EXPLORING INTERNET USERS' VULNERABILITY TO ONLINE DATING FRAUD:

ANALYSIS OF ROUTINE ACTIVITIES THEORY FACTORS

by

Elena Victorovna Garrett

APPROVED BY SUPERVISORY COMMITTEE:

_____

Robert W. Taylor, Chair

_____

Robert G. Morris

_____

Nicole Leeper Piquero

Copyright 2014

Elena Victorovna Garrett

All Rights Reserved

EXPLORING INTERNET USERS' VULNERABILITY TO ONLINE DATING FRAUD: ANALYSIS OF ROUTINE ACTIVITIES THEORY FACTORS

by

ELENA VICTOROVNA GARRETT, BA

THESIS

Presented to the Faculty of

The University of Texas at Dallas

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE IN

CRIMINOLOGY

THE UNIVERSITY OF TEXAS AT DALLAS

December 2014

UMI Number: 1583633

All rights reserved

INFORMATION TO ALL USERS
The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript
and there are missing pages, these will be noted. Also, if material had to be removed,
a note will indicate the deletion.

UMI 1583633

Published by ProQuest LLC (2015). Copyright in the Dissertation held by the Author.

Microform Edition © ProQuest LLC.
All rights reserved. This work is protected against
unauthorized copying under Title 17, United States Code

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

ACKNOWLEDGMENTS

I would like to take this opportunity to express my gratitude to my husband, Michael Garrett, and the friendly staff of the Starbucks Coffee near my home for all they have done to advance my work on this project over the period of many long months. I would also like to express a special thanks to Dr. Robert Morris and Dr. Robert Taylor of the University of Texas at Dallas for their kind guidance through the process of data coding, analysis and writing of this thesis.

November 2014

EXPLORING INTERNET USERS' VULNERABILITY TO ONLINE DATING FRAUD:

ANALYSIS OF ROUTINE ACTIVITIES THEORY FACTORS

Publication No. _____

Elena Victorovna Garrett, MS
The University of Texas at Dallas, 2014

Supervising Professor: Dr. Robert W. Taylor

This paper investigates factors affecting susceptibility to online dating fraud victimization among a sample of 110 Internet users. Demographic factors such as age, income, marital status, employment, education, and country of residence are analyzed. Applicability of Routine Activities Theory to online scams is discussed, and variables such as computer use and proficiency, awareness of online scams, past experience with international dating, and interest in online dating are analyzed. Study differentiates between likelihood and severity of victimization. Findings indicate that factors most likely to affect vulnerability to online dating fraud victimization are: interest in online dating, interest in international dating, and years of computer use. Contrary to expectations, none of the demographic factors and none of the variables measuring level of awareness about online scams were statistically significant. For many variables, patterns of likelihood of victimization were different from the patterns of severity of victimization.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

CYBER CRIMES

Internet access is becoming as ubiquitous as cell phone access. People in countries with a high density of Internet access are gradually integrating their work and leisure activities with Internet use (Hunton, 2009). We interview potential employees, hold business meetings, file our taxes, schedule doctor appointments, and plan our vacations online. Many of our social activities have become more and more virtualized as well. We video chat with family members, text message our friends, read books, watch sporting events, and shop for Christmas gifts from our smartphones.

However, such close daily contact with the virtual environment can lull Internet users into a dangerous illusion of freedom without consequences (Durkin & Brinkman, 2009). We tend to forget that new, unknown attractions can open doors to new, unknown dangers. With growing use of the Internet among the population, criminally-minded individuals have found abundant opportunities to turn this Internet access boom to their advantage (Chang, 2008; Pratt, Holtfreter, & Reisig, 2010). The unique nature of these crimes presents criminologists with unique challenges. This thesis strives to add to our knowledge of these new developments in crime trends.

1.1 PURPOSE AND STRUCTURE OF THIS THESIS

The purpose of this thesis is to explore a particular type of Internet fraud called online dating fraud (or online dating scams), to analyze the features of the scam and the environment in which the scam occurs, and to investigate the factors affecting Internet users' vulnerability to such scams. Internet dating scams are a subcategory of a broad crime phenomenon called "crimes of persuasion" or "crimes of trust". Unlike most crimes, crimes of persuasion require the conmen to assume a fake identity, to use deception to evoke the victim's interest in personal interaction, and then to persuade the victim to voluntarily transfer something valuable (such as money, goods, or information) to the conmen while maintaining an appearance of legitimate interaction.

Chapter 1 provides a review of information about cyber-fraud and crimes of trust. It briefly touches upon the features of phishing and advanced fee scams, and suggests their connection to dating frauds. One specific type of dating fraud defined here as Travel Quest Online Dating Scam is then described and analyzed in detail.

Chapter 2 provides a brief review of the Routine Activities Theory (RAT) and the applicability of it to cyber environments. Two specific aspects of Travel Quest Online Dating Scams – victim targeting and persuasion - are discussed in light of RAT theoretical postulates to identity possible variables responsible for differences in users' vulnerability to this type of victimization.

Chapter 3 reviews previously collected information about demographic and situational factors affecting vulnerability to fraud victimization, identifies gaps or conflicting trends in current knowledge, and suggests possible explanations for these gaps. The author suggests implementation of two distinct measures of online victimization – the likelihood of victimization

and the severity of victimization - to improve theoretical analysis of factors affecting victimization susceptibility.

Chapter 4 describes the data collection method, the sample composition, and the variables collected. Collected data is then presented in the form of 2X2 tables and charts to demonstrate the patterns of likelihood and severity of fraud victimization among study participants.

Chapter 5 provides an overview of the results of the study, points out design weaknesses, and suggests directions for future research.

1.2 DEFINITION OF TERMS

As in any new area of study and exploration, terminology often changes to match industry-wide jargon. For instance, in this study the author uses the terms cybercrime, online fraud, and online fraud victimization, so that common concepts can be discussed. The prefix of "cyber" has now been introduced into our social vocabulary to mean almost anything "real" or "virtual" attached to a computer or network. We now refer to *cyber* (e.g., cyberchat, cybertalk, cybercafes, etc) as a prefix to meaning that the following word is computer, computer network, or Internet related (Taylor, Fritsch and Liederbach, 2015 p. 4). Hence, in this study, the terms "cyber", "digital", and "online" will be used interchangeably. The author will adopt the definition of *cybercrime* provided by Rege (2009), which includes "any crime (i) where [Internet Communication Technology] may be the agent/perpetrator, the facilitator/instrument, or the victim/target of the crime and (ii) which may either be a single event or an on-going series of events" (Rege, 2009, p. 495).

The author will also adopt the definition of the term *cybercriminals* as "offenders who (i) are driven by a range of motivations, such as thrill, revenge, and profit, (ii) commit and/or facilitate

cyber crimes, (iii) work alone, in simple partnerships, or in more formalized settings, and (iv) have varying levels of technical expertise." (Rege, 2009, p 495)

The term *cyber-fraud* will be defined as "any act of dishonesty or deception carried out through the use of the Internet (or computer technologies) that defrauds the public or any person out of property, money, valuable security or service" (Smyth, 2011, p.5) by providing misleading or deceitful information about the sender's intentions to honor agreements entered online, or the sender's intentions on how funds or valuables will be used (Smyth, 2011).

Other terms and definitions will be presented at the time of their discussion.

1.3 CRIMES OF TRUST (CoT)

The subject of victim cooperation or victim facilitation is important in understanding online victimization (Button, Lewis, & Tapley, 2009; Modic, 2012; Schoepfer & Piquero, 2009; Titus & Gover, 2001; Titus, 1999). As Rege's (2009) definition implies, there are many varieties of cybercrimes with varying degrees of interaction between the perpetrators and the victims. Some cybercriminals target electronic data, individual computer devices, or entire networks of computers (Flor, 2009; Gordon & Ford, 2006). These forms of online crimes require no direct interaction between the offender and the victim. Other types of online crimes fall within the definition of online fraud, but their objective can still be achieved with little or no personal contact with the victim. Examples of such frauds would be fraudulent Internet web sites, auction scams, and ransomewear (malicious software that threatens harm to the computer or stored data unless the user pays a fee or purchased special software to eliminate the threat). In these frauds, repeated contacts with the victim are usually not suitable or even desirable.

However, one category of computer crimes – crimes of trust (CoT) – are quite interesting due to two unique characteristics: 1) these crimes usually involve some form of deliberate direct contact with the victim; and 2) they often span a long period of time during which perpetrators are able to secure victims' trust and cooperation through various techniques of deception and persuasion (Menard, Morris, Gerber, & Covey, 2011). In the pre-Internet era, examples of CoT would be investment scams, as well as Ponzi schemes and other get-rich quick scams. Current examples of CoT would be the many manifestations of the advanced fee scams (Stabek, Brown, & Watters, 2009), FBI letter scams, etc.

Many overlapping categories and definitions of CoT are already in existence. In prior literature, these types of crimes have been described as personal fraud (Titus & Gover, 2001), consumer fraud (Langenderfer & Shimp, 2001), confidence frauds (Stabek et al., 2009), mass marketing fraud (Whitty, 2013b) and crimes focusing on persuasion (Freiermuth, 2011; Modic & Lea, 2013). The purpose of this chapter is not to untangle these overlapping definitions, but to describe common characteristics of this constellation of crimes.

A series of AARP surveys were performed in the 1990s to collect information about consumers' susceptibility to these frauds (Menard et al., 2011). However, more recent empirical studies are scarce. Menard et al. (2011) note that crimes of trust were initially classified as a subset of white collar crimes (WCC), and as such have been marginalized in the field of criminology, because many CoT frauds could not be classified either as "conventional" crimes or as "white collar crimes". More recently, CoT frauds are being investigated as a stand-alone category of crimes, perhaps as a result of the ongoing boom in online frauds.

The focus of this thesis is a sub-type of CoT known as online dating scams. However, before online dating scams can be discussed, two additional types of CoT will be presented: *phishing* and the *advanced fee scam*. These crimes are usually embedded within the fabric of the online dating scams and define the structure of the scam.

1.3.1 Phishing

Phishing is perhaps one of most prevalent online frauds in cyberspace (Smyth & Carleton, 2011). Phishing has been described as a "social engineering scam" that tricks Internet users into providing some kind of valuable data that the cyber criminals can use to perpetrate other online crimes (Longe, Mbarika, Kourouma, Wada, & Isabalija, 2009). Typical phishing attempts involve a legitimate looking email from a bank, university, or some other trusted institution. Perpetrators of phishing schemes attempt to lure or "hook" potential victims to fraudulent web sites for the purpose of gathering sensitive personal information. Often times, the email asks the user to immediately login into his or her account to avoid loss of access to the account or to avoid some kind of penalty. Once the user responds to this solicitation using the access link provided in the phishing email, their login and password are recorded by the online criminals, and their account becomes compromised (Abad, 2005; Nhan, Kinkade, & Burns, 2009; Wright & Marett, 2010). Other forms of phishing involve instant messages and fake profiles on social networking sites (Smyth & Carleton, 2011; Longe et al., 2009).

Although phishing in itself may not necessarily fit the definition of crimes of trust (CoT) because the phishing attempt rarely involves repeated or prolonged contacts with the victims, the data collected is usually used to perpetrate other types of offenses, such as identity fraud, credit card fraud, advanced fee fraud, etc (Abad, 2005; Longe et al., 2009; Stabek et al., 2009). This makes

phishing very important to the discussion of CoT. Perpetrators of online fraud often use phishing techniques (placing a legitimate-looking advertisement, creating a legitimate-looking online profile, or sending a legitimate-looking email) to identify potential victims (Isacenkova, Thonnard, Costin, Balzarotti, & Francillon, 2013; Longe et al., 2009; Whitty, 2013a). The apparent legitimacy of the original phishing communication allows those behind the fraud to obtain the victim's confidence. For this reason, and for the purpose of this paper, a phishing attempt will be included in the definition of crimes of trust (CoT).

1.3.2 Advanced Fee (419) Scams

One of the most commonly encountered crimes of trust is the *advanced fee scam*, otherwise referred to as the *Nigerian 419 scam, 419 scam* or *Nigerian scam*, where the user is repeatedly asked to provide financial assistance to enable some very desirable or lucrative event (called "the bait") to take place (Chang, 2008; Freiermuth, 2011; Longe et al., 2009; Nhan et al., 2009). Since its origination in 1989, the online email letter scheme has cost individuals and businesses an estimated one billion dollars globally. The scheme is named "419" after the relevant Nigerian criminal codes that are involved (Taylor et al., 2015, p. 137). The most common theme used to secure a victim's cooperation is the promise of the transfer of a large sum of money to the victim's account as a result of receiving an inheritance or a lottery win, or for assistance with a financial transaction (Freiermuth, 2011). The victim's trust and cooperation are commonly secured through an appeal to personal greed, although appeals to victims' honor and compassion are also common (Freiermuth, 2011; Langenderfer & Shimp, 2001; Modic, 2012; Nhan, Kinkade, & Burns, 2009). For the sake of brevity, the terms 419 scams, advanced fee scams, and

Nigerian scams will be used interchangeably, although 419 scams are only a subset of advanced fee scams.

Those engaged in 419 scams use phishing extensively. They also "spam," or use unsolicited commercial email and junk e-mail to reach a worldwide audience (Isacenkova et al., 2013; Longe et al., 2009). The fraud is conducted in two stages. The first stage utilizes different phishing "approaches" to secure the victim's attention. If the target responds to the initial solicitation, the fraud enters the second stage in which the target is asked to help the scammer overcome numerous financial or legal issues associated with obtaining the "prize" (Chang, 2008; Langenderfer & Shimp, 2001). The fraud is of long duration, often spanning months and even years of intensive email and phone communications between the victim and the offenders (Freiermuth, 2011). Sometimes several offenders take part in the scam, impersonating bank officials, attorneys, accountants, businessmen, and even government officials. In the process, the offenders provide victims with falsified passports, bank letters, and legal correspondence to make their story more convincing (Chang, 2008; Freiermuth, 2011).

The reason that discussion of advanced fee scams is important to the understanding of other types of crimes of trust (CoT), including the online dating scams discussed in the next section, is the ability to use the essential elements of the scam to create many different fraud scenarios (Freiermuth, 2011). The 419 scams appear on the list of the top ten Internet frauds, both in the number of consumers they reach and in the degree of financial damage they inflict on the victims (Button et al., 2009; Nikiforova & Gregory, 2013), underscoring their ability to lure in large numbers of victims year after year.

The remainder of this chapter will be devoted to the discussion of the structure of Online Dating Scams, the specific techniques that scammers use to locate their victims, information on the prevalence and costs of the crime, and a summary of information known about victims of this crime.

1.4 ONLINE DATING SCAMS

The *Online Dating Scam* (ODS) also sometimes referred to as Internet Romance Scam (IRS) is a type of online fraud in which individuals or organized criminal groups engage Internet users in online communication under the pretence of initiating a romantic relationship. The scam unfolds in form of frequent email and phone interactions between *the" bait"* (played by a scam perpetrator using a carefully constructed persona of a lonely person looking for a long-term relationship) and the intended victim – *the "target*" in the scam. During the course of the correspondence, the scam perpetrators utilize various deceptive claims to solicit money or items of value from their victims (Rege, 2009; Whitty, 2013b). Whitty & Buchanan (2012) claim that the ODS originated around 2007 – 2008, although a simple search on the Internet can locate online reports by victims of dating scams dated 2000 and 2001.

An ODS usually combines elements of phishing and the 419 advanced fee scam (Whitty, 2013b). Because the scammers frequently use fictitious names, documents, and identities, elements of identity theft are also a part of the fraud (Rege, 2009; Whitty, 2013b). The victim of an ODS initially encounters a phishing email or an online personal ad featuring the bait. If the victim is tempted by the phishing email to enter into a correspondence, the perpetrators proceed with setting up a scenario in which the target is asked to help the bait to overcome some obstacle preventing a personal meeting in real life. Although the bait in the scam is usually presented as a

picture of an attractive looking man or woman (Whitty, 2013a), the true lure used by the perpetrators is the promise of sexual and emotional fulfillment with a romantic partner committed to a long-term relationship. These types of fraud are significantly different from those criminal activities that solicit prostitution or sexual tourism in that the real intent of the perpetrator is not to provide an illegal activity – prostitution, but rather to lure the victim into a much more sophisticated relationship in order to defraud the victim of money. No sexual service is ever provided in the ODS.

1.4.1 Travel Quest Online Dating Scams

The name "dating fraud" is an umbrella term that can describe several different scenarios that use the pretence of a romantic relationship to trick Internet users into losing money. Among the possible scenarios are medical assistance scams and package reshipment scams that often originate from Nigeria and Ghana (Online Dating Safety Tips, n.d.), extortion scams (Foxworth, 2013), and so-called "gold-digger" scams that often originate from the Philippines (RomanceScamsNow, n.d.).

However, a large percentage of dating frauds feature scenarios where the "bait" in the scam purportedly prepares to travel to meet the victim in real life, and travel expenses become the reason for money solicitation (Foxworth, 2013; IC3, 2012; Steward, 2008). These scams are often operated by small independent criminal networks in Russia and Nigeria (Rege, 2009; Steward, 2008) and closely resemble advanced fee scams. Commonly described features of this type of dating fraud are 1) the use of phishing techniques and mass mailing tools to identify potential victims, 2) a long grooming process that creates an intense intimate connection between the bait and the victims, and 3) reliance on complex, multistep travel scenarios that involve

authority figures such as travel agents, doctors, Customs officers, and attorneys to create an illusion of legitimacy of the money requests, (Rege, 2009; Steward, 2008; Whitty, 2013a, 2013b). The term "*Travel Quest Online Dating Scams* (TQ-ODS)" will be used in this thesis to differentiate this type of scam and define its characteristics more precisely.

1.4.2 Differences between African and Russian dating scams

This type of scam is usually associated with Nigerian and Russian scammers (Rege, 2009). Although the characteristics of the scams are similar, there are some distinct differences between Russian online dating scams and African online dating scams. The African dating scams are more diverse, targeting both male and female Internet users, and frequently include requests for cashing of checks, transfer of money to bank accounts, or for re-shipment of goods (CyberStreetSmart.Org, 2011; Foxworth, 2013; Rege, 2009; Whitty, 2013a). The Russian dating scam perpetrators, although rarely mentioned in the literature, try to appeal primarily to male users, the typical bait is presented as a young Russian woman with a modest income and traditional family values, and the scam is typically limited to simple money transfer solicitations without attempts to involve the victim in money laundering (Smirnova, 2007; Steward, 2008). It is important to emphasize again that TQ-ODS are not connected with the Internet sex trade, online sexual victimization, or online prostitution. This type of scam is a sub-set of advanced fee scams, and stolen photos and fictitious identities are used to create the bait's online persona. The correspondence is carried out almost entirely through email communication, and money requests are made for seemingly legitimate travel preparations and expenses (Rege, 2009; Steward, 2008; Whitty, 2013a).

1.5 STAGES OF THE SCAM

Both Russian and Nigerian ODS are relatively long in duration and undergo a fairly standard set of development stages (Rege, 2009; Whitty & Buchanan, 2012; Whitty, 2013b).

1.5.1 Stage 1: Phishing for victims (targeting)

To be successful in making a profit off their efforts, the online dating scam perpetrators need to locate possible victims and approach those victims in a way that would not evoke suspicion. After all, ODS is a crime of persuasion, and the scammers can only persuade those Internet users who are willing to engage in a prolonged correspondence.

To establish contact with prospective victims, scammers utilize the same approaches as perpetrators of advance fee scams.

- Targeted baiting: Pictures of physically attractive "baits" are placed on dating sites (Rege, 2009; Whitty, 2013a). Internet users who respond to these fake profiles become the targets of the scam.
- Targeted spamming: Electronic databases of users (targets) involved in other scams can be purchased from underground marketplaces (Button et al., 2009). Alternatively, trip wires can be set up on dating sites to collect real-time information about site visitors. Those perpetrators lacking the skills to use spam email lists can simply select a certain number of profiles on the dating sites of their choice and initiate the first contact manually (Longe et al., 2009).
- Social networks phishing and spamming: Users of popular social networks, such as Facebook, can become targets of the scam (Hasib, 2009).

- Untargeted spamming: Various databases of email addresses can be purchased via underground marketplaces. Often those databases are stolen from large online sites such as Yahoo. Past and current users of those web sites become targets of the scam (Nhan et al., 2009).

Once their email addresses are selected, the unsuspecting targets receive an email message inviting them to a conversation, usually accompanied by an attractive picture of their prospective pen pal (Whitty, 2013a). The goal of the scammer at this stage is, first, to reach as many Internet users as possible and, second, to solicit a response to their "phishing" email or spam.

1.5.2 Stage 2: Grooming the victim

Those victims who respond to the initial email inviting them to a conversation become the primary focus of the scammer's attention. They start to receive frequent communications from their new pen pal in form of emails and instant messages (IMs). During this stage, the scammers attempt establish their credibility by presenting the "bait" as a person of strong moral values and good personal history (Koon & Yoong, 2013). Rege (2009) and Whitty (2013b) indicate that establishing a close personal bond with the victim is the main objective of the second phase of the scam. This bond is established through daily emails that repeatedly emphasize that the target is a very special person who is loved, understood, and appreciated, making the target psychologically "dependent" on the email correspondence for a daily dose of "feel-good" emotions (Koon & Yoong, 2013). This stage of the scam usually culminates in the bait's "confession" of strong romantic attraction to the target, and her intense desire to meet the target in person.

1.5.3 Stage 3: The test

As soon as the conversation turns to the subject of a potential meeting between the target and the bait, the scammer presents the victim with a request for assistance requiring a fairly small amount of money to help cover travel costs, such as visa, tickets, travel insurance, and travel agency fees (Rege, 2009). If the victim responds positively, he is provided instructions on how to transfer the money to the bait. This initial request often mentions only a small amount of money and "tests" the target's level of susceptibility (Whitty, 2013a).

1.5.4 Stage 4: Escalation of money requests

If the target responds positively by sending the requested amount, additional requests for urgent monetary assistance quickly follow, often depicting a series of dramatic events such as encounters with robbers, arrests for failure to declare an item of value, and legal problems with the Embassy or Customs and bank officials (Rege, 2009; Steward, 2008; Whitty & Buchanan, 2012; Whitty, 2013a). In cases of dating scams of Russian origin, the scammers often cite non-existent laws and regulations (such as Customs regulations and international travel requirements) that Internet users not familiar with the Russian legal system often find plausible (Steward, 2008). Usually this phase continues for as long as the victim is willing to send financial assistance to the bait.

1.5.5 Stage 5: Revelation

As the victim's monetary losses and psychological fatigue begin to accumulate, they become more and more dissatisfied with the correspondence, but continue to correspond with the scammers in an attempt to re-capture the romantic euphoria of the initial stage of the relationship

(Whitty, 2013b). Often the victims seek out confirmation of their suspicions about the bait's identity and intentions online, or through contacting law enforcement authorities, the embassy, or the dating site (Whitty, 2013a). Because of the extensive monetary and emotional investment into the relationship, many of the victims report feelings of shame, betrayal, and humiliation, making them reluctant to reveal their victimization to others (Whitty & Buchanan, 2012; Whitty, 2013a)

1.6 EXTANT RESEARCH ON PREVALENCE AND COSTS OF ODS

Very little is known on the prevalence and costs of ODS. Whitty & Buchanan (2012) used a representative sample of adults in Great Britain to determine that 0.65% of the sample have been victims of ODS. Whitty & Buchanan (2012) also cite data collected by Action Fraud in the United Kingdom in 2011 that identified around 600 victims in the UK, with about a third of the victims losing over £5,000 GBP due to the fraud. In the USA, a 2012 report by the Internet Crime Complaint Center (IC3), a partnership between the Federal Bureau of Investigation (FBI) and the White Collar Crime Center (WC3), indicated that the agency received over 4,000 reports about dating scams that year, with a total loss amount of over $55 million (see Table 1.2). (IC3, 2012)

Table 1.1. Data Obtained from Russian-Dating-Scams.com

Year	Total Monetary Loss	Lowest Loss Reported	Highest Loss Reported	Mean Loss Reported
2006	$38,704	$480	$11,000	$4,300
2007	$243,771	$200	$22,381	$3,018
2008	$230,590	$270	$18,117	$3,464
2009	$346,802	$100	$57,400	$4,529
2010	$126,610	$320	$9,480	$3,517

1.7 WHO USUALLY FALLS VICTIM TO ODS?

Very little is known about the victims of ODS. Official data usually provides little insight beyond the gender and age of the victims (IC3, 2012). According to the data from IC3 (2012), more females than males report falling prey to the scam. Females also report losing larger sums of money than male victims do. Due to the nature of the scam itself, most of the victims of the scams are single adults. In the USA, the IC3 Annual Report (IC3, 2012) indicates that of the 4,476 instances of ODS reported in 2012, around 66% involved victims older than 40, with the 50-59 year olds being the highest reporting age group. The severity of the financial loss appears to be positively correlated with age of the victim in the IC3 data.

