USRIJ

Journal of University Studies for inclusive Research (USRIJ)

مجلة الدراسات الجامعية للبحوث الشاملة

Journal of University Studies for inclusive Research

Vol.2 , Issue 12 (2021), 2106 - 2132

USRIJ Pvt. Ltd.,

Risk factors for being a victim of Cyber Theft and Cyber Fraud crimes

1 - Abdelghany Etaki, PhD student in Criminal Law and Criminology, Faculty of Law and Political Science, Ferdowsi University of Mashhad.

etkabd90@gmail.com

abdelghany.etaki@mail.um.ac.ir

2 - Seid Mahdi Seidzadeh, Assistant Professor, Department of Faculty of Law and Political Science, Ferdowsi University of Mashhad.

www.seidzadeh@um.ac.ir

3 - Mohammad Moghani Bashi, PhD student in Criminal Law and Criminology, Faculty of Law and Political Science, Ferdowsi University of Mashhad, and a cyber judge.

www.mailto:mbm.1993@live.com

Abstract

In the light of growing dependence on cyberspace in everyday life, the number of cybercrime victims - especially crimes of financial nature - has increased significantly. The aim of this study was to find out the model of cyberspace users with the potential to be a victim of financial cybercrimes. To achieve this goal, the most prevalent factors among actual victims that might lead them toward being victims of these crimes were investigated. Some elements from the routine activity theory, lifestyle theory, and some personal characteristics were used as a theoretical foundation to test and identify common risk factors. To this purpose, data were collected from actual victims who filed a judicial complaint as victims of cyber theft and cyber fraud (N=1334). It was found that the most vulnerable individuals had the following characteristics: aged under 50 years, male, married, with average or less education, with some greed, following a cyber lifestyle in a somewhat dangerous manner, with poor effective protection and behaviors that make them an attractive target for cyber criminals.

Keywords: financial cybercrimes, victims' model, personal features, cyber lifestyle, protection, target attractiveness

الملخص

في ضوء الإعتماد المتزايد على الفضاء السيبراني في الحياة اليومية، زاد عدد ضحايا الجرائم السيبرانية - وخاصة الجرائم ذات الطبيعة المالية - بشكل كبير. الهدف من هذه الدراسة هو معرفة نموذج مستخدمي الفضاء السيبراني الذين يحتمل أن يكونوا ضحية للجرائم السيبرانية المالية. لتحقيق هذا الهدف تم التحقيق في العوامل الأكثر انتشارًا بين الضحايا الفعليين التي قد تكون أدت بهم إلى أن يكونوا ضحايا لهذه الجرائم. تم استخدام بعض العناصر من نظرية النشاط الروتيني ونظرية نمط الحياة وبعض الخصائص الشخصية كأساس نظري لاختبار وتحديد عوامل الخطر المشتركة. لذلك، تم جمع البيانات من الضحايا الفعليين الذين قدموا شكوى قضائية كضحايا للسرقة السيبرانية والاحتيال السيبراني (العدد = 1334). وجدت الدراسة أن الأفراد الأكثر تعرضاً ليكونوا ضحايا هاتين الجريمتين هم من لديهم الخصائص التالية: تقل أعمارهم عن 50 عامًا ،ذكر، متزوج، ذو تعليم متوسط أو أقل، مع بعض الجشع، إتباع أسلوب حياة عبر الإنترنت خطر نوعاً ما، مع حماية ضعيفة وسلوكيات تجعلهم هدفًا جذابًا للمجرمين السيبرانيين.

الكلمات المفتاحية: الجرائم السيبرانية المالية، نموذج الضحايا، السمات الشخصية، أسلوب الحياة السيبراني
،الحماية، جاذبية الهدف.

Introduction

Cyberspace has provided criminals with new ways and techniques to commit crimes in a way differentiated from the past. For instance, theft crimes can be committed in a second by pressing a button. Statistics of cybercrime victims across the world are observable and attentive. In 2018, 23% of the US households were victimized by cybercrime (Renhart, 2018). According to the 2019 Identity Fraud Study from Javelin Strategy & Research, the number of consumers who were victims of identity fraud fell to 14.4 million in 2018, down from a record high of 16.7 million in 2017. However, identity fraud victims in 2018 bore a heavier financial burden: 3.3 million people were responsible for some of the liability of the fraud committed against them, nearly three times as many as in 2016 (Insurance Information Institute, Inc, 2020). In 2017, 978 users were victims of cybercrime in 20 countries. In other statistics, owing to cybercrime, consumers lost $172 billion; $142 per victim on average (Yamani, 2019).

Since the COVID-19 pandemic outbreak, the rate of cybercrime is growing compared to the pre-pandemic period. Given the social distancing and lockdown rules, people are using the

Internet and Cyberspace more voluminously; as a result, cybercrimes especially financial ones are committed more extensively. The aim of this study was to demonstrate and clarify a model of cyberspace users who are put at higher risk of financial cybercrimes (Cyber Theft and Cyber Fraud). The main question in the present study was what are the common characteristics, behaviors, and condition of cyberspace users that make them more vulnerable to be victims of financial cybercrimes in Iran as a Middle Eastern country.

