, p≤.001) all remain statistically significant. Interestingly, when routine activities are controlled for, the relationship between age and victimization changed from a negative to a positive one. Older people are almost 10% more likely to become phishing victims in Model Nine. Men and individuals with higher education, on the contrary, across all three models were consistently found to have higher chances of being phishing victims than women and people with lower education.

It is noteworthy, that in the third model perceptions of risk associated with online shopping become statistically significant (Exp(B)= 1.065, p≤.05). Those with higher perceptions of risk are also more likely to be phishing victims by 6.5%. These results indicate a suppression effect that could be the result of the addition of certain online routine activities to the model.

In this model all but two of the routine activities are related to phishing victimization. Increased use the internet for banking (Exp(B)=1.094, p≤.001) increases the likelihood of victimization by 9%, while using the internet for booking reservations more frequently (Exp(B)=1.220, p≤.001) and making online purchases more often (Exp(B)=1.389, p≤.001) increase the probability of victimization by 22% and 39%, respectively. Belonging to social network websites (Exp(B)=1.420, p≤.001) and using online chat services (Exp(B)=1.350, p≤.001) increases the odds of phishing victimization by 35% and 42%. Interestingly, entering misleading information and regularly changing passwords are found to be significant and positively correlated with phishing victimization. This suggests that regularly changing online passwords increases victimization risk by almost 19% (Exp(B)=1.188, p≤.001). In addition, entering misleading information online increases one's risk of phishing victimization by almost 98% (Exp(B)=1.977, p≤.001). Ryens (2015) suggests that this effect could be due to other activities that promote this behavior. He suggests that those who change their passwords often might feel the need to do so because they visit unsafe websites. The coefficient of determination (R^2) is .192, suggesting that this model explains 19% of the variance.

For phishing victimization three of the four hypotheses about demographic variables were supported. Men, older people, and more educated people are more likely to experience phishing. Hypotheses 3_a (people who use the internet for online banking more frequently are at higher risk of online fraud victimization), 3_b (people who frequently use the internet for booking or reservations are at higher risk of online fraud victimization), and 3_c (people who frequently use the internet to purchase goods or are at higher risk of online fraud victimization) are also supported. Engaging in online activities such as banking, shopping and making reservations online all increase phishing victimization. Lastly, there was a positive relationship between

changing passwords and victimization, however, it was hypothesized that changing passwords would reduce victimization. Therefore, Hypothesis 4_a (people who protect their privacy by regularly changing passwords are at lower risk of online fraud victimization) is rejected.

Summary

The three multivariate regression analyses find evidence for the applicability of Routine Activities Theory. Two of the hypotheses are supported, and five out of the ten posed hypotheses are partially supported, finding evidence in one or two of the types of victimization. Table 18 summarizes the hypotheses testing results based on the multivariate regression analyses.

$H1_a$ (older individuals have a higher likelihood of experiencing online fraud victimization than younger individuals) is supported for phishing, but not for identity theft or consumer fraud victimization. $H1_b$ (gender is associated with online fraud victimization) is supported for phishing and consumer fraud, but not for identity theft victimization. $H1_c$ (more highly educated people have a higher likelihood of online fraud victimization) is supported for phishing and identity theft, but not for consumer fraud victimization.

H2 (those with higher risk perceptions of online crime are less likely to do online shopping, banking and networking and therefore are less likely to experience online fraud victimization) is rejected based on the bivariate analysis and the multivariate results also lead us to reject this hypothesis.

$H3_c$ (people who frequently use the internet to purchase goods or are at higher risk of online fraud victimization) is supported for phishing and consumer fraud, but not for identity theft victimization.

Only two hypotheses, 3_a (people who use the internet for online banking more frequently are at higher risk of online fraud victimization) and 3_b (people who frequently use the internet for booking or reservations are at higher risk of online fraud victimization), are supported for all three crimes: identity theft, consumer fraud, and phishing victimization.

The Negelkerke R^2 in all three regression models suggests that there are other factors that remain undetected in this research. Routine Activities Theory leaves a considerable amount of unexplained variance in consumer fraud, identity theft, and phishing victimization. The implication of these results for future research and policy development will be discussed in the following chapter.

Table 15: Logistic Regression Models for Identity Theft Victimization

Variable	**Model 1**		**Model 2**	
	B(SE)	B(exp)	B(SE)	B(exp)
Demographics				
Education	.164(.041)***	1.178	.160(.041)***	1.174
Gender	-.026(.092)	.975	-.013(.091)	.987
Income	.016(.016)	1.016	.015(.016)	1.015
Age	-.004(.033)	.996	-.010(.034)	.990
Perceptions of risk				
Perceptions of risk of online banking			-.069(.058)	.934
Perceptions of risk of online shopping			.320(.068)***	1.377
Online routine activities				
Use internet for banking				
Use internet for booking and reservations				
Use internet for purchasing goods or services				
Belong to online social networking site				
Use online chat service				
Enter misleading information online				
Deal with known organizations				
Regularly change passwords				
Regularly delete emails				
Constant	-3.227(.182)*	.040	-3.901(.236)*	.020
-2 log likelihood	4137.116		4099.732	
Model X^2	24.385***		51.595***	
Nagelkerke R^2	.008		.016	
N	7,097		7,072	

*P<.05, ** P<.01, *** P<.001

Continued...

Table 15: Logistic Regression Models for Identity Theft Victimization (Continued)

Variable	**Model 3**	
	B(SE)	B(exp)
Demographics		
Education	.093(.043)*	1.098
Gender	.029(.096)	1.029
Income	.002(.017)	1.002
Age	.068(.039)	1.071
Perceptions of risk		
Perceptions of risk of online banking	.018(.062)	1.018
Perceptions of risk of online shopping	.258(.071)***	1.295
Online routine activities		
Use internet for banking	.171(.042)***	1.186
Use internet for booking and reservations	.229(.056)*	1.257
Use internet for purchasing goods or services	.035(.061)	1.036
Belong to online social networking site	.334(.105)***	1.397
Use online chat service	.018(.101)	1.018
Enter misleading information online	.057(.102)	1.059
Deal with known organizations	.061(.144)	1.063
Regularly change passwords	-.059(.096)	.942
Regularly delete emails	.018(.187)	1.018
Constant	-5.396(.393)*	.005
-2 log likelihood	3875.932	
Model X^2	105.184***	
Nagelkerke R^2	.034	
N	6,776	