Table 1.2. Data Obtained from IC3 Annual Report for 2012

Victims	**Com-plaints**	**% of Com-plaints**	**Amount Lost**	**% of Total Loss**	**Average Loss per Complaint**
Under 20	53	1.2%	$13,625.36	0.0%	$257.08
20-29	525	11.7%	$1,044,318.79	1.9%	$1,989.18
20-39	964	21.5%	$4,758,090.92	8.5%	$4,935.78
40-49	883	19.7%	$11,339,331.87	20.3%	$12,841.83
50-59	1152	25.7%	$20,776,222.04	37.1%	$18,034.91
60 +	899	20.1%	$18,060,012.10	32.3%	$20,089.00
Total	**4476**		**$55,991,601.08**		

The IC3 Report does not differentiate between those ODS originating from African countries and those originating from Russia and Ukraine. Information on ODS originating from Russia is very limited, and private sources often provide better information in this area. As an example, information provided by Russian-Dating-Scams.com, the website specializing in reporting ODS

originating from Russia and Ukraine, indicates receiving around 300 reports of monetary victimization due to TQ-ODS scammers in Russia between 2006 and 2010 (Garrett, 2010). Although the Russian-Dating-Scams site does not provide the age and sex breakdown for their reports, the data available on the site provides an interesting statistic on the geographical location of Internet users who submitted reports about Russian and Ukrainian "pseudo-brides" (Garrett, 2010). English-speaking countries (USA, Canada, UK, and Australia) appear to file over 50% of all reports of monetary victimizations received by that website. Among the European countries, Italy, Netherlands, and Sweden appear to have the highest number of complaints reported on that site (Garrett, 2010).

Table 1.3. Data obtained from www.Russian-Dating-Scams.com

Year	% of Reports USA	% of Reports Canada	% of Reports Australia	% of Reports UK	% of Reports Europe	% of Reports Other
2007	34	12	12	12	16	14
2008	27	18	7	8	26	14
2009	30	3	8	13	33	13

Other than approximate gender distribution, age profiles, and geographic distribution, very little is known about victims of ODS crimes (Rege, 2009; Whitty, 2013b). The information that we do have about these scams lacks the demographic details needed to develop any significant theory or policy inferences. Of course, online fraud and ODS are relatively new types of crimes. With the fast proliferation of Internet connectivity among consumers of all ages and walks of life, cyber-fraud attacks on average consumers can be expected to continue to grow as well. Both cyber police practitioners and criminologists risk falling further and further behind on current crime trends if they do not expand their inquiry to include these new categories of offenders and

new categories of victims, which the new millennium has spawned. This study attempts to fill in the gap in the knowledge base about Online Dating Scams (ODS) and its victims.

CHAPTER 2

UNDERSTANDING ONLINE FRAUD VICTIMIZATION

2.1 THE TWO STAGES OF ONLINE VICTIMIZATION

Van Wilsem (2011) states that in order to understand online fraud victimization, we need to keep in mind that fraud victimization happens in two distinct stages: *targeting* and *persuasion compliance*, which are necessary for successful deception. Different personal or situational factors may come into play at each stage of online victimization. Therefore, it would make sense to consider each stage of the victimization process separately, as it is possible (and even likely) that the factors that affect targeting may be different from the factors that affect persuasion compliance among those who were successfully targeted.

Several theories of crime have been used previously to examine cybercrime victimization. Routine Activities Theory has been used to investigate online harassment (Holt & Bossler, 2008; Ngo & Paternoster, 2011), breaches of data security (Ngo & Paternoster, 2011), unwanted exposure to pornography (Marcum, 2008; Ngo & Paternoster, 2011), phishing (Kigerl, 2012; Ngo & Paternoster, 2011), identity theft (Holt & Turner, 2012), and online e-commerce fraud (Van Wilsem, 2011). General Theory of Crime has been used to investigate susceptibility to offers of fake check, boiler room investment scam, pyramid fraud, lottery win, and auction items purchase (Modic, 2012), phishing attacks (Modic, 2012; Sheng & Holbrook, 2010), white-collar crimes (Franklin, Franklin, Nobles, & Kercher, 2012), offline consumer fraud (Langenderfer &

Shimp, 2001), and online consumer fraud(Angelidakis, 2012; Holtfreter, Reisig, & Pratt, 2008; Van Wilsem, 2011). Strain and anomie theory has been used to investigate financial fraud such as Ponzi scheme investments (Trahan, Marquart, & Mullings, 2005).

Fraud victimization is a complex, multistep process that may require a complex, multistep investigation, so it is possible that one theory may not be able to explain all aspects of fraud victimization. However, the author will apply one theory, the Routine Activities Theory of crime, in an attempt to explain at least some aspects of the targeting and persuasion processes.

2.2 ROUTINE ACTIVITIES THEORY (RAT)

Lawrence Cohen and Marcus Felson introduced the Routine Activities Theory (RAT) over thirty years ago, and since then it has became one of the leading theories of crime victimization (Cohen and Felson, 1979). The theory postulates that the likelihood of criminal offense (and, by extension, the likelihood of criminal victimization) is dependent on three factors: presence of motivated offenders at a time and in a place where they have the opportunity to encounter suitable targets lacking sufficient guardianship (Gottfredson, 1982; Ngo & Paternoster, 2011). The theory postulates that targets possess certain characteristics that may affect the likelihood of being "attacked" by an offender. Among those characteristics are the target's accessibility to the offender, its desirability, and its vulnerability (Gottfredson, 1982; Ngo & Paternoster, 2011). Factors of guardianship, when present, can mitigate a target's vulnerability to attack. The theory distinguishes between physical elements of guardianship (such as physical barrier devices), social elements of guardianship (such as the presence of human guardians), and factors of

personal guardianship or self-guardianship, such as the target's ability to avoid the dangerous situation, to fight, or to flee (Bossler & Holt, 2009).

One of the appeals of RAT to researchers studying victimization is the fact that the theory does not attempt to explain characteristics or motivations of the possible offenders (Ngo & Paternoster, 2011). The theory only examines the possible points of the intercept between the motivated offenders, potentially desirable targets, and the elements of guardianship. This focus on the environmental aspects of crime makes the theory easily applicable to a diverse array of offenses, and provides academics and practitioners with a theoretical framework for practical approaches to crime reduction.

Since its introduction into criminological literature, RAT has been successfully applied to predict the likelihood of such non-computer crimes as burglary, larceny, vandalism, rape, assaults, and fraud (Ngo & Paternoster, 2011). Application of RAT to computer crimes is starting to emerge as well. Ngo & Paternoster (2011) found significant correlation between routine activities and the possibility of receiving a virus or becoming victims of online harassment, and Van Wilsem (2011) established a correlation between online shopping behavior and likelihood of online financial victimization. A detailed examination of the process of TQ-ODS victimization lends itself to examination of victims' preferences and activities, and the RAT framework provides a logical method of analysis.

2.2.1 Understanding online targeting from a theoretical standpoint

Before Internet users can be persuaded to swallow the hook, they need to encounter the "bait". Users' victimization is a secondary process entirely dependent on the success of the scam perpetrators' targeting efforts (Van Wilsem, 2011). It is logical, then, that understanding the

mechanisms that affect users' vulnerability to targeting is critical to understanding CoT victimization in general. This author will define that *targeting process* to be all actions taken by the scam perpetrators to identify, locate, access, and successfully solicit communication from suitable targets.

This suggests that the targeting process for online fraud will consist of several steps. First, the scammers need to identify the types of Internet users that can be victimized using a specific fraud scenario. Second, they need to identify the correct environment in which suitable targets can be found in sufficiently high numbers. Third, scammers need to obtain either direct access to that environment (e.g., direct presence in the same digital space) or indirect access (e.g., databases of users of that environment). Fourth, the scammers need to create a "bait" that could fit the target's interests. Fifth, the scammers need to make the bait visible to the potential targets in a way that prompts them to take action. Sixth, the scammers need to actually receive a response from the targets.

From the viewpoint of explaining ODS victimization, this suggests that for an Internet user to be *successfully targeted* (as opposite to being just *targeted*), several events need to occur together. First, the Internet user needs to be a current or a past visitor of those sites that the scammers select for targeting. Second, the online environment in which the user encounters the scammer needs to be sufficiently transient for the user not to feel instantly suspicious of being approached by a stranger. Third, the target needs to have some unfulfilled need for romantic intimacy in order to respond to the phishing communication (or to initiate a communication). Fourth, the type of bait the scammers display needs to be relevant to the target's needs. Fifth, the target must perceive the potential risks of his actions to be lower than the potential rewards of his actions.

2.2.2 Application of RAT concepts in an online environment

The Routine Activities Theory is typically used to account for factors affecting common street crimes, but, as Pratt et al. (2010) write, "The penetration of the Internet into consumer lifestyles represents a key structural change that is relevant to a routine activity explanation of fraud targeting." (Pratt et al., 2010, pp 273-274) There are indeed a few differences between the offline and online environments that may require additional attention when considering the application of RAT principles to online victimization. First, convergence of potential victims and potential offenders in digital space does not require their simultaneous presence in any particular location; offenders can simply collect information about potential targets remotely through phishing, spamming, or by buying their information in the online underground marketplaces (Longe et al., 2009). In fact, an unlimited number of offenders can reuse the victim's data, once harvested, for an unlimited amount of time, as long as the channel by which the target receives information (e.g., a particular email account) remains active. This suggests that it might be more accurate to say the likelihood of online fraud victimization depends on the offenders' ability to access the target through some channel of communication, whether simultaneously shared or not. Second, victim-offender interactions in the digital world are often double-blind interactions, leading to necessary adjustments in a cyber offenders' target selection strategies. Since there are no physical attributes to provide visual or contextual indicators to the identities of other users in cyberspace, a user's online activities (e.g., making particular online purchases, visiting topic-specific Internet chatrooms, etc) play an oversized role in the process of target selection. These actions serve as clues to the potential offenders to indicate which targets are accessible and attractive (Holt & Bossler, 2008; Pratt et al., 2010).

2.2.3 Target factors in the digital environments

According to RAT, the likelihood of crime victimization in the physical world is target-dependent. Not all potential targets are desirable, accessible, or vulnerable to an attack (Gottfredson, 1982). Considering specifics of the digital environment, the author paraphrases Gottfredson (1982) to propose that in the online environment not all targets are desirable, *visible,* accessible, or vulnerable. Those users who already have a romantic partner are not likely to be vulnerable to TQ-ODS phishing efforts, regardless of their visibility or accessibility, and Internet users who *are* lonely and potentially vulnerable may remain invisible to the scammers if their online activities are limited to low profile or low-traffic web sites.

2.2.4 Role of routine activities in the online targeting process

The lack of visibility of any physical clues to online users' physical characteristics forces online scammers to utilize the users' past or current online activities as an indicator of their suitability for some particular type of online fraud. The TQ-ODS scams target individuals lacking romantic or sexual partners, so it would be logical to anticipate that those users who visit online dating sites are more likely to be actively seeking a romantic relationship and be more open to being approached by strangers than an average Internet user. Add to that probability the fact that dating site environments are one of the few digital spaces where scammers and their targets can intersect in real time, and users of those sites are likely to be at the greatest risk of becoming visible and accessible to the scammers.

Other online activities can also put Internet users at risk. As discussed in Chapter 1, scammers also engage in social network spamming and untargeted spamming, so any Internet user whose

data was at one time or another harvested can potentially become visible and accessible to the scammers.

2.2.5 Role of guardianship in the online targeting process

The RAT concept of guardianship with respect to cybercrimes can be applied to *physical guardianship* (e.g., firewalls, anti-spam filters, anti-virus programs) and *personal guardianship* (e.g., the users' general computer skills and their risk awareness) (Angelidakis, 2012; Ngo & Paternoster, 2011). From a theoretical standpoint, any form of suitable guardianship reduces the likelihood of victimization by making the target less vulnerable to an attack. However, current research on the effects of guardianship is not conclusive.

Physical guardianship: A study by Angelidakis (2012) focusing on the relationship between physical guardianship and online e-commerce fraud victimization indicates results that run counter to the theoretical expectations. In that sample the presence of online security software actually produced an increase in the chances of losing money due to non-delivery of online purchases. For other Internet crimes, physical guardianship displays mixed effect on the likelihood of victimization. Studies show it to increase resiliency to identity theft (Holt & Turner, 2012), but it has no effect on the likelihood of online harassment (Holt & Bossler, 2008) or exposure to unwanted sexual materials (Marcum, 2008), and it increases likelihood of breach of data security (Ngo & Paternoster, 2011). This author argues that measures of physical guardianship are likely to be less relevant to TQ-ODS victimization, because users are often targeted while using apparently legitimate channels of communication, such as dating site chat rooms.

Computer use and skills: A study by Halevi, Lewis, and Memon (2013a) shows participants who use the Internet more frequently are more conscious of the risks of the online environment, but measures of personal guardianship in terms of better awareness or computer skills do not guarantee complete resiliency to phishing attacks (Halevi, Lewis, and Memon, 2013a; Sheng and Holbrook, 2010). Review by Wright & Marett (2010) also indicate that users who have better computer skills often have higher Computer Self-Efficacy (CSE), which can lead to a false confidence in their ability to detect online deception and deal with it appropriately (although in their study higher CSE in fact reduced vulnerability to phishing attacks)

2.2.6 Role of awareness in the online targeting process

Awareness of risks associated with particular environments or activities is a form of personal guardianship (Bossler & Holt, 2009; Ngo & Paternoster, 2011; Sheng & Holbrook, 2010), as it allows individuals to take proactive protective measures to avoid victimization. Using postulates of RAT, we could expect that awareness of common phishing techniques would reduce the likelihood of users responding to phishing emails. And indeed research indicates that on average individuals with better awareness of online security are less likely to respond to phishing emails (Halevi, Lewis, and Memon (2013b); Sheng & Holbrook, 2010). However, Halevi, Lewis, and Memon (2013a) found that a subsection of Internet users appear to be highly vulnerable to phishing despite receiving awareness training, and that factors other than lack of awareness may be responsible for phishing vulnerability for that specific subsection of Internet users.

2.3 UNDERSTANDING PERSUASION FROM A THEORETICAL STANDPOINT

If the targeting stage of the fraud fails to elicit a positive response from the Internet user, the TQ-ODS fraud ends with that unsuccessful phishing attempt. However, if the user begins communication with the scam perpetrators, the scam enters the interactive phase that this author would call "the persuasion phase". For the purpose of this study, the *persuasion phase* of the ODS scam will be defined as all stages of *mutual* correspondence between the scam perpetrators and their targets, including grooming, testing, and escalation. Unfortunately, quantitative studies investigating the persuasion phase of any frauds (online or offline) seem to be lacking, but from the standpoint of theoretical arguments, it is still possible to consider and evaluate the process of persuasion using concepts found in RAT literature.

For example, from the standpoint of RAT it would be logical to suggest that the likelihood of victimization may depend in part on the frequency of interaction between the offender and the target, as more frequent contact between them could provide the offender with more opportunities of influencing the target to send money. Assuming that the offender and the target are in frequent communication, then it would also be logical to propose that those targets that have a higher degree of guardianship would be more resistant to victimization.

2.3.1 Role of guardianship in the persuasion process

Computer skills: Computer and Internet literacy during the persuasion phase may become an important factor in determining the target's susceptibility to TQ-ODS victimization. For example, users with specific training in IT security may detect the fact that the correspondence is being carried out using proxy servers, which would then trigger their suspicion about the

correspondence. Those users who are familiar with online data research can use their skills to verify scam perpetrators' claims about travel regulations, Customs requirements, or medical procedures necessary to complete their "travel quest". Or, when presented with falsified documents, those users who have personal experience with image editing software may be able to detect discrepancies in pixel density or color shades in different parts of the document. However, as mentioned in the previous sections on targeting, review by Wright and Marett (2010) indicate higher computer literacy may increase vulnerability, as users with high Computer Self-Efficacy (CSE) may feel confident about their ability to detect fraud, and thus fail to take precautionary measures..

2.3.2 Role of routine activities in the persuasion process

Internet users' online and offline routine activities are likely to play a diminished role in the outcome of the scam once the scam enters the persuasion phase. However, some routine activities can still play a role in terms of influencing Internet users' personal guardianship. For example, those users who spend a lot of time on dating sites or who consume a large amount of information about international dating and immigration may acquire information that would make them more suspicious of the scam perpetrators' claims. Additionally, frequent exposure to online dating sites may increase the chance that multiple scammers will try to approach the same target in a short amount of time, triggering the user's suspicion about such contacts. Offline activities may matter as well, especially if the user has such busy lifestyle outside of cyberspace that they have little time to devote to building an online romantic relationship.

2.3.3 Role of awareness in the persuasion process

Once the fraud enters the persuasion phase, some of the characteristic elements of the TQ-ODS fraud should emerge. Those signs may include characteristic writing styles used by the scam perpetrators, or the types of money request scenarios that the scammers present. Online users who have some prior knowledge about the typical scenarios of TQ-ODS scams may be more likely to become suspicious about the perpetrator's communication, and therefore be less likely to respond to money solicitation.

However, unlike widespread warnings about phishing attacks, information about the characteristics of TQ-ODS is not widely available to the general population of Internet users. The main sources of information on TQ-ODS are websites and forums related to online dating, so those users who do not visit those sites would have less exposure to this information. Awareness about TQ-ODS can also be acquired from family members, friends, coworkers, from stories presented in media, or from the user's prior personal experience with other frauds.

Prior research indicates that, although awareness of online vulnerabilities may not always translate to more risk-conscious behavior, it is still overall associated with lower online victimization risk (Sheng & Holbrook, 2010; Titus, 1999; Wright & Marett, 2010). However, little research has been done to measure awareness of TQ-ODS. One study on this subject by Whitty and Buchanan (2012) tested a sample of British consumers to determine their degree of awareness about ODS. According to their research, about 52% of population in Britain has heard of this type of cybercrime, and around 2% of the population personally knew someone who became a victim of this type of fraud.

2.4 REASON FOR THE LACK OF RESEARCH IS THE LACK OF DATA

From the review above it is clear that the existing academic research on cyber-frauds is limited (Pratt et al., 2010). One of the apparent reasons for this lack of in-depth academic research on cybercrimes in general and on online frauds in particular is the difficulty with data collection. In the United States, data maintained by the National Crime Victimization Survey, US Federal Trade Commission, and the Internet Crimes Complaint Center provide information on a limited number of cyber offenses, and researchers are not able to modify the variables made available by the surveys to add theory-relevant measurements. The same difficulties exist with statistics collected by Canadian Anti-Fraud Centre, the UK National Fraud Authority, and the Australian Bureau of Statistics.

Qualitative case studies of victimization reports or media accounts (similar to ones done by Koon & Yoong, 2013; Trahan et al., 2005), as well as interviews with offenders and victims (similar to those performed by Burgard & Schlembach, 2013; Copes & Vieraitis, 2009; Whitty, 2013a, 2013b), provide rich sources of information and can provide directions for future research. These also present challenges with replication or generalization of results. Large nation-wide or state-wide surveys of consumers (Pratt et al., 2010; Schoepfer & Piquero, 2009; Van Wilsem, 2011; Van Wyk & Mason, 2001; Whitty & Buchanan, 2012) provide large amounts of data that is representative of the general population, but they are difficult to conduct and are few in numbers.

Quantitative studies using student samples (such as those by Bossler & Holt, 2009; Holt & Bossler, 2008; Holtfreter, Reisig, Piquero, & Piquero, 2010; Marcum, 2008) are convenient, allow for flexible study designs, and are cost effective, but they utilize fairly homogeneous

populations from the standpoint of age, social groups, education (Payne & Chappell, 2008), and, perhaps, computer literacy and Internet use. Results provided by IC3 clearly indicate that the predominance of victims who report their victimization to IC3 are in the 30 years and above age categories (*IC3 2012 Internet Crimes Report*, 2012). Additionally, the limited range of students' life experiences and life trajectories makes it difficult to design measurements of serious cyber-frauds and financial frauds such as Ponzi schemes, identity fraud, advanced fee fraud, investment and securities fraud. With the worldwide proliferation of mobile devices such as smartphones, e-tablets, and laptops, cyber crimes affect consumers of very different nationalities and cultures, ages, occupations, and levels of computer security awareness. These factors are significant and should not be overlooked in study designs.

One way to expand data collection, and it has been applied with good results, is to rely on data collected by large private organizations such as Symantec, McAfee, AARP, but with the understanding that data collected for business purposes may have a business-specific bias. Another way to gain access to more diverse data would be to create partnerships with private anti-fraud organizations that are currently at the frontline of fraud prevention efforts to see if specific types of data could be collected from those sites. These could include 419 Eater.com, 419 Baiter, Scams.com, Anti-Scam.Org, and similar organizations (see example with Isacenkova et al., 2013). Lastly, researchers could design ways to collect data on their own, using capabilities offered by knowledge in programming , for example as was done by Abad (2005).

2.5 NEED FOR GREATER SPECIALIZATION OF CYBER CRIME RESEARCH

A trend in several recent studies of online victimization has been what could be called a "multiple-modelization", where one study collects information on multiple forms of online

victimization (for example, see Angelidakis, 2012; Bossler & Holt, 2010; Schoepfer & Piquero, 2009). Due to the multi-modal design of the study, no particular focus is placed on the environments in which the offense takes place or on the unique characteristics of each crime type. This type of design forces researchers to abandon offense-specific variables in favor of more general ones. This can lead to a collection of sometimes conflicting results for each variable that the researchers then struggle to consolidate and correlate.

Reviews of extant research on factors previously linked to susceptibility to online victimization often display a conflicting mix of findings. However, without a clear understanding of which offenses were investigated and how variables were adjusted for offense-specific factors, is it not easy for the reader to determine how the study results compare to one another. Consequently, calls have been made for more research based on offense-specific environments and victim factors (Ngo & Paternoster, 2011)

Offense-specific research could not only provide better measurement and prediction of online victimization, but it could help to identify practical ways to increase protection of consumers within specific online environments (Pratt et al., 2010). Such research could provide critically important information for Internet merchants, policy writers, and the consumers themselves.

CHAPTER 3

DISCUSSION OF VARIABLES

To overcome the previously described shortcomings of research on online fraud victimization, this study will focus only on one particular type of ODS – the travel quest scams (TQ-ODS) originating specifically from Russia and its neighboring country Ukraine. The study will measure a variety of factors that could help researchers develop a more complete model for the prediction of online fraud victimization encountered with this type of scam. The study will also employ a fairly diverse sample of Internet users who were previously targeted by Russian and Ukrainian dating scams.

