Correlates and predictors of online victimisation among undergraduate students attending a South African university

Sarah Ashley Parsons

© University of Pretoria

Correlates and predictors of online victimisation among undergraduate students attending a South African university

by

Sarah Ashley Parsons

A dissertation submitted in fulfilment of the requirements for the degree

Magister Artium (Criminology)

In the Department of Social Work and Criminology

at the

University of Pretoria

Faculty of Humanities

Supervisor: Prof. F. Steyn

Co-supervisor: Ms. L. Sadiki

December 2021

© University of Pretoria

Declaration

I, Sarah Parsons, hereby declare that the dissertation '*Correlates and predictors of online victimisation among undergraduate students attending a South African university* submitted in fulfilment of the degree MA (Criminology) at the University of Pretoria is my own independent work and has not previously been submitted for a degree at another university. In addition, I declare that all sources that I have used or quoted have been indicated and acknowledged.

Sarah Parsons

5 December 2021

Date

© University of Pretoria

Acknowledgements

I would like to express my sincere appreciation to the following people:

- The survey respondents who shared their experiences of online victimisation.
- The University of Pretoria for providing me with the opportunity to continue my postgraduate education.
- A very big thank you to my supervisor, Prof. Steyn, for his insight and guidance and for continually encouraging and supporting me throughout the entire duration of the research process.
- To Ms. L. Sadiki, my co-supervisor, thank you for your advice and willingness to always help.
- A heartfelt thank you to my family, Angie, Trevor and Amy, for their unconditional love. Thank you for motivating me and giving me the strength and courage to finish this year.
- A special thanks to Devan Kerr for believing in me and helping me push through the difficult times.
- To Charlene Birkenstock, thank you for always being there to help and motivate me. I would not have been able to get through this process without you. Your friendship is invaluable.

© University of Pretoria

Abstract

Technological advances continue to shape the world and technology has become a fundamental aspect of everyday life. University students rely on the internet for their academic and social lives, to such an extent that social media has become their primary means of communication. As a result, university students have been recognised as one of the most vulnerable groups in society to fall victim to online victimisation. Although there has been a growing interest in online victimisation, there is a lack of knowledge regarding the phenomenon among South African university students. Therefore, the study set out to describe undergraduate students' access to and use of social media and other electronic platforms through which online victimisation can take place, identify correlates and predictors to construct a profile of undergraduate students who are more likely to experience online victimisation, and determine the nature and extent of and responses to online victimisation among undergraduate students.

The study made use of quantitative data that was descriptive in nature. Data was collected by means of a self-administered questionnaire and 1 001 students who were enrolled for undergraduate Criminology modules at a South African university participated in the survey. Logistic regression and chi-square tests were used to determine relationships, differences and similarities between variables. Evident from the empirical results and corroborating existing literature, respondents were typically between the ages of 19 and 21, mostly female and most commonly from the White and Black population groups. Furthermore, the survey found that the majority of respondents used the internet daily, typically spending four or more hours per day on the internet for study, social media or entertainment purposes.

The survey showed that students from high-income backgrounds were more likely to experience crimes such as identity fraud and the media being used as a slandering tool. In terms of gender, women were more likely to experience crimes that could have detrimental personal consequences such as crimes linked to cyberstalking, online harassment and cyberbullying. Men and students in their third year of university were more susceptible to falling victim to receiving a virus, and lastly, students living in a residence had their personal photos shared more frequently than those living with their family or on their own. The study further reports on the responses to online victimisation, with the most common response being ignoring the harasser. The researcher recommends that future research includes qualitative methods in order to gain a deeper understanding of online victimisation experiences.

Key terms: victimisation, undergraduate students, online crime, correlations, predictors

© University of Pretoria

Table of contents

© University of Pretoria

© University of Pretoria

© University of Pretoria

List of tables

© University of Pretoria

List of diagrams

© University of Pretoria

Chapter 1: Introduction and purpose

1.1 Introduction

South Africa has a total population of more than 58.93 million people and 62% of the population use the internet. Through the advancement of technology, the use of social media networking sites has significantly increased, whereby in 2021, 22.89 million individuals are reported to be social media users (Lama, 2020). It is indisputable that the internet has changed the world and has become a fundamental aspect of everyday life (Akhter, 2020: 2). The internet and social media platforms offer numerous benefits to society by providing increasing social, economic, communication and globalisation opportunities (Harris & Steyn, 2018: 15). Usage of the internet is especially advantageous for university students, as they can benefit academically and socially. Students have more access to information found within online library websites, online databases consisting of scholarly journals and newsgroups (to name a few). Furthermore, social media has become the primary means of communication between university students and their lecturers, family, friends and classmates (Sehlule, 2018: 37). Despite the benefits linked to the internet, the advancement of technology has paved the way for a new dimension in crime and victimisation to take place, known as online victimisation.

The study examines online victimisation experiences among undergraduate students attending a South African university. The study uses a quantitative research approach to determine students' access to and use of the internet and whether factors such as gender, academic year level, economic household status, and living arrangements act as potential predictors for online victimisation. Furthermore, the study investigates the responses to online victimisation among undergraduate students. Although substantial research has been conducted that focuses on online victimisation, it typically targets high school students or victimisation that takes place within an international context. Therefore, the overall aim of the study is to address the gap in research concerning online victimisation among undergraduate students attending a South African university and develop a better understanding of the unique crime typology that is rapidly occurring in the country.

1.2 Origin of the study

The researcher obtained a Bachelor of Arts Honours degree in Criminology at the University of Pretoria in 2020, whereby she wrote a quantitative research report as part of one of her modules. As a result of wanting to further her studies, the researcher approached the

© University of Pretoria

Department of Social Work and Criminology and successfully applied for the Masters of Arts degree in Criminology. However, as the Coronavirus pandemic spread across South Africa, the university was forced to shut down due to lockdown level restrictions, implemented from the 26th March 2020 to the present day (South African Government, 2021). As a result, all contact sessions, consultations, and learning took place online. Online learning poses two challenges for postgraduate students: firstly, there is a difficulty in gaining access to study populations for research purposes, and secondly, online surveys result in fairly low response rates. For example, as part of the Covid-19 International Student Well-Being Study, an online questionnaire was sent to 2 215 students in the Faculty of Humanities yet only 322 completed the questionnaire resulting in a response rate of 15% (Sadiki & Steyn, 2020: 154). With this in mind, the researcher was provided with an opportunity to conduct secondary data analyses of an existing data set that had not been published or used for a postgraduate degree.

Secondary data analysis entails the analysis of an existing data set. It is an empirical exercise that applies the same basic research principles as studies that use primary data sets (Johnston, 2014: 619). There are many advantages and disadvantages of using secondary data. Advantages of secondary analysis include that it is less time-consuming (Davis, Wladkowski & Mirick, 2017: 115) and cost-efficient (Mahoe, 2004: 36). On the other hand, one major disadvantage of secondary data analysis is that the researcher does not design the survey, as they were developed by somebody else (Mahoe, 2004: 36). Using secondary data analyses is an acceptable research approach applied both internationally and locally. For example, a study was conducted that involved an existing dataset and used information routinely collected on young people referred to the Maudsley Hospital in London (Khalid, 2012: 2). Another example is a study that focused on the differences within specific temperament traits or emotional processing bias. The study involved 431 first-year psychology students at a university in South Africa (Muller, 2011: 3).

1.3 Research rationale

The internet is one of the most important tools of communication. Various social media platforms exist and are commonly used amongst students in everyday life (Turan, Polat, Karapirli, Uysal & Turan, 2011: 21). Such social network sites significantly influence the nature of how individuals interact with one another, which may not always be positive (Kokkinos, Baltzidis & Xynogala, 2016: 840). As any person can use social media at any hour during the day and night, it has created an opportunity for individuals to take advantage of such accessibility (Crosslin & Golman, 2014: 14). Individuals may engage in online victimisation due to the perceptions of online anonymity, being unrestricted and the ease of accessing social

© University of Pretoria

networking sites whilst harm can be achieved without any physical interaction (Carter, 2013: 1230).

The extent of online victimisation varies across local and international contexts. For example, research among 254 third-year students attending a Turkish state college found that 81.1% had received harassing emails or instant messages. Additionally, 61.4% indicated that they received unwanted and non-consensual content from others while attending the university (Akbulut & Eristi, 2011: 1162). Another example of research conducted was among 342 undergraduate students attending a university in the United States of America (USA). The study found that 43.3% of the respondents indicated they had experienced some form of online harassment during the past two years and 24.0% indicated that they were harassed by someone they knew (Lindsay & Krysik, 2012: 710).

Some insights have been developed regarding the correlates and predictors of online harassment. For instance, in terms of gender differences in victimisation, research among 288 university students in Hong Kong found that more than half of the male respondents indicated that they had committed cyberbullying, compared to very few females (Xiao & Wong, 2013: 44). However, MacDonald and Roberts-Pittman (2010) found no gender difference in cyberbullying behaviour. Thus, due to such anomalies, further investigation should be conducted in order to determine gender victimisation. Lastly, Gibb and Devereux (2014) found that male college students, who received high scores on subclinical measures of psychopathy, and who have fallen victim to online bullying themselves were more likely to perpetrate cyberbullying.

Research studies have also found that experiencing online victimisation may result in poor mental health and could give rise to behavioural problems. For example, research among 472 students found that cyber victimisation was associated with depression, inappropriate conduct and emotional issues, feelings of unsafety, physical pain and substance misuse (Dooley, Shaw & Cross, 2012: 276). Turan et al. (2011) identified that more than half of the respondents were negatively affected by cyberbullying. Although there is some knowledge on the effects of online victimisation, a better understanding of students' experiences is needed to determine the potential impact it has on victims (Crosslin & Golman, 2014: 14).

It is essential to contextualise the proposed study alongside a previous investigation into student victimisation conducted in the Faculty of Humanities at the University of Pretoria. In 2016, a self-administered survey was conducted to describe the victimisation experiences of

© University of Pretoria

853 undergraduate students. The research found that only 5.4% of the respondents answered yes to having experienced online harassment/bullying, and no differences were found between male and female respondents (Department of Social Work & Criminology, s.a.). Such results show an anomaly, as they are relatively low compared to international research. However, such difference could be due to the underreporting of online victimisation among undergraduate students (Gibb & Devereux, 2014: 8).