1. Hypotheses

Victimology provides numerous answers to questions about probable reasons of being a victim of crimes. Theories related to reasons of victimization are divided into two classes: theories that deal with the probable reasons in the victims like impulsivity, greed, lack of information etc. and those that seek to find out social or economic factors in victims. One of the first aspects that scholars started to study was the role the victim himself had played in the commission of the crim (van der Aa, 2014). The lifestyle theory was developed by Hindelang, Gottfredson, and Garofalo. It posits that lifestyle of some individuals who follow a specific style in their lives makes them within the reach of criminals and turns them into easy targets to the criminals. It is added that some lifestyles create chances to committing the crime and increase the likelihood of being a victim. Routine activity theory was developed by Lawrence E. Cohen and Marcus Felson and later by Felson. According to this theory, a crime is likely to occur when three elements converge in place and time: motivated offender, attractive target and absence of capable protection. The assumption in this theory is that a crime can be committed by anyone who finds the chance.

The main hypothesis in the present study was that factors affect cyberspace users to be victims of cyber theft and cyber fraud are a set of permanence and habitual[1] user characteristics, behaviors and situations related to cyberspace. They constitute an absence of or weak protection, or increased and facilitated likelihood of user being an appropriate target on the one hand, and

[1] Permanence and habitual means non-accidental, i.e., recurrent, which is present in the user or in his dealings with cyberspace permanently. This requirement was met by asking respondents questions, like: Do you give your computer to your friends to use when they ask for it? not like: When was the last time you gave your computer to your friend? Have you given your computer to your friend in the last 6 months?

some risky cyber lifestyles or personal characteristics that assist or facilitate user's victimization of both crimes mentioned on the other hand. From above hypotheses, the following sub-hypotheses are extracted.

Sub-hyp1: There are sets of individuals who follow a certain lifestyle in cyberspace[2] which makes them more vulnerable to being victims of financial cybercrimes. Fifteen risky cyberspace lifestyles were selected and formed as multiple-choice questions and answers were obtained from respondents (actual victims).

Sub-hyp2: Absence or weakness of effective cyber and personal protection level and/or;

Sub-hyp3: Some procedures or conducts that make individuals a suitable target in cyberspace affect cyber theft or cyber fraud victimization.

Not to mention that cyber criminals are present all the time in cyberspace, especially in this study where actual victims and actual offenders were investigated. Eleven situations measuring lack or weakness of effective protection, and 5 situations measuring suitability of target level were selected. Then, they were developed into questions to get answers from respondents (actual victims) showing the two elements mentioned.

Sub-hyp4: Some personal characteristics play an influential role in being victims of financial crimes. Therefore, a set of questions exploring some personal factors in the victims were developed that could lead them to be victims or intervene alongside with some other reasons that make individuals vulnerable to be victims of these crimes.

2. Literature Review

To the best of the authors knowledge, no empirical studies dealing with and studying model of victims of cyber theft and cyber fraud or studying factors influencing on being victims of both crimes have been conducted in Iran. As the present study was conducted in Iran, which is a Middle Eastern Country and differs from Western Countries in terms of environment, customs,

[2] Also called cyber lifestyles.

traditions and personalities of individuals, it was not possible to compare it with other studies conducted in different environments. However, this does not preclude mentioning some studies and their objective differences and similarities.

The study by Whitty (2019) focused on cyber fraud victimization. The aim of this study was to measure and predict the extent to which a person can be a victim of cyber fraud using personal and demographic characteristics and routine activity theory. Psychological, social and demographic characteristics examined in this study include impulsivity, control, addictive tendency, age, education. Results of this study indicated that most psychological traits predict routine activities. In addition, education, loss of tendency, control, and conservation were contrary to what was expected. This study in relation to protection has not been translated into wide or multiple options to confirm the effectiveness of this element. Rather, it was adopted to measure it only by asking individuals how often they visit customer consultation or advice sites.

Another study (Travis C. Pratt, 2010) investigated cyber fraud and the relationship between personal characteristics and online activities on the one hand, and online activities and increased consumer exposure to motivated cyber criminals, on the other hand. The study concluded that demographic characteristics including routine online activities are more important in explaining the targeting of cyber fraud for consumer traits. With an emphasis on major results of this study, the direct relationship with routine online activities and exposure to the risk of fraudulent criminals was investigated, and it was possible to broaden the concept of routine activities and ask respondents about more activities to make the results of the study more robust and decisive; since in this study, there was an indirect relationship between some studied personality traits and exposure to fraudulent criminals.