3.1 DEPENDENT VARIABLE

3.1.1 Likelihood and severity of victimization -- What should we measure?

From the standpoint of fraud victimization, researchers tend to focus on the fact of victimization in an absolute sense, accounting only for the presence or absence of financial or other harm, without regard to the degree of severity of harm inflicted. This appears to be overly simplistic. Measurement and reporting of traditional crimes usually include an indicator of the severity of the offense (e.g., Simple Assault, Aggravated Robbery, Minor Theft, etc). This allows for easier interpretation of the collected statistical data.

This type of "offense severity" classification is missing for the cybercrimes research at this time, although Button et al. (2009) has attempted to introduce a classification of cyber victims by loss

amount and repeat victimization count. The collected data usually cannot differentiate between fraud incidents with minor loss (e.g., under $10) versus fraud incidents with significant loss (e.g., over $10,000). Yet, the circumstances of the offense, the characteristics of the offender, and the characteristics of the victim may be significantly different in those two hypothetical cases and aggregating them together could produce misleading results.

The author proposes that future analysis of cybercrime victimization should be based on two criteria. First, did victimization take place? Victimization could be defined as loss of utility, but other definitions could be established. Second, what was the severity of victimization? "Severity" can be determined by relative amount of utility lost due to victimization. In the case of online fraud, severity of victimization could be measured in total dollar amount lost. In the case of computer crimes targeting data, a percentage loss of system functionality, or a percentage loss of data security (i.e., confidentiality of the compromised data) could be defined as severity of victimization. This paper will attempt to incorporate the analysis of severity of victimization to see whether the proposed new variable warrants further investigation.

3.2 STANDARD VARIABLES

3.2.1 Age

The influence of age on vulnerability to fraud is one of the best-researched aspects of fraud victimization. Although the researchers generally agree that age is one of main correlates of fraud vulnerability, the mechanisms of that interaction continue to be a matter of debate (see reviews by Button et al., 2009; Schoepfer & Piquero, 2009; Titus, 1999). A review by Schoepfer & Piquero (2009) on CoT victimization indicates that younger individuals are more likely to be

targeted and victimized by fraud than older individuals (see also Pratt et al., 2010), are more likely to engage in risk-taking behavior such as online shopping (Pratt et al., 2010), and are more likely to become victims of consumer fraud (Van Wyk & Mason, 2001). Middle-aged individuals (those age 45 and under), on the other hand, are found to be more likely to become victims of investment scams (Trahan et al., 2005) and Ponzi scams (Ganzini, McFarland, & Bloom, 1990). Older consumers are more likely to fit the "Fraud Vulnerability Profile" developed by the Consumer Fraud Division of Denver, Colorado (Lee & Soberon-Ferrer, 1997) and are more likely to be victims of off-line scams than younger individuals (Ganzini et al., 1990).

Effects of age may be offense-specific (Button et al., 2009) and mediated by variables associated with routine activities and self-control (see findings by Muscat & James, 2002; Ngo & Paternoster, 2011; Pratt et al., 2010; Sheng & Holbrook, 2010), as well as by degree of computer proficiency and fraud awareness (Pratt et al., 2010). For example, older Internet users could be less vulnerable to Internet fraud than younger users because they are less likely to engage in online shopping, but they may be more vulnerable to ODS scams because they are more likely to be visiting online dating sites than younger users (Stephure et al., 2009; Valkenburg & Peter, 2007), leading to a higher likelihood of exposure to ODS offenders. The current study may shed some light on the association between age and ODS vulnerability.

From the standpoint of data security, older Internet users certainly seem to be more vulnerable. Review by Grimes et al. (2010) indicates that older Internet users are less likely to have formal computer training provided in employment or educational settings, less aware of potential threats like viruses and phishing, less aware of potential misuse of online data, less likely to utilize

spyware detectors on their computers, and less likely to alter risky online behaviors to reduce risks of identity fraud. As a result, they are more likely to make online purchases from links provided in spam emails (Grimes et al., 2010), making them more vulnerable to phishing attacks.

3.2.2 Country of residency

There is currently a lack of research comparing the vulnerability of users from different countries to fraud victimization, however, such differences could exist. Because the premise of the TQ-ODS originating from Russia lies in the ability of the scammers to convince their victims that certain fictitious travel requirements are in place to prevent easy face-to-face meeting, it seems logical to suggest that users from countries located further away from the Russia could be more likely to believe the scam perpetrators' quest story. Users from those countries would have fewer sources of accurate information about Russian travel and have less access to accurate information about such travel requirements. Additionally, the cost of the "bait's" travel would increase, making users from countries further away from Russia likely to sustain higher losses due to the scam.

3.2.3 Education

No data on the effect of education on likelihood of ODS victimization as whole is currently available, but research on vulnerability to phishing could be relevant to the current investigation. Reviews by Copes, Kerley, Huff, and Kane (2010) and Modic (2012) indicate that researchers have been split on assessment of the influence of formal education on vulnerability to phishing targeting. Education appears to function as a protective factor by increasing the likelihood of obtaining training in computer security measures, and increasing general computer knowledge

and Internet security awareness, which in turn increases protection against online victimization associated with exploitation of the user's personal data (Holt & Turner, 2012). Therefore, during the targeting phase of fraud, evidence indicates that educated users would be less likely to respond to phishing emails (Modic, 2012; Sheng & Holbrook, 2010).

However, in relationship to fraud in general, higher educational attainment appears to be a risk factor for fraud (Copes et al., 2010; Titus, 1999) and identity theft (Pratt et al., 2010). This is probably because more educated individuals tend to spend more time online and to make online purchases (Pratt et al., 2010). Alternatively, it is possible that users that are more educated have higher computer self-efficacy (CSE), which can lead to carelessness (Wright & Marett, 2010). However, the relationship between fraud vulnerability and education does not always reach statistical significance. For example, recent studies (Van Wilsem, 2011) failed to find significant relationship between education and fraud victimization.

3.2.4 Income

Recent research on Internet consumer fraud victimization found no link between income level and the likelihood of online consumer fraud victimization (Van Wilsem, 2011). However, Pratt et al. (2010) indicates that individuals with higher income tend to spend more time online and to be more likely to use the Internet for shopping. Reviews by Button et al. (2009) and Muscat and James (2002) cited studies showing that victims of different types of consumer fraud were found to have above-average incomes. However, their vulnerability to fraud victimization seems to be offense-dependent. For example, a number of prior studies indicate that individuals making $75,000 to $100,000 annually are at the highest risk for certain types of identity theft

victimization (see reviews by Copes et al., 2010), possibly because higher income makes these individuals more attractive as targets of identity theft (Angelidakis, 2012).

Higher income was also correlated with a higher likelihood of Internet fraud and bank account break-in (Angelidakis, 2012). On the other hand, in a study by Langenderfer and Shimp (2001), officials at the Better Business Bureau (BBB) tended to perceive victims of consumer fraud as older and financially desperate or on a fixed income. However, those findings may be a reflection of the types of scams that the BBB officials process (e.g., free prize offers, get rich quick scams).

As can be seen from the review above, relationships between income and fraud victimization appear to be offense-specific and may be mediated by other factors. Although higher income may correlate with more time spent online and higher likelihood of online shopping, these behaviors may not necessarily lead to a higher risk of being targeted for fraud (Pratt et al., 2010), because online scammers frequently use mass-mailing as a way of approaching potential victims, and the victim's income plays only an incidental role in their selection for targeting.

3.2.5 Employment

Some research indicates that employment status may affect susceptibility to such online crimes as phishing. For example, Bailey, Mitchell, and Jensen (2008) found that study respondents (in their case, students) who worked full time were less likely to respond to a phishing email than those respondents who did not work full time. Similarly, Ngo and Paternoster (2011) found that individuals with full employment were less likely to experience online harassment than unemployed individuals. Pratt et al. (2010) found that retired individuals were less likely to engage in such risk taking behaviors as online shopping.

3.2.6 Marital status

Surprisingly little is known about the effect of marital status on vulnerability to fraud victimization (although the effects of marital status on non-fraud cybercrimes have been researched more extensively). So far it has been indicated only that married people are more likely to engage in what is considered to be risky online behaviors, such as online shopping (Pratt et al., 2010). Plus a study by (Ganzini et al., 1990) found that widowed individuals represented a majority of the sample in the study of off-line fraud. Perhaps, part of the reason for the lack of research is because so many studies of online victimization are performed using student samples. There appears to be little information about the effect of marital status on likelihood of ODS victimization.

Due to the nature of the TQ-ODS scam, nearly all respondents in the current study were single or in the process of divorce at the time of their scam experience. It is expected that statuses such as "widower" versus "divorced" may be a factor of the respondent's age. However, for the purpose of obtaining detailed demographic information, the marital status was investigated.

3.3 INDEPENDENT VARIABLES

3.3.1 Computer use and proficiency

A fairly extensive review of the possible link between computer proficiency and vulnerability to online victimization appears in Chapter 2. The link between low computer proficiency and vulnerability to phishing attacks is reviewed by by Halevi et al. (2013b), Sheng and Holbrook (2010), and Wright and Marett (2010), and it is possible that computer proficiency plays a role in the overall susceptibility to the scam. For example, it is possible that during the persuasion phase

of the scam, users who have better IT training may have higher likelihood of being able to detect signs of forgery on the documents used in the scam, of finding information about the scammer online, and of being able to verify the bait's claim about travel regulations, Customs requirements, or necessary medical procedures. However, higher computer literacy may lead the users to over-estimate their ability to control their online environment, which may lead to increased risk taking behaviors online.

Unfortunately, studies that include variables related to computer proficiency usually examine "non-interactive" online crimes. As a result, the effects of computer literacy on the outcome of interactive crimes have not been examined closely.

3.3.2 Fraud awareness

Although awareness of online vulnerabilities may not always translate into more risk-conscious or risk-adverse behavior, it is still associated with an overall lower victimization risk (Sheng & Holbrook, 2010; Wright & Marett, 2010), in part because online security measures provided by third parties (e.g., anti-spam software, online security warnings, etc) are more effective if the users know how to interpret them, or where to look for them.

Limited research has been conducted on the degree of awareness of Internet fraud among consumers. However, this type of research is quickly expanding (Taylor, et al., 2015). Chapter 2 references a study in Britain (Pratt et al., 2010) to determine degree of awareness about ODS. This study reports that about 52% of the population in Britain has heard of this type of cybercrime, and around 2% of the population personally knows someone who became a victim of this type of fraud. However, it is not known how this knowledge affected consumers' chances of avoiding victimization.

Effects of exposure to information or warnings about online frauds would be more pronounced during the targeting phase of the scam. Extant research indicates that those individuals who have been victimized by fraud are more likely to be targeted for victimization again due to the higher likelihood that the victims' contact information will be shared among fraudsters in form of "mooch lists" (Kuo, Cuvelier, Sheu, & Zhao, 2012; Titus, 1999), prompting Titus to suggest that "It appears that one of the surest ways to become a personal fraud victim is to have been a victim." (Titus, 1999, p 7) In application to ODS, it is not uncommon for several scam groups to share resources such as money, Internet access, templates of correspondence, and databases of harvested email addresses (Rege, 2009), making it likely that once a victim's email is acquired by the scammers, the victim will be targeted by other scam groups.

However, it is logical to suggest that those individuals who have prior experience with ODS and other crimes of trust are more likely to be able to detect patterns of deception in repeated communication with scammers, thus making them less vulnerable to victimization during the persuasion part of the scam.

3.3.3 Awareness variables collected and hypothesis

In this study, differentiation will be made between two types of awareness – "remote" awareness that may be acquired as a result of exposure to information about different types of scams vicariously (i.e., through second-hand accounts about characteristics and warning signs of scams being distributed online, though news media, entertainment, and through personal communication) and awareness acquired first-hand during previous victimization experiences. It could be expected that the first-hand experience will be more salient, and have a more

pronounced ability to provide consumers with both conscious and subconscious "alarms" that would be activated if they encounter a particular pattern in a scammers' language or behavior.

3.4 ROUTINE ACTIVITIES VARIABLES

Some variables collected for the purpose of the study were very offense-specific, and have not been investigated previously. However, since this is a dating scam related study, it seems appropriate to make at least some measurements related to the individuals' dating behaviors and interests.

3.4.1 Focus of online search and international dating awareness

Because scam perpetrators frequently choose dating sites as their "phishing" spots (Rege, 2009; Whitty, 2013a), Internet users who visit dating sites or online communities with built-in dating search engines are more likely to be targeted by scammers because their email addresses are more likely to be spammed by the scammers. Those individuals fit the profile that the scammers are looking for: lonely, with enough disposable income to pay for a dating site membership, and not yet successful in finding romance in the non-online environment.

Online dating sites that focus on international dating are likely to attract those Internet users who for one reason or another have a particular interest in finding a partner outside of their own culture. Those users are of particular interest to the scammers because they are more likely to be motivated to invest time, effort, and money into the immigration process for their future mates. Therefore, it could be anticipated that those Internet users who visit web communities that are focused on international dating will have a heightened risk of being targeted by the scammers.

However, during the persuasion phase of the scam, those respondents who have a specific interest in international dating or who have prior experiences with international dating may be less vulnerable to some of the scam deceptions, as they are also more likely to have prior experience with immigration-related requirements than online daters who have never considered the possibility of dating outside of their own culture. Once again, it is important to distinguish between international dating in which the victim in honestly seeking a long-term, romantic relationship versus sex tourism, wherein the individual is seeking international sexual services, many times from a minor in a foreign country. This study does not address sex tourism, but rather focuses on the travel quest-online dating scam (TQ-ODS).

3.4.2 Online activities

Results obtained by Holt and Bossler (2008) indicate that offense-specific vulnerabilities usually manifest themselves in offense-specific online environments (e.g., vulnerability to online harassment was only linked to participation in online chats). From the standpoint of RAT framework, this is not surprising, since in chat rooms the users can easily interact with one another, making potential victims visible and accessible to potential offenders. It would then be logical to suggest that ODS victimization is most likely to affect those Internet users using online dating sites, since the presence of their profile or their email in the online dating site database makes them both visible and accessible to potential offenders. It also allows the scammers to target only those users already expressing interest in finding a romantic partner, and who are more likely to respond to the initial scam invitation for contact.

CHAPTER 4

DATA AND RESULTS

4.1 METHODS

4.1.1 Data collection

Data for the present study is taken from a questionnaire that was accessed and submitted online. The questionnaire consists of 58 items, but only 22 variables from this questionnaire are presented in this study. The questionnaire was constructed by the study author.

4.1.2 Participants

The study participants sample is comprised of Internet users who visited the www.Russian-Dating-Scams.com web site between January 2009 and March 2014. Visitors' names and email addresses collected by the original web site were used to generate invitations to participate in the study and were sent to approximately 300 past users of the site. An advertisement for the study was also placed on the web site's front page, allowing interested users to register for the study after viewing the advertisement.

The study ad specified that only users who encountered travel-quest dating scams were invited to participate. The main characteristics of the TQ-ODS were described in the ad in sufficient detail to prevent confusion with other types of ODS. Users who have experienced more than one TQ-ODS scam were asked to select any incident that they remembered most vividly. Proficiency in

reading and writing in English was listed as a requirement in order to enroll for the study. Users who identified themselves as scam "baiters" were not allowed to participate. Scam baiters are Internet users who derive entertainment from engaging online scammers and exposing the scammers' pictures and data online (Chang, 2008). Because scam baiters are a unique subset of Internet users, they are likely to be not representative of the general population of interest to the study.

Three hundred and ten (310) Internet users submitted applications for study participation. Out of that number, approximately 20 applications were rejected because they were filled out in a language other than English. Additionally, some applications were rejected because the users indicated that they were not 100% sure whether the experience they had could be classified as a scam or not. Nine applications were rejected because the applicants described scams inconsistent with the travel-quest scenarios. Those users whose applications were accepted were sent Informed Consent forms, 140 users signed Informed Consent forms, and 110 filled out the questionnaire.

4.1.3 Privacy concerns

Complete anonymity was guaranteed to all prospective participants. To protect identities of the study participants, only information about participants' email addresses was collected in the Informed Consent form. Participants were asked to choose a code name for themselves to identify themselves in the study.

4.2 DATA - DEPENDENT VARIABLES

4.2.1 Likelihood of victimization

The dependent variable in the study is the total loss amount due to the scam. Participants report the amount lost and currency information. If currency information is not provided, the national currency of the participant's country of residence is assumed to be the currency of the loss. An online currency converter from CCN.Money.com web site is used to convert all amounts into United States dollar (USD) equivalent amounts. Those participants who lost $0 are labeled "Targeted" to indicate that the scam succeeded only on the targeting stage, but it failed at the persuasion stage. Those individuals who lost any amount greater than $0 are labeled "Victims" to indicate that the scam succeeded at both the targeting and the persuasion stages. *Likelihood of victimization* (or victimization rate) for a particular subcategory within a variable will be defined as the percentage of time victimization occurred within this subcategory, and will be calculated using the formula: *Likelihood of victimization = 1 - (Targeted/Victims).*

4.2.2 Severity of victimization

As discussed in Chapter 3, this thesis proposes reporting and analysis of *severity of victimization* (defined as amount of utility lost due to the fraud) in order to improve our understanding of online victimization. Because the main utility lost due to the TQ-ODS scams is financial utility (although psychological distress to the victim cannot be forgotten), severity of victimization in this study will be measured in terms of the amount lost due to the scam. Severity of victimization for a particular subcategory of respondents in this paper will be determined by the average of

dollar loss amount within that subcategory, and calculated using the usual formula for calculation of a statistical mean.

4.3 DATA - INDEPENDENT VARIABLES

Variables relevant to RAT theory are presented, as well as demographic variables.

4.3.1 Demographic variables

The following demographic variables are measured: age at the time of the scam, country of residence, average monthly income, number of years of higher education, marital status at the time of the scam, and employment status.

Table 4.1. Demographic Variables

Demographic		
Age	Age at the time of the scam	Simple numeric value
Country	Country of respondent residence	Assigned a numeric value
Regions	Northern Europe: Iceland, Scotland; Denmark, Norway, Sweden, Finland, Estonia, Latvia , Lithuania Southern Europe: Italy, Portugal, Spain, Albania, Bulgaria, Greece, Macedonia, Serbia, Croatia, Romania, West Europe: Austria, Belgium, France, Germany, Liechtenstein, Monaco, Netherlands, Switzerland Eastern Europe: Albania, Armenia, Belarus, Croatia, Czech Republic, Georgia, Hungary, Kosovo, Macedonia, Slovakia, Slovenia, Ukraine Middle East: Cyprus, Egypt, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Quatar, Saudi Arabia, Syria, Turkey, UAE, Yemen South Asia: Afghanistan, Bangladesh, Bhutan, India, Iran, Maldives, Nepal, Pakistan, Sri Lanka Australasia: Australia, New Zealand, and surrounding islands	

Table 4.1 continued

Marital status	Values: "Never married," "Divorced," "Separated", "Widowed," "Married"	Assigned a numeric value
Education	Years of higher education (post high school)	Assigned a numeric value
Monthly income	Average monthly income	Simple numeric value
Employment status	Values: "Not specified;" "Unemployed without government assistance," "Unemployed with government assistance; "Employed part time," "1 job," "2 jobs," "3 or more jobs," "Self-employed," "Retired"	Assigned a numeric value

- Classification of countries by region was performed according to the United Nations listing "Composition of macro geographical (continental) regions, geographical sub-regions, and selected economic and other groupings" (UN, 2013).
- Information concerning gender was not presented because dating frauds originating in Russia target male Internet users. In this sample only one participant was female.

4.3.2 RAT variables

Online dating search activities are assessed using variables “Seeking partner”, “Online search”, and “Focus of online search”. To obtain an indication of online activities of the respondents, respondents are asked whether they were looking for a romantic partner at the time the scammer approached them, whether they were looking for a romantic partner online, and whether they were looking for a romantic partner from their own or from another country. If the respondents indicate that they were looking for a romantic partner online, it is inferred that respondents are past or current visitors of online dating sites or networks with dating group capabilities. If the

respondents indicate that they were looking for a romantic partner from another country, it is inferred that they are past or current visitors of international dating sites.

As a part of understanding how awareness may be related to guardianship in fraud situations, a number of questions about awareness are included in the questionnaire. The types of awareness assessed are: 1) awareness of logistic issues associated with international dating; 2) awareness of a variety of online fraud scenarios, 3) awareness of phishing, 419 scams, and ODS scams in particular.

As discussed in Chapter 3, differentiation is made between two types of awareness: remote and personal awareness. Respondents are first asked whether they had seen or read anything about

Table 4.2. RAT Variables

Variable	Description	Rule
Seeking relationship	Values: “Not seeking any relationship,” “Wishing for a partner but not actively seeking,” “Actively seeking”	Assigned a numeric value
Online Search	Was the search being carried out online?	Dichotomous variable
Focus of online search	Values: "No online search;" "Not interested in int'l dating;" "Open to all possibilities;" "International focus"	Assigned a numeric value

the 11 different types of online frauds in print media. They are then asked whether they have encountered any of those types of frauds personally. Lastly, they are asked whether they had ever lost money to any online scams prior to the incident with the ODS scam. The three most common CoT crimes (ODS, 419, phishing) are listed among the 11 types of scams offered for selection. As these are checked off by the participants, they are calculated into a separate awareness score.

International dating issues awareness is assessed using variables "Prior consideration of international dating" and "Prior international dating partners."

Table 4.3. International Dating Awareness Measurements

Variable	Description	Rule
Prior consideration of international dating	Did the respondent consider possibility of international dating prior to the scam?	Dichotomous variable
Prior experience with international dating	Number of romantic partners from other countries	Simple numeric value

Scam awareness is assessed using variables "Total remote awareness", "CoT remote awareness", "Total personal experience with Scams"; "CoT personal experience", "Prior online victimization".

Table 4.4. Scam Awareness Variables

Variable	Description	Rule
Total remote awareness score	Categories of fraud provided: Advanced fee scams, Bank transfer scams, Western Union transfer cashing scams, Check cashing scams, Credit card transfer scams, Online investment scams, Donation scams, Phishing scams, Pharma scams, Dating scams, Marriage scams	1 point added for each type of scam checked off by participant
Remote awareness level	Grouped the values from the previous variable;	
CoT remote awareness score	Based on the answers to the previous question. CoT categories included "Dating scams," "Advanced fee scams," or "Phishing scams"	1 point added for each type of scam checked off
ODS remote awareness	Based on the answers to the previous question. If the category "Dating scams" was checked off, it was noted as "yes".	Dichotomous variable
419 remote awareness	Based on the answers to the previous question. If the category "Advanced fee scams" was checked off, it was noted as "yes".	Dichotomous variable
Phishing remote awareness	Based on the answers to the previous question. If the category "Phishing scams" was checked off, it was noted as "yes".	Dichotomous variable

Table 4.4 continued

Total personal awareness score	Categories of fraud provided: Advanced fee scams, Bank transfer scams, Western Union transfer cashing scams, Check cashing scams, Credit card transfer scams, Online investment scams, Donation scams, Phishing scams, Pharma scams, Dating scams, Marriage scams	1 point added for each type of scam checked off by participant
CoT personal awareness score	Based on the answers to the previous question. CoT categories included “Dating scams,” or "Advanced fee scams"	1 point added for each type of scam checked off
ODS personal awareness	Based on the answers to the previous question. If the category “Dating scams” was checked off, it was noted as “yes”.	Dichotomous variable
419 personal awareness	Based on the answers to the previous question. If the category “Advanced fee scams” was checked off, it was noted as “yes”.	Dichotomous variable
Prior cyber-victimization	Number of prior online victimization	Simple numeric value

Computer use is assessed using variables “Years as Internet user” and “Daily hours of Internet use”. *Computer literacy* is assessed using the “*IT training*” variable.

