Cyber-Crime in Online Videogames and its Reporting by School-aged Children

By: Ayman Chalak

Supervisor: Associate Professor Michael Hitchens

MACQUARIE University

A thesis submitted to Macquarie University

For the degree of Master of Research

Department of Computing

March 2020

I certify this thesis has been reviewed by my supervisor prior to its submission

Declaration

I, Ayman Chalak, certify that the thesis entitled as "**Cyber-crime in Online Video-games and its Reporting by School-aged Children** "has not previously been submitted as part of the requirements for a degree to any other university other than Macquarie University. I also certify the thesis is an original piece of research and written by myself under the supervision of Professor Michael Hitchens, and any sources are referenced in the thesis to address the work contributed by original researchers.

Ayman Chalak 25/03/2020

Acknowledgment

First and most of all, I would like to express my gratitude to Prof Michael Hitchens, my supervisor, for his personal wisdom, guidance and professionalism in guiding me throughout the process of writing this thesis. His dedication and keen interest of help, had been mainly responsible for completing my work. Moreover, I would like to extend my sincere gratitude to the faculty of Science & engineering, more specifically, to the department of computing in providing me the accessible resources such as Library, E-library, and books among others to finish the thesis. Finally, I would like to thank my family – my parents, in encouraging me to pursue my MRES program .They all kept me going, and this thesis would have not been possible without them.

Abstract

Cyber-crime is a large and growing issue. The problems presented by cyber-crime will not be addressed unless its true extent is known and an important factor in this is the reporting of cyber-crime events by its victims. Children are particularly vulnerable to cyber-crime due to their inexperience and the amount of time they spend on the internet, particularly playing online videogames. There has been limited attention in the literature to the reporting of cyber-crime by school aged children and the reasons why they may not choose to report an incident of cyber-crime. This research involved a group of 47 participants, aged 18 to 25. Participants were surveyed about their video game playing habits, cyber-crime experience and the reporting of those experiences while they were of school age. The age range of participants was chosen so that they would have sufficient recall of their experiences of cyber-crime while of school age but would have the emotional maturity to deal with the recall of potentially traumatic events. Frequency of experience of cyber-crime showed variation depending on the type of cyber-crime. Participants reported a low level of reporting of cyber-crime experiences, for reasons that included guilt, embarrassment and not considering the event important enough to report. Gender differences were found in the frequency of experience of cyber-crime and reporting of some categories of cyber-crime, including hacking and cyber-pornography.

Contents

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Background of the study

Technologies, such as computers and the Internet, are playing an increasing role in youngster's lives. With this trend it has become apparent that the Internet presents both risks and opportunities for users (Shu & Subrahmanyam, 2009). One of the primary means that young people employ the internet is to play online videogames. These games come in a multitude of forms and may be played in a range of geographical locations. Children may play online games using their desktop computer or gaming console. Others utilize a smart phone to engage in online games. Still other children use a tablet such as an IPad.

According to New Zoo's report, there are 2.3 billion active gamers worldwide and 47% of them (1 Billion gamers) spend money while playing online games (Mcdonald, 2017). Online gaming was expected to generate $USD108.9 billion in revenues in 2017 (Mcdonald, 2017) . According to (Diele, 2013) 44% of internet users play online games. With 3.9 billion users of the internet, this gives 1.7 billion online game players. Many of these players will be young people. The gaming industry is generating revenues in billions of dollars due to the increasing number of online players. Use of the internet exposes players to various risks, including cyber-crime. David Wall (2007) defined Cybercrime as "a crime-taking place in space rather than on site. In addition, it signifies the occurrence of harmful behaviour related to the misuse of networked computer system" (wall, 2007). Therefore, cybercrime is a criminal activity that constitutes an alteration of data or information for personal benefits. Sirohi (2015) defines Cybercrime as "a computer mediated activity which is either illegal or considered illicit and can be conducted via global network, and has been identified as an activity in which computers and networks are a tool of criminal activity to be occurred" (Sirohi, 2015). Although online games are a form of entertainment, they can also be considered as a tool for cyber criminals to attack the players through many forms like cyber-bullying, cyber-harassment, distributed denial of service (DDOS) attacks & online identity theft.

1.2 Problem Statement

Due to the importance of the gaming industry financially, Cyber criminals are targeting online gamers through many tactics and techniques. There are a range of possible attacks such as hacking online gaming user name and passwords, sending viruses to their machines, gold fishing, and gaming bots etc. These various techniques are harmful to the users. Cyber-

crime can only be combatted, and those that experience assisted, if the range of crime is understood. This requires reasonably high levels of reporting. It is likely that the nature of cyber-crime will vary with the exact methods and avenues of attack. With the increasing exposure of underage people to cyber-crime through online video game play, it is important to understand what level of reporting of cyber-crime they are giving and the reasons why they may not be reporting instances of cyber-crime. This research will address the questions of what types of cyber-crimes are experienced by school-aged children and do they report the experience of such crimes?

1.3 Outline of the study

This research examines the experience of school-aged people of cyber-crime. Participants were aged between 18 and 25 to both avoid the problems associated with underage participants (such as obtaining permission from parents and guardians) while still allowing for sufficient recall of the relevant experiences. Participants were asked to complete a survey which detailed their gaming habits, knowledge of cyber-crime and experience of cyber-crime whilst of school age, as well as other relevant information.

1.4 Organization of the thesis

Chapter 1- Introduction includes the background, problem statement, outline of the study and organization of the thesis.

Chapter 2 – Literature review includes the definition of online games and size of game market. This is followed by a review of both the amount of time spent playing online videogames and the percentage of the children that play such games. The definition of cyber-crime is discussed. Plus, various types of cyber-crimes are given. Several case studies that have dealt with cyber-crime targeting school-aged children are presented. Theoretical frameworks such as RAT theory, that can be used to understand cyber-criminality, and economic and psychological models that explain why victims intend to report or not report the cyber-crime are presented. Finally, factors that affect the reporting or not reporting of crime are examined.

Chapter 3 – Methodology contains research questions, and the methodology of the study, including participants, their recruitment, data collection techniques, study approach and survey questionnaire.

Chapter 4 – Findings presents the data gathered from survey questionnaire.

Chapter 5 - Discussion provides interpretation and explanation for the interrelation between the outcome of the survey and the theories that framework the study, as well as providing an

explanation of the survey outcome. In addition, it states answers to the main research question and subsidiary questions.

Chapter 6 - Conclusion summarises the findings of this study, details the limitations of the study and provides recommendation for both future research work research and strategies to better prepare school aged children for experiences of cyber-crime.

Chapter 2 Literature Review

2.1 Introduction

The online videogame market has been growing rapidly with new products and technology worth nearly $138 billion a year (Ell, 2018). Young people are spending considerable amount of time playing online videogames as part of their daily activities (Griffiths, Kuss, & King, 2012). It has become one of the most addictive internet activities among young players. Online videogames expose players to all facets of the internet, including the illegal ones. Cyber-crime is the criminal use of computer technology. It can occur in many forms such as fraud, cyber-harassment, cyber-bullying and online identity theft (Pedneker, 2013). Players of online videogames may be victims of cyber-crime (Przybylski, 2018).

A number of studies have discussed the prevalence of cyber-crimes targeting both elementary and secondary school students while playing online games at both college and University (Chisholm, 2014). While these studies are typically focused on a single type of cyber-crime, taken together, they give an overview of the types of cyber-crimes that can be experienced by players of online videogames. However, they are often concerned with the specifics around the occurrences of such crimes and not wider issues, such as their reporting. Typically, many crimes, not just cyber-crimes, go unreported, for a variety of reasons, including fear of consequences and lack of knowledge. However, there is limited existing research into the reporting of cyber-crimes by school-aged children. Such victims form a particularly vulnerable subset of internet users, due to their lack of experience as victims of crime and unequal power balance in their relation to authority figures. In order to be able to better protect school-aged children from cyber-crime, it is worthwhile understanding what crimes they are experiencing and what reporting actions, if any, they take. To gain a complete perspective on the commission of cyber-crime, it is worth considering what is required to create a situation in which a cyber-crime may occur. Routine active theory (RAT), which has been developed by Cohen and Felson (1979), is a theoretical framework that takes an ecological perspective on criminal behaviour. It states that a number of elements must be concurrently present for a crime to be committed, including the availability of a target

(victim), the lack of a capable guardian, e.g., technology (such as a firewall or CCTV) or capable guards (such as police or a parent) and a motivated offender (in the case of cyber-crime, a cyber-criminal) (Cohen & Felson, 1979).

2.2 Definition of online games & size of game market

Online videogames are played through a networked medium, internet or other telecommunication platform, typically in concert with other players who are similarly connected to the network. The technical requirements for playing online games are an appropriate piece of client software, plus a network connection. The client software maybe a stand-alone application or the game may be played through a web browser. In the latter case, the games are often called browser-based games or web games (Chen, 2005). There are many types of online videogames, including Massively Multiplayer Online Role Playing Game (MMORPGs), Multiplayer Online Battle Arena (MOBA), Real Time Strategy (RTS), Massively Multi-player Online (MMO) shooters and social games. Many others exist and there are also various sub forms. For example, MMO shooters may be present either first or third person viewpoint to the player.

MMORPGs are videogames played over the internet with thousands of players connected to the same server. Compared to single player, in MMORPG, players can accomplish their goals in cooperation and collaboration with other players or may be against their opponents. Examples of MMORPG include World of Warcraft, Ever Quest, Guild Wars and Run escape (Achiterbosch, Pierce, & Simmons, 2007).

MOBA are games played between two teams. Each player controls a single character. The aim is to destroy the opposing team's main structure with the assistance of computer-controlled units. Examples of MOBA's include Heroes of the Storm, DOTA 2, and League of Legends.

RTS games typically involve two players competing against each other. Players need to gather resources and build a base and military power in order to defeat their opponents (by destroying their base and army). RTS games are real time, with players taking actions simultaneously. This can be compared to traditional games such as Chess, where players take turns and may have several minutes to decide the next action. Skilled RTS players can issue a high number of orders to their virtual armies in a limited amount of time (Wu, Xiong, & Iida, 2016). Examples of RTS games include StarCraft II and Supreme Commander (Ontañon, et al., 2013). MMO shooter games are designed for players to engage in combat with other players while controlling a single character. They differ from MOBAs in their viewpoint,

MOBAs typically using an isometric perspective, whereas shooters use first- or third-person. Examples of MMO shooters include Counter Strike, Fortnight and online versions of Call of Duty. Jansz and Tanis (2007) stated that MMO shooter players are almost exclusively young men (Mean age 18 years old) who spend their leisure time playing this type of game (2.6 Hour Per day). In addition, MMO shooters are typically not played in isolation, instead more than 80% of the respondents were members of a group who played together. The study also found that a social interaction motive was the strongest predictor of the time actually spent on gaming (Jansz & Tanis, 2007).

Social games are played online, often using mobile devices, and involve interaction and cooperation with online players such as friends or opponents. Example of social games include Farmville, Mafia Wars and Frontier Ville.

According to a report conducted by (Warman, 2018), the value of the game market value was $US35bn in 2007. This grew to $US137.9bn by 2018. The Asia-Pacific region generated $US71.4 bn in 2018, which is 52% of total game revenues due to the continued growth in smart-phone gaming. Moreover, Asia dominates in terms of the highest number of online game players, followed by North America by a percentage of 23% of global game market. In terms of North America, the total revenues increased year by year, and it is projected to reach $32.7 bn in 2021. The next largest region was Europe, the Middle East and Africa, which represents 21% of the market with revenue of $US28.7 bn in 2018. Then, Latin America grew to $US5bn in game revenue in 2018 taking 4% of the market. The largest single market will continue to be China, which is projected to reach revenue of $US50.7 bn in 2021 (Warman, 2018).

2.3 Amount of time online-players spend playing online games

Online game addiction has become a common phenomenon that affect many individuals and societies (Xu, Turel, & Yuan, 2017). Although not all online games are harmful, some games like massively multiplayer online games can be addiction-prone (Liu & Peng, 2009). Teenagers are as susceptible to this as any other videogame player. While only a small fraction of players become addicted, the sufferer will experience numerous negative effects in the same way that any other addiction (such as alcohol or drugs) can have. They become preoccupied with gaming, spending unusually high amounts of time playing. They may lose their interest in other activities as well as withdraw from family and friends for the sake of online games (Leung L. , 2004). A mother recounted the experiences of her son (aged 13 at the time) who was described as addicted to technology, especially online games. She stated that her son spent most of his

time in his room playing online games, and barely engaged in social interaction with any members of the family. In addition, he rarely completed his homework. On one occasion, when she tried to take his tablet off him, he became aggressive.

Cole and Griffiths (2007) conducted a study stated that 22.85 hours per week is the mean average time online gamers spend playing MMORPGs. Males spend 23.3 hours playing on average whereas females average 21.7 hours. According to the data provided in the study, 3.6 % of online gamers play over 60 hours a week (Cole & Griffiths, 2007). Another report (Brand, 2015), which examined a broader cross-section of online games, found that males spend more time playing online games compared to females. The study found that females play for 75 minutes a day on average, while males play for 100 minutes on average.

A more recent report, (Limelight, 2019), found that young online game players, whose ages range between 26 to 35 years old, spend more time playing online games compared to elderly players. This report was based on responses from 4,500 players who play video games at least once a week and are of minimum 18 years old of age. The participants were located in France, Germany, India, Italy, Japan, Singapore, South Korea, the United Kingdom, and the United States. For young players the average amount of time spent playing online videogames per week was 8 hours and 12 minutes compared to those over 60 years old who spend 5.63 hours playing online games per week. The study found that online game players play an average 1 hour and 22 minutes at a time.10% of participants have played for 10 or more hours consecutively. Overall, the report found that video gamers spend an average of 7.1 hours each week playing online games in 2019. This is an increase of 19.3% over the 2018 figure. By nationality, German gamers spend the most time playing online games at an average of 8 hours per week. South Korea which had the lowest weekly average at 6.69 hours. Germany and the US had the highest percentage of gamers who play more than 20 hours each week, at 11.6% (Limelight, 2019).

A 2009 study interviewed 813 students of Brigham Young University who played online videogames (Jensen & Walker, 2009). According to the study, there is a correlation for young adults between amount of time spent playing videogames and the frequency of engaging in risky behaviours such as drinking and drug abuse. For example, young adults who play video games daily reported smoking pot almost twice as often as players who played less frequently, and three times as often as those who never play. In addition, they reported other reasons that prolong the amount of time playing online games, such as poor family situation. The more time players spent playing online video games, the less connection was reported

with parents. Again this indicates that young adults who spend excessive time playing online games are likely to have removed themselves from important social settings.

Greenfield (2019) conducted a study related to the number of hours children spent weekly playing games in UK from 2013 to 2017, classified by age group. In 2013, children, aged 12 to 15, spend most of their time playing games for approximately 10.7 hours per week, compared to 2017, they spend 12.2 hours on weekly basis. However, Children, aged 3 to 4, play games for 5.9 hour per week (Greenfield, 2019).

2.4 Percentage of Children Playing Online games

Reisinger (2011) conducted a confirmed report that 91% of US children, aged 2 to 17, are playing online video games, and that American children, aged 2 to 5, have increased their gaming time by 17% since 2009. Moreover, the study found that 8% of children played games on mobile platforms in 2009, and that figure increased to 38% in 2011. In addition, it can be confirmed that 91% of them are attracted to online games by the need to find satisfaction and to share the experience with other people. Moreover, the percentage of the population playing online videogames is an indication of the potential impact on children of cyber-crime (Reisinger, 2011).

Children make extensive use portable gaming devices such as the PlayStation Portable (PSP) and carious Nintendo devices to engage in online games. In a study conducted by Amanda Lenhart (2009), youngsters, aged 12 to 14, own mobile gaming devices predominantly. 67% of the children in this age range surveyed owned a portable gaming device compared with 44% of teenagers, aged 15 to 17 years old. Males are more like to own mobile devices (61%) versus females (49%) (Lenhart, 2009).

A report conducted by Brand et al. (2018) stated 88% of children fall victim to online game cybercrime and are also faced with the challenge of staying safe. Moreover, this study reported a higher percentage of people under 18 played online games (76%) when compared to people 18-65 (65%) and those over 65 (43%) (Brand, Todhunter, & Jervis, 2018).

In a report conducted by the e-safety commissioner's research office (Grant, 2018), it was found that amongst Australians, aged 8 to 17, 81% played an online game by themselves and 64% played with others in the twelve months to June 2017. Playing online games with others was more popular with teens (14 to 17 year olds) (67%) than younger children (8 to 13 year olds) (62%) and males (71%) versus females (51%). For young people, the overall figures by gender are slightly lower, with boys (64%) more likely than girls (40%) to play with others (Grant, 2018). Another report, (Bouckley, 2019), found that 58% of children aged from 8 to 11

and 66% of children aged from 12 to 15 play online games. Finally, Lenhart (2015) reported 75% of teenagers in New Zealand, aged 13 to 17, were found to play video games (without distinguishing between online or offline video game playing). The report stated 74% of all children under the age of 18 in New Zealand were video-game players (Lenhart, 2015).

2.5 Definition of Cyber-crime and Types of Cyber-crimes

2.5.1 Definition of Cyber-crime

Cyber-crime is defined as unlawful acts where the computer is either a tool to commit cyber-crimes or considered as a target perpetrated by cyber-criminals. It may be used as a tool to perform several illegal activities such as cyber-pornography, cyber-stalking, cyber-harassment among others. However , it may be a target for unlawful acts that comes into many forms like unauthorized access to computer-application or system , theft of info contained in Electronic form etc. (Suman, Srivastava, & Pandit, 2014).

Related to the current study, cyber-crime, which is perpetrated by cyber-criminals, targets school-aged students (18 to 25 years old) playing online games. It occurs through many forms such as cyber-harassment, cyber-pornography and online identity theft among others. Chapter 4 (findings) is going to present the types of cyber-crimes targeting school-aged students while playing online games. Cyber-criminals exploit technology to target victims playing online games through various online gaming platforms such as E-mail, blogs, and live chat. These targets occur into many locations such as home, internet café, school etc. The study is going to identity the locations where school-aged students were targeted. Finally, when cyber-crimes occur, victims might be traumatized when targeted by cyber-criminals. It may affect them emotionally, psychologically, financially and socially. Moreover, it can change their view of life and living, and leave them with difficult feelings and reactions they may not understand (Wasserman & Ann Ellis, 2010). So, this study will identify whether school-aged students report or don't report cyber-crimes after being traumatized and the causes of non-reporting & reporting it. Details are found in chapter 5 more specifically section 5.4 called Reporting & Non-reporting Cyber-crimes.

2.5.2 Types of cyber-crimes

Cyber-crimes target victims through the online environment. It comes in many forms such as Identity theft, Cyber-laundering, Phishing, Online auction Fraud, Computer Fraud, spam, pornographic material, hacking and cracking, and cyber-harassment (Gercke, 2012) and (Nurse, 2018). **Hacking** is the unauthorized use of a computer system for criminal purposes. It includes many activities like breaking into a computer system, developing or using viruses,

destroying or altering files, and accessing private (health or financial) data related (Rogers, Smoak, & Liu, 2006). It has resulted in considerable loss of information and system unavailability. Quinn & Arthur (2011) describe an attack on the Sony PlayStation. Seven million customers were affected, with their names, passwords, and credit card stored on the PlayStation Network (PSN) were stolen. This gaming network was taken offline for multiple days while the system was upgraded to prevent further intrusions (Quinn & Arthur, 2011).

Phishing is an activity where the victims are lured into revealing information that allow the attackers to hack into systems and accounts (Marcum, Higgins, & Ricketts, 2014) .

Denial of Service (DOS) is an attack attempted by the cyber-criminal to prevent legitimate users accessing a desired service. For example, DOS attackers may attempt to overwhelm a server by launching so many requests that cannot respond to legitimate users. Webb (2018) describes an attack by a Utah-based hacker, Austin Thompson, 23, who targeted gaming networks including PlayStation network and XBOX Live. He prevented online game players from participating in online games by disrupting the gaming networks, and faced 10 years in jail. He announced the attacks in advance via the @DerpTrolling Twitter account and later shared screenshots and tweets as evidence of a successful attack (Webb, 2018).