The study by Junger, Montoya, Hartel and Heydari (2017) determined the relationship between social and economic characteristics and routine activities of users and three types of crimes: 1) online shopping fraud, 2) online banking fraud and 3) cyber-attacks. The aim of mentioned study was to investigate the risk factors associated with three types of crimes, and to determine whether social and economic characteristics and routine activities of users are associated with becoming a victim of online fraud compared to traditional crimes. The study found that users who were online via a tablet, laptop or TV were at higher risk. As interpreted in the study, the probable reason, is that they have no knowledge of communications and information technology. It was also found that repeated browsing online and shopping online affect persons' victimization of fraudulent online shopping. In general, there were few differences in terms of gender. Younger users were at higher risk of online shopping fraud, while older ones were at higher risk of online banking fraud. In addition, some economic characteristics were connected with victimization. It can be said that measuring the internet usage volume by asking users about the time they spend online is better than asking about the frequency of Internet usage, because the time spent gives a clearer and more accurate idea of the volume of activities than the frequency of Internet use. Moreover, regarding the measurement of the dependent variables, namely online shopping fraud and online banking fraud, the idea of the question was general and abstract for users. In other words, despite the clarity of the idea of these two crimes in the way it was formed for some respondents, questions with general legal terms may raise difficulties in the minds of other respondents compared to when the question included clear and simplified elements without any general and abstract legal terms.

The study by Song, Lynch & Cochran (2015) dealt with victims of cyber theft with a different perspective from the present study. It examined the relationship between the theory of criminal opportunity and victims of cyber theft, and according to the authors, "the unique aspect of our research is that our results suggest that community structure can affect the internet risk and hence risk of cyber-theft victimization"(p15).

The study by Reisig, Pratt, and Holtfreter first concentrated on the victims of credit card theft. Then, they investigated the effect of some characteristics and behaviors on visualizing victimization risks in this crime and examined the relationship between them, which differed from the theme of the present study.

The aim of the study by Drew & Farrell (2018) was to gain a better understanding of the knowledge and behaviors of self-protection and crime prevention for potential victims of cyber fraud in the light of victimization risk. They found that users at higher risk of cyber fraud victimization fail to use online prevention strategies despite accurate perceptions of risks and knowledge of self-protection behaviors in the Internet space. Therefore, the main theme in this study had two points: The first was to realize and learn self-protection methods and the risks of falling victim to cyber fraud. The second point was to determine the extent to which these protective measures are used or not by potential victims to protect themselves. Although the study dealt with victims of cyber fraud, the aim and method in the study differed from the goal and method used in the present study for victims of cyber fraud.

Although there are previous studies dealing with victims of cybercrime investigated from different aspects, there is no defect from more insight, depth and accurate interpretation and studying of this phenomenon. Therefore, the present study extended previous literature on the knowledge and studied victims of cybercrime to help protect them from this kind of crimes as much as possible. The differences between the present study and other studies were as follows. The present study examined actual victims while other studies investigated potential victims. This study examined cyber theft and cyber fraud related to cyberspace as a whole without specifying whether it happened online or not.

3. Methodology

This was a technical study; since some of our questions were related to the computers and cyber space. One the other hand, some variables or questions (items) fail to have the same role or effect in comparison to others. Therefore, some questions in the questionnaire were presented to cybercrime experts and asked them about the possible relation between content of question and being victim of cybercrime using the following question: *With due respect, the questions in this questionnaire are concerned with victims of financial cybercrime. As a technical expert and specialist in this field, you are asked to express your technical opinion about items 1 to 10 on the value of the answers to each of the following questions*. For example, what kind of passwords do you use? A- Very simple like 123456; B. Simple like 187350093; C. Complex like 19tiie6o; D- Very complicated like @kj: # 123uy; E- I don't have a password. Now, the supposed value of item A is 8, which means that the likelihood of victimization is 8, i.e., 8 out of 10 people are victimized (80%). The supposed value of item B is 5, i.e., 5 out of 10 (50%). 0= The likelihood of victimization is 0%. 10= The likelihood of victimization is 100%.

3.1. Data Collection and Sample Size

The aim of this study was to know the common probable reasons or factors behind financial cybercrimes victimization. The study sought to implement the independent and dependent variables in the form of questions to examine them in actual victims of financial cybercrimes (Cyber Theft and Cyber Fraud). The spatial scale of the study was the SPECIAL COMPUTER CRIME UNIT in Mashhad-Iran where every individual was referred to the court for claiming of being a victim of cyber theft or cyber fraud. Victims were given the questions to answer. The sample size was 1334 victims (N=1334) and within three months, 42 questions were answered. The questionnaire consisted of 42 items. It is worth to say that the collected data represent different categories of people across Mashhad, Iran.

3.2. Variables

The aim of this study was to determine the effect of four factors on financial-cybercrimes victimization. Cyberspace lifestyle (variable 1) was divided into 13 items (sub-variables) and it was conceptualized by asking the victims questions related to *spending more time online, depending on cyber space entirely, using cyber space for financial purposes, paying money to activate apps or games, not reviewing previous opinions before downloading, not asking experts about downloading apps or games, communicating with friends through social media, paying deposit online, downloading from websites that have free or discounted materials, opening hyperlinks without checking, using free Internet, giving unused active SIM card to the others, and not informing official authorities when the credit card is lost*. These items were multiple-choice questions.