Table 4.5. Computer Use and Literacy Variables

Variable	Description	Rule
Years of Internet use	Years of Internet use	Simple numeric value
Hours per day	Categories of daily hours of computer use offered	Assigned a numeric value
Prior IT training	Values: "No special IT training," "Very little IT training," "Some training," "Extensive training"	Assigned a numeric value

4.4 RESULTS - DEMOGRAPHIC VARIABLES

4.4.1 Age

Nearly 74% of participants in this sample are over 40 years old, with 40 - 49 years old age category having the highest number of participants, followed by 50-59 years old. The 70+ category has only one participant, and thus has no variance in the data, so it is excluded from

analysis. In terms of number of victims in each age category, the highest risk category appears to be the 30-39 years olds (with 58% of participants in that category losing money to scam). Both the 40-49 years old and the 50-59 years old have 55% victimization risk. The lowest victimization risk in this sample is in the 20-29 years olds category (29%).

Table 4.6. Likelihood and Mean Loss Amount by Age Group

Age Category	Victimization Rate	Percent of Sample Total	Mean Loss Amount
<19	0.5	0.02	$5,459.00
20-29	0.29	0.06	$10,512.50
30-39	0.58	0.17	$3,642.36
40-49	0.55	0.37	$4,064.14
50-59	0.55	0.28	$3,885.94
60-69	0.33	0.08	$2,217.00
70+	1	0.01	$200.00

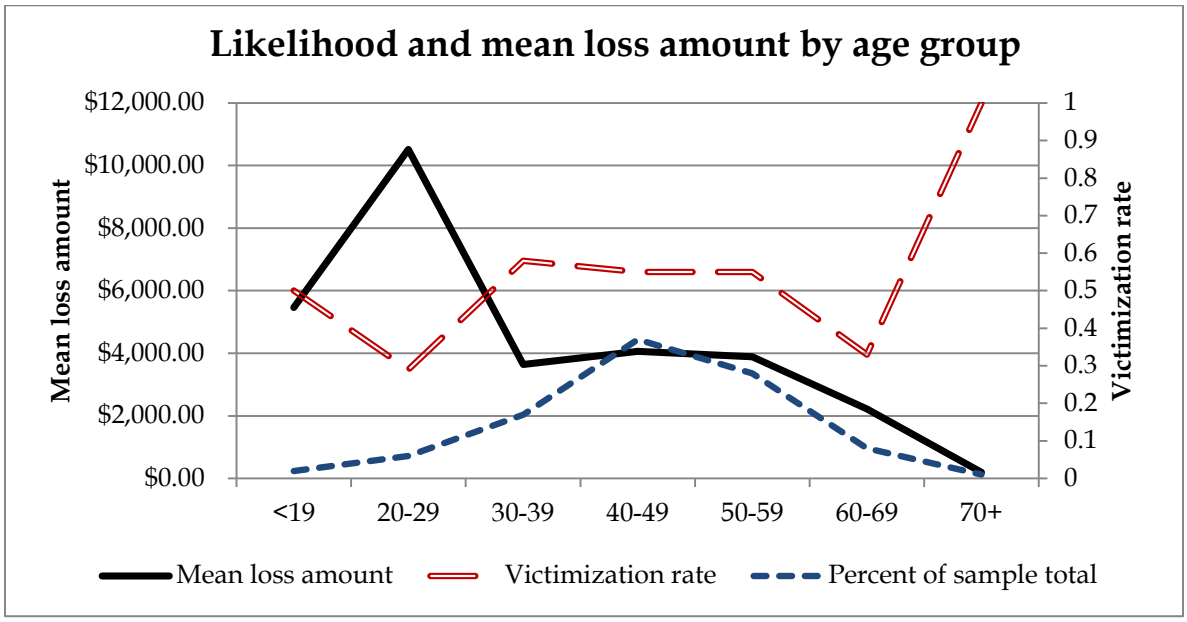

Figure 4.1. Likelihood and Mean Loss Amount by Age Group.

However, in terms of mean amount of loss across age categories, 20-29 years olds report the highest mean loss amount ($10,512.50), followed by those under 19 years old ($5,459). For both categories, however, the data seems to be skewed by one exceptional case with a high amount of loss that stands in contrast with the overall low reported losses. The individuals in the 40-49 years old category are the most consistent "losers" in every loss category, followed by 50-59 years old and by 30-39 years old.

T-test of age for groups Victims and Targeted gives t = 0.2164 and for Ha: diff != 0 Pr(|T| > |t|) = 0.8404

4.4.2 Country

The largest percentage of study participants (75%) is from English-speaking countries: United States (44%), followed by UK (14%), Canada (8%), and Australia (7%). This might be because one of the study participation requirements was the ability to read and write in English. Among European countries, Netherlands (West Europe) has the highest number of respondents. Excluding those countries that have only one respondent, the countries with the highest victimization rates (within-group percentage of Victims) are Australia (75% victimization rate), Norway (67%), France (67%), and Sweden (67%). The most "scam resistant" countries within this sample (among those that had variance in the table) are Italy (0% victimization rate), Netherlands (33%), and Canada (33%).

Table 4.7. Likelihood and Severity of Victimization by Country

Country	# of Participants	Percent of Sample Total	Victimization Rate	Mean Loss Amount
Australia	8	0.07	0.75	$8,623.50
Belgium	3	0.03	0.33	$20,691.00

Table 4.7 continued

Canada	9	0.08	0.33	$1,350.67
Costa Rica	1	0.01	0	$ -
Czech Republic	1	0.01	1	$3,480.00
Finland	2	0.02	0.5	$2,648.00
France	3	0.03	0.67	$3,103.50
Italy	2	0.02	0	$ -
Liechtenstein	1	0.01	1	$6,799.00
Netherlands	6	0.05	0.33	$1,828.00
New Zealand	1	0.01	1	$5,975.00
Norway	3	0.03	0.67	$4,130.00
Pakistan	1	0.01	0	$ -
Slovakia	1	0.01	1	$2,138.00
Spain	2	0.02	0.5	$ 469.00
Sweden	3	0.03	0.67	$1,551.50
USA	48	0.44	0.54	$2,662.62
United Kingdom	15	0.14	0.53	$5,320.50
Total	110			

Collapsing the sample data into regions, we see that the Australasia region shows the highest victimization rate (78%), followed by Northern Europe (63%), and UK (53%). The most "resistant" region in Europe appears to be Southern Europe (25% victimization rate). Leading the regions with the highest mean loss are Australasia, West Europe, and UK. The lowest mean loss amounts are observed in Southern Europe.

Table 4.8. Likelihood and Severity of Victimization by Region

Region	**Number of Participants**	**Percent of Sample Total**	**Victimization Rate**	**Mean Loss Amount**
Australasia	9	0.08	0.78	$ 8,245.14
Central America	1	0.01	0	$ -

Table 4.8 continued

Eastern Europe	2	0.02	1	$ 2,809.00
Middle East	1	0.01	0	$ -
North America	56	0.51	0.5	$ 2,438.71
Northern Europe	8	0.07	0.63	$ 2,802.20
South Asia	1	0.01	1	$ 4,996.00
Southern Europe	4	0.04	0.25	$ 469.00
UK	15	0.14	0.53	$ 5,320.50
West Europe	13	0.12	0.46	$ 6,225.50
Total	110			

4.4.3 Marital Status

Respondents report their marital starus as 47% “Never married,” followed by 35% “Divorced” and 15% "Separated." The “Widowed” category has only 1 respondent, and therefore will be excluded from the analysis. The lowest risk of victimization is in the “Married” category (0%), while the highest risk is in the “Never married” category (62%). However, the highest mean loss amount is in the “Separated”category, followed by “Never married”.

T-test for this variable produced t = 1.7753 and Pr(|T| > |t|) = 0.0787.

Table 4.9. Likelihood & Severity of Victimization by Marital Status

Marital status	**$0**	**> $1000**	**$1,000 - $2,999**	**$3000 - $4,999**	**$5000 - $9,999**	**$10,000 - $50,000**
Never married	20	8	8	8	7	1
Separated	10	1	0	1	3	1
Divorced	19	5	8	5	1	1
Widowed	1	0	0	0	0	0
Married	2	0	0	0	0	0
Total	52	14	16	14	11	3

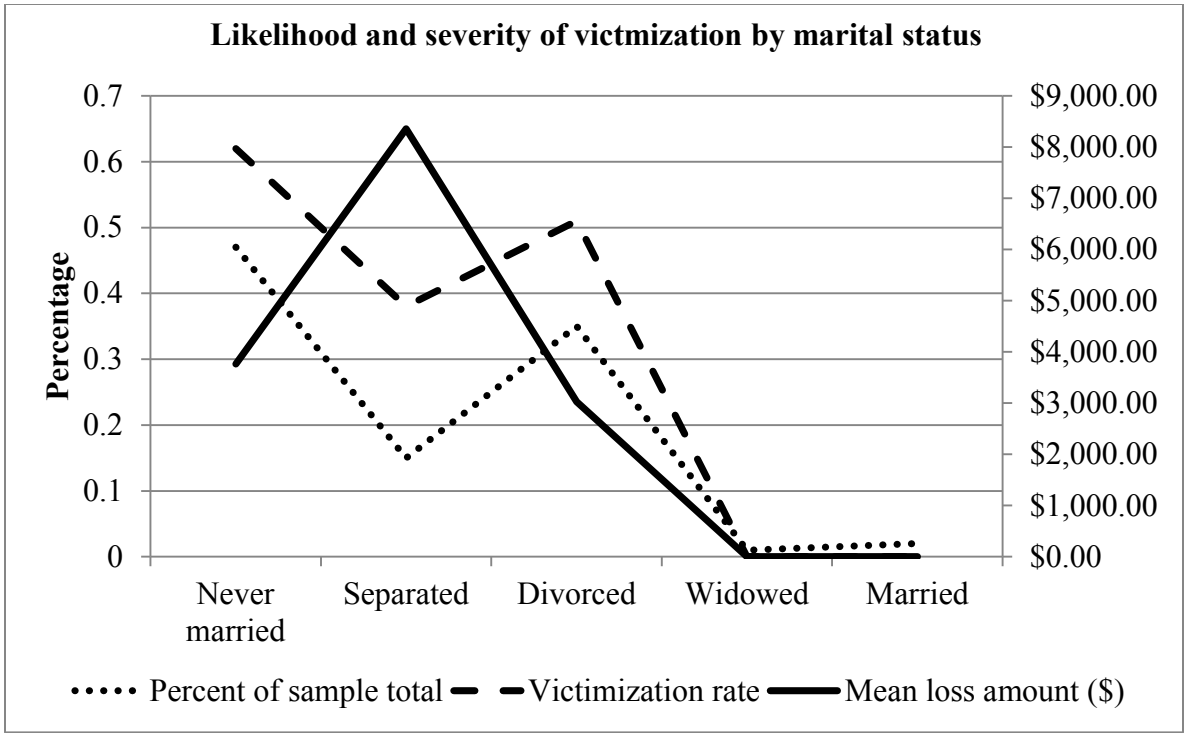

Figure 4.2. Likelihood & Severity of Victimization by Marital Status.

4.4.4 Employment status

From the standpoint of employment status, the highest victimization risk is found among the following groups: Part time employed (100% victimization rate), employed with 2 jobs (74%), and unemployed (64%). The lowest victimization rate is associated with groups "self-employed" (20%), "unemployed without government assistance" (33%), and "employed, with 3 or more jobs" (33%). The group "employed, with one job" has a 48%% victimization rate.

In terms of severity of victimization, the highest mean loss amounts are recorded for participants in the "part time" ($6,403), "self-employed" and "employed, with 2 jobs" (approximately $5,800 for both groups). The lowest mean loss amount is recorded for the "employed, with 3 jobs" group ($400). The variable did not reach significance (t = 0.9229 Pr(|T| > |t|) = 0.3581).

Table 4.10. Likelihood & Severity of Victimization by Employment Status

Employment Status	Number of Participants	Percent of Sample Total	Victimization Rate	Mean Loss Amount
Not specified	1	0.01	1	$1,784.00
Unemployed; no government assistance	3	0.03	0.33	$2,648.00
Unemployed; with government assistance	11	0.1	0.64	$3,891.88
Employed; part time	4	0.04	1	$6,403.00
Employed; 1 job	52	0.48	0.48	$2,752.48
Self-employed	22	0.2	0.5	$5,882.82
Employed; 2 jobs	8	0.07	0.75	$5,738.67
Employed; 3 or more jobs	3	0.03	0.33	$400.00
Retired	5	0.05	0.4	$2,850.00
Total	109			

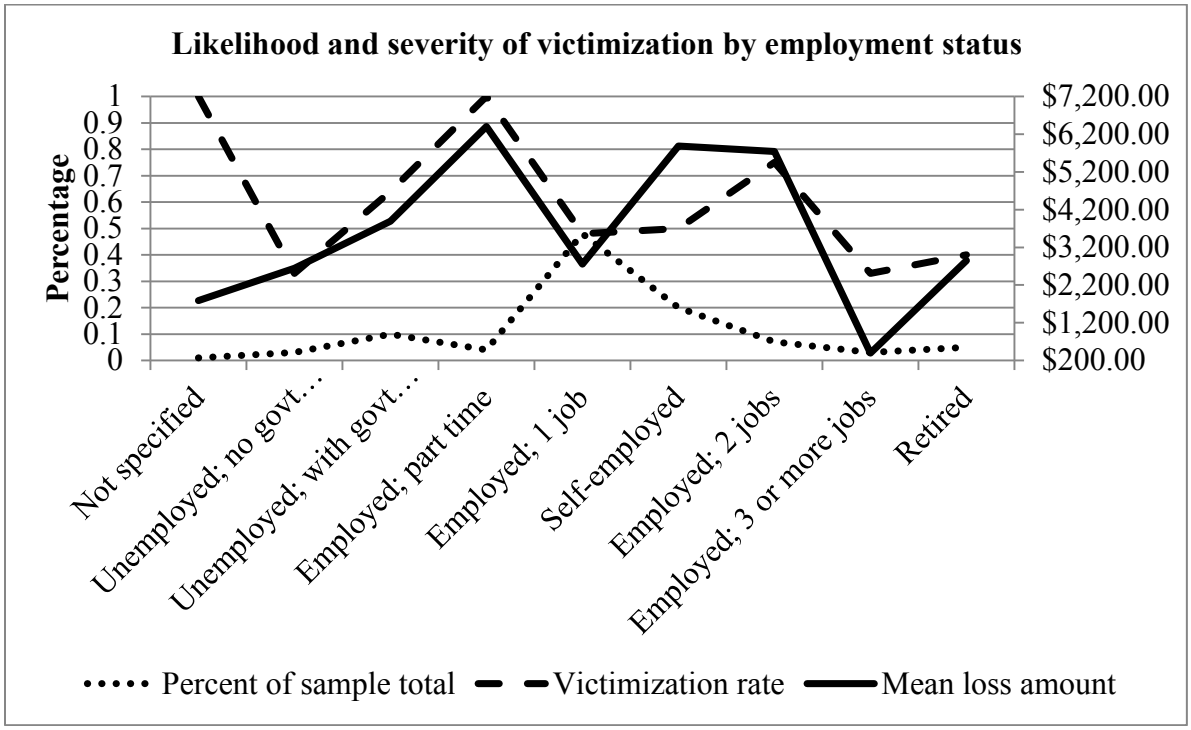

Figure 4.3. Likelihood & Severity of Victimization by Employment Status.

4.4.5 Monthly income

About 55% of the respondents have a monthly income of less than $3,000 USD. Categories "$10,000-$14,999" and "$15,000+" have only one entry each and, therefore, will be excluded from analysis. Likelihood of victimization is highest for the "$2,000-$2,999" category (65%), followed by the "$1,000-$1,999" (61%) and "$5,000-$7,999" categories (57%). Generally speaking, the highest income categories in this sample are associated with a lower likelihood of victimization (the exception being the "$5,000-$7,999" category).

Mean loss amounts, however, do not follow any particular pattern. The highest lost amount of $7,926 is in the "$8,000-$9,999" category, followed by mean loss of $7,526.75 in the "$0-$999" category. The "$2,000-$2,999" category also shows a very high mean loss as compared to the rest of the categories for this variable. Overall, the higher income categories are associated with lower mean loss amounts (the exception being the "$8,000-$9,999" category).

T-test for this variable produced t = 0.2145 and Pr(|T| > |t|) = 1.2487

Table 4.11. Likelihood & Severity of Victimization by Income Category

Monthly Income Category	# of Participants	Percent of Sample Total	Victimization Rate	Mean Loss Amount
$0 -$999/mo	15	0.14	0.53	$7,526.75
$1,000 - $1,999/mo	28	0.26	0.61	$2,967.65
$2,000 - $2,999/mo	17	0.16	0.65	$6,754.33
$3,000 - $3,999/mo	17	0.16	0.35	$2,401.50
$4,000 - $4,999/mo	13	0.12	0.38	$2,495.40
$5,000 - $7,999/mo	14	0.13	0.57	$2,184.88
$8,000 - $9,999/mo	3	0.03	0.33	$7,926.00

Table 4.11 continued

$10,000 - $14,999/mo	1	0.01	1	$200.00
$15,000+ / mo	1	0.01	0	$3,366.50
Total	109			

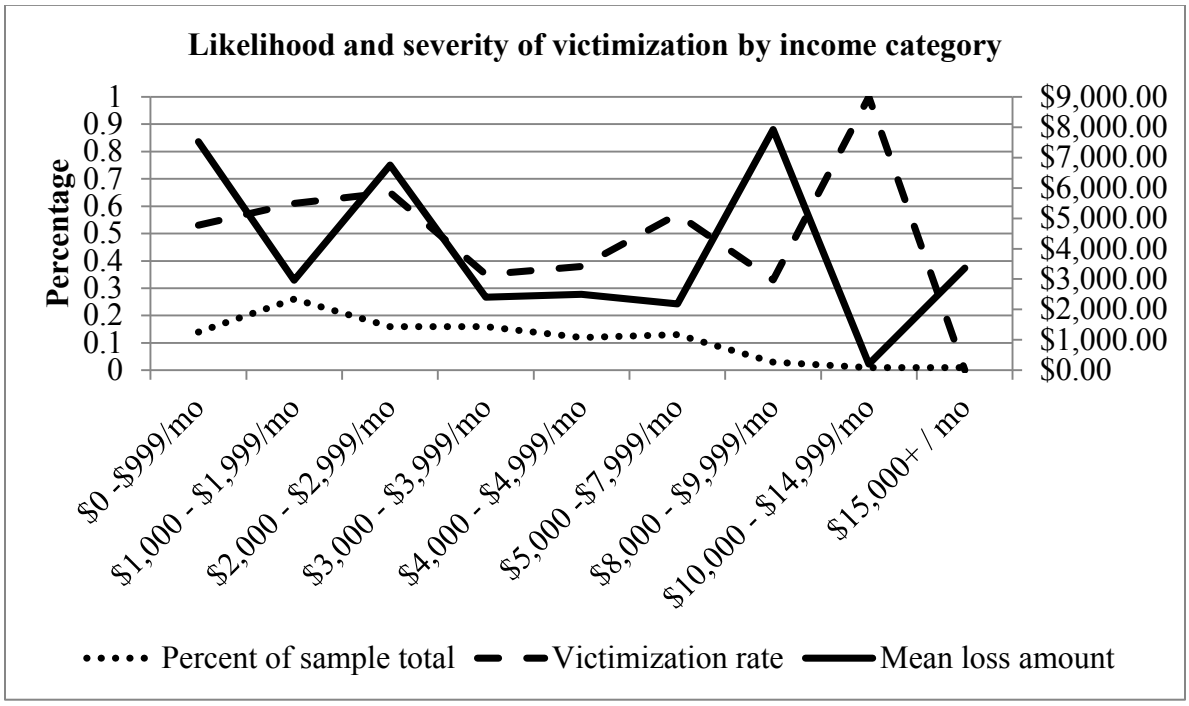

Figure 4.4. Likelihood & Severity of Victimization by Income Category.

4.4.6 Education

Post-high school education is indicated by 69% of the participants, and out of those, slighly less than half indicate having 5 years of higher education or more. Surprisingly, college graduates and non-college graduates show similar vulnerability to victimization. The highest risk groups are "without high school diploma" (80% victimization rate), and those with 7 years of college education and above.

The highest mean loss amounts are recorded for participants with 3 years of college education

($7,897.40) and for those with 10+ years of college education ($4,778.50). Overall, there is no trend observed, perhaps also due to the fact that some groups consist of only 4-5 individuals, making the data suseptable to greater fluctuations. The variable does not reach significance (t = 0.4650, Pr(|T| > |t|) = 0.6428).

Table 4.12. Likelihood and Severity of Victimization by Years of Higher Education

Years of Higher Education	Number of Participants	Percent of Sample Total	Victimization Rate	Mean Loss Amount ($)
No HS Diploma	5	0.05	0.8	$2,918.00
HS Graduate	26	0.24	0.58	$4,171.60
2 yrs	26	0.24	0.54	$3,689.64
3 yrs	11	0.1	0.45	$7,897.40
4 yrs	10	0.09	0.3	$3,245.00
5 yrs	15	0.14	0.47	$4,351.71
6 yrs	5	0.05	0.6	$1,844.00
7 yrs	4	0.04	0.75	$2,496.33
8 yrs	1	0.01	0	$ -
9 yrs	3	0.03	0.67	$1,424.00
10+ yrs	4	0.04	0.5	$4,778.50
Total	110			

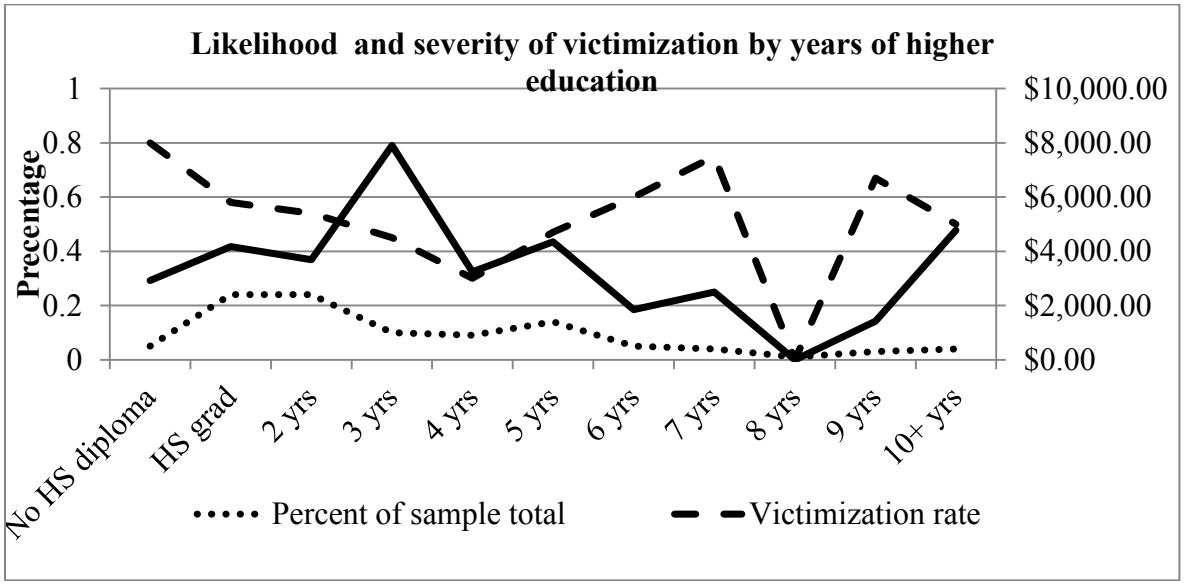

Figure 4.5. Likelihood & Severity of Victimization by Years of Higher Education.