*P<.05, ** P<.01, *** P<.001

Table 16: Regression Models for Consumer Fraud Victimization

Variable	**Model 4**		**Model 5**	
	B(SE)	B(exp)	B(SE)	B(exp)
Demographics				
Education	-.008(.029)	.992	-.011(.029)	.989
Gender	.243(.070)***	1.275	.252(.071)***	1.286
Income	-.022(.013)	.978	-.023(.013)	.977
Age	-.161(.027)***	.851	-.162(.027)***	.851
Perceptions of risk				
Perceptions of risk of online banking			-.087(.044)*	.917
Perceptions of risk of online shopping			.204(.050)***	1.227
Online routine activities				
Use internet for banking				
Use internet for booking and reservations				
Use internet for purchasing goods or services				
Belong to online social networking site				
Use online chat service				
Enter misleading information online				
Deal with known organizations				
Regularly change passwords				
Regularly delete emails				
Constant	-1.302(.121)*	.272	-1.610(.159)*	.200
-2 log likelihood	6167.953		6139.563	
Model X^2	75.355*		91.441*	
Nagelkerke R^2	.018		.021	
N	7,083		7,059	

*P<.05, ** P<.01, *** P<.001

Continued...

Table 16: Logistic Regression Models for Consumer Fraud Victimization (Continued)

Variable	**Model 6**	
	B(SE)	B(exp)
Demographics		
Education	-.072(.030)*	.930
Gender	.211(.074)**	1.235
Income	-.039(.013)**	.961
Age	-.045(.031)	.956
Perceptions of risk		
Perceptions of risk of online banking	-.047(.046)	.954
Perceptions of risk of online shopping	.215(.053)***	1.240
Online routine activities		
Use internet for banking	.139(.032)***	1.149
Use internet for booking and reservations	.094(.042)*	1.099
Use internet for purchasing goods or services	.266(.047)***	1.305
Belong to online social networking site	.247(.082)**	1.280
Use online chat service	.187(.075)*	1.206
Enter misleading information online	.294(.075)***	1.342
Deal with known organizations	-.391(.095)***	.677
Regularly change passwords	.091(.071)	1.095
Regularly delete emails	.207(.145)	1.230
Constant	-3.326(.279)	.036
-2 log likelihood	5801.234	
Model X^2	250.518***	
Nagelkerke R^2	.060	
N	6,808	

*P<.05, ** P<.01, *** P<.001

Table 17: Logistic Regression Models for Phishing Victimization

Variable	**Model 7**		**Model 8**	
	B(SE)	B(exp)	B(SE)	B(exp)
Demographics				
Education	.314(.016)***	1.369	.319(.016)***	1.376
Gender	.540(.039)***	1.716	.543(.039)***	1.722
Income	.043(.007)***	1.044	.042(.007)***	1.042
Age	-.093(.013)***	.912	-.089(.013)***	.915
Perceptions of risk				
Perceptions of risk of online banking			-.011(.023)	.989
Perceptions of risk of online shopping			-.006(.026)	.994
Online routine activities				
Use internet for banking				
Use internet for booking and reservations				
Use internet for purchasing goods or services				
Belong to online social networking site				
Use online chat service				
Enter misleading information online				
Deal with known organizations				
Regularly change passwords				
Regularly delete emails				
Constant	-1.710(.065)*	.181	-1.678(.088)*	.187
-2 log likelihood	16830.930		16657.372	
Model X^2	891.456*		892.070*	
Nagelkerke R^2	.089		.090	
N	11,996		11,875	

*P<.05, ** P<.01, *** P<.001

Continued...

Table 17: Logistic Regression Models for Phishing Victimization (Continued)

Variable	**Model 9**	
	B(SE)	B(exp)
Demographics		
Education	.221(.017)***	1.247
Gender	.569(.042)***	1.766
Income	.011(.008)	1.011
Age	.092(.16)***	1.097
Perceptions of risk		
Perceptions of risk of online banking	.045(.026)	1.046
Perceptions of risk of online shopping	.063(.028)*	1.065
Online routine activities		
Use internet for banking	.090(.016)***	1.094
Use internet for booking and reservations	.199(.026)***	1.220
Use internet for purchasing goods or services	.328(.025)***	1.389
Belong to online social networking site	.351(.046)***	1.420
Use online chat service	.300(.045)***	1.350
Enter misleading information online	.682(.049)***	1.977
Deal with known organizations	.075(.060)	1.078
Regularly change passwords	.172(.042)***	1.188
Regularly delete emails	.372(.076)	1.450
Constant	-4.290(.147)*	.014
-2 log likelihood	15130.704	
Model X^2	1921.262***	
Nagelkerke R^2	.192	
N	11,473	

*P<.05, ** P<.01, *** P<.001

Table 18: Summary of Hypotheses and Results

Hypotheses	**Results**
Demographics	
$H1_a$: Older individuals have a higher likelihood of experiencing online fraud victimization than younger individuals.	Partially supported
$H1_b$: Gender is associated with online fraud victimization (Studies are inconsistent in terms of directionality, suggesting that this relationship is crime-specific and cannot be predicted	Partially supported
$H1_c$: More highly educated people have a higher likelihood of online fraud victimization.	Partially supported
$H1_d$: Greater income is associated with a higher likelihood of online fraud victimization.	Rejected
Perceptions of risk	
H2: Those with higher risk perceptions of online crime are less likely to do online shopping, banking and networking, and therefore are less likely to experience online fraud victimization.	Rejected
Online routine activities	
$H3_a$: People who use the internet for online banking more frequently are at higher risk of online fraud victimization.	Supported
$H3_b$: People who frequently use the internet for booking or reservations are at higher risk of online fraud victimization.	Supported
$H3_c$: People who frequently use the internet to purchase goods or are at higher risk of online fraud victimization.	Partially supported
$H4_a$: People who protect their privacy by regularly changing passwords are at lower risk of online fraud victimization.	Rejected
$H4_b$: People who protect their privacy by regularly deleting e-mails are at lower risk of online fraud victimization.	Rejected

CHAPTER FIVE: DISCUSSION AND CONCLUSION

The results of this research suggest that online victimization is much more complicated than expected. The main goal of this thesis was to answer the following questions: (1) Is everyone equally likely to be a target of online crime? and (2) What factors might lead to online victimization? This research was successful in answering those two research questions. The results provided support for Routine Activities Theory (RAT) and its online extension as proposed by Eck and Clarke (2003) as a framework to study online crime victimization. Moreover, this thesis also produced valuable knowledge about what could increase online identity crime victimization among the Canadian population.