Distributed Denial of Service (DDOS) is a form of DOS attack where many source computers are used to overwhelm the targeted resource. This may be a server, or the network as a whole (Lau, Rubin, Smith, & TrajkoviC, 2000). A report conducted by Mesmer (2013) defined it as a destructive crime that is directed at game developers and servers dedicated to the operation of online games. By doing so, it prevents online videogame players from playing online games (Messmer, 2013). Another example attack was described by Zeifman (2015) where the Lizard Squad group of hackers targeted game servers with DDoS attacks in order to take down PlayStation, Xbox, Nintendo and League of Legends (Zeifman, 2015).

Ransomware is a form of malicious software that threatens harm by denying the users access to his/her own data. The cyber-criminals demand a ransom from the victim to restore the data upon payment (Fruhlinger, 2018). Such ransomware is deployed for financial gain. However, it can also be used to direct victim activity. For example, the *PUBG ransomware* encrypts user data and gives as one option for recovery that the victim play the popular Battle-royal shooter, PUBG. The ransomware monitors the computer and once it sees the PUBG file *TslGame.exe* being executed it unencrypts the files (McMullan, 2018).

Grooming is a form of cyber-crime where online predators target children through a variety of avenues, such as social media or online games. One report (Katersky, 2012) described incidents where sexual predators used online video games as a medium for meeting and

trapping children. For example, a 12-year-old boy playing games on Xbox LIVE met a predator named Richard Kretovic, who used online game chat for a period of three months in order to create a relationship with the boy and convince him to travel to the perpetrators unaccompanied. When he arrived at the predator's home; he was subject to sexual abuse.

Online identity theft is a cyber-crime where, through hacking or other means, the perpetrator obtains personal information that allows them to impersonate the victim and access financial, etc., information. For example, cyber-criminals have interacted with children playing *Fortnite* and lured the victims into revealing their parent's banking details or personal information such as user name and password preventing them to get back to the game (Henry, 2018).

Cyber-harassment is a broad category that includes a number of activities, such as bullying and cyber-stalking. Corcoran et al. (2015) define Cyber-bullying as "an abusive behaviour perpetrated by cyber-criminals using mobile phones and computers with internet access for the goal of causing harm for the victims who face difficulty in defending themselves" (Corcoran, Gucking, & Prentice, 2015). Bullying may be carried out by people known to victim or by strangers and may be anonymous. An example of cyber-bullying was presented in an article that discussed the impact of age, gender, and experience on cyber-bullying in multi-player online gaming environments (Fryling & Cotler, 2014). 1025 adolescents and adults (age range 12-70 years old) were surveyed and the participants (62% female and 38% male) were recruited from an online gaming forum. According to the results, more than one-third of the participants didn't play online games due to concerns about cyber-bullying, and nearly eighty percent of the participants were cyber-victims, one in three were cyber-bullies, and over 90% had been involved in cyber-bullying as eyewitnesses (Fryling & Cotler, 2014).

Cyber-stalking is defined by Maran & Begotti (2019) as "the use of electronic communication devices such as the internet and E-mail in order to stalk another person. It has an impact on victim's wellbeing .It leads into the increase in physical and emotional symptoms, anxiety and depression" (maran & begotti, 2019). Thaier & Maple (2013) discuss Cyber-stalking as involving the use of ICT to perpetrate illicit activities by an individual or a group for the goal of harming victims using internet services such as live chat or through sending e-viruses and unsolicited e-mail (Thaier & Maple, 2013). When directed at children cyber-bullying/ stalking/harassment can be intended to humiliate them and adversely affect their confidence and self-esteem (Leukfeldt & Yar, 2016). Cyber-bullying may lead to incidents such as suicide or self-harm (Farhat, Himani, Rehmatullah, Azim, & Temuri, 2014).

As noted in this section, there are a range of possible cyber-criminal activities targeting victims through the online environment. Some of these have additional issues when the victims are children, or are specifically aimed at children. Several reports were conducted to illustrate the issues. Bilchik (1999) recognizes that children are at increased risk of crime victimization in the US. They may be exposed to crimes such as child-pornography and child abuse, amongst others. The effect of these crimes on children can be disturbing (Bilchik, 1999). Children may be exposed to pornography through the Internet at ages below the age of consent (Zhao, 2018). Lack of parental control grants young people freedom to access adult sites and click on malicious links that may expose them to sexual offenders. Children are innocent and require protection from illicit activities perpetrated by cyber-criminals (Winther, 2017). Grooming and human trafficking are amongst the serious crimes that can target children through online platforms. Extensive online contact is carried out with the children, aimed at building relationships which can then be used to lure the children into meeting strangers in unsafe places. Alotaibi et al. (2016) mentioned that online games expose children to sex pests and paedophiles through easy retrieval of personal information (Alotaibi, Furnell, Stengel, & Papadaki, 2016). Children may be exposed to cyber-stalking and cyber-harassment and their lack of maturity may leave them less able to deal with this victimization. The rise of terrorism has also led to increase recruitment through social media platforms and online gaming. Therefore, placing the children under significant risk. Children can be recruited into extremist groups, such as ISIS or Al-Qaeda, without the knowledge of their guardian. Criminals are able to monitor their victims' conversations without consent and pose significant danger (Alotaibi, Furnell, Stengel, & Papadaki, 2016).

This section presents several case studies related to cyber-crime targeting children in online games. A number of case studies have been presented in the literature that examine the occurrence or prevalence of cyber-crime targeting students playing online videogames. Chang et al. (2014) conducted a study to examine how students were targeted by cyber-bullying while playing violent video games. The study participants were 2315 Taiwanese students of grades 10 and 11. Participants were drawn from twenty-six high schools. The study asked the participants how often someone posted embarrassing or nude photos to them online, how often rude comments were posted about them in an online platform and how often others spread rumours about them or made threatening comments online. Not all of the participants experienced cyber-bullying. Others experienced cyber-bullying in the 11^{th} grade but not in the 10^{th} grade, while other respondents who had been cyber-bullied in 10^{th} grade did not experience it in the 11^{th} grade. Finally, some respondents were cyber-bullied in both

10th and 11th grades. More than half of the students reported that they had played online videogames during the past week. According to the data provided, students who had higher risk factors, such as high weekly online game use, experienced an increase in cyber-bullying victimization. Males were found to spend more time playing online games than females, and were in turn more likely to be victimized by cyber-bullying. The study found that more frequent online playing games in grade 10 predicted the emergence of cyber-bullying victimization in grade 11 (Chang, et al., 2014).

Moreover, Shu (2012) examined the relationship between online gamer's (student's) preferences in online violent games and their experiences of cyber-bullying and victimization while playing videogames. The participants were recruited from 16 elementary schools in southern Taiwan. In terms of gender, 52.17% were male, and 47.83% were female. Preference for violent games was measured by the degree of enjoyment the students derived from playing online violent games. Cyber-bullying victimization was measured with the 28-item Cyber-bullying Behaviour Scale (CBS) for online games that classifies cyber-bullying into many forms such as harassment, flaming and impersonation among others. The CBS measures the students' perceptions of how often they were bullied while playing online games in the past 6 months. Their responses were based on scales indicating 0 (never), 1 (1-3 times), 2 (4-6 times), 3 (7-9 times), or 4 (more than 10 times). A relationship was found between male gender and preferences in videogames as a predictor of hostile behaviour. Also, the more a male experiences cyber-bullying, the more likely they are to display aggressive behaviour in daily life. Preferences in videogames had a significant indirect effect on the extent of being cyber-bullied, which was mediated by hostility. Aggressive behaviour and the extent of being cyber-bullied both had significant direct effects on the likelihood of cyber-bullying others (Shu Y. , 2012).

DePaolis & williford (2014) conducted a research that examine the nature and prevalence of cyber-victimization among 3rd to 5th elementary school students in six elementary schools in the United States. It also considered whether students do or do not report cyber-victimization by taking into consideration differences in gender and grade level when experiencing cyber-attack. Around 660 students completed the online survey and 17.7% (N=114) reported being a target of cyber-crime while playing online videogame. Out of the 114 victimized students, only 43 recognized the identity of the cyber-criminals and almost 50% reported they did not inform anyone about the cyber-crime incident. Of the victims, 59% (N=67) reported being victimized weekly via online games. This was the most common venue, followed by text messages, where cyber-crime was experienced by 32% (N=37) of participants. In terms of

Grade levels, of the 114 victims, 29% (N=33) were 3rd graders, 25% (N=28) were 4th graders and 46% (N=53) were fifth graders. 91 victims (80%) reported that cyber-victimization happened outside school while only (N=15, 13%) indicated that the cyber-crime happened at school. Males were significantly more likely to be victimized through online videogames compared to female, although this was in line with the nature of the participant sample (DePaolis & Williford, 2014).

Leung & McBride-chang (2013) addressed the cyber-bullying experience of 626 Hong Kong 5th and 6th Chinese students in an online videogame context. 626 students (318 males and 308 females) from the fifth and sixth grades of four primary schools participated in the study. Factors examined included demographics, videogame playing habits, parental monitoring of computer use, social competence, and friendship satisfaction that children gained from their game playing. Finally, school victimization is used also as a measure to check the frequency of such events happening to participants. Students reported playing four types of games: massively multiple player online games (MMOG), solitary games, handheld video games such as Nintendo DS or PlayStation and home video console games. Males played significantly more than females in MMOGs, solitary computer games, and handheld video games, but did not differ significantly in time spent on home video consoles. Among the cyber-crime found, the most prevalent was victimization, followed by bullying. (Leung & McBride-Chang, 2013).

A study conducted by Lam et al. (2013), discussed the exposure of adolescents cyber-bullying victimization while playing online games. 1278 high school students of age between 13 to 18 years old participated in the survey. The mean age of the respondents was 14.7 and 48.4% (619) of the respondents are males while 51.6% (659) were female. The majority of the participants (N=933, 74.3%) did not experience cyber-bullying or victimization in the 7 days prior to completing the survey. Only 184 respondents reported being victimized via cyberspace, and 31 admitted they had bullied others, while 117 reported being both bullies and victims. In terms of the exposure to online videogames, 486 (41.2%) indicated they had spent less than 1 hour playing online games per day, 342 (29.2%) 1–2 hours, and 250 (21.5%) more than 3 hours per day. It was noted that exposure to violent online games was associated with both bullying-victimization and bullying only. Students who had been involved in cyber-bullying and being victimized were two times as likely to have been exposed to violent online games. For those involved in bullying students via cyber-space, it was nearly 4 times as likely that they had been played violent online games (Lam, Cheng, & Liu, 2013)**.**

2.6 Non-Reporting of Crimes

As discussed by some of the studies mentioned earlier, cyber-crime can be significantly under-reported. For example, roughly half the participants in the study of DePaolis & williford (2014) stated they did not report their experience of cyber-crime. There are various reasons why crimes, both cyber-crimes and those outside the digital word, go unreported (DePaolis & Williford, 2014).

Beck & Warrington (2014) discussed in a report that children are victims of (non-digital) crime. They stated non-reporting of incidents to authorities or parents can be due to many factors, such as for the fear of the police uncovering illegal activity that the victims themselves might be involved in or if the victim is already known to the police as a criminal. For example, if a victim is stabbed during a drug deal, he may be hesitant to go to the police. (Beckett & Warrington, 2014). Moreover, Beck & Warrington (2014) stated other reasons include victims fearing that the police may not believe them or will give them a hard time during the investigation. Another factor is fear of their parents finding out they have lied about where they were or what they were doing at the time when the crime took place. Victims may fear being exposed to physical risk in retaliation for informing the police, and reporting may put them under threat of physical assault, rape or sexual harm. Plus, there is a lack of knowledge of how to report the incident to authorities (Beckett & Warrington, 2014). In an article written by Yates (2006) , Some victims lack of confidence in the criminal justice system (Yates, 2006) or experience feelings of shame or embarrassment at being a victim (Birdsey & Snowball, 2013). Children's lack of trust and confidence in the police has been identified as one of the most significant barriers in reporting of incidents (Massey, 2014). Darwen (2014) found that many victims did not think the police would take any action to prosecute the criminal (Darwen, 2014). Finally, police discrimination toward the victims who come from minority backgrounds can be a reason for not reporting the incidents to the police (Rypi, Burcar, & Akerstorm, 2019). A report conducted by Yoon (2015), found a number of reasons for non-reporting, including a fear of retaliation from the offender, extensive paperwork to be filled out, and the intimidation of being interviewed by investigation police, and if the case goes to court, the victims possibly being required to testify (Yoon, 2015).

In a study conducted by Sable et al. (2010) regarding the barriers in reporting sexual assault for both men and women to law enforcement agencies, two hundred and fifteen college students were surveyed. 54.7% of the respondents were female and 45.3% were male. It was noted that many obstacles prevented the victims reporting sexual assault, such as shame,

embarrassment and not wanting friends and family to know about the event. In addition, there were concerns about confidentiality and the fear of not being believed. Participants were asked to respond using a Likert scale where 5 denotes extremely important and 1 denotes not important at all. To the question of whether consideration of not prosecuting family or friends was relevant, females responded with an average of 3.4 and males responded with an average of 3.1. For the question of addressing lack of belief in the possibility of successful prosecution of the offender, the average response in terms of importance of this consideration was, for females, 3.3 and, for males, 3.5. There was lower, but still noticeable evidence, of an overall level of distrust in the justice system, with an average response of 2.4 from females and 2.6 from males as to whether this was an important consideration in not reporting the crime. Other reasons given for not reporting the offences included lack of knowledge and resources to obtain help (Sable, Danis, & Gallagher, 2010).

Finkelhor et al. (2001) examined overall reporting of crime and found that most are not reported to police. This includes serious crimes, such as rape, sexual and physical assault and robbery. There were many reasons found for not reporting a crime. These were classified into categories such as definitional, material, jurisdictional and emotional. The definitional category considers whether the law considers the event a crime. For example, juveniles not being considered offenders when perpetrating crimes against other juveniles. As a result, assaults, robberies and thefts that involve young people are sometimes called a normal part of youth learning experiences rather than crimes. This can lead to juvenile on juvenile victimization being defined as problems or struggles where responsibility is shared rather than perpetrator to victim crimes, and the cases are handled by branches of justice system (such as juvenile courts) not to police. The police may then take reports of events less seriously. If this is known to victims they may be less willing to make reports. The material factor covers identifiable loss, such as financial, that may accompany reporting of a crime. The emotional factor includes such issues as embarrassment, fear of retaliation by the perpetrator, fear of not being believed or being blamed and any sense of powerlessness. Additionally, when the victims are children, their parents might prevent reporting of the crime to law enforcement agencies for the fear of the situation getting worse by upsetting and embarrassing the child and the family. This extend the concerns about the children potentially being doubly traumatized by the experience of reporting, especially if they are not believed by the judge or jury. Another factor in the emotional category is children's sensitivity to harming their reputation amongst their peers, for example, either by being seen as weak for reporting a crime or by being embarrassed by having their experiences known. The

jurisdictional factor includes conflicts between law enforcement agencies and also parents attempting to handle the situation by themselves without reporting the case to police. For example, the work of (Finkelhor, Wolak, & Lucy, 2001), where it was reported that 90% of parents did not report child abuse, instead preferring to handle the situation by themselves (Finkelhor, Wolak, & Lucy, 2001). Severe crimes may have particular problems in terms of non-reporting. In an article written by joneset al. (2009), women declined to report sexual assault to the police for several reasons. The participants of that study were all female, aged 13 years and above, who had all been sexually assaulted and presented to a local Hospital Emergency Department for treatment. The study took place over an 18 month period from November 2001 to April 2003. According to the findings, there are many reasons for not reporting sexual assault to police. Apart from lack of faith in a positive outcome, other reported reasons were victims not wanting the assailant to go to jail, fear of retaliation from the offender, especially if they are known to the victim, involvement of the victim in on-related criminal activities, previous poor experiences with the police and pressure from family and friends to not report the incident (Jones, alexander, Wynn, & Rossman, 2009).
Bowles et al. (2009) examined decision making around the reporting of crime by taking an economic approach. The work identified the potential costs from the victim's perspective, including taking into account the risk of intimidation and retaliation by the offender. There are hidden costs associated with reporting incidents to the police, such as the time and effort to assemble evidence and contact the police. Other factors include the time involved in case preparation and attending court hearings plus the stress of having to spend time as a witness in a court and being cross-examined. Such costs can dissuade victims from making a report. Solutions proposed include reducing the costs of reporting by giving victims the option to report the incidents to the police on the web (Bowles, Reyes, & Garoupa, 2009).
A study conducted by Fisher at al. (2003) discussed sexual victimization & reporting and non-reporting of sexual harassment to police and others such as family and friends. The study found that victims most often report incidents when they feel that reporting would result in a positive outcome, such as catching and convicting the offenders. If victims perceive a limited chance of a successful outcome, they have little motivation to report crimes (Fisher, Daigle, & Cullen, 2003).
Tarling & Morris (2010) examined the changes in reporting of crime by victims to police between 1991 and 2008 in the UK. A number of reasons were found for non-reporting. Victims may consider the crime to be insufficiently serious. A significant number of participants thought the police would not be interested or could not solve the case and, as a

result, it would be a waste of police time to report the crime. Another important reason was that the victim regarded the matter as private and preferred to deal with the matter themselves without any other parties becoming involved (Tarling & Morris, 2010). Rather than considering the barriers to reporting, some studies have examined reasons why reports may be made. Victims may report the crime to another authority rather than law enforcement agencies, such as a mobile phone network provider or the issuer of a credit card, as these are seen as more helpful and less intimidating. When victims report a crime to a legal authority, it may be in the hope that this will lead to the apprehension and punishment of the offender. In addition to achieving justice, reporting may be beneficial in reducing crime, as it would avoid repetition of the crime, either to the victim themselves or others (Tarling & Morris, 2010).
A study done by Richard et al. (2002) attempted to identify the factors that enable the victims to report crime to law enforcement agencies. These factors are based on incentives. An example is reporting of the crime for reasons of self-protection and protection of others. Either the victim wants to stop an ongoing attack, to address the "immediate crisis" or they hope to deter future attacks. They may think they have a personal duty to report a crime so that an offender gets "out of harm's way". (Richard, Messner, Hoskin, & Dean, 2002)

2.7 Reporting of Cyber-Crime

The studies noted in the previous section dealt with non-digital crimes. There has been limited work on the lack of reporting of cyber-crimes. Yoon (2015), examined reporting the incidents of cyber-crimes to law enforcement agencies, such as the police. Similar to the last studies mentioned above, this work looked at why reports may occur, rather than the barriers to making reports. Victims of cyber-crime may take a rational decision based on a cost-benefit analysis in which they calculate how much effort will be required for them to report the crime and the risks associated. Benefits may include recovering a stolen item or being re-assured that the offender will not target to the victim again. Police or support services may help them relieve distress and reduce vulnerability of future crime. Finally, they may want the offender to be caught, or simply to stop the crime from happening again (Yoon, 2015).
Other work examines only a single type of cyber-crime. Wozencroft (2015) investigated the prevalence of cyber-bullying amongst university students and their reporting intentions for cyber-bullying incidents to their University. 282 students, aged between 18 and 25, completed the survey. All were from an Australian University. 204 participants, 72.3% of whom were female and 27.7% of whom were males. According to the study, there were many barriers to the reporting of incidences of cyber-bullying. 81.6 % of the students were

confident in managing cyber-bullying themselves without reference to their University. 45.7% participants reported being too busy, especially when it comes to family and occupation, to report incidents of cyber-bullying. 33.7 % of them felt too embarrassed to discuss cyber-bullying with any University employees. 37.6 % of students reported they would not expect a favourable outcome to occur if they reported cyberbullying to the university. 66% of the respondents mentioned that the University did not provide enough information in order to report an incident of cyber-bullying. Finally, 76% of the participants stated they were uncertain how to report cyberbullying to the University. This was partly due to the fact that, as cyberbullying occurs via a digital platform, victims can be targeted outside University hours. Students were also unsure of the University's responsibilities in this situation (Wozencroft, Campbell, Orel, & Kimpton, 2015).