In South Africa, very little is known about university students' experiences as victims of online victimisation. For instance, when entering key search words such as "student", "university", and "online victimisation" in the University of Pretoria's online library, only sixteen articles were suggested. Of these articles, the majority dealt with online victimisation in secondary education (i.e., schools), and only four articles focus on the online victimisation of international university students. What is especially concerning is that no information is provided that focuses on the online victimisation of university students within a South African context. By neglecting to focus on South African university students as vulnerable targets to online victimisation, it results in a lack of understanding of how they experience and respond to such victimisation. Researchers need to examine how online victimisation impacts university students, as adolescents have been found to suffer from detrimental consequences due to being victimised. For example, in 2021, a tenth-grader overdosed on pills after a video of her being bullied went viral (Adams, 2021).

Furthermore, in South Africa, there are officially 21 crime categories that are covered and presented by the South African Police and Victims of Crime Statistics (Governance, Public Safety and Justice Survey, 2020: 2). However, online victimisation is not one of them. Overall, due to the little knowledge available and lack of understanding regarding online victimisation among South African undergraduate students, there is a clear need for further investigation, thus highlighting the necessity of the research. Subsequently, the research question of the study is: What are the experiences of online victimisation among undergraduate students attending a South African university?

1.4 Aim and objectives

The aim of the study was to determine the experiences of online victimisation among undergraduate students attending a South African university. In order to achieve the aim, the following objectives were pursued:

© University of Pretoria

- Describe undergraduate students' access to and use of social media and other electronic platforms through which online victimisation can take place.
- Identify correlates and predictors in order to construct a profile of undergraduate students who are more likely to experience online victimisation.
- Determine the nature and extent of and responses to online victimisation among undergraduate students.

1.5 Value of the research

Attending university is an important step in students fulfilling their life goals. Universities offer a wide range of opportunities and a sense of independence that encourages students to understand better who they are. However, if a student experiences online victimisation, far-reaching negative consequences may completely alter their university experience. The study aims to expand and build on existing findings and to develop further a deeper understanding of online victimisation that specifically takes place in universities. Due to the limited amount of knowledge available, the study aims to fill the knowledge gap between online victimisation among adolescents within an international context that is presently available and the much-needed research regarding online victimisation experienced by undergraduate students attending a South African university. The study is also of significant value as it assists criminologists to gain a better insight into the correlates and predictors of online victimisation by examining the differences in gender, academic year levels, economic household statuses and living arrangements. Therefore, developing a profile of undergraduate students who are more likely to fall victim to online victimisation. By establishing a profile of likely victims, the study proves valuable as such observations can prevent future students from experiencing the impact of victimisation.

The study's findings will provide researchers with basic knowledge and a point of reference to conduct future research and can be used to inform policies within the various universities in South Africa. Although many limitations have been identified when attempting to apply the traditional victimology theories and models to online victimisation, the study is valuable, as it provides a comprehensive, integrated model, which can be used as a foundation for future theories to be built upon.

1.6 Definition of concepts

The key concepts that are used in and are relevant to the study are defined below.
Universities can be defined as higher learning institutions that provide facilities for teaching

© University of Pretoria

and research and are authorised to grant academic degrees (Merriam-Webster, 2021). Universities can further be defined as institutions that bring all individuals to a high level of intellectual development in various professional disciplines. They also signify a community of people engaged in study and research (Alemu, 2018: 211). In the study, universities refer to a place where students may be at greater risk of online victimisation.

A student can be defined as a person engaged in study, devoted to learning and, seeking knowledge from professional teachers or books. A student may be someone who attends a university or college (Webster Dictionary, 2021). Furthermore, a student can be defined as any person, regardless of age and gender, enrolled in a university and receives an education from professionals (Law Insider, 2021). In the study, a student refers to an undergraduate student attending the University of Pretoria.

Gender refers to the social attributes and opportunities associated with being male and female that are constructed and learned through socialisation (United Nations, 2012). Gender includes the behavioural, cultural or psychological traits typically expected and associated with one sex (Merriam-Webster, 2021). In the study, gender refers to the social characteristics associated with being male or female.

Victimisation is defined as the process whereby a person suffers harm through the violation of intentional criminal laws and recognised norms related to human rights (National Policy Guidelines for Victim Empowerment, 2007: 29). A distinction is made between primary and secondary victimisation. Primary victimisation refers to an individual victim who experiences harm from a face-to-face offence, is threatened or has property stolen or damaged (Meadows, 2007: 23). Secondary victimisation can refer to the processes, actions and omissions that may intentionally or unintentionally contribute to the re-victimisation of a person who has experienced a traumatic incident. Re-victimisation may occur through the victim not being believed, blaming the victim and experiencing a lack of support services to assist the victim at an interpersonal, institutional and social level (South African Victims' Charter, 2008: 23). In the study, victimisation refers to the harm or humiliation that victims experience, which is perpetrated through electronic platforms.

Online victimisation includes a variety of behaviours that inflict harm, such as posting derogatory and belittling remarks and images through the use of computers, cell phones and other electronic devices. Online victimisation may be experienced in one incident or repeatedly over time (Tynes, Rose & Williams, 2010). Online victimisation may be seen as an umbrella

© University of Pretoria

term that includes various electronic deviant actions (Marret & Choo, 2017). In the study, online victimisation refers to cyberbullying and online harassment through online social media platforms.

Cyberbullying is not restricted by time or space and refers to any form of harassment or bullying that occurs through technology or electronic devices. It can take the form of text messages, direct messages, pictures or videos, emails and can occur across various social networking sites (Harris & Steyn, 2018: 17). Cyberbullying can also be defined as the intentional and repetitive aggressive behaviour perpetrated by an individual, that takes place individually or by a group using internet technology, against a person who is not able to defend themselves (Ševčíková, Šmahel & Otavová, 2012: 323). In the study, cyberbullying refers to bullying that takes place online through various social media platforms. The perpetrator may, for example, harass, impersonate, exclude or post information about their victim online for a large audience to see.

Online harassment can be regarded as threats or other offensive behaviour targeted directly at an individual through new online channels, such as text messaging or posted online for others to see (Jones, Mitchell & Finkelhor, 2012: 54). Online harassment can simply be referred to as repeated messages that are threatening, insulting or harassing (Lindsay, Booth, Messing & Thaller, 2016: 3176). In the study, online harassment refers to targeting another person online through unwanted and harmful behaviour.

Social media can be defined as a collection of websites and applications designed to build and enhance online communities for networking and sharing information (Osborne-Gowey, 2014: 55). Social media also refers to a social instrument of communication that can be characterised through participation, openness, conversation, community and connectedness (Veil, Buehner & Palenchar, 2011: 115). In the study, social media refers to online platforms whereby individuals are provided with opportunities to interact and communicate with one another online rather than in person.

A victim is defined by the Victim Empowerment Programme of the Department of Social Development (2020) as persons who, individually or collectively, suffers harm (including physical or psychological injury), emotional suffering, economic loss or substantial impairment of their rights through acts or omissions that violate a person's human rights. A victim is an individual against whom a crime has been committed and can also include indirect victims, for example, family members. A person may be considered a victim regardless of whether the

© University of Pretoria

offender is identified, apprehended, convicted or prosecuted (National Policy Guidelines for Victim Empowerment, 2007: 3). In the study, a victim refers to a person(s) who has suffered harm as they have experienced online victimisation committed by a person known or unknown on any online platform.

1.7 Summary of the research methods

Although chapter four consists of a detailed discussion of the research designs and methods used in the study, a brief overview must be included as part of the introductory chapter. A quantitative research approach is the systematic empirical investigation of a social phenomenon that counts and measures a respondent's human behaviour without being influenced by emotional and subjective bias (Burns & Grove, 2005: 23-24). The research approach chosen consisted of secondary data and was used to numerically count and measure the nature and extent of online victimisation among undergraduate students (Kumar, 2011: 13). The study was descriptive in nature, and basic research was carried out, as the study aimed to understand better the experiences of online victimisation rather than to solve practical problems (De Vos, Strydom, Fouché & Delport, 2021: 105). Furthermore, a non-experimental research design was chosen, namely a correlational survey study, as the aim is to identify and explore relationships between existing variables (Wilson & Joye, 2019:2). The quantitative data was collected via self-administered questionnaires, whereby 1 001 students participated and received a two-page questionnaire with 26 closed-ended questions to complete (De Vos et al., 2021: 286-301).

The data were manually coded, recorded and analysed using the Statistical Package of the Social Sciences (SPSS). The Hosmer and Lemeshow test of the regression was also performed to determine possible predictors in online victimisation among undergraduate students. The quantitative data will also be analysed by employing a Pearson's chi-square test with effect sizes (Cramer's *V*), which is a significant test of the relationships between categorical variables (Salkind, 2011: 138). Cronbach's alpha was used to ensure the quality of the data, whereby the alpha coefficients of the scales were above the acceptable level (Taber, 2017: 1273-1274). Reliability and validity were also measured to ensure the quality of the data (Given, 2012: 715). A pilot study was conducted, proving that the questionnaire did not take too much time. The pilot study was able to assist the researcher in developing, refining, and testing the measurement tools and processes (Kumar, 2011: 11). Lastly, various ethical considerations were accounted for, such as voluntary participation, no harm to the respondents and informed consent.

© University of Pretoria

1.8 Structure and layout of the dissertation

Chapter one consists of the introductory chapter, which provides a brief overview of the research topic under investigation. It includes the origin, rationale, aim and objectives, and the value of the research. In addition, the key concepts of the study are defined, and the research methods are summarised.

Chapter two includes the literature review, which discusses previous research concerning the online victimisation experiences of students. The literature review chapter consists of defining key concepts, matters of typology, the extent of the phenomenon, aetiology of online victimisation, the profiles of the victims, impact of offences and responses to online victimisation, including available legislation and policies.

Chapter three presents various victimology theories and models to better understand the online victimisation of undergraduate students. The chapter consists of victim-oriented theories and perpetrator-oriented theories. Additionally, the chapter discusses numerous shortfalls of each of the existing theories, thus explaining the development of an integrated model to understand online victimisation among undergraduate students in a South African context.

Chapter four discusses the research methodology that was employed to guide the study. The chapter consists of an explanation of the research approach, research design, research strategy, the sampling procedure, data collection, data analysis, data quality, ethical considerations, and the challenges and limitations of the study.