RAT posits that a crime will occur in the presence of motivated offenders, the absence of effective guardians, and the availability of suitable targets in the same time and space (Choi et al. 2016; Jackson et al. 2006; Reyns 2013, 2015). Further, activities that formerly required one to be physically present at a specific location, often at a specific time, can now be undertaken regardless of the individual's physical location or time of day, due to the crime being committed online. The extension to RAT by Eck and Clarke (2003) proposed substituting a geographical place by a network suggests that routine activities online will increase online crime victimization.

In this research, I examined what effect online routine activities have on identity theft, consumer fraud and phishing victimization. I also incorporated findings from previous literature that suggest that demographics and perceptions of risk will affect routine activities and which in turn affect victimization.

I found that phishing victimization was best explained by RAT (R^2=.19). This is consistent with Reyns's (2015) finding. His results indicate that RAT best explains phishing victimization compared with hacking and malware victimization. The same number of online routine activities affects consumer fraud and phishing victimization. However, the results suggest that 6% of consumer fraud victimization was explained by demographics, perceptions of risk, and online routine activities (R^2=.06). Further, my results show that online routine activities had the least impact on identity theft victimization (R^2=.034), suggesting that there are other important factors that need to be examined in future research. In the following section, I will review the results in greater detail and explain how RAT is applicable to online identity theft, online consumer fraud, and phishing victimization.

Summary of Results

Is everyone a potential target of online crime? Only education had a consistent statistically significant effect on victimization when routine activities were included in the models. As predicted by previous research (Anderson 2006; Holtfreter et al. 2006; Reyns 2013), when it comes to identity theft and phishing those with higher education are targeted and victimized more often compared with those with lower education. It could be the case that having higher education also affects other aspects of people's lives, which also promotes higher rates of victimization. For example, from the correlation matrix (Appendix A), it is evident that higher education is positively correlated with higher income. This means that those with higher education also have more money to spend shopping online, which makes them attractive targets for offenders who commit identity theft and phishing victimization. Another explanation could be that higher education is linked to increased computer use. Computers are more necessary for

non-labour employment and study. Therefore, it is the time spent online is what makes them more vulnerable to victimization. However, those with higher education were shown to less often be victims of consumer fraud, which is contradictory to past research findings (Anderson 2006; Holtfreter et al. 2006). One possible explanation is that those with lower education (and lower income) try to find "good deals" online, for example from E-bay or Kijiji, and fall victim to consumer fraud where the goods they ordered did not arrive or were not as described. For identity theft, education is the only demographic variable that had an influence on victimization when controlling for routine activities. However, for phishing and consumer fraud there are other demographic factors affect victimization. In both cases, men are more likely to be victims of phishing and consumer fraud compared with women.

Previous research led me to hypothesize that there will be a difference between men and women, but the literature does not provide a consensus on which gender is most at risk (Holtfreter et al. 2006; Menard and Covey 2016). Men are more likely to engage in online activities. At the same time, men are less likely to change passwords regularly, and men are less likely to delete emails on a regular basis to protect their privacy compared with women (see Appendix A). Moreover, men are less likely to be concerned with online shopping and banking, indicating that they are less cautious compared with women. These factors could be a part of the reason why men are more likely to be victimized compared with women.

Income appeared to be related to phishing until routine activities were included in the model. This finding suggests that the effect of income is explained away by routine activities. In other words, income does not have a direct impact on phishing victimization. Those with higher income engage in more online routine activities, and the increased engagement is what consequently leads to phishing victimization. Contrary results were found when examining

consumer fraud victimization. The relationship between income and consumer fraud was revealed when routine activities were taken into account. It was found that as income increases consumer fraud victimization decreases. This suggests an explanation similar to the relationship between education and consumer fraud—it is possible that those with lower income are putting themselves at higher risk to save money online.

Age has a unique relationship with two of dependent variables: online consumer fraud and phishing victimization. Age had a negative relationship with consumer fraud victimization (where other demographics and perceptions of risk were controlled for). This means that younger people are more likely be victims of consumer fraud. However, when routine activities were taken into account, the relationship between age and victimization was reduced below statistical significance. Therefore, the initial relationship is spurious. Younger people are more likely to be victims of consumer fraud because they engage in more online activities. In terms of phishing victimization similar relationships were initially observed. Younger people were at higher risk of victimization when the analysis controlled for other demographics (gender, income, and education). However, when online routine activities were controlled for, the relationship was reversed. Older people were more likely to be phishing victims. This could mean that the higher victimization for younger people is explained by their increased online presence.

Perceptions of risk associated with online banking and online shopping have very different relationships with online victimization. It was found that perceptions of risk associated with *online banking* do not affect online victimization, whereas, perceptions of risk associated with *online shopping* are associated with all three types of victimization. People with higher perceptions of risk associated with online shopping were found to be more likely victims of phishing, consumer fraud, and identity theft victimization. One possible explanation is that those

who had previously experienced online victimization where they suffered monetary loss were more suspicious of online shopping. Prior victimization may shape subsequent apprehension.

To answer the second research question (What factors might lead to online victimization?), I turn to describe which online routine activities might lead to online victimization. Routine Activities Theory suggests that those who have greater involvement in online activities are more likely to be victimized because they expose themselves more often to potential offenders online. My research found support for this component of the theory. Using the internet for banking, making reservations or bookings, and belonging to online social network websites increased online identity theft, consumer fraud, and phishing victimization. In addition, using the internet for purchasing goods or services or using online chat services increased victimization for consumer fraud and phishing, but not for identity theft. This is interesting because personal information can be stolen during online interactions such as online shopping and chatting. It would be intriguing to explore why these two online activities are not associated with identity theft, whereas banking, making online reservations and social networking are associated with online identity theft.