2.8 Summary of Reporting

In summary, there are several factors that influence victims reporting cyber-crime. There is also a significant under-reporting of crime, with many victims deciding not to report their experiences. The reasons they decide not to report crimes include fear of retaliation, involvement in other illegal activity, previous poor experienced with the police and the time it costs them when it comes to case preparation, attending court hearings, and the stress of spending so much time as a witness in a court. On the other hand, some studies found that victims report the incidents to the police for many reasons such as self-protection, protection of others. Plus, they report it for the benefit of reducing crime for the future, the attainment of justice, and the relief of victim's distress.

Related to the current study, both reporting and non-reporting cybercrimes by participants are analysed in section 4.2.7 and detailed in Chapter 5- Discussion , more specifically 5.4 (reporting and non-reporting cyber-crimes) that discuss the reasons victims don't report cyber-crimes to any one and the causes of reporting it to law enforcement agencies, parents.

2.9 Theoretical Framework

Cyber-crime in online games is a real issue facing players. Previous sections considered the literature around victims' reporting of crime. Crime only exists where there is a perpetrator. There are also, as seen above, numerous reasons why victims do or not report crimes. A number of theoretical models have been advanced to explain these phenomena. These include Routine Activity Theory (RAT) to describe the committing of crimes and various economical & psychological models to explain victims' intent of reporting or not the cyber-crime to law enforcement agencies such as police. RAT was proposed in 1979 (Cohen & Felson, 1979).

The authors developed it as an ecological perspective on criminal behavior. RAT distinguishes between criminal inclinations and criminal events compared to other theories that emphasize the individual or groups, and motivation tools as key causations behind a crime. RAT can be applied to online games as a theoretical framework for the goal of explaining and understanding criminals and crime. It is important in research as sociologists and criminologists use it to identify crimes, criminals and understand their behaviors and decisions resulting in crime. It is an ecological approach to crime causation by depending on the ability to localize offenders and targets in the same space and time (crime occurs when both motivated offender and target exist in the same space and time while a capable guardian is absent). RAT states that a number of elements must be present concurrently in order for a crime to be committed. First of all, the availability of a target which may be an object, a place or a person. Secondly, the lack of capable guardian who may prevent the crime from occurring, including staff, friends, CCTV system or police. Finally, there is a need for a motivated offender. All three factors must be in operation for a crime to be committed. Under RAT, if there are no intentional actions of harming another fellow, there cannot be a victim or a crime. For instance, an offender plans to burglarize a home but changes his mind after seeing a police car pass by. In this case the police are considered as a guardian and their presence prevents the crime from occurring for the attempted robbery perpetrated by the criminal. The RAT framework is depicted in figure 3.

Figure 1 - Routine Active Theory Model

RAT identifies three elements that need to be presented in order for a crime to exist, and must occur at the same time and in the same space. Sociologists have applied RAT theory to many cyber-crime types such as cyber-harassment, cyber-bullying and online identity theft among others (Hsieh & Wang, 2018). However, as the cyber world has no territorial boundaries due to technological advancements, an offender is able to commit a crime and quickly disappear into cyberspace. For example, it has become easy for a cyber-criminal from Belgium to

cyber-attack a victim physically situated in Germany through cyberspace without leaving Belgium. Cyber-crime is not by bounded by geographical limitations in the same way as other crimes (Ibekwe, 2015).

Several studies in the form of self-report studies, online panels, telephone surveys etc. have used RAT to explain cyber-crime victimization. To start with, Choi (2008) conducted a self-report survey among 204 college students into victimization by computer viruses. He looked at both online activities (e-mail and downloading), and the use of anti-virus as a guardian. According to the study, college students with a technical capable guardian (antivirus installed in their computers) have a decreased risk of virus victimization. Furthermore, both risky on-line behaviours and on-line leisure activities increases the likelihoods of virus victimization (Choi, 2008).

Moreover, Marcum et al. (2010) studied cyber-crime victimization by three types of offences (unwanted sexually explicit material, unwanted non-sexual harassment and unwanted sexual solicitation) among 744 freshmen students. RAT theory has been applied in this study. Its elements included are visibility (online activities such as instant messaging & social networking sites), accessibility (12 types of info shared on social networking sites), and guardianship (using of filtering or monitoring software by parents). The author concluded that exposure to motivated offenders will increase the target of attacking victims which in turn increase the odds of the three types of victimization measured in this study. However, he concluded that protective measures such as a capable guardians do not decrease the chances of victimization (Catherine, Higgins, & Rickets, 2010).

Pratt et al. (2010) conducted a telephone survey among 992 adults in Florida in 2004. The study stresses on 13 types of consumer fraud such as an investment deal that turned out to be phony" and "agreed to buy a product or a service for a certain price but was later charged a lot more". Respondents were asked how the scammer contacted them. It is noticeable that scammers contacted them through an internet auction, from a website and by e-mail. Pratt et al. only looked at hours spent on-line and website purchases. Both activities increased the odds for Internet fraud targeting due to the lack of capable guardians to protect them from illicit activities (scam) (Pratt, Holtfreter, & Reisig, 2010).

Holt and Bossler (2009) used a self-report survey among 578 college students to investigate on-line harassment. RAT was applied, and it looked at the effects of routine computer use such as times spent on-line shopping and emailing. In addition, they stressed on the social guardianship (peer involvement in computer crime) and physical guardianship (use of protective software or application). It is concluded that most of the measures of RAT theory

do not affect the odds of being harassed on-line. However, only time spent in chats room and involvement in computer deviance increases the risk. So, general exposure to others on-line does not increase victimization, but spending time on-line with others in a specific context does (Holt & Bossler, 2009).

Reyns et al. (2011) applied RAT to cyberstalking victimization among 974 college students. The authors looked at the effects of online visibility, accessibility, and guardianship. They noted that online exposure variables did not produce effects across the types of pursuit behaviours". Among the online proximity variables, only "adding strangers" appears to be related to victimization. Furthermore, having a profile tracker is not a protective variable, but increases the odds of victimization (Bradford, Henson, & Fisher, 2011).

Bossler and Holt (2009) investigate cyber-crime victimization by malware among 570 college students. They included both online activities such as shopping, chatting and online banking and online guardianship (computer skills, antivirus etc.). They concluded that most routine activities on the computer as well as physical guardianship, are not associated with data loss from malware victimization (Bossler & Holt, 2009).

In regards to Economical and psychological models, they can be used to understand a victim's intent about whether or not to report a cyber-crime to law enforcement agencies such as police. In economic models, the decision to report a crime or not is based on a cost-benefit calculation by the victim for determining whether it is worth contacting the police. The victim will not lodge a report if the expected costs of reporting are higher than the expected benefits. Therefore, crimes resulting in little or no financial losses or physical injury will be less reported as reporting a crime always take time and costs money while the expected benefits of reporting are low in offence categories where the police may be expected to expend little effort in solving the case (Goudriaan, 2006). Victims may avoid going to the police due to financial costs. While making a phone call requires little time and effort, involvement in the legal process can result in both direct and indirect costs. These include testifying in court as a witness, as this can be time-consuming, as can effort into assembling evidence and co-operating with the police. On the other hand, victims may conclude that it is beneficial for them to report incidents, as it may help making an insurance claim that is based on a formal report or reference number. They may also benefit from compensation via a criminal victim support scheme after reporting the incidents to police (Bowles, Reyes, & Garoupa, 2009).

In an article written by Wasserman and Ellis (2010), and from a psychological viewpoint, victims are often emotional or fearful in the aftermath of a crime. This can limit their ability to make rational decisions about whether or not to report the crime to the police. Fear, stress

and other effects of trauma can influence the decision-making of victims. Additionally, previous experience in reporting crime to the police, including how the police responded, can affect the victim's emotional and psychological state in the immediate aftermath of a crime. If the previous experience was negative, a report is unlikely to be made, while conversely previous positive experiences can heighten the likelihood of a report of a subsequent crime (Wasserman & Ann Ellis, 2010).

2.10 Conclusion

Online videogames are a large a growing segment of the worldwide entertainment market. They are played by a large number of people, including a significant section of the population under 18 years of age. Young players can spend considerable amount of time playing online videogames. This activity exposes as potential victims of cyber-crime. Cyber-crime can take many forms, such as cyber-bullying, harassment, identify theft and pornography. When a crime occurs, a victim may or may not choose to report this to police, other law enforcement agencies or other authorities. This holds true for cyber-crime. Previous studies have demonstrated, that for general criminal situations, there are a multitude of reasons why a victim may not report a crime. Existing research has also shown that players of online video games, especially children, can be exposed to cyber-crime. They will therefore face the same choices, of whether to report or not, as a victim of other types of crime. There has, however, been little general research into the reporting of cyber-crime by people under the age of 18. Finally, we have also discussed RAT and both economical and psychological models of reporting crimes or not to law enforcement agencies.

Regarding the current study, which discuss Cyber-Crime in Online Videogames and its Reporting by School-aged Children, both RAT theory and psychological models were considered. The study illustrates that online game players were exposed to several cyber-criminal activities perpetrated by cyber-criminals who used the online gaming platforms in the form of cyber-harassment, cyber-pornography and online identity theft to target the victims. So, cyber-crimes exists, and the participants are being considered the victims of online game cyber-crime. So both elements of RAT (Victims and offenders) were presented. However, the lack of capable guardian and its presence were not discussed in the current study to prevent the crime from occurring. However, it is presented in the future recommendations section 6.2 that present the roles of parents , schools , law enforcement agencies and online gaming companies in combatting cyber-criminals targeting victims.

However, the study stresses on psychological models that state the reasons victims did report or not the incidents of cyber-crime. Some of the participants reported the incidents of cyber-

crime to an authority figure, including parent, teacher and the police. However, most of them didn't report the incidents of cyber-crime to anyone due to many reasons such as they didn't think they would be believed to report it , feeling embarrassed , feeling ashamed , not important to report the cyber-crime or they don't have any idea on how to report it .

Chapter 3 Methodology

3.1 Introduction

This research examined the experience of cyber-crime by players of online games and their reaction to such experiences in terms of reporting of the crimes. As discussed in the previous chapter, players of online games may by exposed to a range of cyber-crimes, including cyber-harassment, online identity theft or cyber-pornography. The participants in the current study ranged in age from 18 to 25 years old. However, they were asked about their experience of cyber-crimes while they were of school attending age. There is a dearth of reporting in the literature of what such victims of cyber-crime do in regards to reporting of cyber-crime. The participant age range that was chosen avoided the need to interrogate actual school age children on the basis that such recall may be potentially emotionally traumatic. More mature participants should experience less trauma, while, at not more than 25 years old, still have relatively recent recall of such events. Recall of memories may bring trauma (Christianson & Loftus, 1990) and it was considered preferable not to subject under age participants in recalling memories in the past to eliminate the probability of having trauma. While cyber-crime may be experienced and reacted differently in different countries, this question is left for future work. We recognise their problems with recall given the time between experiencing cyber-crime and the administering of the survey this has to be balanced against the drawbacks of using underage participants as discussed above. This is a potential limitation of the work. An anonymous online survey was administered to the participants, which asked a set of questions related to their experience in online games, their experience of cyber-crime and whether they reported cyber-crimes to any authority such as law enforcement agencies, teachers or parents. The survey was administered via Qualtrics (www.qualtrics.com) and the functionality of that site was used as part of the analysis of the data. However, errors occurred during survey questionnaire. A Question related to the age of participants "what is your age in years? "Was not displayed due to technical errors occurred in the Qualtric application Settings. After the participants answered the survey questionnaire, it is noted that one option in the Age section's settings was not applied. So, the study disregarded the age of the participants. The responses of the survey questionnaire didn't apply within Australia only.

However, it included international participants due to many criteria such as (age limit between 18 to 25 years old & must have experienced cyber-crime when they were 18 years or younger) mentioned at the beginning of the survey questionnaire that make it hard to get participants from Australia only in a short period of time (2 to 3 months).

3.2 Research questions

Although the literature review identified previous research that investigated the experience of school-aged students of particular types of cyber-crimes, there is a lack of research into how actively victims of cyber-crime, particularly school-aged children, report such attacks. This leaves open the questions of reporting cyber-crime by this group, at what rate and whether this is related to either the types of cyber-crime or the types of games being played. This leads to the main research question: *What types of cyber-crimes are experienced by school-aged children and do they report the experience of such crimes?*

Lack of reporting, if it exists, may be due to a range of factors, such as knowledge of how to report it, lack of importance attached to the experience and frequency of exposure.

Within the main research question, a number of subsidiary questions may be posed:

1. Are school-aged children aware of the risks associated with playing online games?
2. Which Cyber-criminal activity were the school-aged children most concerned about while playing online games while of school age?
3. What types of online game they were playing while experiencing cyber-crime?
4. How frequently they have experienced cyber-crime while playing online game? And where were they playing online games when experienced cyber-crime?
5. What are the reasons of reporting & non-reporting cyber-crimes?
6. How likely are they to report the incident of cyber-crime?
7. Who they report the incident of cybercrime to?

3.3 Participants

47 participants from 18 nations answered the survey questionnaire. Participants must have been active online video game players and have experienced cyber-crime while playing an online video game whilst of school age. As stated previously the age range was restricted to 18 to 25 years old, due to the lower risk of adverse emotional impact for such a group due to a higher maturity level. In addition, school-aged children are minors and dealing with minors present additional challenges, especially within the time frame available for the current research. When surveying participants under the age of 18, it is required by law to get their parent's consent in order to participate in survey questionnaire. For an anonymous survey

potential participants would have to approach their parent or guardian and ask their permission. Given the possibility that such participants had never mentioned the experience of the cyber-crime to their parent or guardian, it is possible that this would be a disincentive to participation.

3.4 Recruitment

Participants were recruited by a variety of means, including posters, E-invitation and survey recruitment sites. Posters were displayed on the Macquarie university campus. E-invitations were sent to participants through many platforms such as gaming websites, Facebook, including the Macquarie University Facebook group page, and the Macquarie University Village community page and through various other social group pages. Finally, the survey was also distributed via the Social Psychology Network (https://www.socialpsychology.org/). The Social Psychology Network is an educational organization founded by Scott Plous in 1996 that allow a surveyor to import a survey questionnaire into SPN or a link to it in order to get as many as respondents to engage in the study (Plous, 1996).

3.5 Procedure/Survey

The survey administered to participants consisted of 54 questions, a mixture of closed and open-ended questions. The study was administered via Qualtrics (www.qualtrics.com). It was expected that the survey would take participants approximately fifteen to twenty minutes to complete. Most of the questions were closed, such as:

1. **How many hours per week did you typically spend playing online video games?**
   - Less than 5 hours per week
   - From 5 to 10 hours per week ; From 10 to 20 hours ; From 20 to 40 hours
   - More than 40 hours per week
2. **How often did you experience Cyber-harassment while playing online games whilst of school age?**
   - Daily ; Weekly ; Monthly
   - Less than Once a year ; Annually or Once

Open-ended questions such as:

1. **As you were aware of the risks associated with playing online games, please give details in terms of what risks you were aware of?**
2. **Why did you not report the incident of cyber-harassment? Please give details.**

were included to either give participants the option of including information not covered by options in the closed questions or to add additional information. The questions of the survey

can be found either in Appendix A (Quantitative Questions) and Appendix B (Qualitative Questions). URL: https://qtrial2019q1az1.qualtrics.com/jfe/form/SV_3PfJJpgFFsSt3oN
Both quantitative and qualitative analysis of the data was undertaken, as described in the next chapter.

Chapter 4 Findings

4.1 Introduction

This chapter discusses the result of the survey questionnaire described in the previous chapter. As noted there, the survey consisted of 54 questions and was completed by 47 participants, aged 18 to 25. While some participants did not complete every question, all participants completed some questions beyond those dealing with basic demographics. The findings will be used to provide answers to the main research question and the subsidiary questions listed in section 3.2. Respondents completed the questionnaire between 2nd May 2019 and 25th June 2019. Data was statistically (quantitatively) analysed through the use of the tools provided by the Qualtrics site, and, for the textual answers to open-ended questions, qualitatively analysed through an approach called Discourse Analysis, which is a group of ideas way of thinking identified in textual and verbal communications (Powers, 2015).

4.2 Data Findings

The survey first asked participants for some basic demographic information before moving on to game playing habits and awareness of the risks of cyber-crimes. After that, the questions dealt with the experience of cyber-crime and reporting, if any, for a number of categories of crime (pornography, harassment, hacking and identity theft). These categories were identified as the most common forms of cyber-crime experienced by videogame players, based on the literature review from chapter 2. For each type of cyber-crime, the participants were asked questions which included whether they experienced a particular type of cyber-crime while playing online games, what type of game they were playing, how frequent was the experience of cyber-crime and whether they reported the experience and, if so, who to. Finally, there was a question about what type of support services they might have found useful. For ease of comparison results, equivalent questions about each type of crime (for example frequency of experience) are presented together rather than separating results by category of cyber-crime.

4.2.1 Demographic factors

The first section of the questionnaire was composed of 4 demographic questions to provide background info about the participants (Age, gender, country of birth, current residence).

Figure 2 - Participant Gender

47 Respondents answered the survey questionnaire. As shown in figure 2 59% of participants (or 27 participants) were male and 41% of participants (or 20 participants) were female. No other gender identification response was received. While the participants were asked their exact age, no responses to this question were received due to a fault in the Qualtrics settings. The country of birth of participants is displayed in table 1. Only 44 respondents answered this question. The most common response was: Australia (11 participants), followed by Lebanon (9 participants), then USA (4 respondents).

What is your country of birth?

Country	Number of Respondents
USA	4
Lebanon	9
Canada	1
Italy	2
Australia	11
Iraq / Sweden	1/1
UK	3
Iran /Puerto Rico/ South África	1 / 1/ 1
India	2
France / Myanmar / Netherlands /Brazil	1/1/1/1
UAE	2
Singapore	1
Sum	**44**

Table 1 - Country of Birth

Table 2 displays the country of residence of participants and 42 respondents answered this question. A much smaller number of countries is represented here and it is likely that a number of participants are international students studying in Australia. 33 out of 47 respondents currently reside in Australia, and three participants reside in the UK and another three in the UAE. Only two participants are located in Lebanon, and 1 participant (US).

Country	Number of Respondents
UAE	3
USA	1
Australia	33
UK	3
Lebanon	2
Not specified	5
SUM	**47**

Table 2 - Country of Residence

4.2.2 Online Game Play

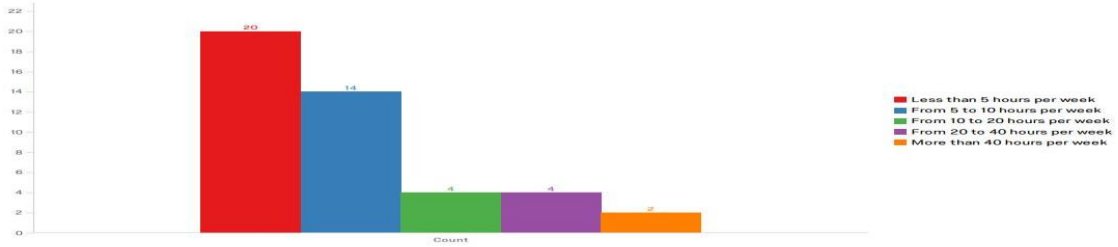


Figure 3 –Weekly hours playing Online Games

Participants were asked to report the number of hours they used to play online games on a weekly basis while they were of school age. 44 participants responded to this question, with the results displayed in figure 3. Almost half (20 out of 44 respondents) played less than 5 hours per week. From there, the number of participants reporting a higher number of playing hours gradually decreases, with fourteen participants reporting spending 5 to 10 hours weekly playing online games, four participants reported spending 10 to 20 hours playing online games per week and four participants reported spending 20 to 40 hours per week. Finally, two participants reported spending more than 40 hours a week playing online games. The final figure may equate to between eight to ten hours a day, which is not out of line with examples of high amounts of game playing reported in the literature – section 2.3, see (Limelight, 2019) and (Greenfield, 2019). There were no reasons to discount any of the responses on the basis of answers to this question.