Chapter five consists of the quantitative empirical results obtained by the study. The chapter highlights the key findings of each of the observations presented in the form of tables.

Chapter six includes a discussion of the empirical results in relation to the aim and objectives, evidence and theory. The results are compared to available evidence previously provided by the literature review, and all anomalies are discussed. The chapter is followed by recommendations made for practice, policy, theory and future research. The dissertation ends with the relevant reference list and appendixes.

1.9 Summary

Although there are many benefits to the advancement of technology and increased use of

© University of Pretoria

social media, various consequences can be identified, such as the development of a unique crime typology, known as online victimisation. The study aims to decrease the gap in knowledge regarding the correlates and predictors of online victimisation among undergraduate students. By highlighting the aim and objectives, important definitions and the origin and rationale, the study can expand criminologists' insights into the nature, extent and consequences of online victimisation. Furthermore, a deeper understanding can be gained from constructing a profile of undergraduate students that are more likely to be victimised. Finally, by presenting a summary of the research methods and the layout of the dissertation, it helps provide direction on how the study was carried out and conducted.

© University of Pretoria

Chapter 2: Literature review

2.1 Introduction

Throughout the past several decades, various advances in technology have resulted in a change in everyday life worldwide. Generation Z consists of individuals born between 1995-2012 and who have grown up in a world with constant internet technology and connectivity (Prakash & Rai, 2017: 115). Social media and the use of the internet have become a fundamental part of students' lives, which has brought about several advantages to how they communicate, interact and learn. However, a new unique crime typology has emerged through technological advances and is rapidly taking form in South Africa. Such phenomenon is known as online victimisation. In the chapter, a review of the available literature on online victimisation among university students is provided. The conceptualisation of online victimisation is discussed, whereby various key definitions are included. The chapter will examine the typologies of online victimisation within a South African and international context, the profiles of the victims and the impact the offence has on the victims. Finally, the chapter will include a discussion on responses to online victimisation, including issues of legislation and university policies, within a local context. It is important to note that the chapter will focus only on factors relating to students/young adults attending a university and excludes adolescents, except for in extreme cases whereby adolescents commit suicide due to online victimisation. Furthermore, the chapter acknowledges a lack of information regarding online victimisation. When searching on Google Scholar and the university's online library platform, no information was revealed concerning online victimisation among undergraduate students attending South African universities.

2.2 Understanding the internet and crime: concepts and dimensions

In the following section, the researcher provides insight into online victimisation by familiarising the reader with an understanding of the internet and crime. Various concepts are identified and defined, such as social media, computer crime/cybercrime, online victimisation, online harassment, cyberbullying and cyberstalking.

2.2.1 Social media

Although scholars assume an understanding of social media based on existing technology, there is no consensus regarding the definition of the phenomenon (Carr & Hayes, 2015: 46).

© University of Pretoria

There is no general consensus because of the fast-changing nature of and the complex characteristics that make up social media, making it too complicated for scholars to define (Bayer, Triệu & Ellison, 2019: 3). However, without an agreed-upon definition, it can result in multiple explanations of the concept, which can then make it difficult to establish a mutual understanding to guide theory and research (Carr & Hayes, 2015: 48). Previously, social media has been defined as digital technologies that provide its users with opportunities to connect, interact and create and exchange content (Kaplan & Haenlein, 2010: 61). However, such definition was regarded as problematic, as it can be applied to other communication technologies, such as email. Therefore, a new definition was required that encompassed social media's unique technological and social aspects (Carr & Hayes, 2015: 48).

Within the past decade, a more complex definition of social media can be found, whereby it refers to any interactive communication channel that allows for two-way feedback. Furthermore, it can be characterised by its possibility of 'real-time' interaction, reduced anonymity, a sense of closeness (regardless of the physical difference between users) and the ability to engage within the online platform whenever it best suits the users (Kent, 2010: 645). Other qualities of social media can include that it is inexpensive and largely accessible to people worldwide (Siddiqui & Singh, 2016: 71). In addition, the definition of social media can be expanded to include that it is internet-based channels consisting of broad and narrow audiences who obtain value from the user-generated content and the perception of interaction with others (Carr & Hayes, 2015: 50). Finally, another author broadly defines social media as a set of interactive internet applications that facilitates any person, or group of people to create, use, build relationships and share content (Davis & Jurgenson, 2014: 477).

There is no denying that social media has become significantly popular, widespread and individualised and is regarded as a source to serve many functions and roles in everyday life (Dyer, 2020: 15-16). For instance, social media provides a space for participation and interaction with other users, who may be friends, family members or strangers who share common interests (Manning, 2014: 1158). Furthermore, it serves as a platform for users to self-reflect, share news, find information, be entertained and perform work functions (Manning, 2014: 1161). Social media can take place in various forms, such as email (electronic mail), text messages, and blogs, and can include social networking sites, such as Facebook or Instagram (Manning, 2014: 1159-1160). Social networking sites are regarded as a subclass of social media and can be defined as any form of social interaction using technology that consists of a combination of words, photographs, videos or audio (Sehlule, 2018: 7). Four elements encompass social networking sites. Firstly, the profile, refers to how users portray themselves through their profile pictures, statuses or other personal information. Secondly,

© University of Pretoria

networks refer to the opportunity's users have to engage and connect with a wide range of people. Thirdly, streaming refers to the content displayed on the networking platforms, and lastly, messages refer to chats, texting, direct messaging and mobile email (Bayer, Triệu & Ellison, 2019: 11 & 13).

2.2.2 Computer crime/cybercrime

Due to the advancement of internet technology, unlimited opportunities are presented to criminals to exploit and commit crimes. Such opportunities are possible because little effort has to be made to commit a crime online, and there are little chances of detection, as policing in cyberspace is unable to keep up with the sophisticated techniques employed by cybercriminals (Ndubueze & Abdullahi, 2019: 19). Much like social media, various authors hold different views on what computer crimes entails. The disagreement is based on whether computer crimes should include every crime that involves a computer, and whether traditional crimes, such as stalking, should be considered a computer crime or if it should be considered a crime that incorporates technology as a means of execution (Kunz & Wilson, 2004: 6).

Furthermore, there is much debate over the differences between computer crimes and cybercrimes. Some authors argue that the two concepts mean the same thing, whereas others believe that it is necessary to distinguish between the two concepts, as computer crimes can be classified as a form of cybercrimes (Choi, 2008: 308). Casey (2000) defines cybercrime as any crime that utilises computers and networks. Thomas and Loader (2000) expand such a definition by stating that cybercrimes are computer-mediated activities conducted through electronic networks and are regarded as illegal. Overall, Choi (2008) proposes that cybercrimes cover a range of crimes, including computer crime, whereby such criminals have more than a basic level of computer knowledge, and merely utilise computers as a tool to facilitate their illegal actions (Choi, 2008: 308 & 309). Computer crimes are referred to as activities that violate the law and make use of electronic systems as a means to disrupt the security of computer systems and computer data (Business Software Alliance, 2004). Despite the debate over what constitutes a computer crime, there is a general consensus regarding the main elements that make up such crime. For instance, computer crimes consist of criminals who use computer resources to obtain goods or resources illicitly, or to cause harm to another person(s) or organisation (Kunz & Wilson, 2004: 9).

Cybercrimes can occur as a direct result of the efficiency and ease of the internet. Typically, there is a clear physical distance between offenders and victims in cybercrime, whereby the two parties can be separated by different countries worldwide. However, the physical distance

© University of Pretoria

between the offender and the victim is now replaced with a shared network (Henson, Reyns & Fisher, 2016: 556). Moreover, within cybercrimes, computers can be the target or be used to target a victim. Various offences exist specifically due to the accessibility of computer resources, such as computer fraud (which includes identity fraud), computer invasion of privacy and harmful content crimes (including online harassment, cyberstalking, spam and sending viruses) (Kunz & Wilson, 2004: 11).

2.2.3 Online victimisation

One of the most fundamental characteristics of the twenty-first century is the continued advancement of internet technologies and the significant impact it has on several aspects of a student's academic and social lives (Ndubueze & Abdullahi, 2019: 19). However, the movement from face-to-face communication to online communication (Harris & Steyn, 2018: 16) has resulted in endless opportunities for criminals to exploit and commit crimes. Such opportunities are escalated because cyberspace is considered an uncontrolled world, with no mediators to intervene when online victimisation occurs (Akhter, 2020: 4). Online victimisation is a relatively new and unique form of victimisation. Although there is no consensus among scholars regarding what online victimisation is, authors agree that it is an umbrella term that refers to intentional digital harm, teasing, threats, harassment, bullying or stalking carried out through online platforms (Akhter, 2020: 3). Grigg (2010) further expands on such definition by adding that it is the intentional harm caused through electronic means to a person or group of people, whereby such actions are considered offensive, hurtful, derogatory or unwanted, by the victim, who is unable to defend themselves (Grigg, 2010: 203).

Online victimisation differs from traditional, offline victimisation in various ways. As mentioned, cyberspace is an uncontrollable environment where offenders have plentiful opportunities to behave in any way they want, which is generally atypical of their offline behaviour. The reason is that, unlike in real life, the offenders do not always have to deal with the immediate consequences of their actions (Akhter, 2020: 4). Furthermore, repetition does not necessarily refer to a person's actions occurring repeatedly; but instead, it refers to multiple online users posting harmful messages to one victim or one message being viewed by various users at the same time (Akhter, 2020: 4). Online victimisation is further described as a unique crime typology due to two more characteristics of the internet. Firstly, the internet offers the perception of anonymity, which reduces the empathy of the offender and presents them with an opportunity to engage in deviant behaviours as they may feel invincible by being able to conceal their identity. Lastly, due to the internet being easily accessible, the offender has ample choice in targeting as many victims as they want (Akhter, 2020: 4).