RAT also suggests that those with less online target hardening and less online guardianship will be more likely to be victimized (Choi 2010). Target hardening is the ability of people to limit access to their personal information which will weaken their online visibility and accessibility to potential offenders. Users can protect themselves by not using unreliable websites and not posting information online. Online guardianship refers to the measures people can take to protect their privacy online. Such security measures may include changing passwords and installing anti-hacking software (Choi 2010; Reyns 2015).

I hypothesized that those who take target hardening measures ($H3_a$, $H3_b$) and attempt to increase online guardianship ($H4_a$, $H4_b$) will be less likely to be victimized online. However, these results suggest the opposite. It has been found that those who deal with known websites, enter misleading information online, regularly change their passwords, and delete emails are actually more likely to be victims of online consumer fraud and phishing. Similar results were obtained by Reyns (2015) who explored phishing, hacking, and malware infection victimization. He also found that those who change passwords and enter misleading information are at higher risk of being victimized. He suggests that it could be because those who partake in those activities do so because of other online activities that might be risky. I argue that there are other *intervening* factors that explain these relationships. Also, because temporal order is not determined, it is possible that victimization happened before the routine activities were adopted by people. In other words, individuals started entering misleading information online and changing passwords after they were victimized. For example, people who download from risky websites or access online gambling websites are more likely to enter misleading information and also change passwords, but at the same time they are more likely to become victims of online consumer fraud and phishing. This is not the case for identity theft. In the case of identity theft, target hardening and increasing online guardianship (dealing only with known websites, entering misleading information online, regularly changing passwords, and deleting emails) neither increases nor decreases victimization.

This study found some important factors that lead to identity theft, consumer fraud, and phishing victimization, such as education and perception of risk associated with online shopping. This study also found that certain online routine activities result in a higher probability of victimization (online banking and making online bookings and reservations). However, the

variables examined in this thesis could be refined through enhanced measures. There are still many unknown causes to identity theft, consumer fraud, and phishing victimization. The unexplained results raised questions for further research.

It is important to mention that there are four advantages to using secondary data analysis. First, it is both time- and cost-effective. Second, the data used are of high quality. They were collected by researchers from Statistics Canada. Third, the General Social Survey (GSS) is a national survey, where the sample was designed to be representative of the Canadian population with the exceptions mentioned in the methodology chapter. In addition, the sample size is large and provides an opportunity for sub-group analyses. Fourth, because the secondary researcher spends no time on data collection, time can be devoted to data analysis and interpretation of results (Bryman, Teevan, and Bell 2009). But like all research, secondary data analysis also has limitations. The next section will highlight the limitations of these data.

Limitations

Although there are clear benefits to using the General Social Survey, the survey also has four shortcomings. First, in order to measure the variables, I had to rely on the available survey items. Some important information might have been lost as a result of the survey questions I used to measure the variables. For example, online routine activities were measured using nine items and none of them captured actual risky on-line routine activities, such as illegal downloading or gambling.

The second limitation is that variables that stem from other theories could have effects on online victimization. It is a limitation in this research because those variables are not accounted

for or tested. In the next section I discuss how Self-Control Theory could be also because applicable to online victimization.

The third limitation is that the data for the General Social Survey's Cycle 23 were collected eight years ago. The year 2009 was the year when victimization was a theme for the GSS, and when specifically asked questions about online victimization. It could be that different results would be found if these data were more recent. Technology is rapidly changing, and in the last eight years significantly more people have gained access to the internet. According to The World Bank (n.d.), in 2009, 80.3% of Canadians had access to the internet at home using any device type and connection, whereas in 2015, 22.5% had access.[10] Unfortunately, there are no more recent Canadian data currently available.

The fourth limitation is that that the GSS is an annual survey, it is still a cross-sectional survey. The questions used in the survey change from year to year depending on the theme of the survey. The use of a cross-sectional survey limits the ability to determine directionality and temporal order. Improved knowledge of causal ordering would be helpful to explain the unique findings from this study. A longitudinal research design could solve this problem. This will be discussed in greater detail in the following section where I propose directions for future research.

Research Implications

These limitations promote a few suggestions for future research on online identity crime victimization. I argue that research needs to develop new methodologies to better measure online

[10] Retrieved on March 20, 2017 (http://data.worldbank.org/indicator/IT.NET.USER.P2?locations=CA)

victimization and online routine activities. The goal of future research should also be to help further develop the theoretical framework of online victimization.

More specifically, there should be incorporation of a broader set of variables that reflect other online routine activities. For example, future research should include actual time spent online and risky online behaviours. In addition, more control variables should be included in future studies. Those could be other demographic factors that were not included in the analysis, such as marital status and ethnicity. Previous research by Weitzer and Kubrin (2004) found that perceptions of risk decrease with age and then increase again for older respondents. My study found some support for their finding. When routine activities were introduced, older people were more likely to be victimized. Future research should take this finding into account and should examine age as a curvilinear effect. Reyns (2015) found that being non-white was associated with increased phishing and hacking victimization. Additionally, he found that married people experience lower hacking victimization rates but higher malware victimization rates. Those two variables, ethnicity and marital status, could provide a more encompassing understanding on how Routine Activities Theory can be applicable to identity theft and consumer fraud victimization. He states that future research should be "working toward standard measures [that would] also require a crime- or victimization- specific approach to measurement, as suggested by opportunity theory" (Reyns 2015: 408)

Also, other theoretical perspectives should be considered when examining online identity theft, consumer fraud, and phishing. For example Reyns (2015), suggests using self-control theory when examining online crime victimization. Gottfredson and Hirschi (1990) theorized that those with low self-control have a preference for risky behavior and for immediate gratification. Previous studies found support for the argument that victims with low self-control

are more likely to experience online victimization (Holtfreter et al. 2008; Reyns et al. 2013; van Wilsem 2011, 2013). Holtfreter et al. (2008) used survey items that measured financial risk-taking. The two measures asked whether respondents enjoyed "making risky financial investments now and then" and whether they agree with the statement: "I don't mind taking chances with my money, as long as I think there's a chance it might pay off." Holtfreter et al. (2008) argue that these two measures of low-self control are more reliable and yield less measurement error because they are context-specific as opposed to global indicators of low self-control. Using these context-specific measures could be very beneficial in studying online identity theft, consumer fraud, and phishing victimization.