4.4.7 Summary of results for demographic variables

In respect to demographic variables, the most reliable predictors of likelihood of victimization appear to be marital status and country of residence. *Marital status* is the only demographic variable to approach significance in t-test (t = 1.7753 and p= 0.0787). Respondents who indicate no prior marriages are more likely to respond to money socitation by the scammers than those who do indicate prior marriages. However, in terms of severity of loss, marital status does not provide a clear pattern. Those who are separated at the time of the scam have the highest mean loss despite having the lowest victimization rate, while participants in the "Never married" and "Divorced" categories have very similar mean loss amounts. Therefore, we could say that marital status appears to be able to predict the likelihood but not the severity of victimization.

A respondent's *age* does seem to play a role in the outcome of the scam. Participants between 30 and 59 years old show victimization pattens that are moderate but very stable both in terms of likelihood of sending money and in terms of mean loss amount.There are very few respondents under 30 years old in the sample, and their results show low oveall vulnerability but high severity of victimization.

The fact that the sample has so few young participants may indicate that young Internet users who do become victimized have some additional qualities (e.g., low self-control, low computer literacy, high strain, or some other factors) that are not visible in the current analysis. For example, the only respondent in the "<19 yo" category to send money indicates unemployment and a high degree of governmental assistance due to Parkinson disease, but that relationship is impossible to detect without close examination of the case information.

In respect to respondent's *country of residence*, a high number of participants from native English-speaking countries could indicate that those countries are heavily targeted by scammers. Australia and countries in Northern Europe appear to both have high victimization rates and hight mean loss amounts. The United States and United Kingdom both display simialr victimization rate (about 50%), but UK respondents have a mean loss amount twice as large as that reported by US respondents. Countries in Southern Europe seem to enjoy a high resistance rate and low mean loss amounts per participant.

The *monthly income* variable, on the other hand, does produce some detectable patterns. Inidivuduals reporting monthly incomes less than $2,999 comprise slightly more than half of the sample, which may indicate that this type of scam draws in a large percentage of lower-income Internet users. The same category of respondents (with monthly income less than $2,999) show the most stable patterns of vulnerability to ODS, both from the standpoint of likelihood of victization and based on mean loss amounts. Victimization rates and severity of victimization for higher-income categories are comparatively low, with few exceptions.

In terms of *employment status*, no particular pattern can be observed, except that respondents with apparent employment instability (e.g., part-time employed, employed with 2 jobs, and unemployed) carry the highest victimization risk, with part-time employed being the highest risk group. It might be worth noting that risk differences within the "employed" category are profound. Respondents with 1 job show a 50/50 chance of responding to the scammers' solicitations and a fairly "average" mean loss amount, while those with 2 jobs have one of the highest victimization rates and mean victimization amounts. Conversely, those with 3 or more jobs have one of the lowest victimization rate and the lowest mean loss amount. Although the

variable did not reach significance, the results may indicate that using simplified categories such as “employed” or “unemployed” may mask important differences among the sub-categories.
The number of *years of college education* variable seems to have no consistent effect on the suceptability to the scam in this sample. The higher mean loss amounts gravitate toward users with less than 4 years of college education, but overall there is no obvious trend observed, perhaps also due to the fact that some goups consist of only 4-5 individuals, making the data suseptable to greater fluctuations. The variable does not reach significance.

4.5 ROUTINE ACTIVITIES

4.5.1 Seeking a partner

The respondents in this study indicate their status in the process of searching for a romantic partner at the time the scammer approached them in one of three catgories. The response options are “Not seeking any relationship,” “Wishing for a partner but not actively seeking,” and “Actively seeking.” Participant responses indicate that the majority are either actively seeking (58%) or wishing for a romantic partner (48%), and only 6% of the responses indicate not seeking any relationship. This may indicate that the scammers are fairly accurate in their targeting efforts. On the other hand, it may indicate that those who are not seeking any relationship are least likely to take part in our study.
The highest likelihood of victimization (66%) is among those activityseeking a romantic partner, followed by those who are hoping but not actively seeking (41%). The lowest victimization rate is among the participants not looking for anyone at all.
From the standpoint of severity of victimization, those who are feeling lonely but not actively

seeking any romantic relationship sustained the greatest loss, followed closely by those who are actively seeking a relationship. Those who are not seeking any relationship have relatively insignificant losses. The different between the groups does reach statistical significance.

t = -3.1664 Pr(|T| > |t|) = 0.0020

Table 4.13. Likelihood and Severity of Victimization by Relationship Search Status

Seeking Relationship	Percent of Sample Total	Victimization Rate	Mean Loss Amount
Not seeking any relationship	0.05	0.17	$469.00
Wishing for partner	0.42	0.41	$4,255.26
Actively seeking	0.53	0.66	$3,939.26
Total	1		

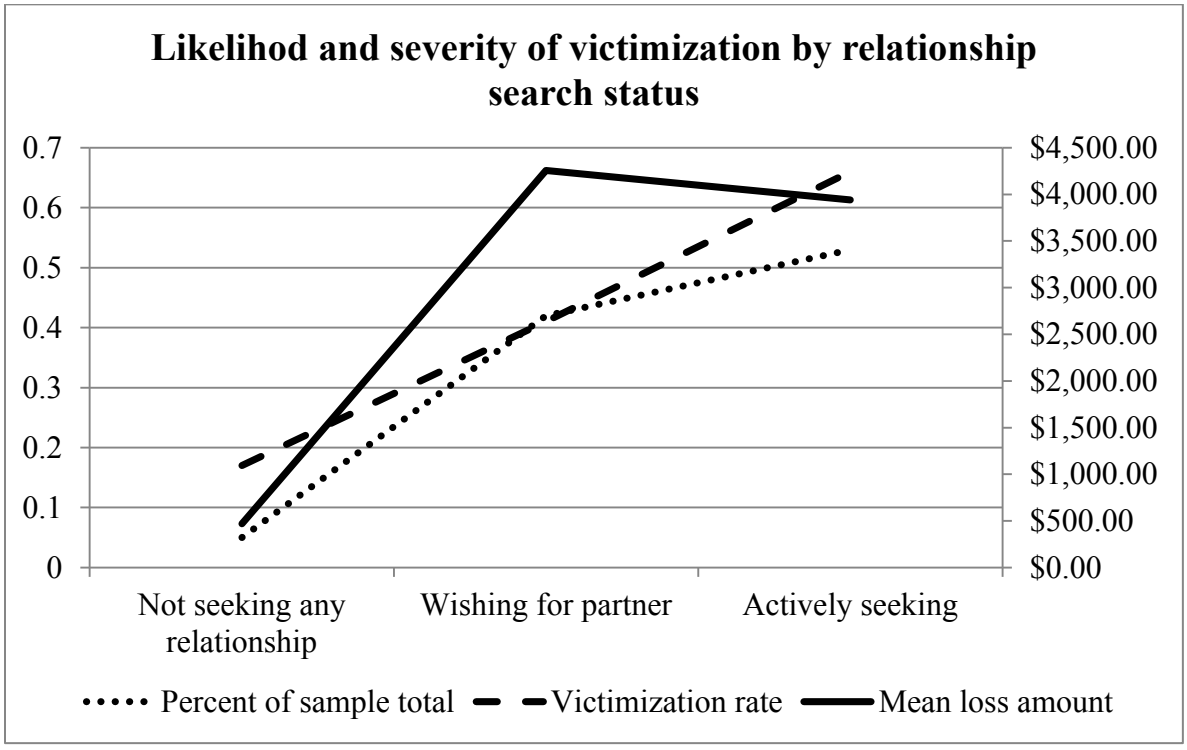

Figure 4.6. Likelihood & Severity of Victimization by Relationship Search Status.

4.5.2 Online search

Internet use for seeking a romantic relationship is another indicator that is tested. A total of 23 respondents (21% of the sample) indicate that they are not using the Internet for their search (out of those 23, six respondents are not looking for any relationship at all). Their likelihood of victimization is comparatively low (30% of respondents in that category lost money). Those utilizing the Internet accounted for 79% of respondents, and they also show highest victimization likelihood (59% of respondents in this category lost money due to a scam).

In terms of severity of victimization, those using the Internet in their search reporte loosing twice as much as those not using the Internet ($4,188.41 versus $2,486, respectively). Although the mean loss for those who did use Internet is still higher, the differences between the groups does reach statistical significance. t = -2.4514 Pr(|T| > |t|) = 0.0158

Table 4.14. Likelihood and Severity of Victimization by Online Search

Online Search	Percent of sample total	Victimization rate	Mean loss amount
No	0.21	0.3	$2,486.00
Yes	0.79	0.59	$4,188.41

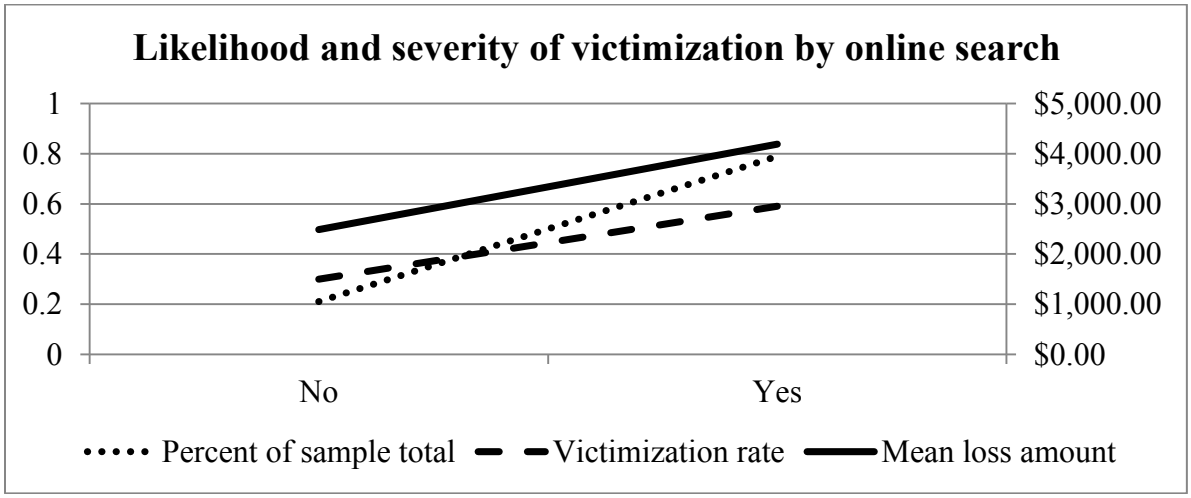

Figure 4.7. Likelihood and Severity of Victimization by Online Search.

4.5.3 Focus of online search

To avoid confusion with terminology, participants are not asked directly whether they are members of international dating sites. Instead, participants are asked whether their online search is focused on finding someone from their own country or from a foreign country. Indication of their search focus is treated as an indirect indicator of the type of dating site they are most likely browsing. When reviewing the results, one needs to keep in mind that visits to international dating sites are inferred, but not directly indicated.

About 46% of the respondents indicate that they are open to all possibilities, while 15% indicate that they are specifically looking for a partner from a foreign country. However, between-group comparisons produce striking results. Likelihood of victimization is very high among those participants who are primarily interested in international dating (over 80% of them lost money due to a scam), followed by those participants in the “Open to all possibilities” category (60% lost money). The category showing the highest resistance to victimization is the "no interest in online search" category (only 30% lost money), followed by those respondents who are looking for someone from their own culture (40%).

Table 4.15. Likelihood and severity of victimization by focus of online search

Int'l focus of online search	Percent of sample total	Victimization rate	Mean loss amount
No online search	0.21	0.3	$2,486.00
No interest in international dating	0.18	0.4	$3,950.88
Open to all possibilities	0.46	0.59	$4,082.60
International focus	0.15	0.81	$4,578.77

Total average loss per respondent follows the same pattern: It is highest among the respondents looking for a partner from another culture, followed by respondents in the “Open to all

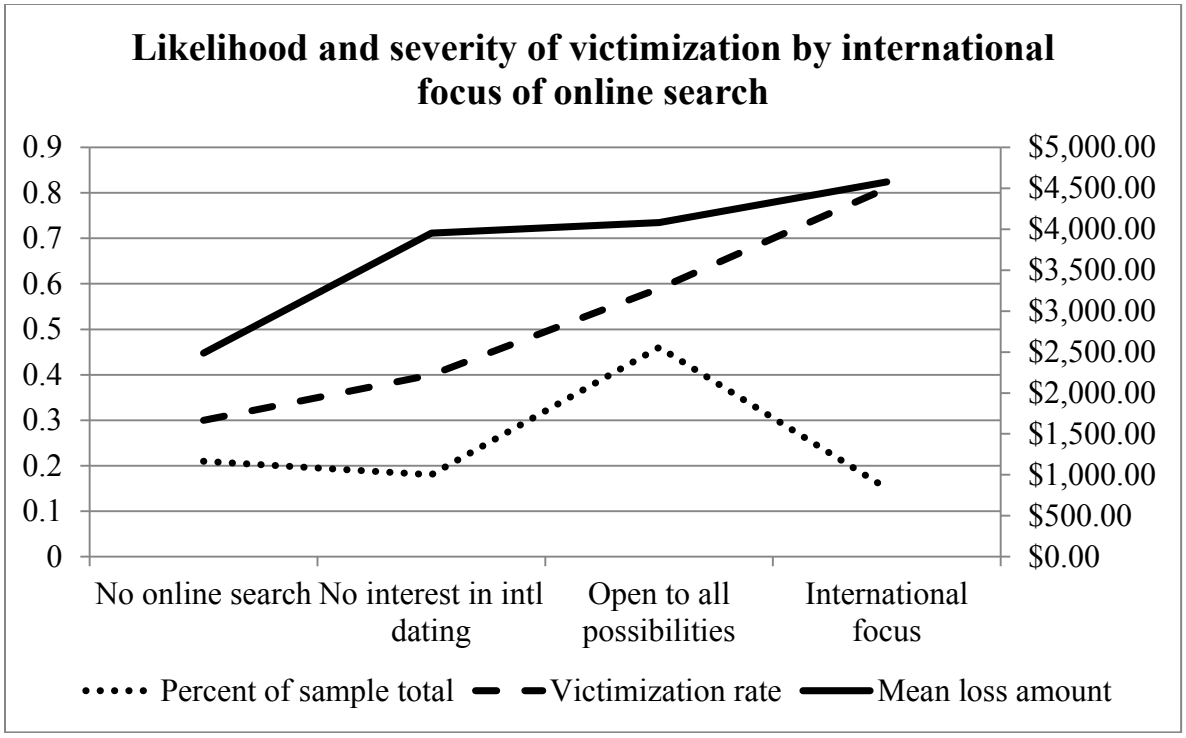

Figure 4.8. Likelihood and severity of victimization by focus of online search.

possibilities" group. Those respondents reporting visiting no online dating sites have the lowest mean loss amount, although their loss was still significant.

Differences between the groups reached statistical significance.

T-test for this variable produced t = -3.5492 and Pr(|T| > |t|) = 0.0006 for Ha: diff != 0

4.5.4 International dating experience

Prior consideration of international dating

Patricipants in this study reporting seriously considered international dating (i.e., dating someone from another country or culture) prior to their encounter with the scam perpetrator comprise nearly 60% of the respondents. Likelihood of victimization, however, is very similar between those who would consider it, and those who would not. It appears that prior consideration of international dating has no significant bearing on the likelihood of victimization.

In terms of severity of victimization, those considering international dating prior to being scammed report higher average losses than those who do not consider international dating. This may indicate that prior consideration of international dating does not necessarily provide Internet users any better ability to protect themselves from online dating scams.

t = -0.2800 Pr(|T| > |t|) = 0.7800

Table 4.16. Likelihood and Severity of Victimization by Prior International Dating Consideration

Prior Consideration of International Dating	Number of Participants	Percent of Sample Total	Victimization Rate	Mean Loss Amount
No	45	0.41	0.51	$3,663.35
Yes	65	0.59	0.54	$4,192.97

Prior experience with international dating

The majority of participants in this study report no experience with dating someone from another country prior to their encounter with the scammer, while 23% report one prior experience. It is interesting that 14% of respondents report having four or more prior dating experiences with international partners, indicating that those users involved in international dating were likely to continue seeking such experiences.

In terms of likelihood of victimization, those who report having four of more prior experiences with international dating also report the highest likelihood of victimization (60%), followed by those with no prior experience (57%), but overall, there are no drastic differences among the groups in terms of likelihood of victimization.

In terms of the severity of victimization there are, however, some discernable differences. Those reporting no prior experience with internaltional dating and those with only one prior experience display nearly identical mean loss amounts ($4,462.31 versus $4,445.60). Those with more than one previous experience show significantly smaller average losses.

t = 0.0150 Pr(|T| > |t|) = 0.9880

Table 4.17. Likelihood and Severity of Victimization by Prior International Dating Experience

Prior experience with international dating	Percent of sample total	Victimization rate	Mean loss amount
Never	0.51	0.57	$4,462.31
On 1 occasion	0.23	0.4	$4,445.60
On 2 occasions	0.12	0.54	$2,456.43
On 3 occasions	0.01	0	$0.00
On 4 occasions or more	0.14	0.6	$2,951.78

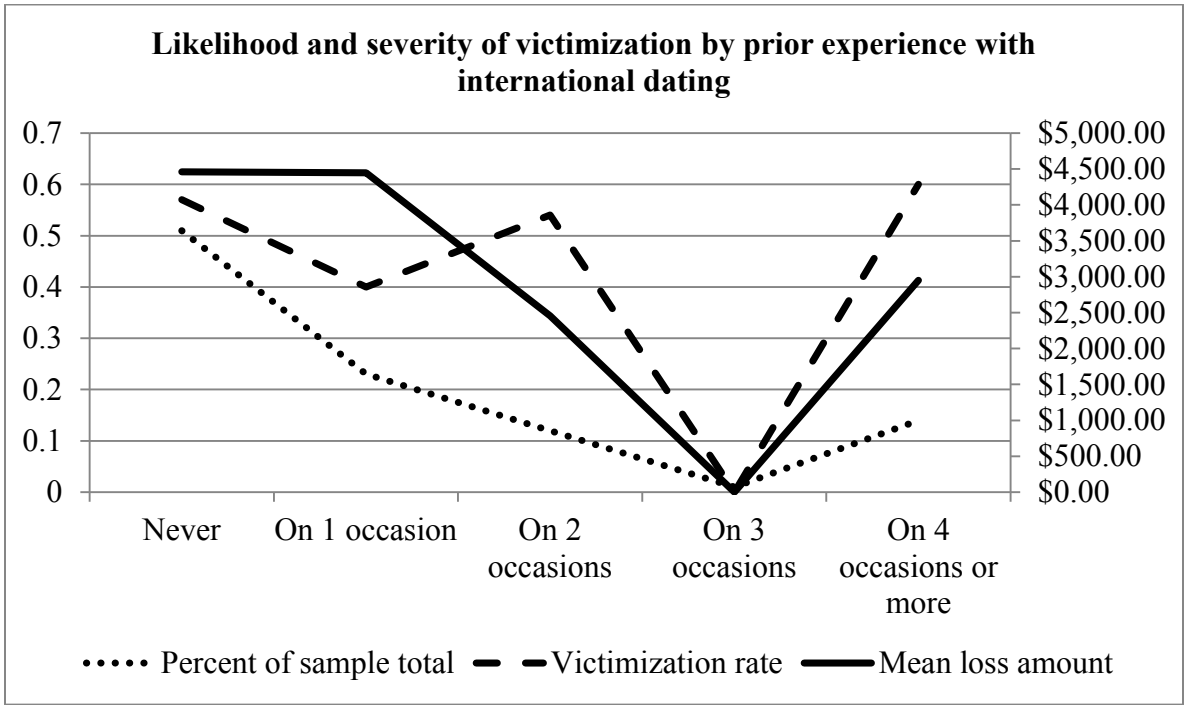

Figure 4.9. Likelihood and Severity of Victimization by Prior International Dating Experience.

4.5.5 Remote scam awareness

In this study, awareness obtained through second-hand accounts is labled as *remote awareness*. Although the information is cognitively processed, it may not have been salient to the recipient of the information at the time it was processed. However, it seems logical to hypothise that

Internet users who have been exposed to iniformation about a greater variety of online frauds would be better able to identify a suspicious communication.

To test that hypothesis, the author first attempts to create a relative scale of "fraud awareness." Each study participant is provided a list of 11 types of common Internet scams and asked to indicate which of those types of scams they have seen discussed in online or offline media. Each type of scam the participant checks off is counted as one point. "Total remote awareness"score (with a possible range of 0-11) is calculated based on the total number of frauds that each participant checkes off. After that, the "levels" of awareness are assigned to the scores.

Given that the "baseline" level of awareness within population or even within the sample is unknown, the preliminary assignment of levels are as follows:

- Score 0 is labled "0"
- Scores 1-2 are labled "very low"
- Scores 3-4 are labled "low"
- Scores 5-6 are labled "average"
- Scores 7-8 are labled "high"
- Scores 9-11 are labled "very high"

Given that this assignment of lables is purely arbitrary, the analysis is performed using raw scores rather than grouped labeles.

As can be seen from the table, about 44% of participants score between 0 and 4 – very low scores of scam awareness. The same group show the highest rate of victimization – 90% of participants scoring "2" went along with the scammers' requests, followed by 60% of those scoring "1", and 55% of those scoring "0." Outside of the lowest scoring category, the risk of

victimization hovers around 30-50% for all groups except for those with the highest scores ("9" and "10"), who have a 0% victimization rate.

In terms of justification for the arbitrary asisgnment of lables to the awareness scores, the results indicate that frequency-wise, the score of "0" was the most frequently occuring score, and that all values with occurrence frequency of over 10 were found below the score of "5." This tentatively indicates that scores above "4" (labled "low") are uncommon within this sample, and thus the lable "average" should not be applied to any score above "4." However, the results collected so far do not provide enough information for the author to determine which awareness scores within this sample could be considered as "low" or "very low."

Table 4.18. Likelihood and Severity of Victimization by Total Remote Scam Awareness Score

Total Remote Awareness	Frequency of Occurrence	Percent of Sample Total	Victimization Rate	Mean Loss Amount
0	22	0.2	0.55	$4,338
1	15	0.14	0.6	$3,346
2	11	0.1	0.91	$4,536
3	11	0.1	0.45	$2,189
4	20	0.18	0.5	$3,571
5	6	0.05	0.33	$3,229
6	6	0.05	0.5	$9,848
7	11	0.1	0.36	$2,614
8	6	0.05	0.5	$3,453
9	1	0.01	0	$0
10	1	0.01	0	$0

In contrast, highest mean amount lost ($9,848) is among the participants scoring "6", followed by those scoring "2" and "0", with both the "2 points" and "0 points" groups having an average loss around $4,500. This indicates that not only is the "0 -2" group highly likely to agree to send money upon request, but they are also very likely to lose a significant amount in the process.

T-test for this variable produced $t = 1.8767$ and $Pr(|T| > |t|) = 0.0633$.