© University of Pretoria

2.2.4 Online harassment

Despite definitions of online harassment somewhat varying across different studies, it is typically described as any occurrence in which an offender annoys, torments, or threatens the victim online, primarily conducted through the use of technological channels, such as online messengers or social networking sites, where the public can see (Henson, Reyns & Fisher, 2016: 557). Online harassment can further be understood as unwanted contact by offenders, negatively impacting the victim's livelihood, well-being, and mental or emotional state (Kunz & Wilson, 2004: 199). Such harassment can typically consist of repeated events whereby the online environment encourages and provides a space for offenders to have more than one hostile interaction with users online (Jones & Mitchell, 2016: 573). Additionally, authors describe it as a form of cyber violence, as it includes actions such as posting defamatory or embarrassing personal information about others, impersonating others, spreading rumours, being called mean names, sending unwanted jokes, stalking people online, and threatening violence and physical and emotional abuse (Kennedy & Taylor, 2010: 5). Such type of interpersonal violence can result in the victims feeling fear, distress and humiliation (Bossler, Holt & May, 2012: 502) as the online harassers can post, comment or share pictures, statuses and videos to large online audiences, at any time of the day (Jones & Mitchell, 2016: 577).

Online harassment is considered a significant and widespread issue that is increasing rapidly as it continues to evolve (Hendricks, Tsibolane & van Belle, 2020: 136). The South African Law Reform Commission (2004) identifies two forms of cyber harassment: direct/physical and indirect harassment. Direct harassment includes threats, bullying or intimidating messages sent directly to the victim through electronic platforms (Badenhorst, 2011: 2). Furthermore, it may include sending viruses, threatening non-verbal messages and muting or excluding a person from an online group (Hendricks, Tsibolane & van Belle, 2020: 136). Indirect harassment includes gossiping, spreading rumours, subscribing to unwanted online services and sharing the victim's personal information on various sites and online platforms (Badenhorst, 2011: 2). A common form of online harassment, especially in South Africa, is online sexual harassment, which refers to receiving unwanted sexual material on the internet by an offender, either in the form of direct messages, videos, posts, jokes or threats (Sehlule, 2018: 7). Finally, online harassment differs from offline harassment in many ways, such as its perception of anonymity, being unconstrained by time, having a larger viewing audience, lack of physical interaction, high incidence of violation and the variety of platforms that can be used to conduct harassing behaviours (Hendricks, Tsibolane & van Belle, 2020: 136).

© University of Pretoria

2.2.5 Cyberbullying

Due to the social change taking place, in the form of technological advances, individuals who cannot adjust to such change are at an increased risk of being victimised by those who can and will use the technology as a digital weapon (Hinduja & Patchin, 2007: 90). For example, the internet has provided the space to accommodate a shift from traditional 'schoolyard bullying' to bullying that takes place online (Dooley, Shaw & Cross: 2012: 276). Such phenomenon is known as cyberbullying, and it is unfortunately not always clearly defined and identified. As a result, individuals may misunderstand how technology can be used as a tool to perpetrate intentional and unintentional acts of cyber aggression and humiliation (Goodno, 2011: 641). The Child Health Promotion Research Centre (2010) defines cyberbullying as over a period of time, one or more offenders use technologies to repeatedly intentionally harm a person who is unable to defend themselves (Dooley, Shaw & Cross: 2012: 276). However, such definition has received two criticisms: firstly, offenders' behaviours are not always intentional, as sometimes the cyberbully may be unaware of the seriousness of their actions; secondly, the offender's actions do not have to occur repeatedly, as one hurtful comment or post can be just as detrimental to the victim (Kota, Schoohs, Benson & Moreno, 2014: 555). For example, if the victim receives a death threat or a credible threat of serious harm (Aftab, 2010).

Despite the disagreement over the definition, authors have agreed that cyberbullying involves a power imbalance between the offender and the victim (Hinduja & Patchin, 2007: 91), which is presented through the perceived anonymity provided by the internet (Schenk, 2011: 3). Cyberbullying is not restricted by time or space, and anyone worldwide can access the internet to commit such hurtful behaviour (Pineiro, 2016: 3). Furthermore, it can be classified as a form of psychological cruelty as it is a more overt form of verbal and written traditional bullying (Mason, 2008: 323). It also differs from offline bullying, as it does not require face-to-face physical interaction, as it can be conducted anonymously online (Schenk, 2011: 2). The National Crime Prevention Council (2010) suggests that cyberbullying can occur through the internet, mobile phones, or social networking platforms, which can be both private or public, whereby the aim is to hurt or embarrass the victim. There are various types of cyberbullying: sending harassing or threatening emails or messages, posting derogatory comments, making physical threats or intimidating a person online. In addition, it can involve spreading rumours or stalking someone online. Lastly, other minor forms of cyberbullying include being ignored, disrespected, excluded or picked on (Hinduja & Patchin, 2007: 91).

© University of Pretoria

2.2.6 Cyberstalking

There is much debate among authors over the definition of cyberstalking for two reasons; firstly, there is a lack of statistics for such crime phenomenon, and secondly, there is no agreed-upon meaning for physical stalking (Abu-Ulbeh, Altalhi, Abualigah, Sumari & Gandomi, 2021: 2). In terms of stalking, it can be defined as harassing or threatening behaviour that an individual repeatedly engages in, such as following a person or making harassing calls. Cyberstalking is thus considered the online version of traditional stalking, whereby it primarily relies on technology to harass, threaten and intimidate victims (Paullet, Rota & Swan, 2009: 641). Despite the confusion regarding the definition, authors have agreed upon three key elements that constitute cyberstalking: 1) repeated unwanted pursuit and/or harassment of an individual; 2) utilising electronic or communication network devices, and 3) aiming to instill fear within a reasonable person (White & Carmody, 2018: 2292). Cyberstalking can take place within a public platform, whereby any online user can witness the offender's actions, and within a private platform, such as through direct messages or receiving computer viruses, whereby only the victim and offender know what is going on (White & Carmody, 2018: 2292). The internet has provided offenders with the freedom to target people they know or strangers and enable them to contact their victims via email, instant messages, phone calls, social networking sites or they can invade the victim's privacy by installing spyware to monitor their online activities (Paullet, Rota & Swan, 2009: 642).

Cyberstalking can be described as utilising technology and the internet, for example, using cell phones or spy technology, to perform a variety of activities, such as finding, monitoring, harassing, threatening or exploiting victims, in order to cause them panic, anxiety or fear (Abu-Ulbeh et al., 2021: 2). Cyberstalking incidents will continue to increase, as the internet provides a safe haven for criminals through the perception of anonymity, no physical contact being needed, the ease of accessing any person who is connected through an electronic device, and there being slight chances of apprehension due to the limitations of the legal systems (Pittaro, 2011: 279). Furthermore, the term cyberstalking can be used interchangeably with online harassment, as the cyberstalker is not a direct threat to the victim but can monitor the victim's activities online and make threats or other forms of verbal intimidation (Paullet, Rota & Swan, 2009: 641). The only difference between the two crime typologies is that cyberstalking must involve repeat pursuit behaviours (Henson, Reyns & Fisher, 2016: 558-559). Cyberstalking may also be known as an extreme form of cyberbullying, as it can be described as a form of emotional terrorism, whereby the offender will utilise technological tools to bully, threaten, harass and intimidate a victim (Schenk, 2011: 2-3).

© University of Pretoria

There is a general consensus regarding what constitutes cyberstalking. Cyberstalking behaviours are premediated, repetitive and aggressive; however, they are not necessarily illegal (Pittaro, 2011: 278). Such behaviours prove themselves to be a danger in the technological world, as they can leave the victims feeling vulnerable, anxious, threatened, and fearful of being physically harmed (Miller & Morris, 2012: 83). There are a wide range of behaviours that make up cyberstalking, for example: receiving unwanted messages that can either be sexual or threatening in nature (Mullen, Pathé & Purcell, 2009: 153); making threats against the victim, their family, friends or colleagues); spreading false accusations; collecting information on the victim either through approaching family or friends of the victim or hacking into their private accounts (Bocij, 2004: 12); impersonating the victim (Bocij, 2004: 13); sharing private or embarrassing information of the victim online (Mullen et al., 2009: 153); encouraging others to harass the victim (known as stalking by proxy); sending viruses to the victim to disrupt their computer systems (Bocij, 2004: 13-14); identity theft (Mullen et al., 2009: 154) and lastly, arranging to meet the victim in an offline setting (Bocij, 2004: 15).

2.3. Typologies and evidence of online victimisation

The section aims to provide a more comprehensive representation of the nature of online victimisation among undergraduate students. The section below will contain a discussion regarding the various typologies of online victimisation of university students, both within an international and local context, by examining existing literature that focused on the phenomenon under investigation. The typologies are clustered into two themes in order to prevent duplication of arguments.

2.3.1 International context

Online victimisation among university students is not an exclusively South African phenomenon. After examining the existing evidence, online victimisation can be found to rapidly be occurring overseas, such as in the USA, Australia and Jordan. There is also a lack of research conducted in South Africa regarding such phenomenon; therefore, it was important for the researcher to examine online victimisation within an international context. Furthermore, to gain a better insight into online victimisation, the researcher needs to examine any similarities or differences between an international and local context.

© University of Pretoria

2.3.1.1 Identity fraud, hacking, distribution of viruses and offenders pretending to be someone else

The advancement of technology has significantly changed how students communicate, live, learn, and conduct various activities around the world. Through such advancements, traditional activities such as banking, dating, shopping, interacting, and entertainment have transformed into activities that students can now complete online (Bossler & Holt, 2011: 317). However, a dark side has emerged as technology continues to evolve; for example, one of the most commonly experienced cybercrimes students encounter is identity fraud. Identity fraud forms part of the larger crime category known as computer fraud, which refers to any fraudulent scheme that utilises one or more elements of the internet, such as email, to achieve such illegal conduct (Kunz & Wilson, 2004: 12). Identity fraud, can further be defined as the acquisition of money, goods, services or other benefits or the avoidance obligations through the use of a fabricated identity, a manipulated identity, or a stolen identity (Seda, 2014: 462). Identity theft, thus, takes place when an individual wrongfully obtains and uses another's personal information without consent or knowledge to commit fraud or theft (Kunz & Wilson, 2004: 13). Typically, victims will have their name, address, identity numbers, or bank account numbers stolen. University students have been identified as a population that is particularly at risk of falling victim to such crime, for example, due to the increased amount of time they spend on the internet and because they are less likely to protect themselves from online identity theft than non-students (Norum & Weagley, 2007: 46).