The best possible way to research online victimization and test whether a theoretical framework can explain such victimization is to create and administer a new targeted survey. If funds were sufficient, the survey should be longitudinal. Longitudinal analysis would help us further understand directionality when examining the applicability of Routine Activities Theory. Longitudinal research design, or more specifically a *prospective panel design*, involving data collection for each variable at two or more time periods would be most useful. In addition, the respondents in the research should remain the same from one time period to the next (e.g., panel data). As well, longitudinal research design would provide the opportunity to analyze data between and among time periods (Menard 1991).

My results suggest that higher perceptions of risk actually increase victimization. This is an interesting relationship that could be explored using a longitudinal design. It would be possible to determine whether perceptions of risk were heightened for some groups prior to victimization, or are perceptions of risk elevated following victimization. In longitudinal analysis, perceptions of risk and routine activities would be initially measured, and the same

respondents would be asked the same questions after a number of years. The change in perceptions of risk and victimization could be measured, and temporal order could be established. Other factors that could be measured are target-hardening activities. My findings show that people who frequently change their online passwords and enter misleading information to protect their identity are more likely to be victimized online. Two possible explanations are that victimization occurred prior to those routine activities, or that the victims of online crime also engaged in risky behaviour. The prospective panel design could determine whether these claims are supported by data or whether other factors explain this finding.

Policy Implications

In Canada in 2007 Bill C-27 was introduced. Its purpose was to amend the *Criminal Code* to include identity theft as a criminal offence. Prior to this bill, identity theft was not considered a crime. Theft and fraud were not considered a crime when there was no loss or damage to physical property. Bill C-27 was meant to make the possession of personal information an offence under the Code. Bill C-27 was enacted and, as a result Section 402.2 of the *Criminal Code* was implemented in 2009.

Section 402.2 (1) states that "everyone commits an offence who *knowingly obtains or possesses* another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence" (Justice Laws 2017).[11] Section 402.1 states that personal information and biological or physiological information, which includes name, address, date of birth, written signature, electronic signature, digital signature,

[11] Retrieved on March 20, 2017 (http://laws-lois.justice.gc.ca/eng/acts/C-46/page-86.html?txthl=402.2#s-402.1)

user name, credit card number, debit card number, financial institution account number, passport number, Social Insurance Number, health insurance number, and driver's licence number. The punishment for this offense is imprisonment not longer than five years or a summary conviction (Justice Laws 2017). If an offender is found guilty of *using* someone else's identity information, that person is liable to punishment of ten years imprisonment (Justice Laws 2017). Furthermore, Section 342(3) governs the offence of fraudulently possessing, using or trafficking in credit card and debit cards data could result in ten years imprisonment (Parliament of Canada n.d.). This means that it is now a criminal offence not only to use someone else's identity to commit a crime but also to possess someone else's personal information.

Canada's anti-spam legislation makes it illegal to use false or misleading representation using any means such as social networking, websites, emails, and any other current or future online platforms. Since July 1, 2014, this law has enabled the Competition Bureau to address false or misleading representations and deceptive marketing practices in the electronic marketplace, and to address misleading electronic messages and website content (Competition Bureau 2015).

Despite the recent legislative changes, privacy advocates and consumer groups claim that there is still a need for a "comprehensive framework involving law enforcement agencies, consumer organizations, businesses and financial institutions that would address the broader issues associated with identity theft (e.g., strengthening and enforcing data protection laws, consumer protection and victim redress and public education)" (Parliament of Canada n.d.).[12] The current laws are incomplete at best: only about 5% of online crime is reported and an even

[12] Retrieved on March 20, 2017 (http://www.bdp.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=C27&Parl=39&Ses=2&Language=E)

smaller portion of online offenders are caught (Competition Bureau 2017).[13] The internet has made it easy for offenders to stay anonymous and avoid detection. I argue that the focus of future policies, laws and practices needs to be on preventative measures that target potential victims and are designed to reduce victimization.

Two Canadian organizations work to promote awareness and propose preventative measures to online crimes. The Consumer Measures Committee publishes annually the *Canadian Consumer Handbook* (2017), to inform consumers about potential victimization. The handbook includes prevention measures for online users and procedures to follow in case of victimization. Identity theft, consumer fraud and phishing are included in the *Handbook*.

The Competition Bureau of Canada, in 2004 established the Fraud Prevention Month to raise awareness about the impact of fraud and to promote ways in which Canadians can protect themselves. The Competition Bureau also released a reference book titled *The Little Black Book of Scams* (2012) to provide information to consumers and business about common scams.

More of these awareness and prevention measures are needed to reduce online identity theft, consumer fraud, and phishing. This study found that frequent online users are the ones who are most at risk of victimization and prevention programs need to be tailored specifically for those people. These programs should encourage people to take more precautions especially when using online shopping or online banking. In addition, this study found that those who use social network sites are at a much higher risk of victimization than those who do not. Prevention programs should combine their efforts with popular social network sites to promote the safe use of those websites and encourage users not to share personal information online. As well,

[13] Retrieved on March 20, 2017 (http://www.bdp.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=C27&Parl=39&Ses=2&Language=E)

prevention measures should also target men, since they, compared with women, are more likely to be victims of online crime.

Conclusion

My thesis has generated findings of value to the research community. First, it has shown that the extension of online Routine Activities Theory by Eck and Clarke (2003) is applicable to online identity theft, consumer fraud, and phishing victimization. Second, it has shown that key demographic factors and specific online activities are more likely to result in victimization. Stemming from these results, I have made suggestions for future studies and for improving policies and laws. Finally, this research adds a Canadian perspective since little research has been conducted in regards online victimization in the Canadian context.