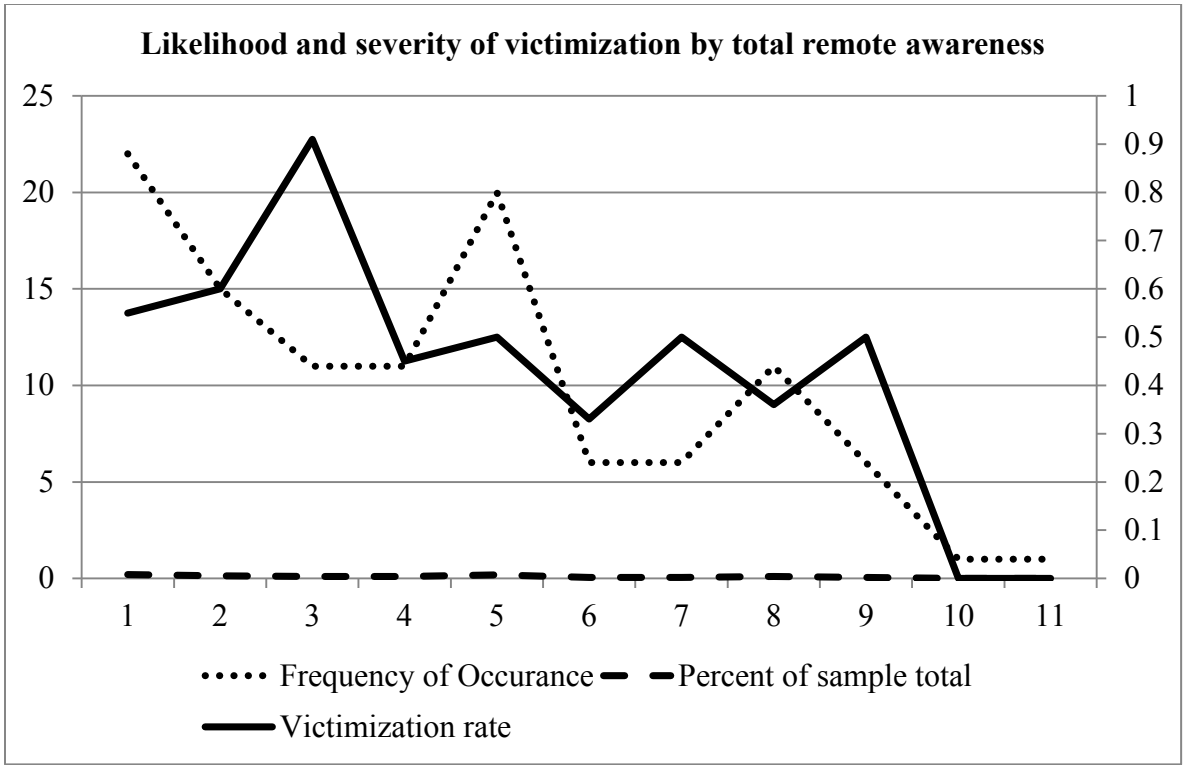

Figure 4.10. Likelihood and Severity of Victimization by Total Remote Scam Awareness.

4.5.6 Remote awareness of crimes of trust

Because the ODS scams combine elements of phishing and 419 scams, awareness scores for the three types of crimes of trust are combined into a separate table. From Table 4.13, it is apparent that awareness about all three frauds hovered in the 30 to 45% range. One interesting point to note is that the more prolific 419 scams received the lowest awareness score.

Table 4.19. Likelihood and Severity of Victimization by Remote CoT Awareness

Remote Awareness	Percent of Sample Total	Victimization Rate	Mean Loss Amount
ODS			
No - Low	0.62	0.57	$4,733
Yes	0.38	0.45	$2,444
419			
No - Low	0.71	0.56	$4,246
Yes	0.29	0.44	$3,156

Table 4.19 continued

Phishing			
No - Low	0.59	0.6	$3,736
Yes	0.41	0.42	$4,490

Participants indicating no remote awareness of these types of scams report higher mean loss per victim (e.g., participants with no knowledge of ODS have a mean loss of $4,732.56 compared to $2,444.26 among those that are aware of this type of scam; participants with no knowledge of 419 scams lost on average $4,246.16 compared to $3,155.71 among those that are aware of this type of scam). Interestingly, the relationship is the reverse for phishing: participants *unaware* of phishing lost on average $3,735.82 compared to $4,490.21 among those that *are aware* of this type of scam, though the amounts lost by both the aware and the unaware groups are very close. Overall, results indicate that remote awareness of crimes of trust correlates with a lower likelihood of victimization and a lower overall severity of victimization.

T-test for remote awareness of ODS produced t = 1.2338 and Pr(|T| > |t|) = 0.2200, for 419 scams - t = 1.7922 and Pr(|T| > |t|) = 0.0759; for phishing - t = 1.8480 and Pr(|T| > |t|) = 0.0673 for Ha: diff != 0

4.5.7 Personal scam awareness

The participants indicating personal experience with any of the Internet scams on prior occasions are expected to recognize signs of such scams more readily than participants that have never personally encountered them. The expectation of this author is that such encounters should generate awareness of and alertness to signs of a scam on a much more personal level, since the information about the scam signs would likely be processed not only on the cognitive level but

also on the emotional level. This should make it more salient and more likely to be recalled in a repeated encounter. In this study, such form of awareness is referred to as "*personal awareness*", to emphasize its difference from remote awareness.

The labeling system initially used applies the same *remote awareness* variables to the *personal awareness* variables. However, frequency-wise it appears the highest frequency of occurrence within this sample is "0" (frequency =50), and no scores above "2" show occurrence of a frequency over 10. Thus, it seems that a score of "0" should be considered as "average" in the *personal awareness* sample, as the majority of respondents in the sample (80%) score between "0" and "2" on total personal scam awareness. This range of awareness scores directly correlates with the highest likelihood of victimization. Participants with lower personal awareness report the highest victimization rates, and participants with higher personal awareness scores generally have a lower likelihood of victimization.

Information on the average amount lost provides an interesting insight. Only a few participants score above "5" on personal scam awareness, and those "high awareness" participants who did send money report losing significant amounts. For the rest of the respondents (scores 0-5), those with the lowest awareness score of "0" have the highest average loss.

Table 4.20. Likelihood and Severity of Victimization by Total Personal Awareness Score

Total Personal Awareness	Frequency of Occurrence	Percent of Sample Total	Victimization Rate	Mean Loss Amount
0	50	0.45	0.56	$4,496
1	25	0.23	0.60	$2,813
2	13	0.12	0.69	$2,520
3	9	0.08	0.22	$3,825
4	5	0.05	0.20	$1,379
5	2	0.02	0.50	$500
6	2	0.02	0.00	$0

Table 4.20 continued

7	1	0.01	1.00	$27,261
8	1	0.01	0.00	$0
9	1	0.01	0.00	$0
11	1	0.01	1.00	$3,449

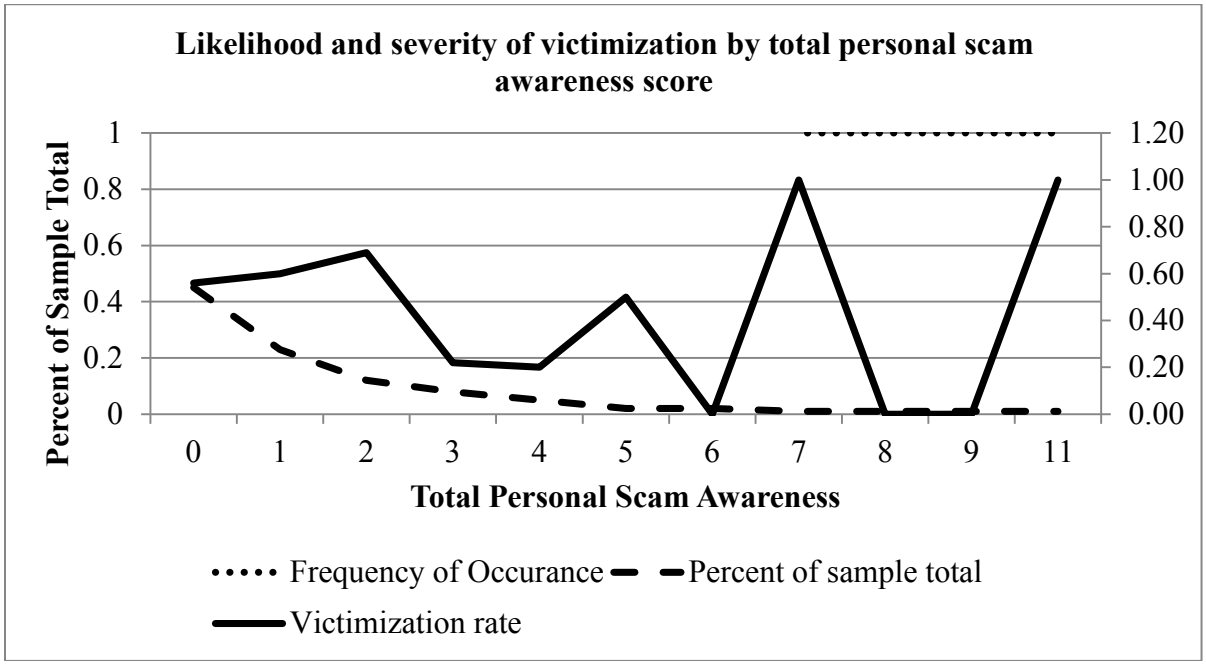

Figure 4.11. Likelihood and severity of victimization by total personal awareness.

4.5.8 Personal experience with crimes of trust

There is no clear pattern in the data regarding prior personal experience with crimes of trust (specifically, the 419 and the ODS scams). Only 10% of participants that sent money indicate that they had prior personal experience with 419 scams, and their victimization rate is fairly low - 27% as opposed to 56% victimization rate among those who did not. On the other hand, 21% of participants had prior experience with ODS, and their victimization rate was high (61%) - slightly higher than among those with no prior experience with ODS.

Table 4.21. Likelihood and Severity of Victimization by Personal CoT Experience

Total personal awareness	Percent of sample total	Victimization rate	Mean loss amount
ODS			
No	0.79	0.51	$4,459
Yes	0.21	0.61	$2,488
419			
No	0.9	0.56	$4,065
Yes	0.1	0.27	$2,483

However, in terms of the severity of victimization, the data is more consistent. Prior experience with both types of scam has a significant impact on the average loss per victim. The "inexperienced" victims lose on average twice the amount that the "experienced" victims do, indicating that those who have prior experience with 419 and ODS scams are able to end the scam far earlier.

T-test for total personal scam awareness variable produced $t = 1.4754$ and $Pr(|T| > |t|) = 0.1430$; t-test for personal knowledge of ODS produced $t = -0.8745$ and $Pr(|T| > |t|) = 0.3838$; for personal knowledge of 419 scam - $t = 1.7922$ and $Pr(|T| > |t|) = 0.0759$.

4.5.9 Prior online victimization

Based on participant reports, about 66% of the sample participants indicate that they had never been defrauded of money online at the time the scammers approached them, while 28% indicate that they were defrauded of money on one prior occasion, and 5% of respondents indicate that they were defrauded online on two prior occasions. Interestingly, 3% of the sample indicates that they have been victims of online scams on five or more occasions, but that group of respondents indicates a very low likelihood and low severity of victimization. The overall lack of respondents

in “repeated victimization” categories may be indicative of the fact that targeting efforts fail against those Internet users who have multiple fraud victimizations.

However, it is worth noticing that all five participants who report having been victims of online scams twice in the past were victimized, making them the highest risk group in the sample (100% victimization rate), followed by those who have been victims once before (with 54% victimization rate). Those who have never been a victims of Internet fraud before have a 50% victimization rate. Those who are victims of multiple online scams, more than twice, have very low to zero victimization rates.

Table 4.22. Likelihood and Severity of Victimization by Prior Online Victimization

Prior online victimization	Percent of sample total	Victimization rate	Mean loss amount
Never	0.66	0.5	$4,834
1 time	0.26	0.54	$3,260
2 times	0.05	1	$819
3 times	0.01	0	$0
5 or more times	0.03	0.33	$500

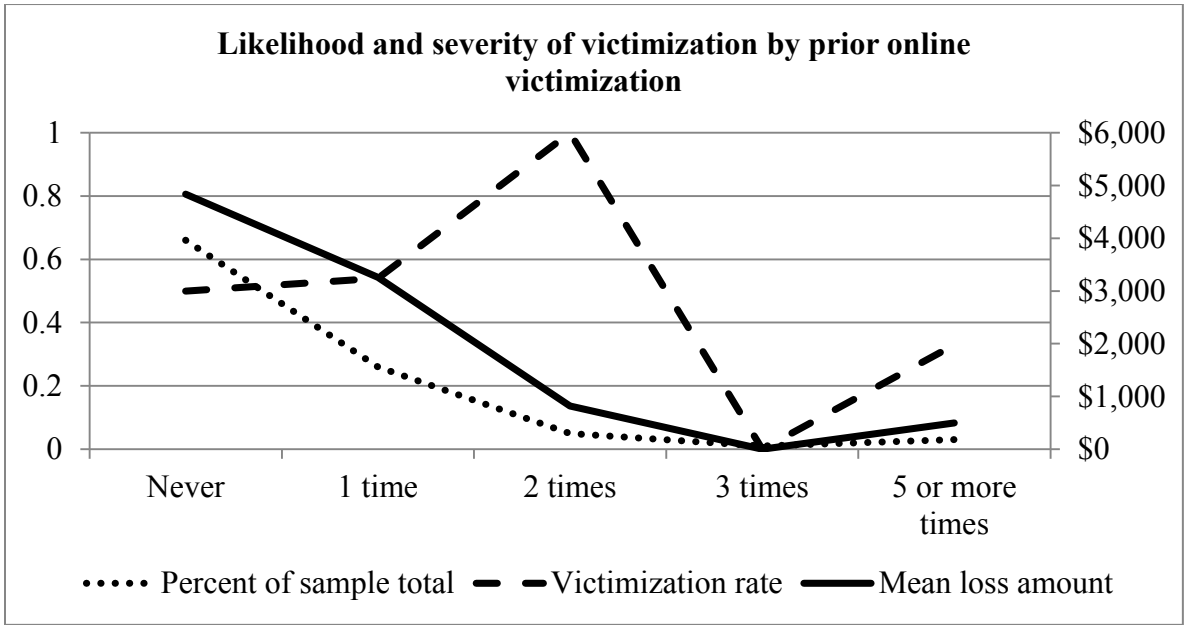

Figure 4.12. Likelihood and severity of victimization by prior online victimization.

Average loss amounts among the groups show a more consistent pattern. Mean amount lost is highest among those participants who never lost money previously due to an online scam ($4,834.47), or those only losing money once ($3,259.53). On the other hand, users in the repeated victimization categories show zero or very low loss amounts. This indicates that Internet users who have been victims of multiple scams stand the best chance of ending their financial involvement in the scam after only one or two transfers, while those with fewer such experiences take much longer to decide whether to end their involvement.

However, differences between the groups did not reach statistical significance for this variable. T-test for this variable produced t = -0.1397 and Pr(|T| > |t|) = 0.8891

4.6 COMPUTER LITERACY

4.6.1 Years of using the Internet

Participants with less than 5 years of Internet experience comprise approximately 25% of the sample. More experienced Internet users (5-10 years of experience) comprise 34% of the sample, and very experienced users (over 10 years of experience) account for about 38% of the sample. Overall, the majority of respondents are either experienced or very experienced Internet users, with likelihood of targeting being fairly equally distributed among the groups. It seems that users who have been using the Internet for less than 5 years are either less likely to be targeted, or less likely to volunteer to participate in an online study.

Those participants with less than 5 years of Internet experience show the highest vulnerability to scams. More specifically, 80% of the users with 3-4 years of experience lost money, followed by 73% among those who reported 1-2 years of experience, and 71% among those Internet users

with less than 1 year of experience prior to the scam. For users with over 5 years of Internet experience victimization rates hover around 40-45%, with only exception in the "11-14 years" group which has a 61% victimization rate.

Table 4.23. Likelihood and Severity of Victimization by Years of Internet Use

Years of Internet use	Percent of sample total	Victimization rate	Mean loss amount
less than 1 yr	0.06	0.71	$2,993
1-2 yrs	0.14	0.73	$6,797
3-4 yrs	0.05	0.8	$4,427
5-6 yrs	0.06	0.43	$2,077
7-8 yrs	0.06	0.43	$3,208
9-10 yrs	0.22	0.38	$3,796
11-14 yrs	0.16	0.61	$3,709
over 15 yrs	0.25	0.44	$2,714

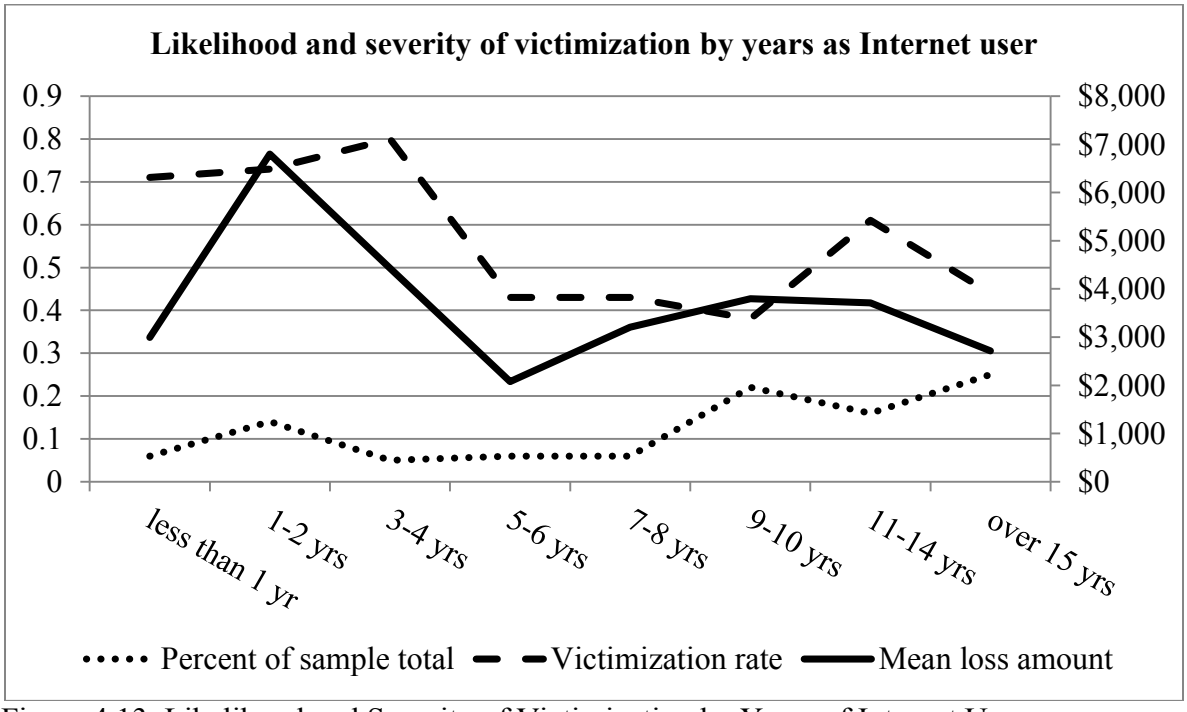

Figure 4.13. Likelihood and Severity of Victimization by Years of Internet Use.

The mean loss amount shows a somewhat binomial distribution. The highest mean loss amount ($6,796) is in the "1-2 years" category, followed by "3-4 years" category ($4,477). The lowest

average loss was in “5-6 years” category ($2,076) and in “over 15 years” category ($2,713.50). The rest of the categories average around three to four thousand dollars mean loss. Thus, it seems that users who have been using the Internet for more than a year but less than 5 years are in the highest danger category both in terms of likelihood of victimization and severity of victimization. Users with less than one year Internet experience have a high likelihood of victimization but with an average severity of victimization. Longer experience with the Internet environment provides only moderate protection from victimization.

4.6.2 Daily Internet use

In terms of daily Internet use, 65% of the sample report using the Internet less than 3 hours per day. Those who use the Internet 3-5 hours per day constitute 21% of the sample. Very few respondents use the Internet more than 5 hours per day, indicating that the sample is heavily tilted toward “light” Internet users who are not deeply immersed in the online environment. Disregarding groups “13 years” and higher, which had only 1 participant in each, the highest victimization rate (75%) is recorded among those who spend less than 1 hour per day online. The next highest risk category is for the “5-7 hours” category with a 70% victimization rate. In the follow-up analysis of the data (which is not possible in this thesis due to space constraints) it would be interesting to correlate the users’ reported years as Internet users with their reported daily Internet usage, as well as their victimization rates.

In terms of severity of victimization, the data indicates that fewer reported hours spent online daily directly correlate with higher mean loss amounts. For example, users with less than one hour of Internet use per day reported the highest mean loss amount ($5,496), followed by users

in the "1-3 hours" category ($4,141) and the "3-5" category ($3,092). However, this correlation does not reach statistical significance.

T-test for this variable produced t = 1.1882 and Pr(|T| > |t|) = 0.2374

Table 4.24. Likelihood and Severity of Victimization by Daily Hours of Internet Use

Hrs of Daily Internet Use	Percent of Sample Total	Victimization Rate	Mean Loss Amount
Less than 1 hr	0.15	0.75	$5,496.08
1-3 hrs	0.5	0.51	$4,141.86
3-5 hrs	0.21	0.39	$3,092.67
5-7 hrs	0.09	0.7	$2,735.00
7-10 hrs	0.04	0.25	$207.00
13-15 hrs	0.01	1	$1,900.00
Over 15 hrs	0.01	0	0

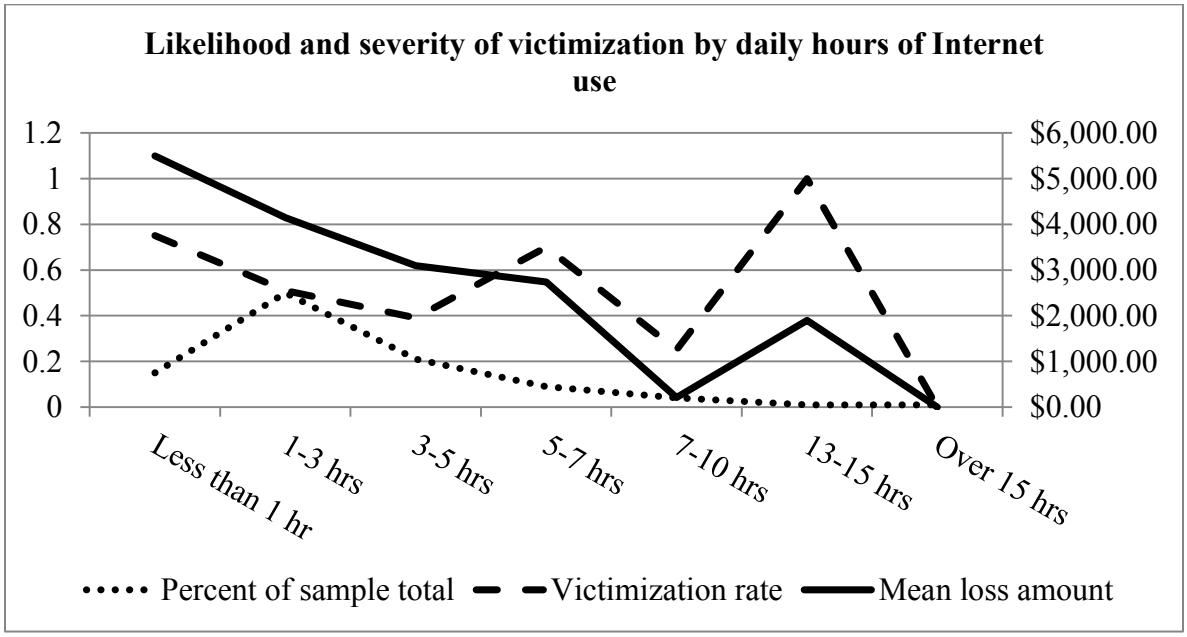

Figure 4.14. Likelihood and Severity of Victimization by Daily Hours of Internet Use.

4.6.3 IT training

IT training is measured as a separate variable, since it may have a strong potential to influence participants' ability to detect suspicious communication. Only 40% of the sample report "some"

or “extensive” IT training, and 40% of the sample report no IT training. This is not surprising, given that 65% of the sample report using Internet less than 3 hours per day, and a quarter of the sample have been internet users for less than 5 years.

As is apparent from Table 4.25, users with no IT training are the most likely to respond to money solicitation, but IT training in itself does not seem to correlate with a lower likelihood of victimization, as participants in the “some IT training” and the “extensive IT training” categories have identical victimization rates (48%), which is only slightly higher than victimization rates for respondents with very little training (42%).