Norum and Weagley (2007) set out to conduct a study to examine how various internet-related practices could lower the risk of a university student falling victim to identity theft. A total of 7 342 web-based questionnaires were completed by both undergraduate and graduate students attending an American university (Norum & Weagley, 2007: 49). In terms of the respondents' online behaviours, two-thirds (66.5%) reported that they were not financially independent; more than two in three (67.8%) had credit cards; over a quarter (28.6%) did not know how to recognise a secure website and nearly four in five (78.5%) reported that they would often make online purchases (Norum & Weagley, 2007: 54). After running two regression tests, the following key information was found, students who owned their own credit cards and made online purchases from sites that were not necessarily secure had an increased risk of falling victim to identity theft. Furthermore, female students were more vulnerable than male students, as they were less wary about using unsecure sites. Additionally, students who were financially independent were more likely than students from the lowest income backgrounds to engage in protective behaviours to avoid having their identities stolen (Norum & Weagley, 2007: 56-57).

© University of Pretoria

Another common cybercrime experienced by university students is the destruction of data files due to malicious software. Malicious software consists of computer viruses, worms and Trojan horse programmes that can disrupt computer systems and programmes (Bossler & Holt, 2011: 318). Computer viruses provide offenders with the ability to destroy data and gain control over the victim's computer to make a functional replica of itself (Urbarhande, 2011: 1). There are different types of computer viruses, with the most common being file-infecting viruses that attach themselves to executable files, which are files ending with '.com'. Following that is the script virus, which spreads and infects files by taking advantage of victims opening emails or web pages (Urbarhande, 2011: 2). Once the malicious malware has been activated on the victim's computer, the programme can disrupt emails, access private files, delete important information and damage the computer software. Such actions may result in identity theft or hacking into private accounts (Bossler & Holt, 2011: 318). A study conducted in the USA focused on victimisation in cyberspace. A total of 284 university students participated in an online survey (Ngo, Piquero, LaPrade & Duong, 2020: 436) and the following key information was found, two-thirds of the respondents (66.0%) were females, the majority (85.0%) were White and nearly two in five (36%) were married (Ngo et al., 2020: 437). In terms of the respondents specifically experiencing computer viruses, almost half (47%) indicated that their computers were infected with a virus, older respondents were less likely than younger respondents to have received a virus, socialising online with others decreased their chances of experiencing computer viruses by 66%, however, posting phone numbers online increased their risk by almost 250% (Ngo et al., 2020: 440 & 443).

As mentioned, receiving malicious malware can lead to a student's private account being hacked. Originally hacking was defined as computer experts accessing computer systems, programmes and private networks to identify and correct any vulnerabilities (Choi, 2008: 309). However, in more recent times, hacking refers to the unauthorised access of systems, accounts or programmes with the intent to cause damage, steal property, or leave evidence of being able to break in successfully (Choi, 2008: 309). Such a crime can be perpetrated against major online companies or personal social media accounts. If hacking occurs through utilising malicious malware, the offenders will typically attempt to overload online sites with electronic connections to disrupt the services to legitimate users (Kunz & Wilson, 2004: 18). In 2012, a study was conducted in the USA, whereby 42 university students participated in a focus group. The study aimed to discuss the respondents' experiences regarding what actions constitute cyberbullying (Kota et al., 2014: 551). Through the discussion, hacking into private accounts was recognised to be a form of cyberbullying. One participant described how his former partner took over his Facebook profile and posted embarrassing information on his account, without his knowledge, with the intent to embarrass him (Kota et al., 2014: 553).

© University of Pretoria

The National Supplemental Victimisation survey (2018) focused on gathering statistics concerning online harassment, specifically looking at identity theft. According to the survey, 23 million persons aged sixteen and older are estimated to have been victims of identity theft. Furthermore, nearly a fifth of the victims (17.0%) experienced misuse of their personal information, and as a result, they were more likely to experience severe emotional distress. The survey interestingly observed that over half of the victims (51.6%) were females, less than three quarters (71.4%) were White, and only a few (7.6%) were between the ages of 18-24 years old. Finally, the survey reported that most victims did not know their offender, and only a few (7.0%) reported such incidents to the police (NSVS, 2018). In terms of other commonly experienced computer crimes, a survey conducted in USA found that over half of the computer technology breaches (52.0%) in 2019 consisted of hacking. In addition, more than a quarter (28.0%) of computer breaches involved viruses. The survey also found that every 32 seconds, a hacker is attacking someone online and in the last five years, over 500 million online gamers have had their data disrupted. Finally, the survey observed that the vast majority (94.0%) of all viruses were transferred through emails, which thus, makes it the weapon of choice for most cybercriminals (Lazic, 2020).

Through the expansion of the internet and the creation of more social media sites, it is not surprising that many online users' profiles are fake. Offenders who pretend to be someone else online is known as 'catfishing', which can be defined as the intentional misrepresentation of various aspects of an offender by creating a fake profile for personal or financial gain (Mosley, Lancaster, Parker & Campbell, 2020: 2). Catfishing is extremely common, whereby in 2013, Twitter reported that 5% of accounts were fake (Fire, Kagan, Elyashar & Elovici, 2014: 2). Individuals online tend to disclose personal information about themselves to others; however, individuals who are pretending to be someone can use such information to blackmail the victims or to customise spam messages to lure them into malicious websites (Fire et al., 2014: 2). Catfishing is also commonly utilised in online dating, whereby offenders pretend to be someone else to gain attention or acceptance (Mosley et al., 2020: 2). Finally, catfishing can also be employed by predators who use social networking sites to contact victims and develop a relationship with their victims. They will use deception to cover their age and their intentions, which are usually sexual or violent in nature. However, such catfishing is more likely to occur with students who are not in university (Wolak, Finkelhor, Mitchell & Ybarra, 2008: 111-112).

2.3.1.2 Online harassment, cyberbullying and cyberstalking

As internet technology continues to evolve, the way in which individuals conduct their daily

© University of Pretoria

lives and interact socially and professionally with each other has significantly changed. Social networking sites are advancing and are increasingly being used by students as part of their daily routines. However, such advances have also facilitated the emergence of online victimisation, which is reported to be a growing issue in society, whereby university students are more likely to fall victim to (White & Carmody, 2018: 2291). Online victimisation includes various crime typologies, such as online harassment, cyberbullying and cyberstalking, where each interlink and can be used interchangeably.

As mentioned, online harassment can be defined as the unwanted contact by offenders, who annoy, torment, humiliate or threaten a victim online or through the use of electronic devices (Henson, Reyns & Fisher, 2016: 557). A study was conducted at the Luminus Technical University College in Jordan, which aimed to investigate cyberstalking victimisation among university students. Data was collected through administering 757 questionnaires (Abu-Ulbeh et al., 2021: 3-4), whereby the following key information was found, two-thirds of the respondents (66.76%) reported that they had been harassed/annoyed by an offender, and more than half (60.0%) experienced someone pretending to be them without their permission. Additionally, nearly two-thirds (64.84%) received threatening/offensive messages via their emails, and lastly, the survey observed that slightly less than two in five (39.92%) experienced someone posting false information about them (Abu-Ulbeh et al., 2021: 25). When an offender posts false information online about their victims, such conduct is known as spreading rumours. Spreading rumours simply refers to the spread of misinformation, whereby in the past, such victimisation was performed through word of mouth. However, the rise in social media has provided offenders with a bigger platform to create and spread rumours about others that can be viewed or told to a broader audience (Turenne, 2018: 1).

Furthermore, a study was conducted in 2002, which examined online harassment experiences of undergraduate students at the University of New Hampshire, USA. The data was collected through administering a self-report survey to 339 students whereby the following key information was found: in terms of the respondent's demographic characteristics, the average age was 20.34; nearly a third of the respondents (32.2%) were juniors in university (equivalent to a third-year student) and the vast majority (92.7%) were White (Finn, 2004 :475). In terms of the experiences of online victimisation, just over a tenth (12.6%) received repeated messages from someone they did not know, that threatened, insulted or harassed them. Additionally, a few (10.1%) continued to receive repeated messages even after the victim had told their harasser to stop. The survey also found that 10% to 15% of the respondents were harassed online by strangers, acquaintances or former significant others (Finn, 2004: 473). Online harassment can also include the media being used as a slandering tool against a victim.

© University of Pretoria

Due to the increased use of social media platforms, such type of victimisation is becoming more prevalent among university students. For example, a total of 354 respondents completed a survey for a study that aimed to examine online victimisation among university students, that took place via social media sites. The study was conducted at a Southwest university in the USA, whereby the following information was found, nearly a quarter of the respondents (n=85; 24.0%) reported that they had been verbally harassed online and (n=82; 23.2%) stated that verbal derogatory statements were posted about them on social media (Kennedy & Taylor, 2010: 11).

As mentioned, online victimisation and numerous other cybercrimes can be defined in various ways. However, online victimisation crime rates are included in broad crime categories and are available and reported internationally (primarily looking at the USA) (Finn, 2004: 476). In terms of online harassment, the Pew Research Center (2021) surveyed adult participants to determine the nature and extent of online harassment in the USA. Overall, three-quarters of the respondents indicated that their harassment took place over social media. However, social media is not the only online platform where such victimisation can occur. For instance, it can take place on online forums or public discussion sites (25.0%), direct messaging apps (24.0%), online gaming platforms (16.0%), personal email accounts (11.0%) or online dating sites or apps (10.0%). Furthermore, the survey examined the most common online harassment behaviours experienced by the respondents. The following key information was found, over three quarters (77.0%) of offensive name-calling took place on social media sites; nearly a third (32.0%) of cyberstalking took place on texting/messaging apps; more than a fifth (22.0%) of physical threats were experienced on an online gaming platform and over a quarter (28.0%) of online sexual harassment took place on online dating apps (Vogels, 2021).