Appendix A: Correlation Matrix of Variables Used in the Study

	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.	18.
1. Consumer fraud	1																	
2. Identity theft	.372*	1																
3. Phishing	.122*	.101*	1															
4. Age	-.083*	.013	.000	1														
5. Gender	.030*	-.002	.138*	-.037*	1													
6. Education	-.022	.063*	.204*	-.041*	-.009	1												
7. Income	-.047*	.030*	.153*	.239*	.286*	.388*	1											
8. Risk of Banking	.000	.027	-.007	.172*	-.026*	.029*	.057*	1										
9. Risk of Shopping	.036*	.065*	-.013	.149*	-.063*	.010	.034*	.590*	1									
10. Online banking	.065*	.064*	.185*	-.097*	.016	.236*	.182*	-.256*	-.010*	1								
11. Online booking	.036*	.076*	.227*	.005	.045*	.309*	.267*	-.085*	-.090*	.367*	1							
12. Online shopping	.082*	.026	.269*	-.088*	.102*	.234*	.195*	-.115*	-.190*	.352*	.486*	1						
13. Online social networking	.085*	.038*	.090*	-.471*	-.078*	-.068*	-.220*	-.145*	-.122*	.170*	.081*	.145*	1					
14. Online chatting	.085*	-.003	.095*	-.372*	.044*	-.039*	-.172*	-.085*	-.075*	.102*	.027*	.099*	.330*	1				
15. Entering misleading information	.092*	.021	.176*	-.263*	.027*	.036*	-.054*	-.045*	-.047*	.104*	.085	.155*	.205*	.246*	1			
16. Dealing with known organization	-.063*	.005	.043*	.056*	-.041*	.119*	.115*	.039*	.054*	.098*	.085*	.062*	-.015	-.044*	-.028*	1		
17. Changing passwords	.027	.010	.059*	-.089*	-.032*	.023*	.016	.002	.015	.095*	.059*	.067*	.078*	.046*	.035*	.082*	1	
18. Deleting emails	.016	.003	.084*	.017	-.053*	.055*	.059*	.022*	.045*	.088*	.089*	.075*	.031*	-.014	.036*	.114*	.095*	1

REFERENCES

Anderson, Keith B. 2004. *Consumer Fraud in the United States: An FTC Survey.* Washington: Federal Trade Commission.

Anderson, Keith B. 2006. "Who Are the Victims of Identity Theft? The effect of demographics." *Journal of Public Policy and Marketing* 25: 160–171.

Anderson, Keith B. 2007. *Consumer Fraud in the United States: The Second FTC Survey.* Washington: Federal Trade Commission.

Anderson, Keith B. 2013. *Consumer Fraud in the United States, 2011. The Third FTC Survey.* Washington: Federal Trade Commission.

Bartel-Sheehan, Kim. 1999. "An investigation of gender differences in on-line privacy concerns and resultant behaviors." *Journal of Interactive Marketing* 13: 24-38.

Berg, Sara E. 2009. "Identity Theft Causes, Correlates, and Factors: A Content Analysis." Pp. 225-250 in *Crimes of the Internet*, edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, New Jersey: Pearson.

Bethlehem, Jelke. 2009. *Applied Survey Methods - A Statistical Perspective.* New Jerzey: Wiley.

Bhatnagar, Amit, Sanjog Misra, and H Raghav Rao. 2000. "On Risk, Convenience, and Internet Shopping Behavior." *Communications of the ACM* 43: 98-105.

Bryman, Alan, James J. Teevan, and Edward Bell. 2009. *Social Research Methods.* Second Edition. Oxford, NY: Oxford University Press.

Caswell Stephen. 2000. "Women Enjoy E-Shopping Less Than Men." *Ecommerce Times,* January 11. Retrieved November 15, 2016 (http://www.ecommercetimes.com/story/2179.html)

Choi, Kyung-shick. 2008. ''Computer Crime Victimization and Integrated Theory: An Empirical Assessment.'' *International Journal of Cyber Criminology* 2: 308-333.

Choi, Kyung-Shick. 2010. *Risk Factors in Computer-Crime Victimization*. El Paso: LFB Scholarly Publishing LLC.

Choi, Kyung-shick, Kyungseok Choo, and Yong-eun Sung. 2016. "Demographic Variables and Risk Factors in Computer-Crime: An Empirical Assessment." *Cluster Computing* 19(1): 369-377.

Cohen, Lawrence E. and Marcus Felson. 1979. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44(1): 588-608

Competition Bureau. 2015. *Canada's Anti-Spam Legislation Enforcement Agencies Sign Memorandum of Understanding*. Retrieved March 20, 2017 (http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/03647.html.)

Competition Bureau. 2017. *Fraud Facts 2017 — Recognize, Reject, Report Fraud*. Retrieved March 15, 2017 (http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/04201.html)

Competition Bureau. 2012. *The Little Black Book, the Canadian Edition.* Retrieved March 15, 2017 (http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/Little-Black-Book-Scams-e.pdf/$FILE/Little-Black-Book-Scams-e.pdf)

Consumer Measures Committee. 2017. *Canadian Consumer Handbook.* Retrieved March 15, 2017 (www.consumerhandbook.ca/)

Cossman, Jeralynn S., and Nicole E. Rader. 2011. "Fear of Crime and Personal Vulnerability: Examining Self-Reported Health." *Sociological Spectrum* 31(2): 141-162.

Cox, Raymond W., Terrence A. Johnson and George E. Richards. 2009. "Routine Activity Theory and Internet Crime." Pp. 302-316 in *Crimes of the Internet,* edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, New Jersey: Pearson.

Eck, John E. and Ronald V. Clarke. 2003. "Classifying Common Police Problems: A Routine Activity Approach." *Crime Prevention Studies* 16: 7-39.

Felson, Marcus. 1998. *Crime and Everyday Life.* (2 ed.). Thousand Oaks: Pine Forge Press.

Ferguson, Kristin M. and Charles H. Mindel. 2007. "Modeling Fear of Crime in Dallas Neighborhoods: A Test of Social Capital Theory." *Crime and Delinquency* 53: 322-349.

Ferraro, Kenneth F. 1995. *Fear of Crime: Interpreting Victimization Risk.* Albany: State University of New York Press, Albany.

Finch, Emily. 2007. ''The Problem of Stolen Identity and the Internet.'' Pp. 29-43 in *Crime Online,* edited by Yvonne Jewkes. Devon, UK: Willan.

Forsythe, Sandra M. and Bo Shi. 2003. "Consumer Patronage and Risk Perceptions in Internet Shopping." *Journal of Business Research* 56: 867–875.

Garbarino, Ellen, and Michal Strahilevit. 2004. "Gender Differences in the Perceived Risk of Buying Online and the Effects of Receiving a Site Recommendation." *Journal of Business Research* 57: 768-775.

Gottfredson, Michael R. and Travis Hirschi. 1990. *A General Theory of Crime.* Stanford, CA: Stanford University Press.