Capable protection variable (variable 2) was divided into 11 items (sub-variables) and it was conceptualized by asking the victims the questions about *not checking reliability or security of websites, little or no cyber knowledge, giving permission to access personal information, weak password or one password for multiple accounts or devices, sharing Wi-Fi with others, giving an unused credit card to others*. These items were multiple-choice questions.

Then, target attractiveness (variable 3) was divided into 5 items (sub-variables) conceptualized and measured by asking questions about *using a personal device by others, transferring money to others without checking, not notifying the authorities when a personal card or SIM card is lost, and giving the credit card to sellers without taking the necessary precautions*. These items were multiple-choice questions.

Finally, personal factors (variable 4) were divided into 10 multiple-choice items and measured by asking questions about *gender, age, family status, education, knowledge of cyber laws, confidence in cyberspace, and greed.*

4. Results

4.1. Cyber Lifestyle

Cyber lifestyle was measured by 21 items and every question expressed part of the victim's cyber lifestyle. These items were weighed using Analytic Hierarchy Process (AHP) so that the final score of a respondent varied from 9 to 126. A low score in this measure means a lower risk and the higher score shows a higher risk. The cyber lifestyle of theft and fraud victims is shown in Table 1.

Table 1

	Very low risk	Low risk	Medium risk	High risk	Average
Score	(9-25)	(26-50)	(51-75)	(76-100)	
Theft victims	11.3	61.5%	26.0%	1.2%	42.1239
Fraud victims	6.1%	55.9%	34.6%	3.4%	46.7908

Cyber Lifestyle Statistics

Surprisingly, in contrary to the primary assumptions, over 72.8% of theft and 62% of fraud victims had a low-risk or very low-risk lifestyle. This study was conducted only on victims, and it was impossible to evaluate this measure in non-victims. some of the main lifestyle features of the victims (table2) in this study include:

- Spending over 4 hours a day online;
- Not having a satellite TV at home and therefore, spending more time online for different purposes;
- Having different reasons for using cyberspace;
- Failing to ask experts about downloading apps or using online services;
- Mostly communicating with friends;
- Downloading from free-websites and not hesitating to buy stuff with discount.

Table 2

Statistics of partial lifestyles most followed by victims

Victims of crime	**Time spent (hour)**	**Having satellite TV**	**Asking expert advice**	**Communicating with**	**Using free websites**
Theft victims	64.6% (1-3) 22.4% (3-6)	92.3% No 7.7% Yes	59.3%No 37.6%yes	56.1% friends 22.9% relatives 7.0% strangers 10.3% some of them known	56% Yes 44% No

				3.8% some of them strangers	
Fraud victims	57.5% (1-3) 25.3% (3-6)	92.4% No 7.6% Yes	61.8 No 37.5%yes	54.5% friends 21.7% relatives 8.9% strangers 10.2% some of them known 4.7% some of them known	63.6%Yes 36.4% No

4.2. Protection and Target Attractiveness

4.2.1. Protection

Protection/Guardianship was measured by 11 items. They were weighed using Analytic Hierarchy Process (AHP) so that the final score of the respondent varied from 0 to 51. A lower score in this measure means a higher risk and a higher score indicates a lower risk (Table 3).

Table 3

Statistics of protection

Protection level	Very weak	Weak	Medium	High	Very high	Average
Score	(0-10)	(11-20)	(21-30)	(31-40)	(41-51)	
Theft victims	9.3%	52.2%	26.0%	8.7%	3.8%	19.9139
Fraud victims	13.7%	50.2%	22.3%	8.5%	5.2%	19.5265

Most of the victims failed to apply good protection measures. For example, only 12.5% of theft victims and 13.7% of fraud victims reported high and very high protection measures.

This finding significantly supports the second sub-hypothesis. Victims had the following features related to effective protection (Table 4):

- They failed to check the security of websites they browse.
- They had no cyber-knowledge.
- They had no idea about E-NAMAD[3].
- They had no password, or a simple or very simple one for their computers, mobile phones or social media accounts.

Table 4

Statistics of protection levels mostly followed by victims

	Checking websites security	Checking the sites by lock mark	Paying attention to symbols	Cyber knowledge	Attention to E-NEMAD	Clicking on E-NEMAD	Password strength
Theft victims	52.7% No	51.3% No	32.9% No	85.5% No 14.5% Yes	47.3% No 32.2%No-information 20.5% Yes	61.5% No 23.0%No-information 15.5% Yes	37.5% Simple 8.0%Very-simple 9.8%No-password
	20.7%No-information	19.8%No-information	16.0%No-information				
	9.2%yes	13.2% Yes	19.9% Yes				
	17.4%yes-sometimes	15.7%yes-sometimes	31.2% Yes-sometimes				
Fraud victims	52.1% No	53.6% No	33.3% No	84.0% No 16.0% Yes	47.7% No 32.6%No-information 19.7% Yes	60.2% No 22.9%No-information 16.9% Yes	38.5% Simple 7.3%Very-simple 13.2%No-password
	18.9%No-information	19.0%No-information	14.3%No information				
	10.9% Yes	10.1% Yes	15.6% Yes				
	18.1%yes-sometimes	17.3% sometimes	36.7% yes sometimes				

[3] E-NAMAD is a symbol given by the of E-Commerce Development Center affiliated to the Ministry of Industry, Mines and Trade of Iran. It is given as a certification of reliability to online stores.