	Less than 5 hours per week	**5 to 10 hours per week**	**10 to 20 hours per week**	**20 to 40 hours per week**	**More than 40 hours per week**	**Total**
Male	11	8	3	4	2	28
Female	9	6	1	0	0	16
Nations	3 Australians 5 Lebanese 12 Others	7 Australians 2 Lebanese 5 Others	1 Lebanese 3 Others	1 Australian 1 Lebanese 2 Others	1 Australian 1 Lebanese 0 Other	12 Australians 10 Lebanese 22 Others
Total	**20**	**14**	**4**	**4**	**2**	**44**

Table 3- Weekly hours playing online games based on Gender and Nationality

Table 3 displays both gender and country of birth (nationality) variations related to the weekly hours playing online game. Note that the nationality options only include Australia and Lebanon as specific examples as most of the participants engaged in the study were Lebanese or Australians. All other nationalities are group under ‘International” for this purpose. From the above table, it can be seen that that males are more likely to record higher amounts of time spent playing video games on a weekly basis than females. For example a

majority (56%) of females reported playing less than 5 hours a week (9 out of 16) whereas the equivalent figure for males was 39%. Also, 32% of males (or 9 out 28 respondents) reported playing for 10 hours or more per week, whereas only 1 female respondent (6%, 1 out of 16 participants) played for that amount of time. The differences based on nationality are less obvious, although there was a slightly different distribution between Lebanese and Australian respondents at the lower end of the playing time scale.

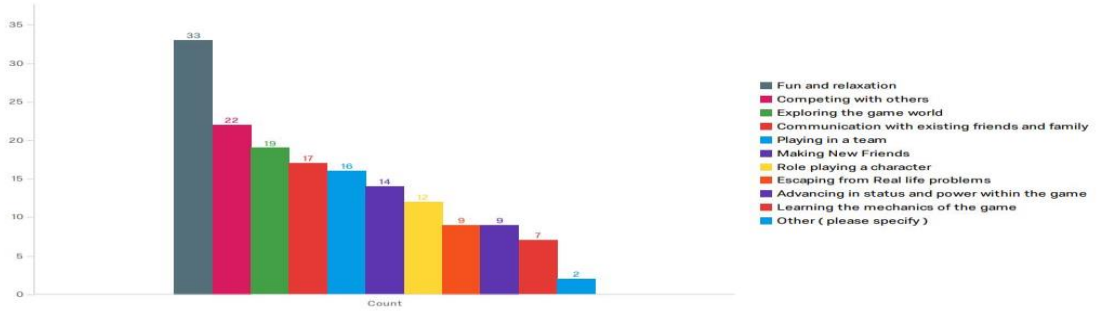


Figure 4 - Reasons for playing online games

Participants expressed a range of motivations for playing online games, as displayed in figure 4. They were presented with a range of options, and allowed to give multiple responses, hence the totals for the column results adding up to more than the number of participants.

	Fun & relaxation	**Competition with others**	**Exploration of the game world**	**Followed his friends by playing online games**	**Spare time while having break from studies**	**Total**
Male	18	13	8	1	1	41
Female	15	9	8	0	0	32
Nations	8 Australians 4 Lebanese 21 Other	7 Australians 3 Lebanese 12 Others	6 Australians 4 Lebanese 8 Others	1 Australian	1 Lebanese	22 Australians 12 Lebanese 41 Others
Total	**33**	**22**	**17**	**1**	**1**	**73**

Table 4- Reasons of playing online video games Based on Gender and Nationality

According to table 4, the most common reason for the majority of the online players (33) to engage in playing online game was for the goal of having fun and relaxation. The next most popular option (22 responses) was competition with others followed by exploration of the game world (19 responses). Note that the figures in table 4 and figure 4 do not always match due to not all respondents stating their gender or nationality. Of the two participants who gave 'other' as the response to the question, one participant followed his friends in playing online games ("My friends played online games. So, I have done the same by following them playing online games"), and the other participant played online games during his spare time

while having a break from studies ("For the goal of wasting time between studies by playing online games during spare time").

4.2.3 Risks and Concerns Associated with Playing Online Games

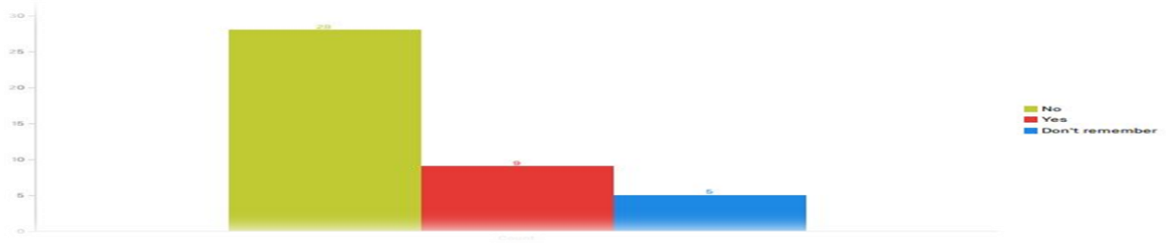


Figure 5 - Awareness of the risks

Participants were asked whether they were aware of the risks of playing online video games. 43 participants responded to this question. As can be seen from figure 5 the majority of participants (68.29% or 29 participants) were not aware of such risks before playing the games. This represents a very low level of awareness of the potential risks amongst school-aged children. To this might be added the five participants (or 12.20%) who could not recall whether or not they were aware of the risks. Together this represents approximately 80% of the respondents to this question. Only nine participants (or 19.51%) stated that they were aware of the risks associated with playing online games. If participants stated that they were aware of the risks they were asked to give more details. Six out of nine participants responded to this question and the results are given in table 6.

	Aware of the risks	Not aware of risks	Didn't specify	Total
Male	6	17	2	25
Female	3	12	3	18
Nationality	3 Australians ; 4 Lebanese 2 Others	6 Australians 6 Lebanese 17 Others	1 Australian 4 Others	10 Australian 10 Lebanese 23 Others
Total	9	29	5	43

Table 5 - Risks associated while playing online games

According to table 5, it can be seen that approximately 70% of males were not aware of the risks associated with playing online games, and 63% of females.

Respondent	Awareness of the risks
1	Knew the risk of the hackers & Account stealing. I was aware of item trading scams
2	Child Grooming & theft
3	Scamming & Cyber-bullying
4	Hacking
5	Wasting of time
6	Many people pretend to be someone and try to get victim's sensitive info by scamming their money

Table 6 – Awareness of the risks

In regards to the respondents who were aware of the risks, their responses are quite varied and represent a range of the possible cyber-crimes, such as child grooming, cyber-bullying, and cyber-harassment and hacking. These are amongst the types of cyber-crime noted in chapter 2. Overall, while some of the participants were aware of the potential risks associated with playing online games, and their variety, most were unaware of such risks.

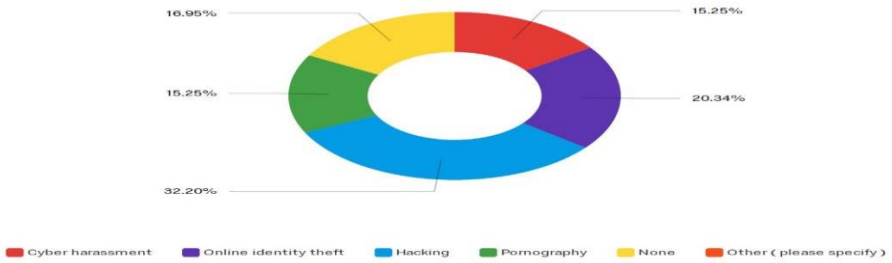


Figure 6 - Cyber-crime concerns

Once people engage in the online world, for example by playing online games, they are likely to become aware of the possibility of experiencing cyber-crime even if they were not previously. Participants were asked which cyber-crime they were most concerned about once they began playing. The results are displayed in figure 6. There are many types of cyber-criminal activities targeting online game players such as cyber-harassment, online identity theft, hacking, cyber-pornography, etc. According to the results of the survey, hacking was the source of most concern, with 32.20% of the participants (19 participants), online identity theft was the second most nominated concern, noted by 20.34% of participants (12 participants). After that comes cyber-pornography (15.25% or 9 participants) and cyber-harassment (15.25% or 9 participants). 16.95% (10) of the participants were not concerned at all. Interestingly, no participants selected the other response to this question.

4.2.4 Experience of Cyber-Crime

Participants were then asked which types of cyber-crime they actually experienced while playing online games. Again, while participants had the option to select multiple cyber-crime types, no participant provided multiple responses. As displayed in figure 7, the most common experiences were of Cyber-harassment and Hacking, both reported by 28.21% of participants (eleven participants each). This was followed by identity theft at 23.08% (or nine participants), and cyber-pornography at 15.38% (6 participants). Two participants gave an ‘other’ response, which they described as Ransomware in their textual response.

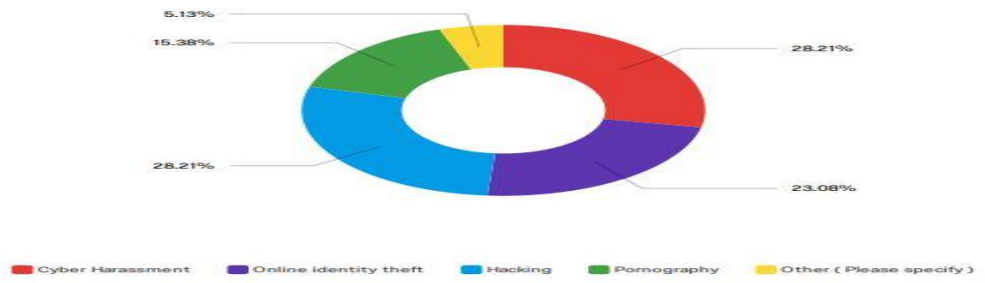


Figure 7 - Cyber-crime experience

From the admittedly small participant pool it can be seen that a range of cyber-crimes can be experienced while playing online games and that no single type dominates the experiences.

	Cyber-harassment	Identity theft	Hacking	Cyber-pornography	Others	Total
Male	4	4	8	4	0	20
Female	7	7	1	2	2	19
Nations	3 Australians 1 Lebanese 7 Others	3 Australians 1 Lebanese 7 Others	7 Lebanese 2 Others	3 Lebanese 3 Others	1 Australian 1 Other	7 Australians 12 Lebanese 19 Others
Total	**11**	**11**	**9**	**6**	**2**	**39**

Table 7 – Types of cyber-crimes based on Gender and Nationality

As can be seen in table 7, the experiences of cyber-crime differed markedly by gender. Hacking was experienced by almost half the male respondents (eight out of 20) but by only one out of 19 female respondents. Conversely, female respondents reported cyber-harassment and identity theft at almost twice the level of male respondents.

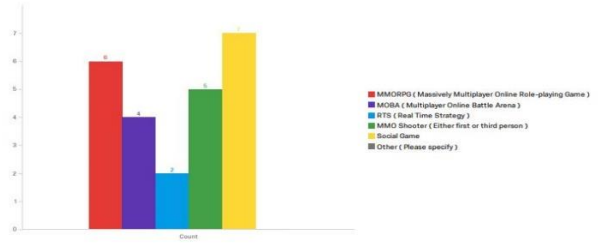


Figure 8- Cyber-Harassment

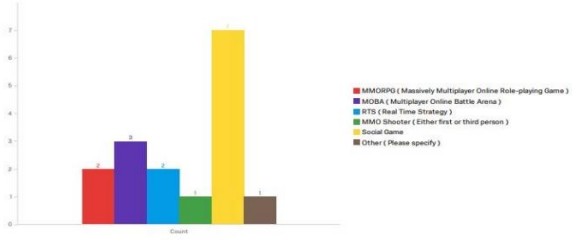


Figure 9- Online Identity theft

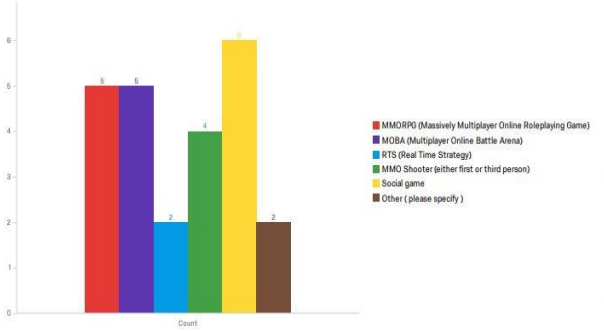


Figure 10 – Hacking

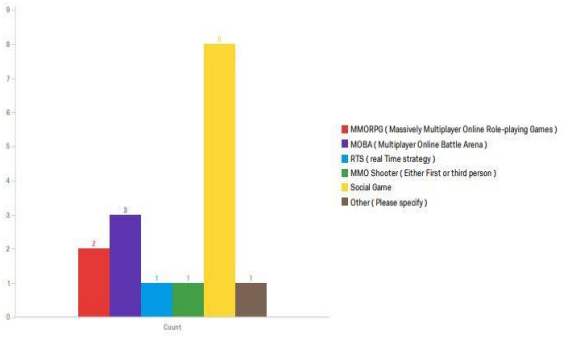


Figure 11 – Cyber-pornography

Once participants had nominated the type of cyber-crime they had experienced they were directed to a bank of questions asking for more details about each type of cyber-crime

experienced. The first question in this section asked what (broad) type of game the participants were playing when they experienced the cyber-crime. The results are given in figures 8 to 11.

	Cyber-harassment	Identify theft	Hacking	Cyber-pornography	Total
Male	12	12	18	12	54
Female	12	4	5	2	23

Table 8 - Cyber-harassment while playing different sort of online games

Table 8 gives the breakdown by gender of the reports of various types of cyber-crime. The figures differ from those of table 7 as while respondents answered only once to the question there (even though they could have given multiple responses) participants did respond to multiple of the detailed question banks. It can be seen that that experience of cyber-crime by gender differs markedly. It is also clear from the figures that the occurrence of cyber-crime is not consistent across the various types of online games. While all types of cyber-crime investigated where commonly reported in social games, hacking and harassment were common in Massively Online Battle Arena (MOBA) games, Massively Multiplayer Online Real Play Games (MMORPG) and online multiple shooter games but much less reported for Real Time (Real Time Strategy) games. Pornography was relatively rarely reported in all cases except social games. This may be due to the difficulty of posting video or graphic images in the other games whereas social media enables the distribution of such material. Indeed, social games appear to be the most common venue of exposure to cyber-crime for players of high-school age. Again, while the participant pool is too small to allow genuine statistical conclusions to be drawn, it can be seen that the occurrence of crime types is not uniform across the various types on online video games.

4.2.5 Frequency of Experience of Cyber-Crime

While the previous set of results dealt with the types of game played while experiencing cyber-crimes, figures 12 to 15 report the frequency at which particularly types of cyber-crime were reported. This question was only answered by a limited number of the participants who nominated experiencing these types of cyber-crime (figures 8 to 11).

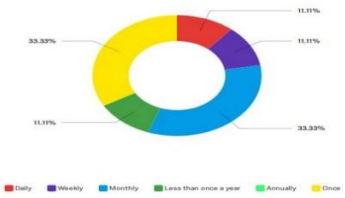


Figure 12- Cyber harassment

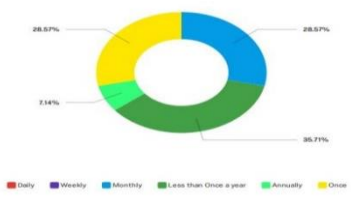


Figure 13- Online Identity theft

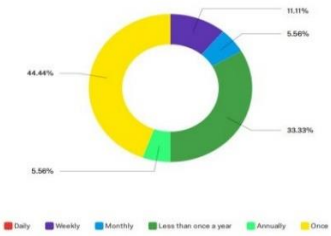


Figure 14- Hacking

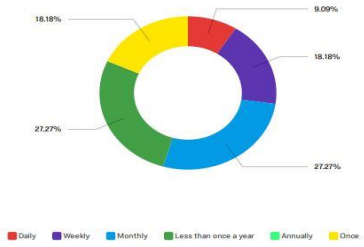


Figure 15 – Cyber-pornography

Again, extensive variance between the types can be noted. For example, a single experience was the most common frequency of experiencing hacking, and equal most common for cyber harassment, online identify theft and pornography were encountered more frequently. Similarly, harassment and cyber pornography were encountered daily by some participants, while this frequency was not reported for the other types. Online identify theft was relatively rarely experienced, with over 60% of responses nominating a frequency of 'once' or 'less than once a year', while over 75% of respondents experienced hacking with those frequencies. On the other hand, over 55% of those experiencing cyber-harassment experienced it on at least a monthly basis. This again demonstrates variance between the types of cyber-crime and indicates that cyber-crimes should not be considered in a homogenous manner. Tables 9 to 12 give the detailed breakdown of responses, while table 13 gives a summary by gender.

	Daily	**Weekly**	**Monthly**	**Less than once per year**	**Once**	**Total**
Male	2	0	3	1	2	8
Female	0	2	2	1	5	10
Nations	1 Australian 1 Other	1 Australian 1 Other	2 Australians 2 Lebanese 1 Other	1 Lebanese 1 Other	1 Australian 6 Others	5 Australians 3 Lebanese 10 Others
Total	**2**	**2**	**5**	**2**	**7**	**18**

Table 9 - Frequency of cyber-harassment occurrence in online games

	Monthly	**Less than once per year**	**Once**		**Annually**	**Total**
Male	3	3	0		0	6
Female	0	2	4		1	7
Nations	3 Lebanese	3 Lebanese	4 others		1 Lebanese	3 Lebanese , 5 Australians 10 others
Total	**3**	**5**	**4**		**1**	**13**

Table 10 - Frequency of Online identity theft occurrence in online games

	Weekly	Less than once per year	Once	Annually	Total
Male	2	5	3	2	12
Female	0	1	5	0	6
Nations	2 Lebanese	2 Lebanese , 1 Australian 3 Others	8 others	2 Lebanese	6 Lebanese , 1 Australian , 11 others
Total	**2**	**6**	**8**	**2**	**18**

Table 11 - Frequency of hacking occurrence in online games

	Daily	weekly	Monthly	Less than once per year	Once	Total
Male	1	1	2	3	0	7
Female	0	1	0	0	3	4
Nations	1 Lebanese	1 Lebanese 1 Others	1 Lebanese 1 Aussie	2 Lebanese 1 other	3 others	5 Lebanese 1 Australian 5 others
Total	**1**	**2**	**2**	**3**	**3**	**11**

Table 12 - Frequency of cyber-pornography occurrence in online games

	Daily	Weekly	Monthly	Less than once per year	Annually	Once	Total
Male	3	3	8	9	2	8	33
Female	0	3	2	4	1	17	27

Table 13 – Overall frequency of experience of cyber-crime by gender

Considerable variation by gender can be seen. Males appear to be much more likely to experience more frequent examples of cyber-crime than females. This may be related to the higher amounts of time spent playing online videogames by males (see table 3).

4.2.6 Physical Location

It is known that online game players participate in such games from various physical locations, such as home, school, internet cafe, or at the home of a friend or family member. Figures 16 to 19 depict, for each type of cyber-crime investigated, where participants where located when they experienced that type of cyber-crime. There is much more commonality of response here between the various types of cyber-crime, with home and internet being the most common responses, except in the case of cyber harassment, where home of a friend or family member was the second most common response. The responses shown are in line with the likely locations at which school-aged children would participate in such games and indicate that their incidence has limited dependence on the physical location of the player.