Grabosky, Peter and Russell Smith. 2001. ''Telecommunication Fraud in the Digital Age: The Convergence of Technologies.'' Pp. 29-43 In *Crime and the Internet,* edited by David Wall. New York: Routledge.

Hankun, He, Li Yafang, Huang Xuemei, and Fan Jing. 2016. “A Comparative Study of China and US Users' Acceptance of Online Payment.” *13th International Conference on Service Systems and Service Management (ICSSSM)* 1-6.

Harrell, Erika. 2015. “Victims of Identity Theft, 2014.” *Bureau of Justice Statistics* NCJ 248991.

Hindelang, Michael J., Michael R. Gottfredson, and James Garofalo. 1978. *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Cambridge, MA: Ballinger Publishing.

Holm, Eric. 2012. "Responding to Identity Crime on the Internet." *International Journal of Cyber-Security and Digital Forensics* 1(2): 67-75

Holt, Thomas J. 2013. “Crime On-line.” Pp. 3-26 in *Crime On-line*, 2nd ed, edited by Thomas J. Holt. Durham, North Carolina: Carolina Academic Press.

Holt, Thomas J. and Adam M. Bossler. 2013. “Examining the Relationship between Routine Activities and Malware Infection Indicators.” *Journal of Contemporary Criminal Justice* 29: 420-436.

Holt, Thomas J. and Michael G. Turner. 2012. “Examining Risks and Protective Factors of On-Line Identity Theft.” *Deviant Behavior* 33(4): 308-323.

Holtfreter, Kristy, Shanna Van Slyke, and Thomas G. Blomberg. 2005. ‘‘Sociolegal Change in Consumer Fraud: From Victim-Offender Interactions to Global Networks.’’ *Crime, Law and Social Change* 44:251-75.

Holtfreter, Kristy, Michael D. Reisig, and Thomas G. Blomberg. 2006. “Consumer Fraud Victimization in Florida: An Empirical Study.” *St. Thomas Law Review* 18: 761-789.

Holtfreter Kristy, Michael D. Reisig, and Travis C. Pratt. 2008. “Low Self-Control, Routine Activities, and Fraud Victimization.” *Criminology* 46(1): 189-220.

Jackson, Linda A., Alexander von Eye, Frank A. Biocca, Gretchen Barbatsis, Yong Zhao, and Hiram E. Fitzgerald. 2006. “Does home Internet use influence the academic performance of low-income children?” *Journal of Developmental Psychology* 42(3): 429-435.

Justice Laws Website. 2017. Criminal Code R.S.C., 1985, c. C-46. Retrieved on March 20, 2017 (http://laws-lois.justice.gc.ca/eng/acts/C-46/page-86.html?txthl=402.2#s-402.1)

Kanan, James W. and Matthew V. Pruitt. 2002. "Modeling Fear of Crime and Perceived Victimization Risk: The (in)Significance of Neighborhood Integration." *Sociological Inquiry* 72: 527-548.

Kay, Fiona M., and John Hagan. 1999. “Cultivating Clients in the Competition for Partnership: Gender and the Organizational Restructuring of Law Firms in the 1990s”. *Law Society Review* 33(3): 517-555.

Kehoe, Colleen, Jim Pitkow, and Kimberly Morton. 1998. Eighth WWW user survey. Retrieved November 15, 2016 (http://www.cc.gatech.edu/gvu/user_ surveys/survey-1998)

Knoke, David and George W. Bohrnstedt. 1994. *Statistics for Social Data Analysis* 3rd ed. Itasca, Illinois: F.E. Peacock Publishing.

Koops, Bert-Jaap and Ronald Leenes. 2006. ‘‘Identity Theft, Identity Fraud and/or Identity-Related Crime: Definitions Matter.’’ *Datenschutz und Datensicherheit* 30: 553-56.

Kruger, Daniel J., Peter Hutchison, Matthew G. Monroe, Thomas Reischl, and Susan Morrel Samuels. 2007. "Assault Injury Rates, Social Capital, and Fear of Neighborhood Crime." *Journal of Community Psychology* 35:483-498.

Levi, Michael. 2001. “Between the Risk and the Reality Falls the Shadow: Evidence and Urban Lengends in Computer Fraud.” Pp. 44-58 In *Crime and the Internet,* edited by David Wall. New York: Routledge.

Liebermann, Yehoshua and Shmuel Stashevsky. 2002. "Perceived Risks as Barriers to Internet and E-Commerce Usage." *Qualitative Market Research: An International Journal* 5(4): 291-300.

Mazowita Benjamin and Mireille Vézina. 2014. “Police-reported cybercrime in Canada, 2012.” *Juristat.* Statistics Canada Catalogue no.85-002-X.

McGarrell, Edmund F., Andrew L. Giacomazzi, and Quint C. Thurman. 1997. “Neighborhood Disorder, Integration, and the Fear of Crime.” *Justice Quarterly* 14: 233-250.

McGrath, Shelly A. and Stacilyn Chananie-Hill. 2011. “Individual-Level Predictors of Perceived Safety: Data from an International Sample.” *Sociological Focus* 44(3): 231-254.

McNally, Megan M. and Graeme R. Newman. 2008. ‘‘Editors’ Introduction.’’ Pp. 1- 8 in *Perspectives on Identity Theft,* edited by M. M. McNally and G. R. Newman. Monsey, NY: Criminal Justice Press.

Menard, Scott. 1991. “Longitudinal Research.” *Sage University Paper Series on Quantitative Applications in the Social Sciences,* 07-076. Newbury Park, CA: Sage.

Menard, Scott and Herbert C. Covey. 2016. “Age and Gender Variations in the Victimization-Offending Relationship in a National Sample, Ages 11–88.” *Victims & Offenders* 11(3): 355-372.

Milne, George R. 2003. "How Well Do Consumers Protect Themselves from Identity Theft?" *Journal of Consumer Affairs* 37(2): 388-403.

Milne, George R., Andrew J. Rohm, and Shalini Bahl. 2004. "Consumers' Protection of Online Privacy and Identity." J*ournal of Consumer Affairs* 38(2): 217-232.

Miyazaki, Anthony D., and Ana Fernandez. 2001. “Consumer Perceptions of Privacy and Security Risks for Online Shopping.” *Journal of Consumer Affairs* 35:27–44.