The above results support the study hypothesis which says that lack of or poor protection expose users to be victim of cyber theft or cyber fraud.

4.2.2. Target Attractiveness

Target attractiveness was measured through 5 items. These questions were weighed using Analytic Hierarchy Process (AHP) and the final score of respondents varied from 0 to 26. A low score indicated low risk and a higher score indicated that the risk of target attractiveness was increasing. Generally, victims of both crimes in the present study showed different target attractiveness levels as shown in Table 5.

Table 5

Statistics of target attractiveness

Target attractiveness	Very low	Low	Medium	High	Very high	Average
Score	(0-5)	(6-10)	(11-15)	(16-20)	(21-26)	
Theft victims	52.1%	35.4%	10.1%	2.2%	0.2%	5.6481
Fraud victims	44.5%	35.4%	14.4%	5.2%	0.4%	6.5371

In general, victims of both crimes have a low or very low level of attractiveness to victimization risk. In details, for target attractiveness element, that victims of both crimes(table6):

- Give their electronic devices to others to use it either in front of them or not.
- They transfer money online without checking the correctness of the claimed actions.

Table 6

Statistics of some factors that make a person a suitable target

	Give my electronic device	Transfer money via text message request
Theft victims	48.9% Give on terms 14.8% Give without restriction 36.3% No	30% Yes 24.6% With restrictions 46.0% transfer after correctness
Fraud victims	41.8% Give on terms 19.4% Give without restriction	37.4% transfer 19.7% with restrictions

	38.8% No	42.9% transfer after correctness

The third hypothesis was partially supported in related to existing of some procedures or conducts making the individual a suitable target in cyberspace will affect cyber theft or cyber fraud crimes victimization.

4.3. Personal Profiling of Sample Victims

According to this study, a cyberspace victim is portrayed as follows: male greedy individuals under 50, married, with pre-university education and medium or low income. The above results support the final hypothesis that some of personal features suggested in the present study play a significant role in being a victim of financial cybercrimes (Table 7).

Table7

Statistics of victim's characteristics

Characteristic	Variable	Number	Percentage
Gender Theft, fraud	Male	966	89.8%
	Female	245	20.2%
	Male	197	82.4%
	Female	42	17.6%
Age Theft, fraud	Male	32.92 Av.	
	Female	32.31 Av.	
Marital status Theft, fraud	Single	413	34.5%
	Married	752	62.8%
	Divorced	32	2.7%
	Single	79	33.3%
	Married	149	62.9%
	Divorced	9	3.8%
Education Theft, fraud	Under diploma	206	16.9%
	Diploma	490	41.3%

Education Theft, fraud	Bachelor	360	30.4%
	Under diploma	33	14.2%
	Diploma	95	40.8%
	Bachelor	76	32.6%
Income Theft, fraud	Under IRR1 million	286	26.2%
	IRR1-2 million	475	43.5%
	IRR2-5 million	295	27.0%
	Under IRR1 million	48	21.7%
	IRR1-2 million	100	45.2%
	IRR2-5 million	62	28.1%

5. Discussion

The aim of this study was to portray major characteristics of victims of financial cybercrimes (cyber fraud and cyber theft). To achieve mentioned goal, a set of risk factors was examined based on lifestyle theory, routine activity theory and some personal characteristics. It is currently known how actual victims share these common risk factors and that if a significant number of them share these factors, the cyberspace users who own it are at a higher risk of victimization. Some risk factors examined here are as follows.

1. Cyber lifestyles consisted of the time spent online, having satellite TV, purpose of cyberspace use, paying money to activate apps/games, reviewing previous opinions before downloading, gaining information from experts, the type of relationship with the people are communicating with, paying deposits online, downloading from free or discount websites,

opening opaque links, using free Internet, giving a gift SIM card to others, losing credit cards.

2. Routine activity theory (capable protection level) included websites security, cyber knowledge, permission to access personal information, passwords, sharing Wi-Fi info, unused credit cards.
3. Target attractiveness included using devices by others, transferring money upon SMS, ID card or lost SIM card, using credit card by others.
4. Personal profile included gender, age, family status, education, income, legal cyber knowledge, being trustful in cyber space, and being greedy.

Some major results are discussed below.