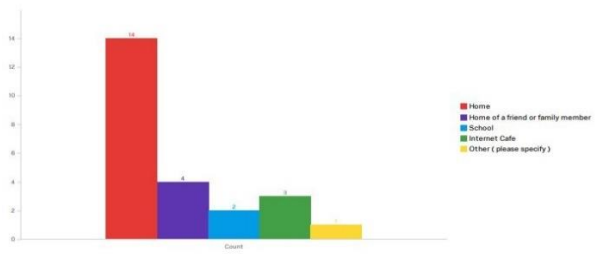


Figure 16- Cyber-Harassment

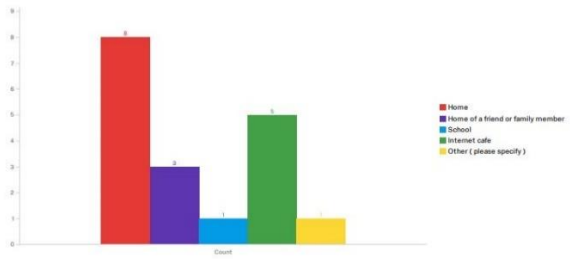


Figure 17 - identity theft

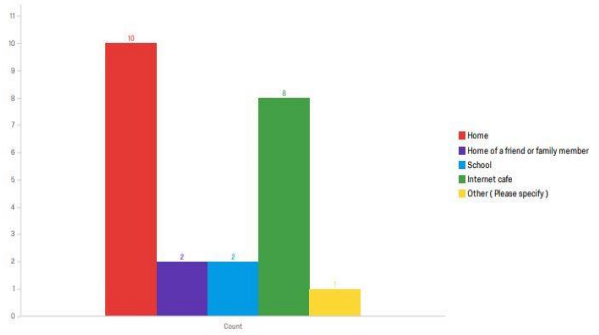


Figure 18 – Hacking

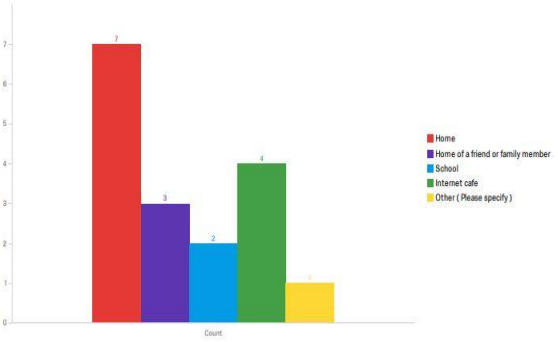


Figure 19 – Cyber-pornography

4.2.7 Reporting of Cyber-crimes

As noted above, cyber-crimes are experienced by victims at different frequencies and in various physical locations. As with most of the results reported so far, there is significant differences in the reporting of cyber-crime between the different categories of crime. Figures 20 to 23 display the ratios of reporting versus non-reporting for the various categories. Table 14 gives the breakdown of reporting by gender for each category. Table 15 gives the overall figures for reporting by gender.

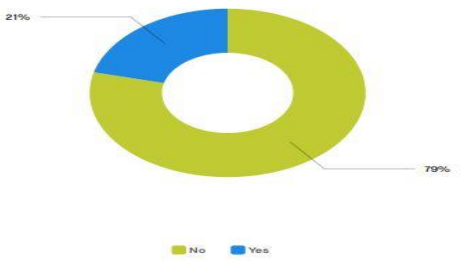


Figure 20- Cyber harassment

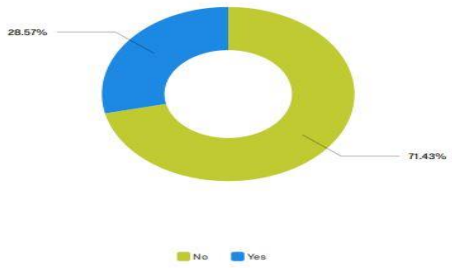


Figure 21- Online Identity theft

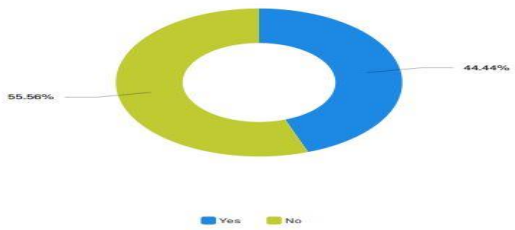


Figure 22 - Hacking

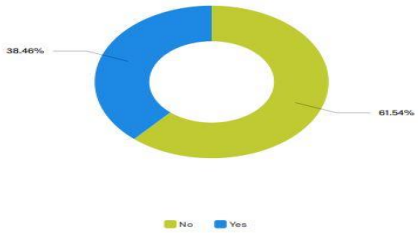


Figure 23 – Cyber-pornography

	Cyber-harassment		Identity Theft		Hacking		Cyber-pornography	
	Reporting	Non-reporting	Reporting	Non-reporting	Reporting	Non-reporting	Reporting	Non-reporting
Male	1	7	1	5	6	7	5	4
Female	2	9	2	6	1	4	0	4
Total	**3**	**16**	**3**	**11**	**7**	**11**	**5**	**8**

Table 14 – Reporting and Non-reporting of Cyber-crime by Category and Gender

	Reporting	Non-reporting	Total
Male	13	23	36
Female	5	23	28
Total	**18**	**46**	**64**

Table 15 – Reporting and Non- reporting of Cyber-crime Overall by Gender

From the tables and figures it can be seen that reporting is far less common then non-reporting and that females are far less likely to report an experience of cyber-crime than males. The reporting / non-reporting trends by gender are reasonably consistent for harassment and identity theft. The differences appear in cases of hacking and cyber-pornography.

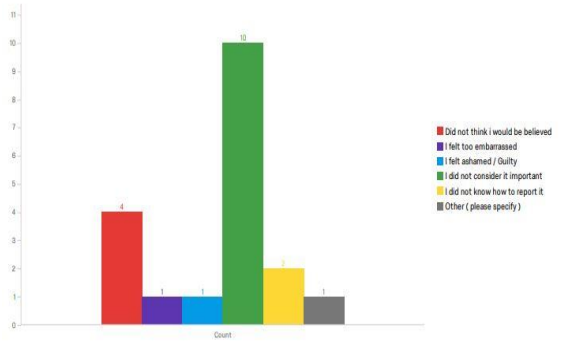


Figure 24 - Cyber-Harassment

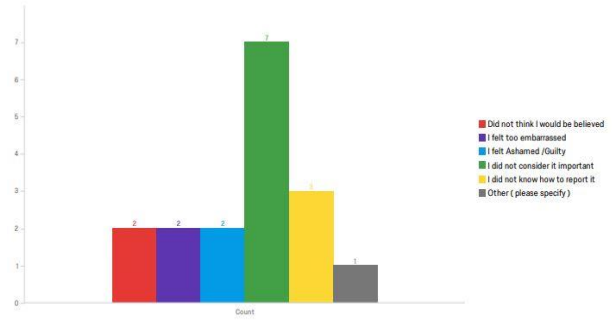


Figure 25 - Online Identity theft

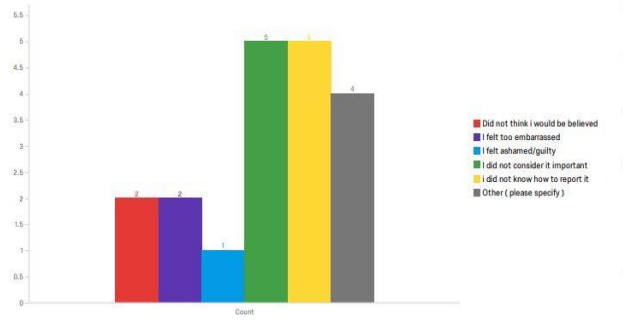


Figure 26 - Hacking

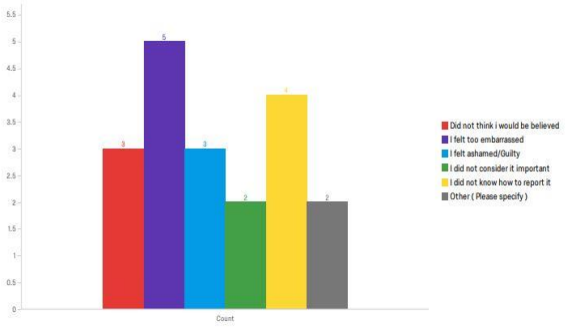


Figure 27 - Cyber-pornography

Figures 24-27 display the reasons given for non-reporting of cyber-crimes, by the categories of cyber-crime investigated here. Again, considerable variation can be observed. While not considering it important enough to report might be understandable in the case of cyber-

harassment, that seven participants considered identity theft unimportant is surprising. However, it must be remembered that the current research was carried out in the context of online video-games and identify theft here may have involved theft of game accounts, and not directly involve financial or other personal data.

The above data indicates a number of barriers to reporting. There is a notable level of ignorance of how to report, especially in the cases of hacking and cyber-pornography. For all categories of cyber-crime, a number of participants did not report the crimes out of a consideration that they would not be believed. Finally, embarrassment, shame or guilt are a common factor in not reporting pornography, but noticeable less so for the other categories.

	Male					
	Didn't think they would be believed	Embarrassed	Ashamed	Not important	No idea how to report it	Others
Cyber-harassment	2	1	1	3	2	0
Online identity theft	2	2	2	3	1	0
Hacking	2	2	1	4	4	**2**
Cyber-pornography	2	4	2	1	2	0
Total	**8**	**9**	**6**	**11**	**9**	**2**

Table 16- Reasons of non-reporting cyber-crimes based on Gender (Male)

	Female					
	Didn't think they would be believed	Embarrassed	Ashamed	Not important	No idea how to report it	Others
Harassment	2	0	0	7	0	1
Online identity theft	0	0	0	4	2	1
Hacking	0	0	0	1	1	1
Pornography	1	1	1	1	2	1
Total	**3**	**1**	**1**	**13**	**5**	**4**

Table 17- Reasons of non-reporting cyber-crimes based on Gender (Female)

According to table 17, the main reason for females not reporting cyber-harassment was the experience not being considered sufficiently important to report. On the other hand, the response varied among males with a much more even distribution of reasons.

This is also true for identity theft, where again there was a distribution of reasons amongst males, but a majority of females considered it not sufficiently important to report it.

In terms of non-reporting hacking, 77 % of the victims were males and 23% females. Both of them didn't report the incident of hacking for several reasons. Related to men, they consider it not important to report it by 30%. Moreover, they didn't have any idea on how to report it by 30%. Very few females reported being victims of hacking. Again, male participants reported a variety of reasons for non-reporting. This was also true for male victims of pornography. However, here females also reported a variety of reasons for non-reporting.

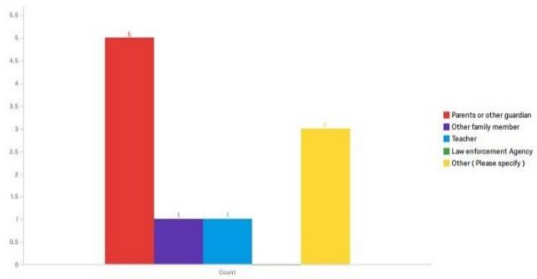


Figure 28 - Cyber-harassment

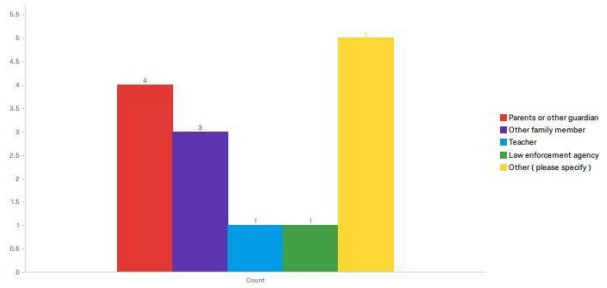


Figure 29 - Identity theft

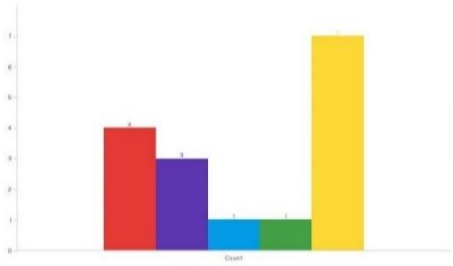


Figure 30 - Hacking

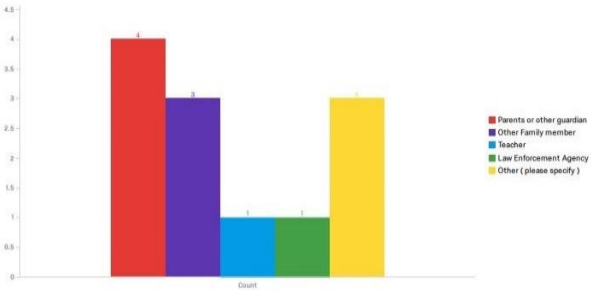


Figure 31 - Cyber-pornography

Victims of cyber-crime may report the event to a range of authority figures. For school-aged children this includes parents and teachers as well as law enforcement agencies. Figures 28-31 display the range of reporting options that participants made use of. There is much more uniformity here than in previous questions. Parents or other guardians, followed by other family members, are the most common specific response in all cases. Reporting to a teacher or to a law enforcement agency occurred in only a very small number of cases. However, for this question, the 'other' response was often given. In the case of cyber-harassment, one of the three respondents (1 F) informed the company that produced the game via the company's website. The remaining two participants (2 F) responding 'other' for this category did not give further details. For online identity theft, of the five participants (3 M and 2 F) selecting 'other' only one male provided useful further information, and again they reported the

incident to the company that produced the game in which the event occurred. In the case of hacking, seven participants (5M and 2 F) selected 'other'. Five of them (5 M) reported the incident of hacking to the game company, one to the PlayStation network support team and the final participant informed their friends. Of the three participants selecting 'other', only one participant provided useful further information and they again reported the incident to the company that produced the game. These results indicate a lack of willingness amongst school-aged children to report incidents of cyber-crime to traditional authority figures, such as teachers and police. Instead, parents and other family members, and the producers of online games, are much more likely to be the recipients of these reports.

4.2.8 Support Services

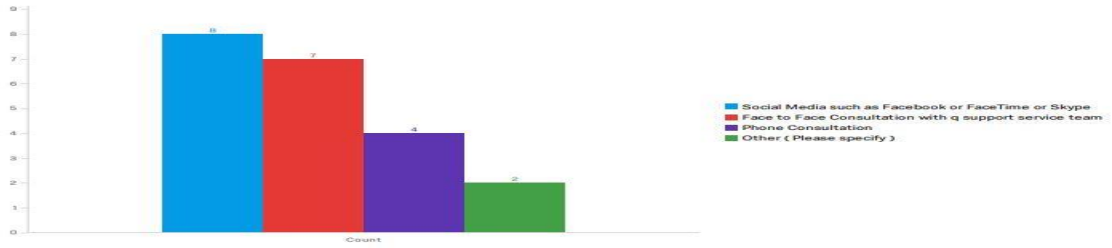


Figure 32 - Support services

As a final question, participants were asked what support services they would have liked to have available when targeted by cyber-crime such as cyber-pornography, cyber-harassment, and online identity theft. The results are displayed in figure 32. Twenty-one participants provided a response to this question. The most popular response was a preference for social media such as Facebook, FaceTime or skype as support services when targeted by cyber-criminals. Participants reported a preference for face-to-face consultation with a support service team, while four other respondents preferred phone consultation. Of the two participants that responded 'other' one participant expressed a preference for a game support team available through an in-game chat room in order to provide help and support in tackling cyber-crimes. Finally, one participant wanted to have one to one online chat with a professional support person.

4.3 Conclusion

This chapter presented the data findings of the survey questionnaire and its interpretation with reference to the literature review discussed in chapter 2. The aim of this study was to investigate the experience and reporting of cyber-crime by school-aged players of online video games. School-aged players of online games appear to have little awareness of the risks and even when they do, the areas of their concern do not match their actual experience.

It can be seen from the results that the experiences of players of different categories of cyber-crime differ vary. The frequency at which different categories are experienced also varies, from only once in the entire time at school to weekly or even more frequently. There were also a number of cases where response by gender differed. Together, this indicates that cyber-crimes should not be treated in a homogenous fashion. Most incidents of cyber-crime appear to go unreported in any fashion. Reporting to traditional authority figures, such as law enforcement agencies or teachers is particularly low. There are a variety of reasons for which victims do not report cyber-crimes. These need to be taken into account in any co-ordinated response to cyber-crimes.

Chapter 5 Discussion

This research examined the experience of people aged between 18 to 25 years old regarding cyber-crime in online games targeting them whilst they were of school age. In order to answer the main research question which is "*What types of cyber-crimes are experienced by school-aged children and do they report the experience of such crimes?*, and subsidiary questions listed in Chapter 3– Methodology – section 3.2, a survey questionnaire was administered. In particular, participants were asked about: their experiences of cyber-crime in online games, the frequency of experiencing it, their awareness of cyber-crimes while playing online games among others. This chapter discusses the issues discovered and also present solutions to problems based on the findings. This is intended to help fill a gap in the literature and reveal opportunities for future research that had not been previously exposed.

5.1 Online game play

The participants experienced cyber-crime while playing a variety of different types of online game. These forms included social games, MOBA, MMORPG, and RTS. According to the data presented in the study, social games were the most commonly played form when players were the victims of online identity theft and cyber-pornography. However, all game forms were reported as venues for cyber-crime. This demonstrates that Cyber-criminals are using the online game medium to target the victims. Other findings from the current study show that school aged victims are not well-prepared with techniques to tackle cyber-crimes.

It is noticeable from table 3 – Chapter 4 (Findings), which displays participants' weekly hours playing online games that males are more likely to record higher amounts of time playing video games on a weekly basis than females, and it seems several reasons lead to the difference between both genders. First of all, stereotypically, most online game players are males (Shaw, 2012) and females typically reveal higher levels of anxiety than males when

playing online games. (Huang, Hood, & Yoo, 2012). In addition, game designers create some online games with female characters that are particularly aimed at of male game players and this lead reinforces the male dominance of the market. With their higher average playing time it is likely that males may be exposed to more instances of cyber-crime than females. Whether it is inherent interest, or other life commitments, that account for this lowered rate of play could not be determined from the data collected. Interestingly, the motivations for play are reasonably consistent across the genders, with fun and relaxation being the most common, followed by competition with others for both genders. To be more specific regarding reasons of playing online video games based on gender and nationality, it is clear that both fun & relaxation as well as exploration were the key of motivation for females to play online games. In compared to men whose interest was based on three factors such as competition, fun & relaxation as well as exploration for the games. However, the small sample size prevents a proper statistical analysis

5.2 Locations of playing online games

It is known that online videogame players engage in playing online games from various locations such as home, internet café or at the home of a friend or family member etc. Participants in the survey reported a reasonably consistent spread of locations of play, regardless of the type of cyber-crime experienced. Most of the respondents were targeted at home and internet cafe, except in the case of cyber-harassment, where home of a friend or family member was the second highest number of responses among participants. It is likely that home is the most common venue of play. However, the increased percentage of identity theft and hacking events at internet cafes point to a potential lack of security at those venues. The physical availability of the hardware at those points may increase the likelihood of cyber-attack. For the home, it is important to address the role of parents in tackling cyber-crimes through supervision and other rules. The role of the parents will be addressed in the recommendation section of this chapter. The enhanced opportunities that internet cafes may be giving attackers is another important issue.

5.3 Risks, Awareness and Target

It can be seen from Table 5 which display the Risks associated while playing online games, that lack of awareness occurs with reasonably equal frequency across gender and nationality. This indicates a real problem amongst online players, who appear to not be equipped with the knowledge in how to tackle cyber-crimes during online games and how to respond to them. So real risks associated with playing online videogames and participants did report awareness of these risks. The most common concern reported, once they began playing, was with

hacking followed by online identity theft. There was awareness of other possible crimes, such as cyber-pornography and cyber-harassment.