IT training also provides little protection against high losses due to a scam. Users in the “no IT training” category report a mean loss of $4,631, while users in the “very little training”, “some training”, and “extensive training” categories all have a mean loss around three thousand dollars. This suggests that users in the “some training” and “extensive training” categories are not much better equipped to detect the scam or end the scam early than users with no IT training.

T-test for this variable produced t = 1.2179 and Pr(|T| > |t|) = 0.2259

Table 4.25. Likelihood & Severity of Victimization by Prior IT Training

IT Training	Percent of Sample Total	Victimization Rate	Mean Loss Amount
No special training	0.43	0.62	$4,631.17
Very little training	0.17	0.42	$3,461.63
Some training	0.21	0.48	$3,223.55
Extensive training	0.19	0.48	$3,355.50

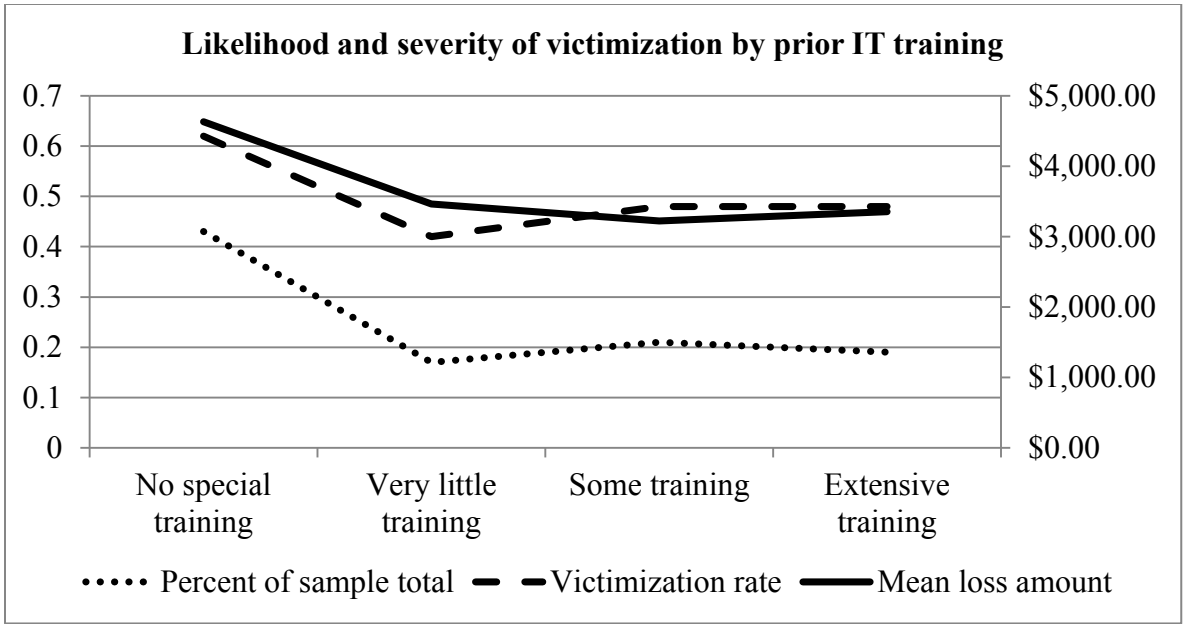

Figure 4.15. Likelihood and Severity of Victimization by Prior IT Training.

4.7 SUMMARY OF RESULTS FOR RAT VARIABLES

Of the 20 theory-related variables, only four variables reached statistical significance. The *online activities* of the participants appear to have the strongest influence on their vulnerability to TQ-ODS.

4.7.1 Online search activities

Over 50 % of the participants of study self-identify as *actively engaged in search* for a romantic partner at the time of their scam encounter, and they display a higher overall vulnerability to the scam ($t = -3.1664$ $Pr(|T| > |t|) = 0.0020$). It is interesting that users who are wishing for a romantic partner but not actively seeking show slightly higher severity of victimization than those who are actively seeking, although their likelihood of victimization is lower. This seems to indicate that users who are actively seeking a romantic partner are able to end the scam earlier.

Participants indicating that they are *using online sites* to search for a romantic partner are nearly twice as likely to send money to scammers and to lose twice as much money as those who do not (t = -2.4514 Pr(|T| > |t|) = 0.0158). Additionally, those participants who are *focused specifically on finding a dating partner* from another country have a very high likelihood of victimization (81%) and high mean loss amount (t = -3.5492 , p=0.0006). It is worth noting that users who are not interested in international dating or who have no specific preference are significantly less likely to send money to the scammers. However, the mean loss amount is very similar among all "online active" groups. Why this is so remains to be investigated.

As far as prior experience with international dating, none of the variables reached significance. Over 50% of Internet users in the sample have at least some *prior interest or experience with international dating*. There are no pronounced differences between participants who considered international dating in the past and those who did not. Surprisingly, prior experience in international dating turns out to be a risk factor, with those respondents scoring highest on number of prior experiences in international dating also showing the highest propensity to respond to money solicitation. It is possible that their prior experiences are positive ones, prompting them to be more trusting in their relationship with the scammer. However, it is worth noting that those who have two or more prior experiences with international dating are able to end the scam with a total loss amount of approximately $2,400-$3,000, while those who have no prior experience or who only have one prior international dating experience lost on average $4,500.

4.7.2 Awareness

Remote scam awareness scores indicate that Internet users with lower levels of exposure to information about various online frauds (i.e., the 11 types of fraud suggested to the respondents) show a higher victimization rate and a higher average loss amount than Internet users with more exposure to that information. Additionally, *overall remote awareness of crimes of trust* (ODS, 419, and phishing) is surprisingly low. Only 38% of the sample have heard of ODS prior to encountering the scammers. Nigerian scams have the lowest awareness rate of 29%, while phishing has the highest awareness rate of 59% of the sample. One needs to remember, however, that the sample is self-selected, and that users with higher levels of scam awareness might successfully avoid targeting efforts, and thus are not part of the study.

In line with the overall results for total remote scam awareness, those who are not aware of crimes of trust prior to being approach by scammers have a higher likelihood of responding to money solicitation. Their average loss amount is also likely to be higher. Overall the total remote scam awareness variable (for all 11 types of crimes) approached but did not reach significance in t-test (= 1.8767, p= 0.0633). In terms of specific scam types, remote awareness of phishing and 419 scams have the strongest correlation to victimization (p=0.06 and p=0.07 respectfully).

Very few respondents in this sample have any *personal experience with scams* before being approached by scammers. Those that have some prior experience with online scams tend to be less vulnerable to money solicitations on average. Unsurprisingly, the lowest personal experience score group also records the highest mean loss amount. Overall, however, the total personal scam experience score failed to reach significance in t-test (t = 1.4754, p= 0.1430).

Within this category of variables, personal experience with crimes of trust scams remains low. Only 21% of respondents report prior personal experience with ODS and only 10% report prior experience with 419 scams. Surprisingly, those who have previously encountered ODS are more likely to send money (61% incident rate) than those who have not (51% incident rate), indicating that having a prior personal encounter with ODS may actually increase chances of becoming a victim.

On the other hand, only 27% of the participants that have encountered 419 scams report losing money (as opposed to 57% of those who did not encounter 419 scams in the past). This may indicate that users who encounter 419 scams become more "immune" to crimes of trust. From the standpoint of severity of victimization, however, users with no previous experience with 419 or ODS scams have average loss amounts twice as high as those who have some previous experience.

The majority of the sample (92%) consists of participants who either have never lost money due to online fraud or who have only one *prior online fraud victimization experience*. However, lack of previous experience with Internet fraud does not translate into higher vulnerability to money solicitation. Those with 2 prior victimization experiences had the highest victimization rate (100%), although the mean loss amount was only $819.40, while those reporting multiple victimizations (5 or more) are very resilient to the scam and have a very low loss amount ($500). Those with no prior scam experiences have a 50-50 chance of victimization, but their mean loss amount is $4,834.47. The overall picture is that users with no prior victimizations or with only one prior victimization were willing to go along with the scammers' requests for money for much longer than users who have already lost money to online scams in the past.

4.7.3 Computer use and literacy

Only 19% of the respondents in the study report extensive *IT training*. However, prior IT training seems to have little effect on the likelihood of victimization or the mean loss amount, but users with no IT training have the highest victimization rate.

Surprisingly, the highest mean loss is reported by users with above average skill levels ($6,849.57), while those with very low computer literacy level have the lowest mean loss amount ($2,642.00) The variable approached significance (t = 1.7872, p= 0.0768) but did not reach it. Only 19% of the respondents of the sample report extensive IT training, and this seems to have little effect on likelihood of victimization or the mean loss amount; while participants with no IT training or very little training both have the highest victimization rates, the mean loss amounts are very close from low to high IT training.

In the *years of experience with Internet* variable, participants with 1 to 5 years of Internet experience have the highest probability of responding to a money solicitation, and they show the highest average losses. For users with over 5 years of experience, the average victimization rate is around 40-45%. This variable reached significance in t-tests (t = 2.0552, p = 0.0423). However, when considering the *daily computer use* variable, the trend is not clear. High victimization rates are reported among users with widely ranging patterns of daily computer use, although those users with fewer hours online daily correlate with higher loss amounts. However, this variable did not reach significance.

Table 4.26. Significance Test for All Variables

Variable	t	p
Age	-0.202	0.840
Country	-0.378	0.706

Table 4.26 continued

Years of higher education	0.558	0.578
Monthly income	0.215	1.249
Marital status	1.775	0.078*
Employment status	1.052	0.295
Seeking relationship	-3.166	0.002**
Online search for relationship	-2.451	0.016**
International focus	-2.152	0.034**
Prior consideration of international dating	-0.280	0.780
Prior experience with international dating	0.015	0.988
Remote scam awareness	1.877	0.063
Remote ODS awareness	1.234	0.220
Remote 419 awareness	1.205	0.231
Remote phishing awareness	1.848	0.067*
Personal awareness	1.475	0.143
Personal ODS awareness	-0.875	0.384
Personal 419 awareness	1.792	0.076*
Number of prior online victimizations	-0.140	0.889
Years as Internet user	2.055	0.042**
Daily hours of Internet use	1.188	0.237
Prior IT training	1.218	0.226

Table 4.27. Summary of Selected Variables

Variable	Mean	Std. Dev.	Min	Max
Percent of victims in sample	0.527273	0.501541	0	1
Amount lost	2100.1	3933.546	0	27261
Age at the time of the scam	45.4	11.59579	0	73
Years of higher education	3.263636	2.489159	0	10
Monthly income	3135.706	2608.832	0	20000
Years as Internet user	9.536364	5.950372	0	20
Daily hours of Internet use	1.454545	1.185821	0	7
IT training indicator	1.163636	1.177209	0	3
Remote awareness	3.272727	2.657546	0	10
Personal awareness	1.409091	2.046682	0	11
Number of prior online victimizations	0.513762	0.977664	0	5

CHAPTER 5

CONCLUSION

This study attempts to fill some of the gaps in our knowledge base about online victimization. This thesis briefly described one specific category of cybercrime - the crimes of trust (CoT). However, this thesis focused on the investigation of a specific type of crime of trust called "Travel Quest Online Dating Scams (TQ-ODS)", originating from Russia. The author reviewed the premise and the stages of the scam, and described the targeting strategies often employed by scam perpetrators utilizing TQ-ODS. In addition, this study examines the methodology of the crime in relation to routine activity theory, and specific variables

The study focused on investigation of factors that affect Internet users' susceptibility to TQ-ODS. Routine Activities Theory was used to guide the selection of variables. The author discussed the general concept of routine activities and guardianship in the context of the online environment, and attempted to apply those concepts to the specific circumstances of the ODS victimization. As an extension of past research, variables such as hours of daily computer use, computer use tenure, and prior IT-related training were collected. The author also attempted to approximate measures of participants' prior familiarity with online frauds. Additionally, offense-specific measures of online activities were constructed. Some standard demographic factors such as age, education, income, and marital status were examined, alongside information about respondent's country of residence and employment situation.

To advance the current endeavors of research, several improvements have been proposed. First, the author agrees with Van Wilsem (2011) that the investigation of fraud victimization needs to be bifurcated into an investigation of factors affecting the targeting of consumers for victimization and a separate investigation into the factors affecting persuasion compliance among the targeted users. Second, the author offers a suggestion that measurements of fraud awareness need to differentiate between "impersonal" awareness obtained from information in general media and "personal" awareness obtained from personal experience with a particular type of fraud. Third, the author suggests that offense-specific awareness will be more effective than non-specific awareness about online fraud. Fourth, the author recommends that future investigations into cybercrime victimization differentiate between measures of the likelihood (or rate) of victimization and severity of victimization. A definition of severity of victimization was also proposed in this study.

Results of the study are summarized below. Analysis of this study is provided in context with extant research whenever possible.

5.1 DEMOGRAPHIC VARIABLES

5.1.1 Age

The majority of previous academic research related to age and consumer fraud focuses on post-retirement age individuals (Grimes et al., 2010; Lee & Soberon-Ferrer, 1997; Muscat & James, 2002; Ngo & Paternoster, 2011; Reisig & Holtfreter, 2013; Smith & Graycar, 1999). Research produces a number of conflicting reports regarding the influence of the victims' age on scam

vulnerability (see reviews by Button et al., 2009; Schoepfer & Piquero, 2009; Titus, 1999). These conflicting results are likely to be explained by offense-specific variables.

For example, prior research indicates that victims of online scams are more likely to be younger individuals (Ngo & Paternoster, 2011), while older individuals are more likely to encounter scams offline (Ganzini et al., 1990) or to become victims of investment scams (Trahan et al., 2005). This seems plausible, given that younger individuals may be more likely to spend more time online or to engage in risky online activities (Van Wyk & Mason, 2001), while older consumers may be more likely to be involved in an active search for retirement investments. However, results of the current study show the greatest number of participants and greatest vulnerability to scam was among participant ages 30-39, 40-49, and 50-59. Younger individuals, on the other hand, comprised a very small part of the sample (only 8% of the sample were under 30 years old), and their likelihood of victimization was low to average.

This study findings are mainly in line with the data provided by the IC3 2012 Annual Report (IC3, 2012), which indicates similar patterns of victimization, with the only difference being in the reported severity of victimization among those age groups. The IC3 report indicates that mean loss amount in their data is directly correlated with age, and that the individuals in the 60+ group carry the highest mean loss amount. The current study, however, indicates younger individuals (under 30 years old) have the highest mean losses and, therefore, higher severity of victimization (although the small sample size makes the data vulnerable to influence of unusual cases). In contrast to the IC3 Report, individuals older than 60 years old are shown to fare better than other age groups.

The prevalence of participants between the ages of 30 and 59 in the current study may indicate that as targets they may be more visible, accessible, or vulnerable to the scammers. It is very likely that this increased vulnerability to targeting is due to the fact that Internet users of those age groups are more likely to be using online dating sites than younger online consumers (Stephure et al., 2009; Valkenburg & Peter, 2007). It is also possible that their vulnerability might be enhanced by other age-related factors (e.g., a more in-depth analysis of this data set may reveal correlations between age and level of computer literacy among the respondents), as well as their level of general fraud awareness. This variable did not reach statistical significance

5.1.2 Country of residency

Prior academic research assessing the connection between Internet users' country of residence and their likelihood of online fraud victimization could not be located during the literature search. The only data available seems to be brief information provided by Russian-Dating-Scams.com (Garrett, 2010). Results of the current study somewhat correspond with that data. In both sets, the majority of study participants were from English-speaking countries, with the United States having the largest number of reported incidents. It is possible that scammers prefer to target English-speaking countries because the templates that they use to correspond with their victims are written in English, but that is just a speculation based on observation. Further, there may also be an erroneous bias to attracting English-speaking victims from the United States because of stereotyping Americans as wealthy and rich, seeking the excitement of an international or "exotic" dating relationship. Again, this is speculation based on rationality and observation only.

Earlier this thesis speculated that countries further removed from Russia and Ukraine geographically and culturally would be more vulnerable to victimization because the travel quest scenario would sound more plausible to residents of those countries. However, the data does not show any particular logic in the distribution of victimization. Some countries further away from Russia (like the United States and Canada) show moderate vulnerability and moderate severity of victimization, while countries fairly close geographically like the UK, Norway and Sweden seem to be particularly prone to victimization. Australia, Norway, Sweden, and UK show the highest victimization rates. It is not clear what makes these regions different from, for instance, countries in the south of Europe that show very low victimization rates and very low mean loss amounts. Further research is needed to investigate these differences. This variable did not reach statistical significance.

5.1.3 Education and income

Similar to Reisig and Holtfreter (2013) and Van Wyk and Mason (2001), this study was not able to find statistically significant differences in victimization rates based on educational background, although the overall trend indicates users with the higher number of years of college education were better at ending the scam earlier. In general, current results contradict previous observations that higher educational achievement is correlated with higher risk of offline fraud victimization (Lee & Soberon-Ferrer, 1997; Titus, 1999).

Also, several prior studies indicate higher-income individuals are more at risk of becoming victims of offline fraud (see Button et al., 2009; Muscat & James, 2002). In contrast, the current data shows a detectable trend toward higher vulnerability among lower-income participants in terms of both likelihood and severity of victimization, although the variable did not reach

significance. Further research might investigate possible correlations between income level, educational level, computer proficiency level, and scam vulnerability.

This variable did not reach statistical significance.

5.1.4 Employment

Study participants who worked part time ("part time" and "employed with two jobs") show significantly higher victimization rates and higher mean loss amounts than full-time employed. Those results are comparable to results obtained by Bailey et al. (2008), who found that students who were part time employed were more likely to respond to a phishing email. Also similar to Bailey et al. (2008), participants who have no employment exhibit a lower victimization rate and lower severity of victimization than partially employed. The lowest victimization rates and lowest mean loss amounts are recorded for the "employed with 3 jobs," the "unemployed with no governmental assistance", and the "retired" groups. These findings are puzzling but may be due to the small sample size and susceptibility to data fluctuations. This variable did not reach significance.

5.1.5 Marital status

Although there has been almost no prior investigation into the effects of marital status on fraud victimization, marital status was the only demographic variable in this study to approach statistical significance, with recipients in the "never married" category showing the highest likelihood of responding to money solicitations, although there were no specific trends in the severity of victimization. Because the study sample contained only one participant who identified himself as widowed, it is not possible to draw comparisons with the results by Ganzini

et al. (1990) which suggest that widowed individuals are more likely to be victims of offline fraud. Given that the vast majority of participants are not married at the time of the scam, it seems curious that of all the demographic variables this one would show such pronounced patterns. More detailed analysis may indicate certain correlations between marital status, age, and the focus of online searches by the participants. This variable approached but did not reach statistical significance.

5.1.6 Online activities

Some variables collected for the purpose of the study are very offense-specific, and were not investigated previously by other researchers. However, an understanding of how ODS scammers target their victims could make it possible to determine which online behaviors could be considered to be more risky in the context of this type of scam, and thus measure those behaviors and assess their influence on the outcome of the scam. Several such variables were investigated in this thesis. For instance, results indicate that nearly all respondents in the study had at least some interest in finding a romantic partner at the time the scam perpetrators approached them, and two-thirds of the participants were using Internet web sites to find potential dating partners. This may suggest that users without such interest are less visible or less accessible for the ODS scammers. The higher number of respondents with an interest in finding a romantic partner positively correlates with the higher likelihood of victimization, and participants that use the Internet in their search for a romantic partner were twice as likely to respond to money solicitation as those searching for a partner offline. ((t = -3.1664 Pr(|T| > |t|) = 0.0020). Results also indicate that those users looking for a romantic partner online are more likely to lose money, and in larger amounts, than those users who do not (t = -2.4514 Pr(|T| > |t|) = 0.0158).

More specifically, users with no interest in long-distance dating prior to the scam appear the least likely to go along with scammers requests for travel expenses, or to send large amounts of money for such expenditures ($t = -3.5492$ and $Pr(|T| > |t|) = 0.0006$). This means that even though these users are visible, desirable, and accessible to the scammers, they are significantly less vulnerable. On the other hand, those users who are already looking for a dating partner from another country are twice as likely to respond to travel expenses solicitation and to spend twice as much on average as the "local dating only" group. Perhaps, these users are prepared to sustain some travel expenses as a price of fulfilling their goals even before the scammers approach them, so that the travel quest scenario does not awake their suspicion. Therefore, the victims' *expectation of interaction* could be a component of scam vulnerability or "susceptibility," making scammers more likely to succeed when the "bait" used in the scam is tailored to answer the expressed or latent interests of the potential victims, and when the interaction between the scammers and the victims falls within the victims' expectations.

5.1.7 Awareness of international dating issues

Given the fact that interest in international dating correlates with the high likelihood of victimization and high loss amounts, the author tried to determine whether all participants who expressed an interest in internaltional dating are equally at risk. At the beginning of this study, the author speculated that prior experience with international dating might act as a personal guardienship factor, because scammers rely on the victims' lack of knowledge about marriage-related immigration issues and international travel requirements to solicit money successfully. To check this assumption, participants received questions designed to test their prior experience with international dating.

Contrary to expectations, patricipants indicateing that they “previously considered” international dating reported higher average losses due to scams than those who did not. Also suprisingly, those participants with a significant amount of prior international dating experience (i.e., four or more prior dating partners from other countries) displayed a high likelihood of victimization and a fairly high average loss amount. On the other hand, in line with author expectations, participants who had no prior experience with international dating had high victimization rates and the highest mean loss amountts. Given the mixed results for this variable, future research could look further into the data from respondents with a high level of prior experience with international dating and attempt to cross-check their levels of scam awareness and computer literacy. These variables did not reach statistical significance.

5.1.8 Total awareness of online frauds (non-CoT-specific)

At the time of its creation, Routine Activities Theory of crime was focused on examining traditional crimes in traditional physical environments. In physical environments, guardianship is often of a physical nature. However, in informational environments there are few physical barriers to user-to-user communications, and therefore other types of guardianship, including self-guardianship, need to be understood and investigated.

Based on research into vulnerability to phishing, users who are aware of common phishing techniques (Halevi et al., 2013a; Sheng & Holbrook, 2010) are less likely to respond to a phishing attempt, making awareness an important factor in victim self-guardianship. Although the author could not devise a direct measurement of online security awareness as a whole, the study measures participants’ prior knowledge about several types of Internet frauds. However, a differentiation between first-hand knowledge (personal awareness) and second-hand knowledge

(remote awareness) is made in order to see whether these factors have similar effects on scam vulnerability.

Overall results suggest that a large proportion of participants were “low scam awareness” Internet users at the time the scammers approached them: 44% scored between “0” and “2” on the remote awareness scale, and 80% scored between “0” and “2” on the direct (personal) awareness scale. Because this group of participants was self-selected, it is difficult to draw conclusions about the broader population of Internet users, but further investigation into levels of awareness about scam among different groups of Internet users may be warranted.

Likelihood of victimization shows a fairly consistent pattern for both the remote and personal scam awareness. Users with lower levels of awareness had high victimization rates.

In chapter 3, the author speculates that personal awareness of fraud could be more effective from the standpoint of guardianship than remote awareness, because information obtained through personal experience is more salient to the recipient of that information. Although neither remote nor personal scam awareness variables reached significance, the distribution of victimization patters for these variables seems to be in agreement with that initial speculation. Users with scores of “0” to “4” on the awareness level scale had high mean loss amounts for both types of awareness. However, remote awareness was not as effective a predictor of victimization as personal awareness. For example, users indicating their remote awareness with a score of “4” had victimization rates of 50% and mean loss amount of $3,571. On the other hand, users with the same score of personal awareness had victimization rates of 20% with a mean loss amount of $1,379.

It is important to note the data for both types of awareness shows several unusual cases of very high loss amounts among participants with very high awareness levels. This may echo the findings by (Halevi et al., 2013a) who found that a certain percentage of users remain highly susceptible to phishing even after undergoing phishing awareness training. A larger sample would be needed to make further evaluation. Only the total remote scam awareness score approached but did not reach statistical significance.