5.1. Risky Cyber Lifestyle

It was found that increased time spent online has no effect on being a victim of financial cybercrimes. However, it was shown that 57 to 64 percent of victims in these crimes spent 1 to 3 hours per day online, which means that the time spent for majority of victims is less than 3 hours. This result corresponds with the study by Pratt, Holtfreter, and Reisig (2010) for fraud crime where the time spent is 1 to 3 hours per day. In other words, when the time spent falls in this range, increased time online affects victimization. Results of this study are important in that spending a long time online does not increase the risk of the being a victim of financial cybercrimes. Rather, spending one to three hours online suffices. The study by Junger, Montoya, Hartel and Heydari (2017) found no relation between increased frequency of Internet use and increased risk of being victim of online purchase fraud, which generally corresponds with this study. However, the present study preferred using a more accurate way for asking about average daily time spent online (how many hours do you spend on Internet per day?) than asking about the time spent in form of frequency or hours weekly. It is likely that the reason of increased risk of financial crime victimization when spending 1 to 3 hours online is that in this period users do some important activities including financial transactions (like online shopping). However, spending more than 3 hours online turns out to do other less important or nonfinancial activities.

In terms of the aim of using cyberspace, the study by Junger, Montoya, Hartel and Heydari (2017) found that risk of being a victim of cyber fraud was related to shopping online and watching TV. As for the study by Mesch and Dodel (2018), communicating (chatting) and doing financial activities online (shopping, purchasing and marketing) affect the risk of being a cyber fraud victim. According to the present study, the relationship between being a victim of financial cybercrimes and the purpose of using cyberspace in an unlimited manner instead of watching TV and selling or purchasing; however, the risk of being victim of financial cybercrimes related to cyberspace usage for various goals. This could be attributed to the fact that the financial process in cyberspace is not only limited to activities with financial goals- such as buying or selling- but also most activities are not financially targeted (such as downloading and buying games and applications, buying academic books, buying a program for playing sports) that require to pay money through the Internet. Therefore, in most cases, the user might be a victim of financial cybercrime, regardless of the purpose of using cyberspace.

It was also shown that majority of financial cybercrime victims have no satellite TV. No study was found on measuring the relationship between being a victim of cyber fraud or cyber theft and having or not having a satellite TV. It could be said that not having a satellite TV makes users depend fully on cyberspace. Nevertheless, this high rate may not indicate an accurate relationship, it is likely that responders give negative answer (I do not have a satellite TV) because having a satellite TV is illegal according to the Iranian law.

There are lots of computer programs and mobile apps on cyberspace, and not all of them are safe to download. Therefore, it is necessary to distinguish the harmful applications or malware that spy, destroy or collect critical information about us before downloading (Cyber Edu:Malware, 2020). We asked respondents whether they were getting information from experts on the source and method of software download. It was found that there is a correlation between downloading apps without getting enough information about it and the risk financial cybercrime victimization, which was the expected result. No study was found to compare the results with it.

Communicating (chatting) with friends online also affects victimization, because a vast majority of victims communicate with different people, especially friends online. It can be said that a person who frequently communicates with his/her friends online, allows flexibility and ease in collecting more information about them to be used for fraud or theft.

In addition, it was found that downloading free apps or apps with a discount is associated with an increased risk of financial cybercrime victimization. This was an expected result because although free and paid apps carry a risk, but free apps are riskier (Team, 2019).

5.2. Capable Protection, Target Attractiveness

There was a link between unsafe or unreliable website browsing and the risk of financial cybercrime victimization. Users who are most likely to be victims of financial cybercrimes are those not assured of the security and reliability of websites they browse, nor do they use verification methods even if they know about it (signs and quality of the language in which the site is written, the lock mark, site security check, etc.). Results of the present study were expected in this case, as many unsafe, unreliable and harmful sites have some signs and signals and there are several reasons for detecting and distinguishing them from others. In addition, results of this study were consistent with the results of the study by Akdemir and Ynal, who concluded that the use of well-known or trusted websites reduces the possibility of becoming a victim of cyber fraud. However, results of the study by Whitty (2019) were partly contrary to the results of the present study in that protective activities online do not protect against falling victim to the crime of fraud. yet, the present study examined the reliability and safety of websites through five questions, while in the mentioned study, they were examined with only one question: Have you visited the consumer advice website?

According to the present study, users who use complex passwords containing numbers, letters and forms are at lower risk of becoming a victim of financial cybercrimes, similar to what found in the study by Akdemir and Ynal. It could be said that this result was close to reality, as easy passwords are more vulnerable to detection and guessing by criminals. Furthermore, having the same password for different accounts and devices (with similar characters) increases the risk of becoming a victim of cyber fraud or theft, which is the opposite of what shown in the study by Akdemir and Ynal (2020), who found that the use of different passwords for different accounts and devices increased the risk of becoming a victim for cyber fraud. Results of present study were close to reality, because detecting and guessing one password used for multiple devices and accounts results in a higher risk of stealing many critical data from these accounts or devices. According to the present study, users with less knowledge of information and communication technology are more likely to be victims of financial cybercrimes, which is consistent with the study by Junger, Montoya, Hartel and Heydari. In general, familiarity with cyberspace knowledge helps diagnose risk and harm points, and leads to avoiding the traps used by cyber criminals.