Moore, Elizabeth and Michael Mills.1990. “The Neglected Victims and Unexamined Costs of White-Collar Crime.” *Crime and Delinquency* 36(3): 408-418

Murray, Keith B. 1991. “A test of services marketing theory: Consumer Information Acquisition Activities.” *Journal of Marketing* 55: 10-25.

Newman, Graeme R. 2008. “Identity Theft and Opportunity.” Pp. 9-31 in *Perspectives on Identity Theft,* edited by M. M. McNally and G. R. Newman. Monsey, NY: Criminal Justice Press.

Parliament of Canada. N.d. Bill *C-27: An Act to amend the Criminal Code (Identity Theft and Related Misconduct)*. Retrieved March 20, 2017 (http://www.bdp.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=C27&Parl=39&Ses=2&Language=E#fn28).

Pratt, Travis C., Kristy Holtfreter, and Michael D. Reisig. 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.

Quinn, Ben and Charles Arthur. 2011. “PlayStation Network Hackers Access Data of 77 Million Users.” *The Guardian*, April 26. Retrieved April 18, 2017 (https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data#top_)

Reisig, Michael D., Travis C. Pratt, and Kristy Holtfreter. 2009. “Perceived Risk of Internet Theft Victimization : Examining the Effect of Social Vulnerability and Financial Impulsivity.” *Criminal Justice and Behaviour* 36(4):369-384.

Rengifo, Andres. F. and Amanda Bolton. 2012. "Routine Activities and Fear of Crime: Specifying Individual-Level Mechanisms." *European Journal of Criminology* 9(2): 99-119.

Reyns, Bradford W., Billy Henson, and Bonnie S. Fisher. 2011. “Being Pursued Online: Applying Cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization.” *Criminal Justice and Behavior* 38(11): 1149-1169.

Reyns, Bradford W. 2013. “Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses.” *Journal of Research in Crime and Delinquency* 50(2): 216-238.

Reyns, Bradford W. 2015. “A Routine Activity Perspective on Online Victimisation” *Journal of Financial Crime* 22(4): 396-411.

Reyns, Bradford W. and Billy Henson. 2016. “The Thief with a Thousand Faces and the Victim with None: Identifying Determinants for Online Identity Theft Victimization with Routine

Activity Theory.*" International Journal of Offender Therapy and Comparative Criminology* 60(10): 1119-1139.

Riek, Markus, Rainer Bohme, and Tyler Moore. 2016. "Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance*." IEEE Transactions on Dependable and Secure Computing* 13(2): 261-273.

Sampson, Robert J. and Janet L. Lauritsen. 1990. ''Deviant Lifestyles, Proximity to Crime, and the Offender-Victim Link in Personal Violence.'' *Journal of Research in Crime and Delinquency* 27: 110-39.

Smith, Russell G. 2010. ''Identity Theft and Fraud.'' Pp. 273-301 in *Handbook of Internet Crime,* edited by Yvonne Jewkes and Majid Yar. Devon, UK: Willan.

Smith, William R. and Marie Torstensson. 1997. "Gender Differences in Risk Perception and Neutralizing Fear of Crime: Toward Resolving the Paradoxes." *The British Journal of Criminology* 37(4): 608-634.

Statistics Canada. 2010. *General Social Survey - Victimization (GSS).* Retrieved September 27, 2016 (http://www23.statcan.gc.ca/imdb/p2SV.pl?Function=getSurvey&Id=49195)

The BBB. 2017. BBB National Top 10 Scams of 2016. Retrieved Feb 15, 2017 (http://www.bbb.org/mbc/programs-services/top-10-scams/top-10-scams-in-detail/).

The World Bank. N.d. *Internet users (per 100 people*). Retrieved March 20, 2017 (http://data.worldbank.org/indicator/IT.NET.USER.P2?locations=CA)

Titus, Richard. 2001. "Personal fraud and its victims." In *Crimes of Privilege: Readings in White-Collar Crime,* eds. Neal Shover and John Paul Wright. Oxford, UK: Oxford University Press.

Tomsich, Elizabeth A., Angela R Gover, and Wesley G Jennings. 2011. "Examining the Role of Gender in the Prevalence of Campus Victimization, Perceptions of Fear and Risk of Crime, and the Use of Constrained Behaviors among College Students Attending a Large Urban University." *Journal of Criminal Justice Education* 22(2): 181-202

Turner, Sarah, Heith Copes, Kent R. Kerley and Gary Warner. 2013. "Understanding Online Work-at-Home Scams through an Analysis of Electronic Mail and Websites." Pp. 81-108 in *Crime On-line*, 2nd ed, edited by Thomas J. Holt. Durham, North Carolina: Carolina Academic Press.

van Dijk, Jan, John van Kesteren, and Paul Smit. 2007. *Criminal Victimisation in International Perspective. Key Findings from the 2004-2005 ICVS and EU-ICS.* The Hague: WODC.

van Wilsem, Jonah. 2011. "Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization." *European Journal of Criminology* 8: 115-127.

Van Wilsem, Johan. 2013. "'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization." *European Sociological Review* 29(2): 168-178.

Vold, George B., Thomas J. Bernard and Jeffery B. Snipes. 2002. "Contemporary Classicism: Deterrence, Routine Activities, and Rational Choice." Pp. 196-208 in *Theoretical Criminology,* 5th ed., edited by George B. Vold, Thomas J. Bernard and Jeffery B. Snipes. NY, NY: Oxford University Press.

Wall, David S. 2001. "Cyber Crime and the Internet." Pp. 1-17 In *Crime and the Internet,* edited by David Wall. New York: Routledge.

Weinbach, Robert W. and Richard M. Grinnell. 2015. *Statistics for Social Workers* 9th ed. Upper Saddle River, New Jersey: Pearson.

Weitzer, Ronald, and Charis E. Kubrin. 2004. "Breaking News: How Local TV News and Real-World Conditions Affect Fear of Crime." *Justice Quarterly* 21(3): 497-520.

Yar, Majir. 2010. "Public Perception and Public Opinion About Internet Crime." Pp. 104-119 in *Handbook of Internet Crime,* edited by Yvonne Jewkes and Majid Yar. Devon, UK: Willan.