Hacking may have been identified as the most common concern due to the prominence of the term in the popular media. However, it can be seen from the data (figure 5, chapter 4) that most of the participants (males) were not aware of the risks associated with playing online videogames before they began playing them. This points to a lack of education and preparation of school-aged students for exposure to the internet. In general, school aged children are not aware of the risks.

Even when they anticipated exposure to cyber-crimes, their actual experience did not match their expectations. There are several reasons of being not aware of the risks associated while playing online games, which are going to be presented in the recommendation section of chapter 5, that address the role of law enforcement agencies, parents and teachers in providing techniques for the victims to be aware of the risks associated while playing online games. While hacking was a common experience, it was matched by cyber-harassment, which was not something that the participants anticipated. Between them, these two categories made up over half the experiences. This is also supported by the frequency of occurrence, where cyber-harassment was the only crime were a daily occurrence was reported by any participants.

Frequency of occurrence did vary, both by game type and cyber-crime-type. As just noted, cyber-harassment was reasonably frequent. Conversely, identity theft was relatively infrequent. Hacking and cyber-pornography showed a more even spread across the participants. Based on the gender variations, it is noticeable that most of the victims of cyber-harassment were females (60%), and that of hacking and cyber-pornography were mostly males (40%). This is in-line with previous work, where it has been noted that females are more likely to be harassed and that males are more likely to encounter pornography.

These variations indicate that cyber-crime cannot be treated as a homogenous phenomenon. Variations in type, frequency and experience by gender indicate that nuanced responses are required.

5.4 Reporting & Non-reporting Cyber-crimes

5.4.1 Non- reporting cyber-crimes

Participants reported a range of reasons for not reporting cyber-crimes to authorities. This included embarrassment, victims feeling guilty or ashamed and having no idea on how to report the incident of cyber-crime. The most common reason overall for not reporting such an

event was not considering important enough. This was most clearly noted in the case of cyber-harassment and online identity theft. It was also important in the non-reporting of hacking. Lack of knowledge of how to report it was also an important consideration for hacking. The most common reason for not reporting cyber-pornography was that participants were too embarrassed to report it while others didn't know how to report it at all. These variations can be understood in terms of the nature of the events. Harassment may simply be written off, but pornography is a far more serious issue and was apparently understood that way by the participants.

There was considerable variation in reporting when the gender of the participants was considered. Most female participants who experienced cyber-harassment stated that it was not important enough to report, whereas this was not true of the male participants. It should be noted that most female participants had low levels of exposure to harassment (50% of those female participants who had experienced it had only experienced it once). This low level of exposure may have led them to ignore the experience.

This borne out by the results for online identity theft. Again, the frequency at which females experienced this cyber-crime was lower than that of the male participants and again females considered it less important. It could be that repeated exposure to a cyber-crime makes school-aged children more likely to take it seriously. This could be addressed by prior education. Online identity theft is a serious issue and victims must take it seriously to prevent their identity (such as Driving license, bank cards, etc.) being stolen or misused. However, males varied in their responses, with some of them stating that is not important at all to report the incident, while others reported being too embarrassed to report it.

For hacking, males again reported more frequent attacks than females did. The main reasons advanced by male participants for non-reporting was not considering the matter sufficiently important to report it or having no idea on how to report such incidents. It is possible that cases of hacking reported were ones where the victim was able to deal with the attack themselves. The technical capacity of school-aged children should not be under-estimated and the availability of cyber-defence tools may lead to a degree of self-reliance.

Unsurprisingly, cyber-pornography showed a very different pattern of reasons for non-reporting than the other types of cyber-crime. Here the nature of the crime itself likely came into play. Embarrassment, shame, guilt and fear of not being believed were all commonly reported. This matches with previous research on lack of reporting of sexually based crimes in general.

The higher rates of experience of cyber-crime experienced by males is likely linked to their higher rates of play. However, the variations noted here again point to the need for responses that are tailored to the particular crime and the circumstances of those that experience it. Given the similarity of reasons for not reporting cyber-pornography to not reporting non-digital cyber-crime, it is possible that lessons learnt in the non-digital arena could be applied to help with reporting in the digital sphere.

5.4.2 Reporting Cyber-crimes

Victims of cyber-crime may report the event to a range of authority figures such as parents, teachers and law enforcement agencies. However, parent, family's members or game companies were much more common avenues of reporting than teachers of law enforcement agencies. Most of the victims of cyber-harassment reported the crime to their parents. This may be understood in terms of the bond or connection between the victims and their parents, and that interrelation may have helped in overcoming any reluctance to report the crime by putting the victims in a safe environment. In regards to online identity theft, there is a variation in reporting the incident to authorities, and many of the victims reported it to parents although other victims informed law enforcement agencies and teachers. In addition, this crime was reported to gaming company too. Companies were often noted as the point of reporting and their role in tackling cyber-crime in online videogames should not be underestimated. In terms of Hacking, most of the victims reported the incident to their parents. That case also applies to cyber-pornography which most of the victims reported the incident to their parents due to real connection or bond among each other. Parents (or other guardian) was the single most common avenue of report for all types of crime. This indicates that the relationship between child and parent is an important factor in dealing with cyber-crime. If there is no connection, reporting of cyber-crimes may not take place.

In terms of gender differentiation in reporting and non-reporting cyber-crimes while playing online games, the date indicates that females report cyber-crimes less often than males (see table 15 – chapter 4). This was especially true for cyber-pornography, where no female participants noted reporting it. The reasons for these are varied, as shown in table 17. The low level of reporting amongst female participants may be due to a lack of social support in and out of the gaming context for female participation. If online video game playing is seen as a primarily male pastime than female players may not wish to report bad experiences (e.g., cyber-crime) because of the risk of being told that they should not have been engaging in the first place. Such a lack of social support leads to both physical and psychological health

problems such as feelings of loneliness and isolation. These are major predictors of health and wellbeing problems. Female reporting of cyber-crime may be enhanced if the overall welcome they are given is improved.

5.5 Discussion of main research question & subsidiary Questions

In terms of the main research question, "*What types of cyber-crimes are experienced by school-aged children and do they report the experience of such crimes?* Respondents experienced several types of cyber-crime such as cyber-harassment, cyber-pornography, online identity theft, online hacking and ransomware while playing online games. To illustrate, Figure 6 – titled as Cyber-crime concerns states the types of cyber-crimes targeting online game players. In terms of reporting, Reporting rates were low, only a minority of victims reported the crime, at an overall average of roughly 25%. While it cannot be said that cyber-crimes are not reported, the reporting rate is less than ideal, and it can be seen from the figures the rate of reporting varies between categories, from maximum 44.44% in the case of hacking, down to 21% in the case of cyber-harassment. Remember that reporting could be to any authority figure, including parent and teacher as well the police. These figures indicate that reporting of cyber-crimes as experienced by school-aged children to law enforcement bodies significantly under-represents the actual rate of occurrence and that bother gender and the actual crime can affect the rates of reporting.

What are the reasons for non-reporting of cyber-crimes? In school, at home, some places
There were several reasons reported by participants for not reporting cyber-crimes, such as embarrassment, feeling guilty or ashamed, not considering the matter important enough to report, and having idea on how to report such incidents. This indicates that there are real barriers to reporting cyber-crimes. The variation in reasons for non-reporting indicate that cyber-crimes cannot be treated as a homogeneous phenomenon.

Are school-aged children aware of the risks associated with playing online games?
Most of the victims or respondents were not aware of the risks associated before playing online games. This awareness improved once play commenced, but even then participants concerns did not entirely matched their experiences. This indicates that better education would help prepare school-aged children for what they will encounter.

Which Cyber-criminal activity were the participants most concerned about while playing online games while of school age?
It is confirmed through the study that respondents (32.20%) are most concerned about hacking while playing online games. As just noted, this did not match their experiences, even though hacking was one of the most commonly encountered forms of cyber-crime.

What types of online game they were playing while experiencing cyber-crime?
Respondents reported playing a range of online games such as MMORPG, MOBA, RTS, and social games when targeted by cyber-criminals. Interestingly, while no cyber-crime was unique to particular type of game (or vice-a-versa), the distribution of cyber-crimes types versus game types did vary. This again indicates the variations that exist and need to be accounted for in any response strategy.

How frequently they have experienced cyber-crime while playing online game? And where were they playing online games when experienced cyber-crime?
Frequency varied from daily to only a single occasion. Variation was again seen across the types of cyber-crime. Cyber-crime was experienced in all playing venues, with the predominance of the home likely being due to its role as the most common playing venue.

How likely are they to report the incident of cyber-crime? The level of reporting were low, at around 25%, with females less likely to report cyber-crimes than males.

Who they report the incident of cybercrime to?
Reporting was to a variety of authority figures, with parents being the most common and law enforcement agencies the least common. In general, it can be seen that significant variations in experience and reporting exist both across the types of cyber-crime and by gender. Any approach to tackling cyber-crime and improving reporting must take account of these variations. The interrelation of cyber-crime defined in 2.2 section and the current study affirm that Cyber-criminals have used the computer as a tool to target victims (school-aged students) through many forms such as cyber-harassment, cyber-pornography, and online identity theft etc. As you can see in section 4.2.4 titled as **Experience of Cyber-Crime,** participants were then asked which types of cyber-crime they actually experienced while playing online games. It is confirmed that victims experienced cyber-criminals activities perpetrated by cyber-criminals and the most common experiences were of Cyber-harassment and Hacking, both reported by 28.21% of participants (eleven participants each). This was followed by identity theft at 23.08% (or nine participants), and cyber-pornography at 15.38% (6 participants). So, the cyber-criminals used the computer as a tool to perform illegal or criminal activities in which respondents faced while playing online games. When it comes to the location of playing online games, victims played it into different locations such as home, internet café, etc. So, cyber-criminals perform cyber-criminal activities in which they considered the victim's computer wherever they are located as a target that comes into many forms such as unauthorized access to the computer to perform online identity theft, to hack their computers and steal personal images etc. by exploiting the victims through many online gaming

platforms such as Blogging, live chat, exchanging messages or video calling to perform criminal activities.

Chapter 6 Conclusion

6.1 Limitations

The current study discussed the types of cyber-crimes experienced by school-aged children and their knowledge of reporting it or not, and what kind of games targeted them while playing online games, and the frequency of the occurrence of the cyber-crimes, etc. There were a number of limitations which must be considered in conjunction with the results. Firstly, the participant pool was relatively small, at 47 respondents. This prohibited thorough statistical analysis of the results. However, the participants did provide detailed responses, allowing conclusions to be drawn. There was a trade-off in the age of the participants (18 to 25 years old) and errors in recall may have occurred. This had to be balanced against the problems involved in directly surveying school-aged children. When surveying young people (17 years old or younger) it is required by law to get their parent's consent in order to participate in survey questionnaire. Such participants may not wish to reveal their experience of cyber-crime to their parents. Also, people under the age of 18 may not be emotionally equipped to deal with the recall of such experiences. There were a number of issues that the study did not address, such as the relationships between children and parent, which could have affected their choice of reporting avenue. Further research may examine this in more details. The sources of information about cyber-crime that participants made use of, such as teachers or law enforcement agencies, were also not investigated. Finally, a technical problem in the Qualtric settings prevented display of questions related to the age of participants when they began playing on line games and when they first experienced cyber-crimes.

6.2 Recommendations

There are a number of possible areas for future study, including some revealed by the limitations noted in the previous section. Consideration can be given to directly surveying school-aged children. The limited time available for the current research prohibited this, given the issues already discussed, but with more time these could be addressed. Future work could also investigate in more details the relationship between game playing habits and experience of cyber-crime, how experience of reporting affects likelihood of future reporting and the impact of other factors on reporting, such as personality and relationships. More

details may be revealed by face-to-face interviews with participants with students at school (after getting approvals from both parents and guardians). From the results obtained a number of recommendations can be made in addressing cyber-crime. Given the frequency of choice of parents as a reporting avenue, the role of parents in guiding their children regarding playing online games and how to respond to the cyber-criminals should not be under-estimated. To solve this issue, parents must provide guidance to their children by performing the following activities:

- Set time limits for their children playing online games (weekly or daily)
- Check the age rating of the games their children are playing
- Inform their children not to share personal details online, and warn them about the dangers of sharing such information.
- Encourage their children to play properly and treat other gamers with respect.
- Make sure their children‘s computers are up-to-date by having an updated anti-virus software as their computers or devices might be exposed to the risks of viruses.
- Ensure their children know how to report or block other players who engage in committing cyber-crimes in the form of cyber-pornography, ransomware etc.

Parents themselves will need access to appropriate education to be able to provide this support to their children. Teachers are another important avenue for reporting. Schools need to provide information to students, as outlined above, especially in cases where parents are not sufficiently technically literate. Provision of cyber-security courses, prevention and awareness programs related to cyber-crimes and how to tackle it could all be placed within a school’s remit. This could include training for students that discusses and explains effective defence against criminals and how to reduce the risk of becoming a victim. Schools need to be advising students on appropriate protection methods and putting that in a code of use and their security policies.

Law enforcement agencies (e.g., police) could assist by providing in holding workshops for school-aged students at schools with the goal of guiding them in how to tackle cyber-crime incidents when targeted. In order to make sure that every online game player is knowledgeable in reporting cyber-crimes, government agencies have an important role, for example in providing educational materials. More specifically, government’s agencies must be presenting guidelines for users in how to report the incidents of cyber-crimes targeting them in the online game medium. This may be in co-operation with the online game

companies. The guidelines could also presents details of bodies that help in countering cyber-crimes and the steps to be taken in reporting cyber-crimes.

Such bodies include the following:

1. Stay Smart Online https://www.staysmartonline.gov.au/
2. Office Of The E-safety Commissioner https://www.esafety.gov.au/
3. Australian Cyber-security Centre https://www.cyber.gov.au/report
4. ACORN https://www.acorn.gov.au/
5. CERT Australia https://www.auscert.org.au/
6. ThinkYouKnow https://www.thinkuknow.org.au/

In regards of the online gaming company, they could provide guidance for online game players in how to protect themselves from cyber-criminals. This could be presented as part of the normal sign-up procedure. The guide should present information on how to secure personal gaming accounts with a strong password, avoid using the same password used elsewhere, never share login details with other people, and remember to logout when finished. Players need to be warned to keep their personal details private and beware of oversharing or revealing too much when playing games online or when communicating with fellow players, especially those they do not know well. This can help reduce the risk of cyber-harassment, ransomware, cyber-stalking, and even identity theft and so on.

6.3 Conclusions

The aim of this research was to investigate the experience of cyber-crime by school-aged children and their reporting of those experiences. It was found that the participants had a varied experience of cyber-crime and likewise varied in their reporting. Cyber-crime was experienced in various forms and with varying frequency. Some participants experienced it very rarely, some almost constantly. There was variation across the types of cyber-crime and by gender. Reporting was uniformly low. While this varied from crime to crime, for no type was it higher than 44%. Reasons for this varied, with lack of importance attached to the crime being one of the most common. This indicates the need for enhanced education of school-aged children about cyber-crime and how to deal with it. There was noted variation between crimes as to the reasons for non-reporting, although this was in-line with what might be expected given the nature of each type. Interestingly, females were less likely to report cyber-crime than males, although a larger participant sample would be needed to confirm the validity of this result. These variations indicate that efforts to tackle cyber-crime must not adopt a "one size fits all" approach, but must be tailored to the nature of the crime and allow for the individual circumstances and motivations of those experiencing cyber-crime.

Bibliography

Achiterbosch, L., Pierce, R., & Simmons, G. (2007, October). Massively multiplayer online role-playing games: The past, present, and future. *ACM Computers in Entertainment*. Retrieved from https://www.researchgate.net/publication/220686344_Massively_multiplayer_online_role-playing_games_The_past_present_and_future

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A Review of Using Gaming Technology for Cyber-Security Awareness. *International Journal for Information Security Research*, 660-666. Retrieved from https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security-Awareness.pdf

Asanka, N., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Elsevier*, 304-312. Retrieved from http://ac.els-cdn.com/S0747563214003331/1-s2.0-S0747563214003331-main.pdf?_tid=c7e54068-1048-11e6-9f32-00000aab0f02&acdnat=1462181725_b966736ccbf524f36da39fa158aab998

Bachman, R. (1998). The factors related to Rape reporting behaviour and Arrest . *Ameerican association for correctional psychology* , 8-29. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/0093854898025001002

Beckett, H., & Warrington, C. (2014). *Suffering in silence:children and unreported crime .* Bedfordshire . Retrieved from https://www.victimsupport.org.uk/sites/default/files/Suffering%20in%20silence%20-%20Children%20and%20unreported%20crime.pdf

Bilchik, S. (1999). Reporting Crimes against juveniles . *OJJDP*. Retrieved from https://www.ncjrs.gov/pdffiles1/ojjdp/178887.pdf

Birdsey, E., & Snowball, L. (2013). Reporting Violence to Police: A survey of victims attending domestic violence services. *NSW Bureau of Crime Statistics and Research* , 1-8. Retrieved from https://www.bocsar.nsw.gov.au/Documents/BB/bb91.pdf

Bossler, A., & Holt, T. (2009). On-line Activities, Guardianship, and Malware Infection : An Examination of Routine activities theory . *International Journal of Cyber Criminology*, 400-420. Retrieved from http://www.cybercrimejournal.com/bosslerholtijcc2009.pdf

Bouckley, H. (2019). *Fortnite to Call of Duty: Keep your children safe playing games online.* Hannah Bouckley . Retrieved from https://home.bt.com/tech-gadgets/computing/gaming/online-gaming-for-kids-advice-for-parents-how-to-protect-your-child-11364060707336

Bowles, R., Reyes, M., & Garoupa, N. (2009). *Springer*, 365-377. Retrieved from https://link.springer.com/content/pdf/10.1007%2Fs10610-009-9109-8.pdf

Bowles, R., Reyes, M., & Garoupa, N. (2009). *European Journal on Criminal Policy and Research*, 365-377. Retrieved from https://link.springer.com/content/pdf/10.1007%2Fs10610-009-9109-8.pdf

Bradford, R., Henson, B., & Fisher, B. (2011). BEING PURSUED ONLINE Applying Cyberlifestyle–Routine Activities theory to cyber-stalking Victimization . *Criminal Justice and behaviour* , 1149-1169. Retrieved from http://journals.sagepub.com/doi/pdf/10.1177/0093854811421448

Brand, J. (2015). Bond , UK: Brand , Jeffrey. Retrieved from http://theconversation.com/gaming-through-the-ages-older-australians-are-embracing-video-games-44899

Brand, J., Todhunter, S., & Jervis, J. (2018). Gold Coast. Retrieved from https://www.igea.net/wp-content/uploads/2017/07/Digital-Australia-2018-DA18-Final-1.pdf

Catherine, M., Higgins, g., & Rickets, M. (2010). Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory. *Deviant Behaviour* , 381-410. Retrieved from https://www.tandfonline.com/doi/full/10.1080/01639620903004903

CERT. (2019). *Distributed denial of service Attack*. Retrieved from CERT AUSTRALIA: https://www.cert.gov.au/threats/common-threats/denial-service

Chang, F.-C., Chiu, C.-H., Miao, N.-F., Chen, P.-H., Lee, C.-M., Huang, T.-F., & Pan, Y.-C. (2014). *Online gaming and risks predict cyberbullying perpetration and victimization in adolescents.* Swizerland: Swiss School of Public Health. Retrieved from https://link.springer.com/content/pdf/10.1007%2Fs00038-014-0643-x.pdf

Chang, J.-H., & Zhang, H. (2008). Rapid Communication. *CYBERPSYCHOLOGY & BEHAVIOR*, 711-714. Retrieved from https://www.liebertpub.com/doi/pdf/10.1089/cpb.2007.0147

Chen, Y.-C. (2005). *An analysis of online gaming crime characteristics.* China: Emerald Group Publishing Limited. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/10662240510602672/full/html

Chisholm, J. (2014). Review of the Status of Cyberbullying and cyberbullying prevention . *Journal of Information Systems Education* , 77-84. Retrieved from https://jise.org/volume25/n1/JISEv25n1p77.pdf