With regard to the procedures that make users an attractive target, it was found that users giving their devices (laptop, mobile, and tablet etc.) to other people in order to use it for some purposes on the one hand, and users who transfer money (little or much) to other people they do not even know based on a text message or others that came from people they know; these two types are more likely to become victims of financial cybercrimes. These results were logical, because a person who performs such harmful and dangerous measures is considered and noticed cyber criminals, whether they are friends or not, and they find an easy and attractive target to carry out their criminal projects. The above result was identical to the results of Akdemir and Yenal (2020) regarding the attractiveness of the target in that the more the user has the attractive target ingredients, the more likely he/she will be a victim of cyber fraud. However, the content of ingredients in two studies was different. Whereas, the study by Akdemir and Yenal (2020) measured the targets attractiveness by the type of device used, this study measured the targets attractiveness with the user's personal actions regarding the device or transferring money to others. It could be said that the individuals becoming an attractive target is not only related to the interaction within cyberspace or the type of devices, but also, it has to do with the persons characteristics or procedures they take in real life which are extended to cyberspace.

5.3. Personal Characteristics

It was found that users aged under 50, especially those in their 26 to 35 years old (42% to 44% of victims in both crimes) are more likely to be victims of these crimes. This was expected since younger users use cyberspace more often than others on a frequent basis which makes them more vulnerable to cyberspace risks. These results were in line with the study of Pratt, Holtfreter and Reisig (2010) on cyber fraud, the study by Junger, Montoya, Hartel and Heydari for purchase fraud but not for banking fraud, and the study by Song, Lynch and Cochran for cyber theft victimization. However, they were contrary to the results of study by Whitty (2019) who indicated that victims of cyber fraud were more likely to be older, score high on impulsivity measures of urgency and sensation seeking, score high on addictive measures and engage in more frequent routine activities that place them at great risk of becoming scammed.

In addition, a relation was found between education and being a victim of financial cybercrimes risk, where 32% of victims had a college degree and 54% had a pre-university degree. It means that those with a higher level of education (masters and PhD) are less likely to be victims which is in line with the results of Whitty (2019). One possible explanation is that people with a higher education degree (masters and PhD) have more knowledge and information. In addition, they find less time to spend online, unlike people with an academic or pre-university degree. Although university educated people have the information and knowledge, they spend more time online than others, and people with a pre-university degree have less experience and information than others.

The present study found that male users are more likely to be victims of financial cybercrimes in line with the studies by Pratt, Holtfreter and Reisig (2010), and Song, Lynch and Cochran (2015). The logical explanation is that male users do more diverse activities online than female users. Married users are more likely to be victims of financial cybercrimes according to the results of the present study, due to the fact that married people usually have more obligations than single ones including financial obligations (such as paying the house rent, buying the house needs, paying the children's school installments) which increase their online activities with a financial purpose. In addition to what was previously mentioned, a relationship was found between low income and higher risk of financial cybercrime victimization. One of the explanations for this is that low-income users always look for cheaper/discount services or applications online, and as mentioned earlier, these services or applications are riskier than others. The previous explanation corroborated the relationship found between variables of income, download from free or discount websites and financial cybercrimes. With regard to victims of cyber theft who have an income of less than one to three million IRR, 55% downloaded or bought applications or services from free or discount websites, with similar rates of cyber fraud. Finally, a correlation was found between the nature of greed and the risk of becoming a victim of financial cybercrimes, as those with financial greed constitute 77% of the total number of victims of both crimes. This was confirmed by the strength of the relationship between the variables of financial cybercrimes on the one hand, and the size of greed, willingness to pay low amounts of money, and download or purchase from free or discount websites on the other hand where over 75% of victims were interested in paying less money and had some greed; they were interested in downloading or buying applications or services from free or discount websites. This result is explained by the fact that greedy people in general measure everything with money and seek to obtain anything at the cheapest prices, and it is known that there are cyber criminals or fraudulent and harmful websites or applications that seek to attract these people through delusions and mislead them by free or discount price.

It is recommended to conduct similar studies in the future on the relationship between increased time spent online and the change in the type of activities on the Internet and their relationship to being a victim of cybercrime. It is also suggested to conduct more researches in the future on the application of target attractiveness in cybercrime so that this element be translated into different and various parts for testing. It is also suggested to address the greed of individuals broader and deeper in order to study its relationship with becoming a victim of financial cybercrimes.

One of the limitations of the present study was that the number of victims of cyber fraud (239) was less than the number of victims of cyber theft (1211). This affected the difference in strength and extent of generalization of the results between the two crimes. Another limitation was that the present study dealt with one type of fraud, which means that results of this study cannot be circulated conclusively to all types of cybercrime fraud.