One common form/category of online harassment, is online sexual harassment. As mentioned, such victimisation refers to victims receiving unwanted sexual material via the internet, either in the form of messages or videos that are either posted on public or private domains. In addition, it also includes receiving unsolicited sexual jokes or threats of a sexual nature (Sehlule, 2018: 7). As a result, it can leave the victim feeling threatened, distressed and uncomfortable (Sehlule, 2018: 35). Such type of victimisation often takes place anonymously as the internet provides endless access to a range of victims, that offenders can then choose from. Offenders may sexually harass victims through email, direct messages, online gaming sites or social media platforms (Sehlule, 2018: 35). Online sexual harassment is becoming a widespread problem whereby an increased number of university students are at risk of falling victim to such a crime. For example, Kennedy and Taylor conducted a study between 2007-2008 that focused on examining the prevalence of online victimisation via social networking

© University of Pretoria

sites, among 354 university students. The following key information was found, slightly less than a quarter of the respondents (n=86; 24.3%) reported that an offender had made verbal statements, of a sexual nature to them online and more than a fifth (n=84; 23.7%) received unwanted sexual material (Kennedy & Taylor, 2010: 11). Another study conducted at the Luminus Technical University College that aimed to investigate cyberstalking victimisation among 757 university students, confirmed that online sexual harassment is common among university students. The study found that nearly two-thirds of the respondents (64.6%) were sent unwanted sexual material (Abu-Ulbeh et al., 2021: 25).

According to a National Study on Sexual Harassment and Assault (2019), the report confirms that sexual harassment, including online sexual harassment, is a widespread problem in the United States. The report includes findings from a survey completed by 1 182 women and 1 037 men, who were 18 years and older. The following key information was found: all of the respondents who had experienced online sexual harassment reported that it took place between 18-24. Additionally, two in five (40.0%) women and nearly a fifth (21.0%) of men experienced such harassment through text messages, phone calls, or on online platforms. More than a tenth (15.0%) of men experienced someone repeatedly phoning them or sending them messages; both men and women commonly experienced receiving unwanted sexual messages over email, Snapchat or Facebook and over a quarter (27.0%) of women and very few (10.0%) men reported that the harassment took place over social media sites. Finally, the report observed that those who admitted to sexually harassing someone online had previously experienced it themselves (UCSD Center on Gender Equity and Health, 2019).

Another example of online sexual harassment, is online sexual solicitation, which refers to a variety of behaviours that include unwanted requests and discussions about sex or sexual activity in an online format. In some cases, such requests are made on either a personal or group level, and the harasser will actively coerce the victim into engaging in unwanted sexual conversation (Ybarra & Mitchell, 2008: 352). A study conducted at a North-Eastern American university further confirmed the prevalence of online sexual harassment among university students. A total of 483 respondents completed a survey that examined their personal experiences with online victimisation. The study found the following results, over a fifth of the respondents (n=108; 22.8%) received unwanted sexually explicit material, such as pornography, slightly less than a third (n=144; 30.8%) were harassed in a non-sexual manner, whereby they received unwelcome emails or direct messages and lastly, very few (n=45; 9.6%) received solicitation for sex (Marcum, 2011: 264-265). Sending unwanted sexual messages or images, is also known as sexting. Sexting consists of sending, receiving and/or forwarding sexually suggestive/explicit photos and/or messages via online platforms (Harris &

© University of Pretoria

Steyn, 2018: 15). Although consensual sexting is not illegal, an individual who shares their personal photo with someone else, has no control over what they will do with it. For example, an offender could distribute such photo to friends or post it on social media for others to see (Badenhorst, 2011: 3). As sexting takes place across electronic devices and the internet, a clear relationship can be identified between sexting and cyberbullying (Badenhorst, 2011: 3).

Cyberbullying is the use of technology to deliberately and repeatedly harass, threaten, or bully an individual or groups of people, who are unable to defend themselves (Burton & Mutongwizo, 2009: 2). Typically, cyberbullying is presumed to only occur within adolescents or students attending high school. While such may be the case, it is also important to acknowledge that more and more university students are experiencing such online victimisation. For example, Schenk (2011) conducted a study that examined the prevalence, psychological impact and coping strategies of American college students who had experienced online victimisation. A sample of 799 students from the West Virginia University participated by completing a self-report survey online (Schenk, 2011: 17). In terms of the respondents who had been cyberbullied, over two-thirds (n=34; 68.0%) of the female students had their self-worth attacked compared to less than half (n=9; 47.4%) of the male students. More than two in five females (n=22; 44.0%) were bullied about their sexual activity compared to only less than a third of the males (n=6; 31.6%). Additionally, nearly two in five females (n=19; 38.0%) and males (n=7; 36.8%) experienced being cyberbullied about their appearance. Finally, male students (n=8; 42.1%) were more likely to have their sexual orientations attacked compared to only a few females (n=2; 4.0%) (Schenk, 2011: 54).

Moreover, a study was conducted that focused on determining the prevalence rate of cyberbullying among university students. A total of 471 university students attending a public liberal arts college in the USA participated in the study by completing a survey (Kraft, 2010: 80). The study found the following key information: over a quarter of the respondents (28.0%) had been cyberbullied once; half (50.0%) experienced it between two to five times and more than a tenth (13.0%) were cyberbullied more than ten times (Kraft, 2010: 81). In terms of who the perpetrators were, more than a quarter (28.0%) reported that they were cyberbullied by their ex-boyfriend/ex-girlfriend, and (26.0%) indicated it was either students from the same university or another university. Furthermore, nearly two in five (37.0%) did not know who the offender was (Kraft, 2010: 81). Lastly, the study found that nearly half (43.0%) of the cyberbullying incidences took place over text messaging, less than two in five (39.0%) received harassing phone calls and nearly a quarter (22.0%) were posts made on Facebook (Kraft, 2010: 82).

© University of Pretoria

A report was written up that examined the extent of electronic aggression, which included online harassment and cyberbullying, amongst the American population. Both types of online victimisation were found to have taken place via email, chat rooms, direct messaging or blogs. The report found the following key information: between 9% and 35% of young people indicated that they have been a victim of some form of electronic aggression; nearly two-thirds (64.0%) of victims who received an aggressive message, knew the offender; nearly a third (32.0%) experienced someone writing a rude or nasty comment online about them; more than a tenth (13.0%) reported that rumours have been spread about them online and nearly a fifth (14.0%) indicated that they have been threatened online (Morin, 2019). The report proposed that cyberbullying, as a form of electronic aggression, was a growing crime phenomenon experienced by more university students each year. Such increase in the victimisation can be illustrated in an online survey that was completed by 439 students. Nearly a quarter (22.0%) of the students reported that they had been cyberbullied while at university; slightly less than two in five (38.0%) were cyberbullied by someone they knew and very few (9.0%) admitted to cyberbullying someone else (Morin, 2019).

As observed in the above research, cyberbullying takes place when students use the internet, cell phones or other electronic devices to send, post or text images, with the intention to hurt or embarrass someone else (National Crime Prevention Council, 2010). There are various types of cyberbullying techniques that offenders can employ, for instance, outing which refers to the process of revealing someone else's secrets, personal information, or images that would have typically never been shared by the victim (Burton & Mutongwizo, 2009: 3). Flaming consists of arguments that occur over chat rooms or text messages, and typically includes vulgar language (Burton & Mutongwizo, 2009: 2). Happy Slapping involves taking and then later sharing online, a video of another person getting slapped and/or physically assaulted (Burton & Mutongwizo, 2009: 3). Harassment, which includes repeatedly sending offensive and hurtful messages, to cause a victim pain and distress (Burton & Mutongwizo, 2009: 2). Furthermore, denigration is when offenders send or post rude messages or false information, with the intention of damaging a person's relationships and reputation (Burton & Mutongwizo, 2009: 2). Impersonation involves using the victim's identity and pretending to be them, without consent, in order to ruin relationships or get the victims into trouble or danger (Burton & Mutongwizo, 2009: 2). Trickery consists of using deception to get a victim to reveal personal and embarrassing information about them, which can then be later spread online (Burton & Mutongwizo, 2009: 3). Exclusion involves alienating a person from being a part of a group online (Burton & Mutongwizo, 2009: 3). Lastly, cyberstalking involves threatening, harassing, or intimidating the victim online (Burton & Mutongwizo, 2009: 3).

© University of Pretoria

Cyberstalking can be described as the new way to commit the crime of stalking while utilising the internet or others forms of electronic devices (Paullet, Rota & Swan, 2009: 641). As mentioned, cyberstalking can be defined as repeated pursuit behaviour, such as unwanted contact, harassment, sexual advances and/or threats of violence, that occur via the social media platforms or communication devices (Henson, Reyns & Fisher, 2016: 558-559). Cyberstalking is becoming an increasingly noticeable problem for university students. Researchers have found that the more students share their personal information online, such as their phone numbers, address and the name of the university they are attending, the more vulnerable they are in becoming victims of cyberstalking (Paullet, Rota & Swan, 2009: 645). For example, a study conducted in 2013 by White and Carmody, examined university students' experiences with online harassment and cyberstalking. Data was collected through conducting seven focus groups, with a total of 41 undergraduate students (22 male and 19 female) attending an East Coast university in the USA. The following key information was found: the majority of the participants experienced online tracking, which includes the constant 'liking' of posts, receiving repeated messages and being befriended by an offender with a fake profile. Furthermore, nearly one in five respondents (19.0%) reported being stalked online, whereby the offender would monitor their activities especially on Facebook or Foursquare[1] (White & Carmody, 2018: 2296 & 2299- 2300). The observation of university students increasingly becoming victims of cyberstalking can be confirmed by a study conducted at the Luminus Technical University College, whereby 757 university students indicated, through completing a questionnaire, that more than half of the respondents (61.3%) had experienced someone monitoring their activities online (Abu-Ulbeh et al., 2021: 3 & 25).

Cyberstalking is found to be a prevalent form of online victimisation experienced by many individuals worldwide. The National Crime Victimisation Survey, conducted in the USA, included stalking incidents in its Supplemental Victimisation Survey (2016). The following key information was found, 3.1 million people aged sixteen or older have experienced cyberstalking. Furthermore, every 15 in 1000 people above the age of eighteen have been victims of stalking, whereby one in four incidences were cyberstalking. More than two thirds (67.0%) of the victims repeatedly received unwanted messages or phone calls; slightly less than a fifth (19.0%) reported that the offender spied on them and monitored their online activities, for example, through listening devices and more than a quarter (27.0%) experienced the offender posting or threatening to post personal information about them on the internet (Stalking Victimisation, 2016: 1-4). Additionally, according to the Working to Halt Online

[1] Foursquare is a social networking service for smartphones, that provides individuals opportunities to discover and share information about businesses and attractions that are close in proximity to their community (Poirier, n.d.).