Choi, K.-s. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 308-333. Retrieved from https://www.cybercrimejournal.com/Choiijccjan2008.htm

Christianson, S.-A., & Loftus, E. (1990). Some characteristics of people's traumatic memories. *Bulletin of the Psychonomic Society*, 195-198. Retrieved from https://link.springer.com/content/pdf/10.3758/BF03334001.pdf

Clough, J. (2012). *THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME: Defining Crime in a digital world.* Monash , Australia: Clough , Jonathan. Retrieved from https://link.springer.com/content/pdf/10.1007/s10609-012-9183-3.pdf

Cohen, l., & Felson, M. (1979). *SOCIAL CHANGE AND CRIME RATE TRENDS: A routine Active Approach.* Urbana: American Sociological Association. Retrieved from American Sociological Association: https://www.jstor.org/stable/pdf/2094589.pdf?refreqid=excelsior%3A0d83f29abd04f4531f78c069139c10f2

Cohen, L., & Felson, M. (1979). *SOCIAL CHANGE AND CRIME RATE TRENDS: A ROUTINE ACTIVITY APPROACH.* Urbana: American Sociological Association. Retrieved from https://www.jstor.org/stable/pdf/2094589.pdf?refreqid=excelsior%3A4d6c50a44fb2125a7c8b815e0d6915ce

Cole, H., & Griffiths, M. (2007). *Social Interactions in Massively Multiplayer Online Role-Playing Gamers.* Nottingham , UK : Mary Ann Liebert. Retrieved from http://ocw.metu.edu.tr/pluginfile.php/2372/mod_resource/content/1/ColeGriffiths.PDF

Commonwealth, A. (2017). *Fraud.* Australian Instituite of criminology. Retrieved from https://aic.gov.au/publications/rpp/rpp129/fraud

Corcoran, L., Gucking, C., & Prentice, G. (2015). Cyberbullying or Cyber Aggression?: A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression. *Societies*, 247. Retrieved from https://www.researchgate.net/publication/277595086_Cyberbullying_or_Cyber_Aggression_A_Review_of_Existing_Definitions_of_Cyber-Based_Peer-to-Peer_Aggression

Darwen, B. (2014). *"It's all about trust": Building good relationships between Children and police .* Retrieved from https://www.ncb.org.uk/sites/default/files/uploads/documents/Policy_docs/appgc_children_and_police_report_-_final.pdf

Dashora, K. (2011). Cyber Crime in the Society: Problems and preventions . *Journal of Alternative Perspectives in the Social Sciences*, 240-259. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.452.5880&rep=rep1&type=pdf

DePaolis, K., & Williford, A. (2014). *The Nature and Prevalence of Cyber Victimization Among Elementary School Children.* New York : Springer Science. Retrieved from https://link.springer.com/content/pdf/10.1007%2Fs10566-014-9292-8.pdf

Diele, O. (2013). *State of Online Gaming report .* Retrieved from http://auth-83051f68-ec6c-44e0-afe5-bd8902acff57.cdn.spilcloud.com/v1/archives/1384952861.25_State_of_Gaming_2013_US_FINAL.pdf

Ell, K. (2018). *Video game industry is booming with continued revenue .* Ell , Kellie ;. Retrieved from https://www.cnbc.com/2018/07/18/video-game-industry-is-booming-with-continued-revenue.html

Farhat, S., Himani, J., Rehmatullah, S., Azim, F., & Temuri, H. (2014). Trauma experience of youngsters and Teens: A key issue in suicidal behavior among victims of bullying? *Pakistan journal of medical sciences*, 206-210. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3955573/pdf/pjms-30-206.pdf

Finkelhor, D., Wolak, J., & Lucy, B. .. (2001). Police reporting and professional help seeking for child crime victims . *SAGE Social Science Collections*, 17-28. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/1077559501006001002

Fisher, B., Daigle, L., & Cullen, F. (2003). Reporting Sexual victimization to police and others. *American Association for Correctional Psychology*, 6-38. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/0093854802239161

Fruhlinger, J. (2018, 12 19). *What is ransomware? How these attacks work and how to recover from them*. Retrieved from CSO: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html

Fryling, M., & Cotler, J. (2014). Cyberbullying or Normal Game Play? . *AITP*, 1-8. Retrieved from http://proc.conisar.org/2014/pdf/3307.pdf

Gentile, D., Lynch, P., Linder, j., & walsh, d. (2004). The effects of violent video game habits on adolescent hostility,aggressive behaviors and school performance . *Journal of Adolescence* , 5-22. Retrieved from https://drdouglas.org/drdpdfs/Gentile_Lynch_Linder_Walsh_2004.pdf

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. *ITU*, 1-366. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Goudriaan, H. (2006). *REPORTING CRIME.* Netherland: Universal Press. Retrieved from https://openaccess.leidenuniv.nl/bitstream/handle/1887/4410/Thesis.pdf

Grant, J. (2018). *State of play - youth and onlin gaming in australia.* Australia. Retrieved from https://www.esafety.gov.au/about-the-office/research-library

Greenfield, M. (2019). *Hours children spend gaming weekly in the United Kingdom (UK) from 2013 to 2017, by age group (in hours).* Retrieved from https://www.statista.com/statistics/274434/time-spent-gaming-weekly-among-children-in-the-uk-by-age/

Griffiths, M., Kuss, D., & King, D. (2012). *Video Game Addiction: Past, Present and Future.* Adelaide - South Australia : Griffiths , Mark ; Kuss , Daria ; King , Daniel ;. Retrieved from https://irep.ntu.ac.uk/id/eprint/5976/1/211418_PubSub798_kuss.pdf

Grüsser, S., Thalemann, R., & Griffiths, M. (2007). Excessive Computer Game Playing: Evidence for Addiction and Aggression? *CYBERPSYCHOLOGY & BEHAVIOR*, 290-291. Retrieved from https://www.liebertpub.com/doi/pdf/10.1089/cpb.2006.9956

Henry, J. (2018, 5 15). *GameRant*. Retrieved from Fortnite: 13-Year Old's Account Hacked After Being Tricked by Fellow Player: https://gamerant.com/fortnite-13-year-old-account-hack/

Holt, T., & Bossler, A. (2009). Examining the Applicability of Lifestyle-Routine Activities theory for cyber-crime victimization. *Deviant Behaviour*, 1-25. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/01639620701876577?needAccess=true

Hsieh, M.-L., & Wang, S. (2018). Routine Activities in a Virtual Space: A Taiwanese Case of an ATM Hacking Spree . *International Journal of Cyber Criminology* , 333-348. Retrieved from https://www.cybercrimejournal.com/Hsieh&WangVol12Issue1IJCC2018.pdf

Huang, W., Hood, D., & Yoo, S. (2012). Gender divide and acceptance of collaborative Web 2.0 applications for learning inhigher education. 57-65. Retrieved from https://reader.elsevier.com/reader/sd/pii/S1096751612000085?token=DE5263151BFF45ED45F516FB1AB73D8FEA73FCF9E804999C88067C567609E2FB815D7B04ABA63995049D850939E9E59C

Ibekwe, C. (2015). *The Legal Aspects of Cybercrime in Nigeria.* Ibekwe , Chibuko. Retrieved july 2015, from https://dspace.stir.ac.uk/bitstream/1893/22786/1/Ibekwe%20PHD%20THESIS.pdf

ITU. (2012). *Understanding cybercrime: Phenomena, challenges and legal response .* ITU. Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Jansz, J., & Tanis, M. (2007). Appeal of Playing Online First Person Shooter Games. *CYBERPSYCHOLOGY & BEHAVIOR*. Retrieved from https://www.liebertpub.com/doi/pdf/10.1089/cpb.2006.9981

Jensen, A., & Walker, l. (2009, January 25). *Video Games Linked To Poor Relationships With Friends, Family*. Retrieved from ScienceDaily: https://www.sciencedaily.com/releases/2009/01/090123075000.htm

Jones, j., alexander, c., Wynn, b., & Rossman, l. (2009). Violence: Recognition,Management and Prevention. *The Journal of Emergency Medicine*, 417–424. Retrieved from http://reader.elsevier.com/reader/sd/pii/S0736467908000358?token=EA249FAD689DAC0212C6A88F6E3A7226F47BE74A79B16F8587A124B8FD0BEF53E3A4120CDE71B7FAD9BDD55C14634D53

Katersky, A. (2012, 4 5). Online Gaming Is Becoming Predator's Playground. Monroe, New York, US. Retrieved from https://abcnews.go.com/US/online-gaming-predators-playground/story?id=16081873

Lam, L., Cheng, Z., & Liu, X. (2013, 03 15). Violent Online Games Exposure and Cyberbullying/Victimization Among Adolescents. *Cyberpsychology, Behavior, and Social Networking*. Retrieved from https://www.liebertpub.com/doi/pdf/10.1089/cyber.2012.0087

Lau, F., Rubin, S., Smith, M., & TrajkoviC, L. (2000). *Distributed Denial of Service Attacks.* Calgary: IEEE. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=886455&tag=1

Laub, J. (1981). ECOLOGICAL CONSIDERATIONS IN VICTIM REPORTING TO THE POLICE . *Journal of criminal justice* , 419-430. Retrieved from https://reader.elsevier.com/reader/sd/pii/004723528190088X?token=CD360E28C2125C7D437AC4D7C4C1C722C8E7C72AF2C673EA85B3A7EA5E54AFF8AF23C7AE3AC50FC32C1FB8F9DE17B4C9

Lenhart, A. (2009). Washington D.C. Retrieved from https://www.pewinternet.org/wp-content/uploads/sites/9/media/Files/Reports/2009/PIP-Teens-and-Mobile-Phones-Data-Memo.pdf

Lenhart, A. (2015). US. Retrieved from https://www.pewinternet.org/2015/08/06/chapter-3-video-games-are-key-elements-in-friendships-for-many-boys/

Lenhart, A. (2015). *Video Games Are Key Elements in Friendships for Many Boys.* US. Retrieved from https://www.pewinternet.org/2015/08/06/chapter-3-video-games-are-key-elements-in-friendships-for-many-boys/

Leukfeldt, E., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A theoritical and empirical analysis . *Deviant Behaviour* , 263-280. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/01639625.2015.1012409?needAccess=true

Leung, A. N.-m., & McBride-Chang, C. (2013). Game On? Online Friendship,cyberbullying and Psychosocial adjustment in Hong Kong Chinese children . *Journal of Social and Clinical Psychology* , 159-185. Retrieved from https://guilfordjournals.com/doi/pdf/10.1521/jscp.2013.32.2.159

Leung, L. (2004). Net-Generation Attributes and Seductive Properties of the internet as predictors of online activities & internet addiction. *CYBERPSYCHOLOGY & BEHAVIOR*, 333-346. Retrieved from https://www.liebertpub.com/doi/pdf/10.1089/1094931041291303

Limelight. (2019). *MARKET RESEARCH the state of online game 2019 .* France, Germany, India, Italy, Japan, Singapore, South Korea, the United Kingdom, and the United States. Retrieved from https://img03.en25.com/Web/LLNW/%7B02ca9602-173c-43a4-9ee1-b8980c1ea459%7D_SOOG2019_MR_8.5x11.pdf

Liu, M., & Peng, W. (2009). Cognitive and psychological predictors of the negative outcomes associated with playing MMOGs. *Computers in Human Behavior*, 1306–1311. Retrieved from https://msu.edu/~pengwei/Cognitive%20and%20psychological%20predictors%20of%20the%20negative%20outcomes%20associated%20with%20playing%20MMOGs.pdf

maran, d., & begotti, t. (2019). *Prevalence of Cyberstalking and Previous offline victimization in a sample of Italian university students.* Torino: maran, daniela; begotti, tatiana. Retrieved from socsci-08-00030.pdf

Marcum, C., Higgins, G., & Ricketts, M. (2014). Hacking in High School: Cybercrime Perpetration by juveniles . *Deviant Behaviour* , 581. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/01639625.2013.867721?needAccess=true

Massey, B. (2014). *"It's all about trust": Building good relationships between Children and the police ".* UK: National Children's Bureau . Retrieved from http://www.ncb.org.uk/sites/default/files/uploads/documents/Policy_docs/appgc_children_and_police_report_-_final.pdf

Mcdonald, E. (2017). *Newzoo's 2017 Report: Insights into the $108.9 Billion Global Games Market.* US: Newzoo. Retrieved from https://newzoo.com/insights/articles/newzoo-2017-report-insights-into-the-108-9-billion-global-games-market/

McDowell, M. (2013, february 06). *Understanding Denial-of-Service Attacks*. Retrieved from US-CERT: https://www.us-cert.gov/ncas/tips/ST04-015

McGuire, M., & Dowling, S. (2013). *Cyber-dependent crimes.* McGuire , Mike;Dowlin , Samantha. Retrieved from http://www.justiceacademy.org/iShare/Library-UK/horr75-chap1.pdf

McInroy, L., & Mishna, F. (2017). Cyberbullying on Online Gaming Platforms for Children and Youth. *Research Gate* , 1-23. Retrieved from file:///C:/Users/44707525.MQAUTH.045/Downloads/McInroyMishnaGamingArticlePre-Print%20(1).pdf

McMullan, T. (2018, 4 11). *PUBG Ransomware is a new type of malware that locks your files unless you play PlayerUnknown's Battlegrounds*. Retrieved from Alphr: https://www.alphr.com/security/1009024/malware-pubg-PlayerUnknown-Battlegrounds-ransomware

Messmer, E. (2013). Online gaming company recounts fighting for survival vs. DDoS attacks. *Network World* . Retrieved from https://www.networkworld.com/article/2166252/online-gaming-company-recounts-fighting-for-survival-vs--ddos-attacks.html

Nurse, J. (2018). Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit. *Oxford Handbook of Cyberpsychology*. Retrieved from https://arxiv.org/pdf/1811.06624.pdf

Ontañon, S., Synnaeve, G., Uriarte, A., Richoux, F., Churchill, D., & Preuss, M. (2013, october 8). *A Survey of Real-Time Strategy Game AI Research and competition in starcraft.* Retrieved from Hal Archives-ouvert: https://hal.archives-ouvertes.fr/hal-00871001/document

Park, J., Song, Y., & Ten, c. (2011). Exploring the Links Between Personality Traits and Motivations to Play Online Games. *CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING*, 747-750. Retrieved from https://www.liebertpub.com/doi/pdf/10.1089/cyber.2010.0502

Pedneker, P. (2013). Cyber Crimes: An Overview. *Online international Interdisciplinary Research Journal* , 130. Retrieved from https://www.academia.edu/4763100/Cyber_Crimes_An_Overview

Plous, S. (1996). *Online Social Psychology Studies*. Retrieved from Social Psychology Network : https://www.socialpsychology.org/expts.htm

Powers, P. (2015). The Philosophical Foundations of Foucaultion discourse analysis . *Critical Approaches to Discourse Analysis across Disciplines CADAAD* , 18-34. Retrieved from https://www.lancaster.ac.uk/fass/journals/cadaad/wp-content/uploads/2015/01/Volume-1_Powers.pdf

Pratt, T., Holtfreter, K., & Reisig, M. (2010). Routine Online activity and internet fraud targeting : Extending the generality of routine activity theory . 267-296. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/0022427810365903

Przybylski, A. (2018, 03 18). Exploring Adolescent Cyber Victimization in Mobile Games: Preliminary Evidence from a British Cohort. Oxford, Oxford, UK. Retrieved from https://www.liebertpub.com/doi/pdf/10.1089/cyber.2018.0318

Quinn, B., & Arthur, c. (2011, 4 27). *PlayStation Network hackers access data of 77 million users.* Retrieved from The Guardian: https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data

Rabjohn, J. N. (1976). Crime by Computer. *DePaul Law Review*. Retrieved from http://via.library.depaul.edu/cgi/viewcontent.cgi?article=2628&context=law-review

Reisinger, D. (2011, 10 11). *Cnet*. Retrieved from Online children playing onlien games: https://www.cnet.com/news/91-percent-of-kids-are-gamers-research-says/

Richard, F., Messner, S., Hoskin, A., & Dean, G. (2002). REASONS FOR REPORTING AND NOT REPORTING DOMESTIC VIOLENCE TO THE POLICE*. *CRIMINOLOGY*, 617-644. Retrieved from https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1745-9125.2002.tb00968.x

Rogers, M., Smoak, N., & Liu, j. (2006). A Big-5, Moral Choice, and Manipulative Exploitive Bahavior analysis . *Deviant Behavior* , 245-268. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/01639620600605333?needAccess=true

Rouse, M. (2010, 9 21). *Cyber-crime* . Retrieved from Techtarget : https://searchsecurity.techtarget.com/definition/cybercrime

Roy, T., & Burnside, N. (2019). *Online abuse, harassment, cyber trolling costing Australians $3.7 billion.* Australia: Roy , Tahlia ; Burnside , Niki . Retrieved from https://www.abc.net.au/news/2019-01-28/online-abuse-harassment-costing-australians-3.7-billion/10754196

Rypi, A., Burcar, V., & Akerstorm, M. (2019). Refraining from reporting crimes: accounts from young male crime victims with an immigrant background . *Nordic Social Work Research*, 131-146. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/2156857X.2018.1491010?needAccess=true

Sable, M., Danis, F., & Gallagher, S. (2010). Barriers to Reporting Sexual Assault for Women and men . *Journal of American College Health*, 157-161. Retrieved from https://www.tandfonline.com/doi/pdf/10.3200/JACH.55.3.157-162?needAccess=true&

Sarre, R., Lau, L., & Chang, L. (2018). Responding to cybercrime: current trends. 515-518. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/15614263.2018.1507888?needAccess=true

Sharry, J. (2015). *Ask the Expert: My 13-year-old son is addicted to online gaming.* The Irish Times. Retrieved from https://www.irishtimes.com/life-and-style/health-family/ask-the-expert-my-13-year-old-son-is-addicted-to-online-gaming-1.2443077

Shaw, A. (2012). Do you identify as a gamer? Gender, race, sexuality, and. *new media & society*, 28-44. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/1461444811410394

Shu, A., & Subrahmanyam, K. (2009). Youth Internet use: risks and opportunities. *Child and adolescent psychiatry*, 351–356. Retrieved from https://pdfs.semanticscholar.org/bd7e/3359ea8c64f0a0d97eff1dd6d2aadfb26ed3.pdf

Shu, Y. (2012). *PATHS TO BULLYING IN ONLINE GAMING.* Baywood. Retrieved from https://journals.sagepub.com/doi/pdf/10.2190/EC.47.3.a

Sirohi. (2015). *Transformational dimensions of cybercrime .* New Delhi : Alpha editions . Retrieved from https://books.google.com.au/books?id=AdRxCgAAQBAJ&pg=PT5&dq=cyber+crime+definition&hl=en&sa=X&ved=0ahUKEwi1tZ2GvPzbAhWLmZQKHbkgDuIQ6AEIUzAH#v=onepage&q=cyber%20crime%20definition&f=false

Smith, P., Mahdavi, J., Carvalho, M., Fisher, S., & Russell, S. (2008). Cyberbullying: its nature and impact in secondary school pupils. *CHILD PSYCHOLOGY AND PSYCHIATRY*, 376-385. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1469-7610.2007.01846.x/pdf

(2018). *STATE OF PLAY — YOUTH AND online video games .*

Suman, S., Srivastava, N., & Pandit, R. (2014). Cyber Crimes and Phishing Attacks. *International Journal on Recent and Innovation Trends in Computing and Communication*, 334-337. Retrieved from https://s3.amazonaws.com/academia.edu.documents/35435287/Cyber_Crimes_and_Phishing_Attacks.pdf?response-content-disposition=inline%3B%20filename%3DCyber_Crimes_and_Phishing_Attacks.pdf&X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWOWYYGZ2Y53UL3A

Tarling, R., & Morris, K. (2010). Reporting Crime to the Police. *BRIT. J. CRIMINOL*, 474–490. Retrieved from azq011.pdf