Conclusion

The incidence and growing interaction and meeting the needs through cyberspace is a feature of this era. However, it does not hide the many negative aspects that accompany this development one of the most important of which is falling victim to cybercrimes. Although there are several individual, social, economic, and technical reasons for the incidence of cybercrime in general and financial cybercrimes in particular, focusing on the individual causes and identifying and clarifying them leads to individual's enforcement and development of their knowledge and their ability to avoid falling victim to these widespread crimes. This makes a huge contribution and effectively reduces the rate of these crimes to the lowest possible rate. From this standpoint, the significance of the present study lies in the fact that it defines the model of cyberspace users by identifying and clarifying personal and technical risk factors shared by users in order to show them to individuals or criminal justice agencies, to take it into consideration when knowing or searching for measures that prevent the incidence of these crimes as much as possible.

References

Bradford W., R., & Billy, H. (2015). The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *International Journal of Offender Therapy and Comparative Criminology, 60*(10). doi:10.1177/0306624X15572861

Cyber Edu:Malware. (2020). Retrieved from forcepoint: https://www.forcepoint.com/cyber-edu/malware

Eric Rutger, L., & Majid, Y. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior, 37*(3). doi:10.1080/01639625.2015.1012409

Girvan, C. (2018). What is a virtual world? Definition and classification. *Education Tech Research Dev, 66*, 1087–1100. doi:10.1007/s11423-018-9577-y

Hyojong, S., Michael, J. L., & John, C. (2015). A Macro-Social Exploratory Analysis of the Rate of Interstate Cyber-Victimization. *American Journal of Criminal Justice, 41*(3). doi:10.1007/s12103-015-9308-4

Insurance Information Institute, Inc. (2020). *Facts + Statistics: Identity theft and cybercrime.* Insurance Information Institute, Inc.

Jacqueline, M. D., & Lucy, F. (2018). Online victimization risk and self-protective strategies: developing police-led cyber fraudprevention programs. *Police Practice and Research, 19, NO. 6,*, 537–549. doi:10.1080/15614263.2018.1507890

kahramani, B. p. (2018). a comparative study of mechanisms for protection of cybercrime victims in Iranian criminal law and international documentation with emphasis on the Budapest Convention. *Journal of Criminal Law*.

Marianne, J., Lorena, M., Pieter, H., & Maliheh, H. (2017). Towards the normalization of cybercrime victimization. *IEEE.* London: International Conference On Cyber Situational Awareness, Data Analytics And Assessment. doi:10.1109/CyberSA.2017.8073391

Meghan, H., Marcus, F., & Brandon, W. (2013). The capable guardian in routine activities theory: A theoretical and conceptual reappraisal. *Crime Prevention and Community Safety, 15*(1), 65-79. doi:10.1057/cpcs.2012.14

Miethe, R. F. (2009). Understanding Theories of Criminal Victimization. *Crime and Justice*, 459-499.

Miró, F. (2014). Routine Activity Theory. In F. Miró, *The Encyclopedia of Theoretical Criminology* (p. 2).

Monica T., W. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime, 26*(1), 277-292. doi:10.1108/JFC-10-2017-0095

Naci, A., & serkan, y. (2020). Card-not-present fraud victimization: a routin activities approach to understand risk factors. *Güvenlik Bilimleri Dergisi*, 243-268. doi:10.28956/gbd.736179

Nicholas, P., Michael, H., & Darren, P. (2013). A Direct Insight into Victims of Cybercrime. *International Conference on Trust, Security and Privacy in Computing and Communications.* Melbourne: IEEE. doi:10.1109/TrustCom.2013.74

Renhart, R. (2018). *One in Four Americans Have Experienced Cybercrime.* Gallup.

Steve G.A, v. d., & Eric Rutger, L. (2017). Big Five Personality Traits of Cybercrime Victims. *Cyberpsychology, Behavior, and Social Networking, 20*(7). doi:10.1089/cyber.2017.0028

Suzan, v. d. (2014). Introduction to victimology and victims' rights. (pp. 6-12). Strengthening judicial cooperation to protect victims of crime.

Team, A. (2019, 11 19). Retrieved from Absolute : https://www.absolute.com/blog/archive/the-dangers-of-free-mobile-apps/

Thomas J, H., & Adam M, B. (2009). examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 1-25. doi:10.1080/01639620701876577

Travis C., P., Kristy, H., & Michael, R. (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

Uğur, A., & Murat, D. (2016). Examination of Routine Activities Theory by the property. *International Journal of human sciences*, 1188-1198.

wardy, F. e. (2018). victim compensation for cybercrime. *the4th international congess of rligous culture and thought* . Qom.

Williams, M. L. (2020). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *Centre for Crime and Justice Studies*. doi:10.1093/bjc/azv011

Yamani, A. (2019). *978 million victims of cybercrime in 20 countries.* Mecca: Makkah Newspaper.

zararahk, E. (2011). cybercrime victimology. *Parliament and strategy*, 127-158.