© University of Pretoria

Abuse's cyberstalking statistics (2013), victims were most likely to be females (60.0%), with the harassers most commonly being males (40.0%). More than half of the respondents (53.0%) did not know the harasser; however, if they did, they were most likely to be an ex-intimate partner (47.0%). The harassment typically took place over Facebook (30.0%), and more than a third (37.0%) reported such victimisation to the police (WHO@, 2013).

Behaviours that are displayed by cyber stalkers are similar to the behaviours of traditional stalkers. For instance, both types of cyber stalkers are driven by desire and the need to have power, control and influence over the victim. As a result, such actions could escalate into a potentially dangerous physical interaction between the two parties (Pittaro, 2011: 280). The internet is considered to be an attractive forum to commit a crime, as offenders are drawn to its relatively inexpensive costs, the ease of use and the perception of anonymity to select a victim and avoid apprehension (Pittaro, 2011: 284). Victims can either be randomly chosen or they could be individuals that the offenders have had a prior relationship with (including being friends or former partners), regardless of whether it was perceived or real (Pittaro, 2011: 280). The internet also provides a space for offenders to retaliate or get their revenge on victims. For example, a website called "the payback" purposely conceals and protects the offender's name and personal information, when they want to send anonymous threatening or aggressive emails to various individuals (Bocij, 2005: 26). The offenders may also utilise social networking sites, as a place to post harmful, negative and private information about the victim. Such behaviour is known as 'cybersmearing' and can occur simultaneously with 'flaming', which is when a victim is made fun of and belittled over a live public forum (Pittaro, 2011: 285-286). The duration of cyberstalking varies, as some incidents may last for weeks, months or even years (Pittaro, 2011: 291).

Finally, McFarlane and Bocij (2005) have observed that there are four distinct types of cyber stalkers. Firstly, a vindictive cyber stalker is regarded to be the most dangerous as they are more likely to repeatedly harass their victims by excessively spamming, email bombing and using the victim's identity, without consent, to subscribe or purchase services that may be sexually explicit in nature. They are also known to use viruses to access the victim's computer in order to monitor them or to disrupt the computer's system and data (McFarlane & Bocij, 2005: 8). Secondly, a composed cyber stalker will typically target victims in a calm manner. The main purpose of harassing their victims is to cause constant distress through employing a range of threatening behaviour (McFarlane & Bocij, 2005: 8). Thirdly, an intimate cyber stalker, will attempt to establish a relationship with the targeted victim. Such type of stalker will seek the attention of the victim in order for them to gain feelings for the offender. Their behaviours are purely driven by infatuation and obsession, and they are typically strangers,

© University of Pretoria

friends or individuals who have had a prior relationship with the victim (McFarlane & Bocij, 2005: 9). Lastly, collective cyber stalkers consist of two or more offenders who target the same victim. They employ techniques such as spamming, mailbombing and utilising intimidating multimedia, to harass their victims (McFarlane & Bocij, 2005: 9).

2.3.2 South African context

In South Africa, several social networking sites are used as a means of communication for university students. The reason could be that such networks are relatively cheap, easy to access, interactive and fast (Business Tech, 2019). Despite the countless benefits of technology for university students, such as growing social connections, various opportunities for academic and social support, identity exploration and cross-cultural interactions, such advancements have widened the gap of opportunities for offenders to target students online (Popovac & Leoschut, 2012: 1). As mentioned, online victimisation includes an array of different crimes, including cyberstalking, cyberbullying and online harassment. Although such crime typologies are increasingly featuring among university students in South Africa, after reviewing the existing literature, there is a clear gap in knowledge concerning online victimisation within a South African context. Thus, the section below contains only a limited amount of information and does not represent the real issue that university students in our country are currently facing.

In 2013, a study focusing on cyberstalking victimisation among South Africans was conducted. The researcher forwarded a link to her envisaged research to ten known online users of a popular social networking site, who further recruited two additional participants. This resulted in twelve participants, all of whom had been victims of cyberstalking, participating in the study (Sissing, 2013: 4 & 22). The researcher used an online email interviewing technique to collect data (Sissing, 2013: 24). As part of the study, the participants were asked about their personal cyberstalking experiences whereby the following key information was obtained: eleven respondents reported that they were cyberstalked on Facebook, thus indicating that social media was the most common platform for such victimisation to occur. Other common responses included being cyberstalked through text messages and phone calls (Sissing, 2013: 97). Furthermore, six respondents indicated that they knew their offender, as they were either a friend, landlord or an individual who mistook their relationship for something romantic. Six other respondents indicated that the offenders were strangers (Sissing, 2013: 99). Finally, the study found that the most common cyberstalking behaviours experienced by the victims included receiving threatening messages, repeatedly receiving unwanted messages over the phone or on Facebook messenger, identity theft, receiving unwanted sexual pictures and

© University of Pretoria

messages, having their private accounts hacked, whereby an offender ended up sending hurtful messages to the victims' friends, rumours were spread and finally having social media being used as a slandering tool, whereby offenders (and friends of the offender) would post statuses that were demeaning and hurtful towards the victims (Sissing, 2013: 101-108).

Evidence shows that cyberbullying among university students is on the rise, as students are more likely to protect themselves against physical harm than from the dangers of the internet and social media sites (Sissing, 2013: 12). Pillay and Sacks (2020) conducted a study that confirms that university students are at risk of online victimisation. The qualitative study focused on the experiences of cyberbullying of ten undergraduate students attending the University of the Witwatersrand. The following key information was collected through face-to-face interviews: in terms of the respondents' demographic characteristics, there were six females and four males, the average ages were 20-22 years old and eight reported to be White, and two were Black. Furthermore, the study found that nine respondents knew their bully, and only one reported that the bully was a stranger (Pillay & Sacks, 2020: 8-9). The study also found that the most common cyberbullying behaviours experienced by the victims included rude comments being posted onto the respondent's social media page and receiving hurtful or threatening text messages (Pillay & Sacks, 2020: 11).

Pillay and Sacks (2020) also examined how the victims were impacted after experiencing cyberbullying, whereby the following key information was found: female respondents were more likely to feel hurt, betrayed, humiliated and isolated. On the other hand, male respondents commonly felt anger, fear and confusion. Respondents often experienced self-blame whereby they could not understand why they were chosen as victims (Pillay & Sacks, 2020: 11). Finally, the study sought out to examine how the participants responded after being cyberbullied, and the following key information was found: all six of the female respondents were inclined to seek help, such as they spoke to friends, family or their lecturers; however, all four of the males chose not to tell anyone (Pillay & Sacks, 2020: 11). Of the females who informed family members, two of the parents went to the university and fought for disciplinary actions to be taken against the bullies. One of the respondents, who received a threatening text message, went to the police and was told to take out a restraining order if the offender continued to send her messages (Pillay & Sacks, 2020: 12).

As the popularity of social media increases, the more common it is for individuals, especially students, to interact online rather than face-to-face. As a result, students are more exposed to experiencing online sexual harassment (Sehlule, 2018: 3-4). A 2018 study set out to examine the prevalence of online sexual harassment experiences of female students at the University

© University of Pretoria

of Venda, Limpopo. The qualitative data was collected from one-on-one semi-structured interviews with twenty female students who had been victims of online sexual harassment (Sehlule, 2018: 5). In terms of respondents' demographic characteristics, all participants were female, and between the ages of 19 to 35, ten were undergraduates, and ten were postgraduate students, and all of the participants had a phone on which they accessed the internet and social media (Sehlule, 2018: 62-63). The respondents were then asked about their online victimisation experiences. The study found that the most common behaviours included receiving unwanted sexual images, whereby the respondents felt shocked and disgusted (Sehlule, 2018: 80). Furthermore, the respondents were asked to send images of a sexual nature to the offenders (Sehlule, 2018: 80), and lastly, the respondents received unwanted sexual jokes that made them embarrassed and uncomfortable (Sehlule, 2018: 83).

Sehlule (2018) further sought to examine where the online sexual harassment incidences took place, whereby the study observed that the two main social media platforms used to conduct such victimisation were Facebook and WhatsApp. The researchers found that WhatsApp was mostly used by perpetrators who knew the victims, whereas the offenders on Facebook were most likely to be strangers (Sehlule, 2018: 84 & 86). Finally, the study examined the responses/coping strategies employed by the respondents after being sexually harassed online. The following key information was found, in terms of immediately after the offence, most participants ignored or blocked the harasser, some tried to confront their harassers and asked them why they did it and to stop, and others threatened to report the crime (Sehlule, 2018: 88 & 90).

South Africa currently has a total population of more than 58.93 million people, whereby 62% of the population use the internet. Through the advancement of technology, the use of social media networking sites has significantly increased, whereby in 2021, 22.89 million individuals are reported to be social media users (Lama, 2020). A total of two in five of the social media users (40.4%) are between the ages of 18-24 years old, whereby the average daily time spent on the internet is nine hours and 22 minutes. Such statistics further confirm how much influence the internet has on the lives of university students and how dependent they have become on using technology as part of their daily routines. Therefore, it highlights an expanding space for which online victimisation can increase (Pillay & Sacks, 2020: 2). However, as online victimisation and its relevant typologies have no agreed-upon definitions, it has resulted in there being a lack of statistics regarding such crime phenomenon (Finn, 2004: 476).

Precise prevalence rates are impossible to know in South Africa for various reasons, such as

© University of Pretoria

computer crimes are typically undetected. Although policing in cyberspace has improved, it cannot keep up with cybercriminals' sophisticated and advanced techniques. For instance, cybercrime can occur through various methods, for example, utilising encryption devices or accessing third-party systems. Therefore, it makes it challenging for law enforcement to find and apprehend such offenders (Choi, 2011: 230). South Africa is rated among the countries showing the highest rates of cybercrimes globally (Dlamini & Mbambo, 2019: 3); however, the South African Police Service and the Victims of Crime survey do not include online victimisation as part of their annual crime statistics. The reason might be that some of the actions performed by offenders when victimising others online are not regarded as illegal. However, online victimisation is becoming an increasingly significant problem in South Africa. The lack of crime statistics on such victimisation provides a space for more offenders to commit cybercrimes, which will continue to have detrimental impacts on the victims (Dlamini & Mbambo, 2019: 1).