Thaier, H., & Maple, C. (2013). Online Harassment and Digital Stalking. *International journal of computer applications* . Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.8620&rep=rep1&type=pdf

wall, D. (2007). *Cybercrime : transformation of the crime in information age .* UK: David wall . Retrieved from https://books.google.com.au/books?id=swEgF0SgaFEC&pg=PA10&dq=wall+1997+about+cyber+crime&hl=en&sa=X&ved=0ahUKEwjv5-HFyavOAhWCEpQKHSlFByIQ6AEIMzAA#v=onepage&q=wall%201997%20about%20cyber%20crime&f=false

Wan, c., & Chiou, W.-B. (2006). Why Are Adolescents Addicted to Online Gaming? 762-766. Retrieved from https://www.academia.edu/1227475/Why_Are_Adolescents_Addicted_to_Online_Gaming_An_Interview_Study_in_Taiwan

Ward, M. (2018). *'I was having panic attacks': online gaming addiction is real.* Canada : SMH. Retrieved from https://www.smh.com.au/lifestyle/health-and-wellness/i-was-having-panic-attacks-online-gaming-addiction-is-real-20181011-p5094a.html

Warman, P. (2018). NEWZOO. Retrieved from https://cdn2.hubspot.net/hubfs/700740/Reports/Newzoo_2018_Global_Games_Market_Report_Light.pdf

Warman, P. (2018). *2018 Global Games market report .* Retrieved from https://cdn2.hubspot.net/hubfs/700740/Reports/Newzoo_2018_Global_Games_Market_Report_Light.pdf

Wasserman, E., & Ann Ellis, C. (2010). IMPACT OF CRIME ON VICTIMS. *National Victim Assistance Academy*, 6-15. Retrieved from https://ce4less.com/Tests/Materials/E075Materials.pdf

Webb, K. (2018, 11 10). *he hacker who targeted Xbox Live and PlayStation Network is facing 10 years in jail for knocking the gaming networks offline*. Retrieved from Business insider Australia : https://www.businessinsider.com.au/utah-hacker-pleads-guilty-denial-of-service-attacks-xbox-live-playstation-network-steam-2018-11?r=US&IR=T

WHO. (2018, 6 18). *Gaming addiction is now officially classified as a mental disorder*. Retrieved from Triple J Hack: https://www.abc.net.au/triplej/programs/hack/gaming-addiction-is-now-classified-as-a-mental-disorder/9882722

Winther, K. (2017). *Children in a digital world .* Retrieved from https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

Wozencroft, K., Campbell, M., Orel, A., & Kimpton, M. (2015). University students' intentions to report cyberbullying. *Australian Journal of Educational & Developmental Psychology*, 1-12. Retrieved from https://files.eric.ed.gov/fulltext/EJ1070770.pdf

Wu, M., Xiong, S., & Iida, H. (2016). *Fairness Mechanism in Multiplayer Online Battle Arena Games.* China: Shuo Xiong. Retrieved from https://www.researchgate.net/publication/309662487_Fairness_Mechanism_in_Multiplayer_Online_Battle_Arena_Games

Xu, Z., Turel, O., & Yuan, Y. (2017). Online game addiction among adolescents: motivation and prevention factors. *European journal of information system* , 321-333. Retrieved from https://orsociety.tandfonline.com/doi/pdf/10.1057/ejis.2011.56?needAccess=true

Yates, J. (2006). 'You Just Don't Grass': Youth, Crime and 'Grassing' in a working class community . *The National Association for Youth Justice* , 195-210. Retrieved from https://journals.sagepub.com/doi/pdf/10.1177/1473225406069494

Yee, N. (2006). Motivations for Play in Online Games. 772-775. Retrieved from https://www.liebertpub.com/doi/pdf/10.1089/cpb.2006.9.772

Yoon, S. (2015). *Why Do Victims Not Report?: The Influence of police and criminal justice on teh drak figure of crime .* New York : CUNY Academic Works. Retrieved from https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=2209&context=gc_etds

Zeifman, I. (2015, 04 20). *Why Lizard Squad and others target game servers with DDoS attacks*. Retrieved from VB Games: https://venturebeat.com/2015/04/20/why-lizard-squad-and-others-target-game-servers-with-ddos-attacks/

Zhao, C. (2018). Cyber Security Issues in Online Games. Wuhan: AIP Publishing. Retrieved from https://aip.scitation.org/doi/pdf/10.1063/1.5033679

Appendices

Appendix A- Quantitative Questions

Q6. **While you were at school , how many hours per week did you typically spend playing online video games ?**

- ◯ Less than 5 hours per week
- ◯ From 5 to 10 hours per week
- ◯ From 10 to 20 hours per week
- ◯ From 20 to 40 hours per week
- ◯ More than 40 hours per week

Q7. **For which of the following reasons did you play online video games while you were at school ? (select all that apply)**

- ☐ Communication with existing friends and family
- ☐ Making New Friends
- ☐ Playing in a team
- ☐ Exploring the game world
- ☐ Role playing a character
- ☐ Escaping from Real life problems
- ☐ Fun and relaxation
- ☐ Competing with others
- ☐ Learning the mechanics of the game
- ☐ Advancing in status and power within the game
- ☐ Other (please specify)

Q8. **Were you aware of the risks associated with playing online games ?**

- ◯ Yes (complete Q 9)
- ◯ No (Complete Q 10)
- ◯ Don't remember (Complete Q 12)

Q10. **Which cyber-criminal activity were you most concerned about while playing online games while of school age ? (Select all that apply)**

- ☐ Cyber harassment
- ☐ Online identity theft
- ☐ Hacking
- ☐ Pornography
- ☐ None
- ☐ Other (please specify)

Q11. **Which of the following types of cyber-crime did you experience while playing online games while of school age ? Select all that apply)**

- ☐ Cyber Harassment (Complete Q12 to Q19)
- ☐ Online identity theft (Complete Q20 to Q27)
- ☐ Hacking (Complete Q28 to Q35)
- ☐ Pornography (Complete Q36 to Q43)
- ☐ Other (Please specify and complete Q44 to Q51)

Q12. **How old were you when you first experienced Cyber harassment while playing online games ?**

- ○ 7-10
- ○ 11-14
- ○ 15-18
- ○ 19-21
- ○ 22-25

Q13. **How old were you when you last experienced Cyber harassment whilst still of school age ?**

- ○ 7-10
- ○ 11-14
- ○ 15-18
- ○ 19-21
- ○ 22-25

Q14. **What type of online game were you playing when you experienced Cyber harassment ? (Select all that apply)**

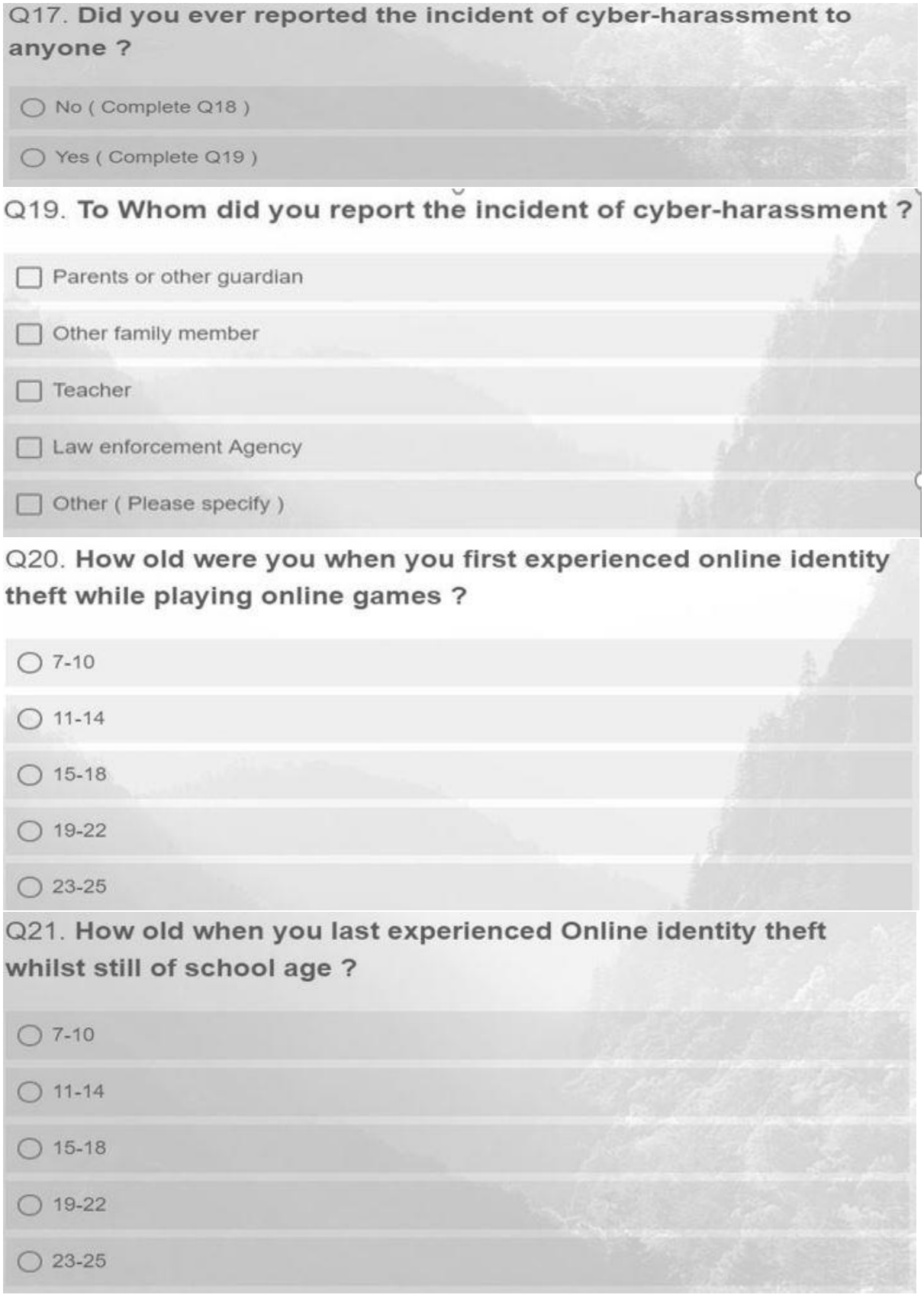
- ☐ MMORPG (Massively Multiplayer Online Role-playing Game)
- ☐ MOBA (Multiplayer Online Battle Arena)
- ☐ RTS (Real Time Strategy)
- ☐ MMO Shooter (Either first or third person)
- ☐ Social Game
- ☐ Other (Please specify)

Q15. **How often did you experience Cyber Harassment While playing online games whilst of school age ?**

- ○ Daily
- ○ Weekly
- ○ Monthly
- ○ Less than once a year
- ○ Annually
- ○ Once

Q16. **Where were you playing online games when you experienced the incident of cyber harassment ? (Select all that apply)**

- ☐ Home
- ☐ Home of a friend or family member
- ☐ School
- ☐ Internet Cafe
- ☐ Other (please specify)


Q17. Did you ever reported the incident of cyber-harassment to anyone ?
No (Complete Q18)
Yes (Complete Q19)
Q19. To Whom did you report the incident of cyber-harassment ?
Parents or other guardian
Other family member
Teacher
Law enforcement Agency
Other (Please specify)
Q20. How old were you when you first experienced online identity theft while playing online games ?
7-10
11-14
15-18
19-22
23-25
Q21. How old when you last experienced Online identity theft whilst still of school age ?
7-10
11-14
15-18
19-22
23-25

Q22. **What type of online game were you playing when you experienced online identity theft ? (Select all that apply)**

- ☐ MMORPG (Massively Multiplayer Online Role-playing Game)
- ☐ MOBA (Multiplayer Online Battle Arena)
- ☐ RTS (Real Time Strategy)
- ☐ MMO Shooter (Either first or third person)
- ☐ Social Game
- ☐ Other (Please specify)

Q23. **How often did you experience online identity theft while playing online games whilst of school age ?**

- ◯ Daily
- ◯ Weekly
- ◯ Monthly
- ◯ Less than Once a year
- ◯ Annually
- ◯ Once

Q24. **Where were you playing online games when you experienced the incident of online identity theft ? (Select all that apply)**

- ☐ Home
- ☐ Home of a friend or family member
- ☐ School
- ☐ Internet cafe
- ☐ Other (please specify)

Q25. **Did you ever report the incident of identity theft to anyone ?**

- ◯ No (Complete Q 26)
- ◯ Yes (Complete Q 27)

Q27. **To Whom did you report the incident of identity theft ?**

- ☐ Parents or other guardian
- ☐ Other family member
- ☐ Teacher
- ☐ Law enforcement agency
- ☐ Other (please specify)

Q28. **How old Were you when you first experienced hacking of your account while playing online games ?**

- ◯ 7-10
- ◯ 11-14
- ◯ 15-18
- ◯ 19-22
- ◯ 23-25

Q29. **How old were you when you last experienced Hacking Whilst still of school age ?**

- ◯ 7-10
- ◯ 11-14
- ◯ 15-18
- ◯ 19-22
- ◯ 23-25

Q30.
What type of online game were you playing when you experienced Hacking of your account (select all that apply)?

- ☐ MMORPG (Massively Multiplayer Online Roleplaying Game)
- ☐ MOBA (Multiplayer Online Battle Arena)
- ☐ RTS (Real Time Strategy)
- ☐ MMO Shooter (either first or third person)
- ☐ Social game
- ☐ Other (please specify)

Q31.

How often did you experience Hacking of the account while playing online games whilst of school age?

- ◯ Daily
- ◯ Weekly
- ◯ Monthly
- ◯ Less than once a year
- ◯ Annually
- ◯ Once

Q32.

Where were you playing online games when you experienced the incident of Hacking (select all that apply)

- ☐ Home
- ☐ Home of a friend or family member
- ☐ School
- ☐ Internet cafe
- ☐ Other (Please specify)

Q33. **Did you ever report the incident of hacking theft to anyone ?**

- ◯ Yes (complete Q 35)
- ◯ No (complete Q 34)

Q35. **To Whom did you report the incident of hacking ?**

- ☐ Parents or other guardian
- ☐ Other family member
- ☐ Teacher
- ☐ Law Enforcement Agency
- ☐ Other (Please specify)

Q36. **How old were you when you first experienced Cyber Pornography while playing online games ?**

- ◯ 7-10
- ◯ 11-14
- ◯ 15-18
- ◯ 19-22
- ◯ 22-25

Q37. **How old were you when you last experienced Cyber Pornography whilst still of school age ?**

- ◯ 7-10
- ◯ 11-14
- ◯ 15-18
- ◯ 19-22
- ◯ 22-25

Q38.

What type of online game were you playing when you experienced Cyber Pornography (select all that apply)?

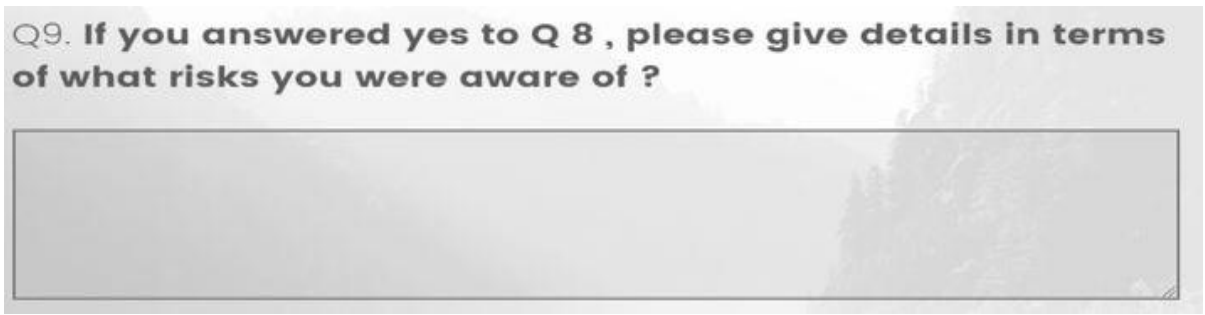
- ☐ MMORPG (Massively Multiplayer Online Role-playing Games)
- ☐ MOBA (Multiplayer Online Battle Arena)
- ☐ RTS (real Time strategy)
- ☐ MMO Shooter (Either First or third person)
- ☐ Social Game
- ☐ Other (Please specify)

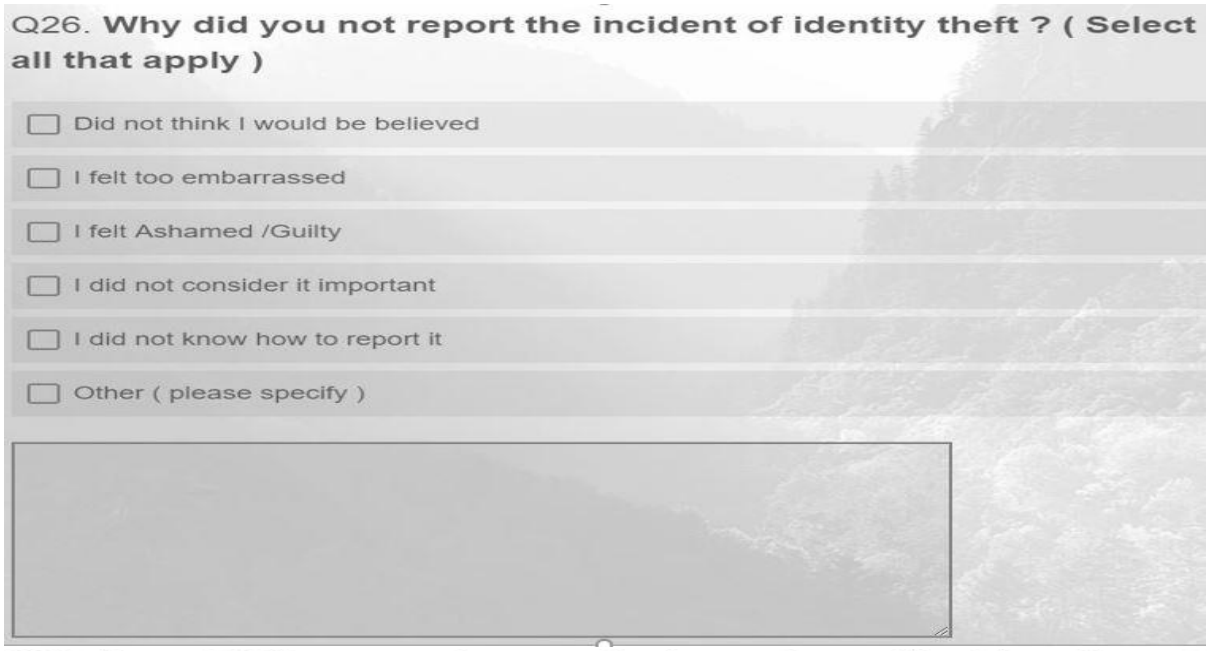
Q39.

How often did you experience Cyber Pornography while playing online games whilst of school age?

- ◯ Daily
- ◯ Weekly
- ◯ Monthly
- ◯ Less than once a year
- ◯ Annually
- ◯ Once

Appendix B – Qualitative Questions




Q26. Why did you not report the incident of identity theft ? (Select all that apply)
Did not think I would be believed
I felt too embarrassed
I felt Ashamed /Guilty
I did not consider it important
I did not know how to report it
Other (please specify)


Q28. How old Were you when you first experienced hacking of your account while playing online games ?
7-10
11-14
15-18
19-22
23-25


Q34. Why did you not report the incident of hacking ? (Select all that apply)
Did not think i would be believed
I felt too embarrassed
I felt ashamed/guilty
I did not consider it important
i did not know how to report it
Other (please specify)


Q42. Why did you not report the incident of cyber pornography? (Select all that apply)
Did not think i would be believed
I felt too embarrassed
I felt ashamed/Guilty
I did not consider it important
I did not know how to report it
Other (Please specify)

Appendix C of this thesis has been removed as it may contain sensitive/confidential content