5.1.9 Crime of Trust (CoT) related awareness

Analysis of the study data shows that prior remote awareness about 419 (advanced fee) scam, ODS, and phishing in the sample was low - only 29% of respondents had heard about 419 scams, 38% had heard about ODS, and 42% had heard about phishing scams at the time they were approached by the scammer. Awareness numbers for ODS in this study are lower than those reported by Whitty and Buchanan (2012), but because the sample is self-selected, it is difficult to generalize these finding to a larger population of Internet users. However, given that 69% of the participants indicate having post-high school education, and out of those, slighly less than a half indicate having 5 years of higher education or more, the low levels of awareness about such widespread scams as the advanced fee scams and phishing seems to be striknng.

In terms of personal experience with these scams, only 10% of respondents report encountering 419 scammers, but 21% report previously encountering ODS scammers. This is possibly due to the fact that many of the participants were in the process of a search for a dating or marital partner, and consequently had more opportunities to encounter dating scammers than 419 scammers as a result of their activities.

Comparison of the results of victimization vulnerability and victimization severity for this variable presents a puzzling picture. As expected, both remote and personal awareness about 419 scams correlate with a lower likelihood and severity of victimization among study participants. However, personal knowledge of ODS scams correlates with higher (rather than lower) likelihood of victimization, even though mean loss amounts are lower among individuals with personal awareness about ODS. This may indicate that for some reason users previously familiar with ODS are less resistant to scammer requests, but are able to detect the signs of a scam close to the $2,000 mark in the relationship. Remote awareness of phishing scams correlates with a lower likelihood of victimization (as expected), but the mean loss amount among users who had heard about phishing is higher than among those without such knowledge, which may mean that knowledge of phishing techniques does not provide Internet users with an understanding of more complex and interactive scams. Among CoT-related awareness variables, none reached significance.

5.1.10 Prior online victimization

Responses to questions about prior instances of actual online fraud victimization (sending money to scammers) show that 66% of participants have no prior online fraud victimizations. However, due to the self-selection of participants in this study, these results may not be representative of the population of Internet users as a whole. It is worth noting that victimization rate and highest among those who had one or two prior victimizations, although severity of victimization is worst among those who are new to the victimization process. Both the rate and the severity of victimization dropped dramatically among the study participants with three or more prior victimizations.

Overall, these results contradict previous conclusion by Kuo et al. (2012) and Titus (1999) that one of the most reliable predictors of future targeting and victimization is prior victimization. Rather, current results indicate that the effectiveness of the targeting and persuasion efforts seem to be negatively correlated with the number of prior online victimizations, although a small sub-section of Internet users may be highly susceptible to fraud victimization regardless of the number of prior scam experiences. It is possible that due to some personal characteristics, some Internet users may have "victim personalities" and fall for scams repeatedly (Halevi et al., 2013b) . This variable approached but did not reach statistical significance.

5.1.11 Computer use and literacy

Only 25 percent (1/4) of recipients report being Internet users for less than 4 years, but this group had the highest rate of severity of victimization. The years of computer use variable is the only computer-literacy related variable to reach statistical significance in this study ($t = 2.0552$ and $Pr(|T| > |t|) = 0.0423$), and it may indicate that consumers who only recently became Internet users are highly vulnerable to online scams, possibly because they lack the experience needed to protect themselves during the targeting stage or to evaluate the validity of the scammers' claims during the persuasion stage. However, data also shows that fairly high loss amounts are present among users with widely different computer use tenures, which may indicate that measurement of years of online experience alone may not be enough to provide Internet users with tools needed to verify scammers' claims quickly.

Data on the number of hours of daily Internet use is also considered. Although this variable did not reach statistical significance, there is a fairly clear indication that the majority of the sample participants were "light" Internet users, reporting less than 3 hours of computer use per day, and

those users have high victimization rates and mean loss amounts. Overall the number of hours spent online daily directly correlates with lower victimization rates, except for the group reporting 5-7 hours online daily, who had one of the highest victimization rates (although their mean loss amount was below average).

Lastly, prior IT training does not seem to make a significant difference in terms of the likelihood or severity of victimization. Users with no IT training at all (approximately 44% of the sample) have a higher likelihood of victimization, but users with extensive IT training (which constituted a surprisingly large percentage of the sample) do not fare much better than users with very little training. Mean losses and victimization rates are very similar, suggesting that general computer literacy provides online consumers with little assistance in detecting TQ-ODS. This may simply be an indication that IT training in itself does not provide information about phishing and fraud awareness. On the other hand, this may serve to further confirm suggestions that higher computer proficiency may lead to higher Computer Self-Efficacy (CSE) levels (Wright & Marett, 2010), creating a false perception of self-protection among those Internet users. The IT training variable approached but did not reach statistical significance.

5.1.12 Likely victims of TQ-ODS

Overall, the following trends are observed among the participants in this sample. Highest likelihood of victimization is observed among Internet users between 30 and 59 years old from Australasia, Northern Europe, or UK, with no prior marriages, with less than 5 years of college education, with unstable work situation (part time, unemployed, or working two jobs), and with a monthly income below $2,999. Higher income, higher level of education, and more stable work

situation are generally associated with a lower chance of victimization. Users from the USA and Canada show higher resistance to TQ ODS than users from other English-speaking countries. From the standpoint of situational factors, highest likelihood of victimization is among Internet users who are seeking a romantic partner online, who are specifically interested in international dating, who have heard about several types of scams from the media, and who have encountered two or three online frauds and lost money on one or two prior occasions. From the standpoint of computer literacy, these users have one to three years of experience with the online environment, spend less than an hour per day online, and have no special IT training.

5.2 DATA LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

Data for this thesis were subjected only to rudimentary, non-parametric analysis. Additional investigation and more sophisticated statistical analysis may well reveal undetected correlations. Implications of the current findings are difficult to assess due to the self-selected nature and the small size of the sample in the study. Variables such as online research status, focus of online research, and degree of awareness of issues associated with international dating are experimental constructs and may be criticized from the standpoint of validity. The data for these and other variables from the study questionnaire are available for further analysis in the future. Recommendations for future research include the following:

1. Concepts of targeting and victimization need to be separated except in those types of cybercrimes when targeting automatically ensures victimization.
2. Information about severity of victimization needs to be analyzed whenever it is possible in order to investigate patterns of victimization with greater precision.

3. Investigation of susceptibility to victimization needs to include considerations of the environments and motivations specific to each type of cybercrime compared to "general" (or offense non-specific) variables.
4. Investigation into the connection between *expectations of interaction* and vulnerability to victimization for Internet users may warrant further attention.
5. Investigation into differences in susceptibility to victimization among users from different countries and cultures could lead to a deeper understanding of factors affecting targeting and victimization.
6. Further investigation into factors affecting susceptibility to phishing may be key to understanding susceptibility to online fraud in general.

The current study is an attempt to empirically examine susceptibility to Online Dating Scams (ODS) victimization from the viewpoint of a Routine Analysis Theory (RAT) framework. Overall results of this study indicate that certain RAT concepts (such as routine activities) can be linked to the likelihood of online fraud victimization. Additional study using the RAT framework appears to be a valid, future research direction.

REFERENCES

Abad, C. (2005). The Economy of Phishing: A Survey of the Operations of the Phishing Market. *First Monday*, *10*(9). doi:dx.doi.org/10.5210/fm.v10i9.1272

Angelidakis, P. (2012). *Computer Crime Victimization: Role of Security Software and Online Behavior*. Tilburg University. Retrieved from http://arno.uvt.nl/show.cgi?fid=123074

Bailey, J. L., Mitchell, R. B., & Jensen, B. K. (2008). Analysis of Student Vulnerabilities to Phishing. In *Americas Conference on Information Systems 2008 Proceedings* (pp. 1–10). Retrieved from http://aisel.aisnet.org/amcis2008/271

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

Bossler, A. M., & Holt, T. J. (2010). The Effect of Self-Control on Victimization in the Cyberworld. *Journal of Criminal Justice*, *38*(3), 227–236. doi:10.1016/j.jcrimjus.2010.03.001

Burgard, A., & Schlembach, C. (2013). Frames of Fraud: A Qualitative Analysis of the Structure and Process of Victimization on the Internet. *International Journal of Cyber Criminology*, *7*(2), 112–124.

Button, M., Lewis, C., & Tapley, J. (2009). *Fraud Typologies and Victims of Fraud*. London, UK. Retrieved from http://eprints.port.ac.uk/3989/1/NFA_report3_16.12.09.pdf

Chang, J. J. S. (2008). An Analysis of Advance Fee Fraud on the Internet. *Journal of Financial Crime*, *15*(1), 71–81. doi:10.1108/13590790810841716

Copes, H., Kerley, K. R., Huff, R., & Kane, J. (2010). Differentiating Identity Theft: An Exploratory Study of Victims Using a National Victimization Survey. *Journal of Criminal Justice*, *38*(5), 1045–1052. doi:10.1016/j.jcrimjus.2010.07.007

Copes, H., & Vieraitis, L. M. (2009). Bounded Rationality of Identity Thieves: Using Offender-based Research to Inform Policy. *Criminology & Public Policy*, *8*(2), 237–262. doi:10.1111/j.1745-9133.2009.00553.x

CyberStreetSmart.Org. (2011). Other Types of Dating Scams. Retrieved November 20, 2014, from http://www.cyberstreetsmart.org/dating/dating_other.html

Durkin, K. F., & Brinkman, R. (2009). International Journals 419 FRAUD : A Crime Without Borders in A Postmodern World. *International Review of Modern Sociology*, *35*(2), 271–283. Retrieved from HTTP://www.jstor.org/stable/41421358

Flor, R. (2009). Fraud, Computer-related Fraud and Identity-related Fraud. Verona, Italy: Faculty of Law, University of Verona, Italy. Retrieved from http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres_roberto flor_abstract.pdf

Foxworth, D. (2013). Looking for Love? Beware of Online Dating Scams. *The Federal Bureau of Investigations (FBI)*. San Diego, CA: Federal Bureau of Investigation. Retrieved from http://www.fbi.gov/sandiego/press-releases/2013/looking-for-love-beware-of-online-dating-scams

Franklin, C. A., Franklin, T. W., Nobles, M. R., & Kercher, G. A. (2012). Assessing the Effect of Routine Activity Theory and Self-Control on Property, Personal, and Sexual Assault Victimization. *Criminal Justice and Behavior*, *39*(10), 1296–1315. doi:10.1177/0093854812453673

Freiermuth, M. R. (2011). Text, Lies and Electronic Bait: An Analysis of Email Fraud and the Decisions of the Unsuspecting. *Discourse & Communication*, *5*(2), 123–145. doi:10.1177/1750481310395448

Ganzini, L., McFarland, B., & Bloom, J. (1990). Victims of Fraud: Comparing Victims of White Collar and Violent Crime. *The Bulletin of the American Academy of Psychiatry and the Law*, *18*(1), 55–63. Retrieved from http://www.jaapl.org/content/18/1/55.full.pdf

Garrett, E. (2010). *Updated Summary Data: Submitted Requests for Assistance with Filing Criminal Prosecution Cases Against Russian and Ukrainian Visa-and-Tickets Scammers 2006-2010*. Retrieved from http://www.russian-dating-scams.com/scams/stat/sum5-6-10.htm

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology and Hacking Techniques*, *2*(1), 13–20. doi:10.1007/s11416-006-0015-z

Gottfredson, M. (1982). On the etiology of criminal victimization. *The Journal of Criminal Law and Criminology*, *72*(2), 714–726.

Grimes, G. A., Hough, M. G., Mazur, E., & Signorella, M. L. (2010). Older Adults' Knowledge of Internet Hazards. *Educational Gerontology*, *36*(3), 173–192. doi:10.1080/03601270903183065

Halevi, T., Lewis, J., & Memon, N. (2013a). *Phishing, Personality Traits and Facebook*. *erXiv.org*. Retrieved from http://arxiv.org/pdf/1301.7643v2.pdf

Halevi, T., Lewis, J., & Memon, N. (2013b). Pilot Study of Cyber Security and Privacy Related Behavior. In *WWW '13 Companion Proceedings of the 22nd international conference on World Wide Web companion*. International World Wide Web Committee (IW3C2). Retrieved from http://precog.iiitd.edu.in/events/psosm2013/9psosm5-halevi.pdf

Hasib, A. Al. (2009). Threats of Online Social Networks. *International Journal of Computer Science and Network Security*, *9*(11), 288–293.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25. doi:10.1080/01639620701876577

Holt, T. J., & Turner, M. G. (2012). Examining Risks and Protective Factors of On-Line Identity Theft. *Deviant Behavior*, *33*(4), 308–323. doi:10.1080/01639625.2011.584050

Holtfreter, K., Reisig, M. D., Piquero, N. L., & Piquero, A. R. (2010). Low Self-Control and Fraud: Offending, Victimization, and Their Overlap. *Criminal Justice and Behavior*, *37*(2), 188–203. doi:10.1177/0093854809354977

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low Self-Control, Routine Activities, and Fraud Victimization. *Criminology*, *46*(1), 189–220. doi:10.1111/j.1745-9125.2008.00101.x

Hunton, P. (2009). The Growing Phenomenon of Crime and the Internet: A Cybercrime Execution and Analysis Model. *Computer Law & Security Review*, *25*(6), 528–535. doi:10.1016/j.clsr.2009.09.005

IC3. (2011). The Dangerous Side of Online Romance Scams. Retrieved November 20, 2014, from http://www.ic3.gov/media/2011/110429.aspx

IC3. (2012). *IC3 2012 Internet Crime Report* (pp. 1–43). Retrieved from http://www.ic3.gov/media/annualreport/2012_IC3Report.pdf

Isacenkova, J., Thonnard, O., Costin, A., Balzarotti, D., & Francillon, A. (2013). Inside the SCAM Jungle: A Closer Look at 419 Scam Email Operations. *2013 IEEE Security and Privacy Workshops*, 143–150. doi:10.1109/SPW.2013.15

Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, *30*(4), 470–486. doi:10.1177/0894439311422689

Koon, T. H., & Yoong, D. (2013). Preying on Lonely Hearts: A Systematic Deconstruction of an Internet Romance Scammer's Online Lover Persona. *Journal of Modern Languages*, *23*, 28–40.

Kuo, S.-Y., Cuvelier, S. J., Sheu, C.-J., & Zhao, J. S. (2012). The Concentration of Criminal Victimization and Patterns of Routine Activities. *International Journal of Offender Therapy and Comparative Criminology*, *56*(4), 573–598. doi:10.1177/0306624X11400715

Langenderfer, J., & Shimp, T. (2001). Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion. *Psychology & Marketing*, *18*(7), 763–783.

Lee, J., & Soberon-Ferrer, H. (1997). Consumer Vulnerability to Fraud: Influencing Factors. *The Journal of Consumer Affairs*, *31*(1), 70–89.

Longe, O. B., Mbarika, V., Kourouma, M., Wada, F., & Isabalija, R. (2009). Seeing Beyond the Surface: Understanding and Tracking Fraudulent Cyber Activities. *International Journal of Computer Science and Information Security*, *6*(3), 124–135. Retrieved from http://arxiv.org/ftp/arxiv/papers/1001/1001.1993.pdf

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

Menard, S., Morris, R. G., Gerber, J., & Covey, H. C. (2011). Distribution and Correlates of Self-Reported Crimes of Trust. *Deviant Behavior*, *32*(10), 877–917. doi:10.1080/01639625.2010.514221

Modic, D. (2012). *Willing to Be Scammed: How Self-Control Impacts Internet Scam Compliance*. University of Exeter, England. Retrieved from https://ore.exeter.ac.uk/repository/handle/10871/8044

Modic, D., & Lea, S. (2013). Scam Compliance and the Psychology of Persuasion. *Journal of Applied Social Psychology*. University of Exeter, England. doi:dx.doi.org/10.2139/ssrn.2364464

Muscat, G., & James, M. (2002). *Older People and Consumer Fraud - Australia* (No. 220). *Australian Institute of Criminology, Trends and Issues in Crime and Criminal Justice Series.* (pp. 1–6). Retrieved from http://aic.gov.au/documents/B/F/4/{BF470867-F031-490E-B80C-F05494A7DBA5}ti220.pdf

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An Examination of Individual and Situational Level Factors. *International Journal of Cyber Criminology*, *5*(1), 773–793. Retrieved from http://www.cybercrimejournal.com/ngo2011ijcc.pdf

Nhan, J., Kinkade, P., & Burns, R. (2009). Finding a Pot of Gold at the End of an Internet Rainbow: Further Examination of Fraudulent Email Soicitation. *International Journal of Cyber Criminology*, *3*(1), 452–475. Retrieved from http://www.cybercrimejournal.com/nhanetalijcc2009.pdf

Nikiforova, B., & Gregory, D. W. (2013). Globalization of Trust and Internet Confidence eEmails. *Journal of Financial Crime*, *20*(4), 393–405. doi:10.1108/JFC-05-2013-0038

Online Dating Safety Tips. (n.d.). Online Dating Safety: TOP 10 SCAMS. Retrieved November 20, 2014, from http://www.onlinedatingsafetytips.com/Top10Scams.cfm

Payne, B. K., & Chappell, A. (2008). Using Student Samples in Criminological Research. *Journal of Criminal Justice Education*, *19*(2), 175–192. doi:10.1080/10511250802137226

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296. doi:10.1177/0022427810365903

Rege, A. (2009). What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud. *International Journal of Cyber Criminology*, *3*(2), 494–512. Retrieved from http://www.cybercrimejournal.com/AunshulIJCCJuly2009.pdf

Reisig, M. D., & Holtfreter, K. (2013). Shopping Fraud Victimization Among the Elderly. *Journal of Financial Crime*, *20*(3), 324–337. doi:10.1108/JFC-03-2013-0014

RomanceScamsNow. (n.d.). RomanceScamsNow - Philippines Gold Diggers. Retrieved November 20, 2014, from http://romancescamsnow.com/dating-scams/philippines-gold-diggers-how-to-tell/

Schoepfer, A., & Piquero, N. L. (2009). Studying the Correlates of Fraud Victimization and Reporting. *Journal of Criminal Justice*, *37*(2), 209–215. doi:10.1016/j.jcrimjus.2009.02.003

Sheng, S., & Holbrook, M. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10 (2010)* (pp. 373–382). ACM Press. doi:10.1145/1753326.1753383

Smirnova, N. (2007). How the Scammers Were Fooling the Foreign Grooms-to-Be. *Moskovskiy Komsomolets*. Retrieved from http://www.russian-dating-scams.com/scams/media/mk-aug07.htm

Smith, R. G., & Graycar, A. (1999). *Fraud & Financial Abuse of Older Persons* (No. 132) (pp. 1–6). Retrieved from http://www.aic.gov.au/documents/0/B/7/%7B0B74C6E7-9241-4D54-903D-2B1E084FBE77%7Dti132.pdf

Smyth, S. M., & Carleton, R. (2011). *Measuring the Extent of Cyber-Fraud in Canada: A Discussion Paper on Potential Methods and Data Sources* (No. 20) (pp. 1–64). Retrieved from http://publications.gc.ca/collections/collection_2011/sp-ps/PS14-4-2011-eng.pdf

Stabek, A., Brown, S., & Watters, P. (2009). The Case for a Consistent Cyberscam Classification Framework (CCCF). In *2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing* (pp. 525–530). Ieee. doi:10.1109/UIC-ATC.2009.77

Stephure, R. J., Boon, S. D., MacKinnon, S. L., & Deveau, V. L. (2009). Internet Initiated Relationships: Associations Between Age and Involvement in Online Dating. *Journal of Computer-Mediated Communication*, *14*(3), 658–681. doi:10.1111/j.1083-6101.2009.01457.x

Steward, W. (2008, March 28). Scamski City, Where Online "Russian Brides" Turn Out to be Mafia Conmen | Mail Online. *Daily Mail*. Retrieved from http://www.dailymail.co.uk/femail/article-542276/Scamski-city-online-Russian-brides-turn-Mafia-conmen.html

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). *Digital Crime and Digital Terrorism* (3rd ed.). Upper Saddle River, NJ: Pearson, Inc.

Titus, R. M. (1999). The Victimology of Fraud. In *Paper presented at the Restoration for Victims of Crime Conference*. Melbourne: Australian Institute of Criminology. Retrieved from http://www.aic.gov.au/media_library/conferences/rvc/titus.pdf

Titus, R. M., & Gover, A. R. (2001). Personal Fraud: The Victims and the Scams. *Crime Prevention Studies*, *12*, 133–151. Retrieved from http://www.popcenter.org/library/crimeprevention/volume_12/08-Titus.pdf

Trahan, A., Marquart, J. W., & Mullings, J. (2005). Fraud and the American Dream: Toward an Understanding of Fraud Victimization. *Deviant Behavior*, *26*(6), 601–620. doi:10.1080/01639620500218294

UN. (2013). United Nations "Composition of macro geographical (continental) regions, geographical sub-regions, and selected economic and other groupings." Retrieved from http://unstats.un.org/unsd/methods/m49/m49regin.htm#europe

Valkenburg, P. M., & Peter, J. (2007). Who Visits Online Dating Sites? Exploring Some Characteristics of Online Daters. *CyberPsychology & Behavior*, *10*(6), 849–852. doi:10.1089/cpb.2007.9941

Van Wilsem, J. (2011). "Bought It, but Never Got It" Assessing Risk Factors for Online Consumer Fraud Victimization. *European Sociological Review*, *29*(2), 168–178. doi:10.1093/esr/jcr053

Van Wyk, J., & Mason, K. A. (2001). Investigating Vulnerability and Reporting Behavior for Consumer Fraud Victimization: Opportunity as a Social Aspect of Age. *Journal of Contemporary Criminal Justice*, *17*(4), 328–345. doi:10.1177/1043986201017004003

Whitty, M. T. (2013a). Anatomy of the online dating romance scam. *Security Journal*, (February 11), 1–13. doi:10.1057/sj.2012.57

Whitty, M. T. (2013b). The Scammers Persuasive Techniques Model: Development of a Stage Model to Explain the Online Dating Romance Scam. *British Journal of Criminology*, *53*(4), 665–684. doi:10.1093/bjc/azt009

Whitty, M. T., & Buchanan, T. (2012). The Online Romance Scam: A Serious Cybercrime. *Cyberpsychology, Behavior, and Social Networking*, *15*(3), 181–183. doi:10.1089/cyber.2011.0352

Wright, R. T., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems*, *27*(1), 273–303. doi:10.2753/MIS0742-1222270111

VITA

Elena Garrett was born in Russia. She met her future husband, Michael, on an online dating site and moved to the United States. Her knowledge of Russian laws and culture, as well as her experience with international dating and immigration issues allowed her to identify a growing problem of proliferation of online dating scams originating from Russia and countries of Former Soviet Union. She created a non-profit web site Russian-Dating-Scams.com to collect individual case data, statistics, and knowledge articles related to Russian dating scams. Elena also established contacts with private investigators in Russia and Ukraine to make fraud detection services in Russia and Ukraine available to international Internet users.

During the last 10 years of her work on cases of Russian dating scams, Elena has assisted Russian law enforcement with prosecution of cases of online dating scams ranging from individual scammers to large scam "rings". In 2010, Russian police in Mari El Republic of Russia awarded Elena a medal in recognition of her role in facilitating prosecution of these crimes. Elena has been interviewed as an expert on the subject of Internet dating scams by television media in the United States and in Belgium. She has also written multiple articles on the subject of Russian dating scams.

Elena initially earned an Associate of Arts degree from Collin County Community College, followed by a Bachelor of Arts in criminology from the University of Texas at Dallas, graduating in 2011 summa cum laude. Elena then entered the graduate school of UTD for a Master of Science in criminology.