2.4 Profile and characteristics of victims of online crime

With the increased usage of computer technology, social media users are more exposed to a unique crime typology, known as online victimisation. As university students use the internet as their primary means of communication, they are especially at risk of falling victim to crimes online. University students are more likely to fall victim to online crimes, depending on two factors. Firstly, university students' demographic characteristics might influence their risk of being victimised online. A study conducted by Schenk (2011) examined 799 American college students' experiences of online victimisation (Schenk, 2011: 17). The following key information was found: nearly three-quarters of the respondents (n=50; 72.5%) were female, and over a quarter (n=19; 27.5%) were male; just less than two in five (n=27; 39.1%) were second-years compared to only less than a fifth (n=13; 18.8%) being first-years. In addition, over four in five (n=61; 88.4%) identified as White (Schenk, 2011: 45). The study further broke down the online victimisation experiences, specifically examining the victim's gender. The following key information was found: female respondents were more likely to experience cyberbullying than males. Within such result, the vast majority of females (n=45; 90.0%) and males (n=17; 89.5%) both experienced cyberbullying over text messages, and more than a third of females (n=17; 34.0%) experienced it over the internet compared to one in five males (n=4; 21.1%). More than a quarter of males (n=5; 26.3%) experienced cyberbullying on their pictures or videos posted online compared to a fifth of females (n=10; 20.0%); more than two-thirds of females (n=35; 70.0%) and males (n=14; 73.7%) experienced cyberbullying over phone calls and finally, over a quarter of females (n=14; 28.0%) and males (n=5; 26.3%) interacted with an

© University of Pretoria

offender pretending to be someone else (Schenk, 2011: 52). Research further confirmed that females are more at risk of experiencing online victimisation, as a study conducted in Europe, found that women are more likely to be sexually harassed and coerced online compared to men (Golbeck, 2018: 1).

A study conducted by Kraft (2010) further illustrates other demographic characteristics that could influence university students' risk of online victimisation. The study focused on determining the prevalence rate of cyberbullying and cyberstalking among 471 American university students (Kraft, 2010: 80). The respondents were found to live in various settings; for example, just over a third (34.0%) lived on campus and (34.0%) lived with their families. Furthermore, the study found that the majority (83.0%) were White and (80.0%) were under the age of 25 (Kraft, 2010: 80-81). Students who were younger than 25 were found to more likely become victims of cyberbullying (n=41; 11.0%) and cyberstalking (n=34; 9.0%) compared to those who were older than 25 (n=5; 5% and n=7; 8.0%). The authors proposed that maybe younger students were more at risk of online victimisation because when compared to older students, younger students have less family responsibilities; they typically live within a residence, and they might spend more time on social media. Therefore, offenders have more opportunities to victimise younger students (Kraft, 2010: 83-84).

The second factor to consider that might influence a university student's risk of falling victim to online victimisation includes the student's voluntary risky behaviours online. For instance, the extent to which students disclose personal information online, the amount of time spent on the internet and social media and their attitudes towards privacy settings might all play a role in their victimisation. Researchers have found that students are often willing to share private information online, as they might find it to be impulsive and easier to share such details with strangers (Jalil & Sinnamon, 2019: 396-397). Kennedy and Taylor (2010) sought to confirm that students who engage in risky behaviour online are more at risk of online victimisation. Data was collected from 354 American students, whereby the following key information was found: the majority of the respondents (80.0%) were using some form of social networking, whereby over a third (34.9%) had their online profiles open for others to view their personal information. Three-quarters (75.0%) shared information such as where they live, which university they are attending, and a third (33.0%) revealed their place of employment (Kennedy & Taylor, 2010: 9). Furthermore, as students enter into university life and become independent from their families and friends for the first time, they may spend an increased amount of time on the internet and social media platforms to stay connected (Schenk, 2011: 6). However, researchers have indicated that the likelihood of a student experiencing online victimisation positively correlates with the student's access to and use of the internet (Jalil & Sinnamon,

© University of Pretoria

2019: 397).

A study conducted online by Jalil and Sinnamon (2019), included a total of 55 students from Bond University, Australia, who completed a survey to determine whether a relationship exists between users' attitudes towards online risk-taking behaviour and the risk of being victimised online (Jalil & Sinnamon, 2019: 400). The following key information was found: over a third of the female respondents (34.1%) had at least five social media profiles, whereas slightly less than a third of males (28.6%) had five profiles. The majority of the respondents indicated that they spend less than two hours a day on social media, with little differences between males and females. Two in five (41.8%) indicated that they update their profiles or statuses at least once a week, while very few females (9.8%) and no males update their profiles once a day. Just over a fifth (23.7%) indicated that they have shared personal information online, such as their name, address and phone numbers, with little differences between males and females. In terms of posting 'selfies', very few females (n=3; 7.3%) and males (n=1; 7.1%) reported that they post 'selfies' one to two times a week (Jalil & Sinnamon, 2019: 403, 407). Furthermore, Marcum (2008) conducted a study whereby 483 first-year students completed a questionnaire to determine what activities the university students perform online. The following key information was found, nearly all of the respondents (n=459; 95.2%) used the internet for research, and (n=435; 90.2%) used it to socialise with others, while nearly two thirds (n=300; 62.5%) used Facebook as their primary social networking site. Furthermore, over half (n=259; 53.7%) used the internet for online gaming (Marcum, 2011: 257, 260). Additionally, Marcum (2011) found that the vast majority (n=447; 92.9%) accessed the internet through their computers whilst being at home. Over half (n=264; 55.0%) of such respondents indicated that their computers had no online restrictions and nearly two thirds (n=291; 60.9%) had no filtering/blocking software for protection/safety measures (Marcum, 2011: 262, 264).

2.5 Profile and characteristics of perpetrators of online crime

Online victimisation can be understood through Jaishankar's (2008) space transition theory, which refers to the shift from an offline environment to an online setting. The theory suggests that individuals with inhibited criminal behaviour tend to commit crimes online, which they would not typically perform in the real world. As cyberspace offers identity flexibility, dissociative anonymity and a lack of deterrence, victimising others online becomes an attractive crime for potential offenders (Jalil & Sinnamon, 2019: 397- 398). Online victimisation is found to manifest itself at university, where more and more students are engaging in deviant behaviours for various reasons. Firstly, the anonymity of the internet, paired with students' inherent nature to take more risks when entering university life, can result in individuals

© University of Pretoria

participating in social misconduct, such as cyberbullying, online harassment and cyberstalking (Kraft, 2010: 77). Secondly, as online communication lacks nonverbal cues, such as facial expressions and tone of voice, students who anonymously engage in online victimisation can avoid the consequences of their actions, as they do not have to face their victims. Additionally, it might encourage them to say and do things online that might be atypical of their offline behaviour (Kraft, 2010: 77). Researchers have also found that because the internet provides a place for offenders to hide from the repercussions of their behaviour, they are often more likely to have lower levels of guilt, shame and remorse when victimising others (Cilliers, 2021: 2). It has also been found that there is typically a continuation of cyberbullying from high school to university. Some cyberbullies in university indicate that they also engaged in bullying others in high school. The reason might be because the offenders view their behaviour as acceptable and normal, and they are generally held less accountable for their actions by their parents and university management, which as a result, might escalate their behaviour (Meyers & Cowie, 2017: 1177).

Marcum, Higgins, Freiburger and Rickets (2014) conducted a study that focused on the differences in online bullying behaviours of males and females. Data was collected by means of an online survey, in which 1139 students, who were attending a South-Eastern public university in the USA, participated. In terms of the offender's profile, the study found the following key information: individuals, including male and female students, who had lower levels of self- control, were found to more likely engage in cyberbullying by posting hurtful messages or pictures about their victims online. The reason being is because of the lower levels of self- control, offenders were more likely to be risky and impulsive (Marcum, Higgins, Freiburger & Rickets, 2014: 545). The study also observed an interesting result in that both sexes who cyberbullied others reported to have previously been victims of online victimisation themselves. The finding indicates that experiencing online victimisation can push a person to act out in a hurtful way to retaliate for that hurt and loss of control. While being bullied can be hurtful, bullying someone else can cause the same individual to feel powerful and vindicated (Marcum et al., 2014: 545). Lastly, the study found that male students who spent an increased time on social media were more likely to cyberbully others by posting gossip about their victims. The researchers propose that the more time an individual spends online, the more comfortable and confident it makes them with their internet persona, thus, encouraging them to victimise others (Marcum et al., 2014: 546). In terms of the female offenders, the study found that they are more likely to engage in cyberbullying seeing that they feel more confident when they belong to a large peer group online (Marcum et al., 2014: 546).

Within traditional offline bullying, males are more likely to be the offenders than their female

© University of Pretoria

counterparts. If female students engage in offline bullying, they will typically participate in more indirect forms of bullying, such as psychological and emotional harassment and aggression (Marcum et al., 2014: 539). As cyberbullying includes more forms of indirect harassment, researchers assume that females are just as likely to be involved in such victimisation as their male counterparts (Marcum et al., 2014: 540). Past research has found that there are several reasons for such an assumption. Firstly, females tend to be more verbal than males; therefore, cyberbullying might be their preferred method, as such victimisation consists of verbal communication online. Furthermore, females are less confrontational face-to-face, often due to cultural constraints and gender role expectations. However, as the internet provides the perception of anonymity, females can engage in cyberbullying as they have the protection of hiding behind a computer screen. Lastly, females often participate in bullying involving emotional and psychological abuse, such as gossiping or spreading rumours about another person (Underwood, Galen & Paquette, 2001: 252).

2.6 Impact of online offences on victims

Although the impact of online crime on victims was not a specific focus of the current study, there is a growing interest in examining the negative impact online victimisation has on individuals mental, emotional, physical and social functioning (Dooley, Shaw & Cross, 2012: 276). The anonymity of online offenders, the ease of accessibility of a variety of victims, the large online viewing audience, the lack of physical interaction and the emergence of global offenders, has made online victimisation experiences potentially more detrimental than their counter traditional offline ones (Alhaboby, Barnes, Evans, Short, 2017: 2). The emotional harm online victimisation has on its victims can vary from minor annoyances to life-changing suffering. However, studies have found that experiencing online victimisation is associated with depression, behavioural and emotional problems, developing post-traumatic stress disorder, influencing academic achievements and frequent smoking and the misuse of alcohol (Dooley, Shaw & Cross, 2012: 276).

As mentioned, online victimisation can have varying effects on the victim, whereby they might experience a range of emotions. Such varying effects can be seen in a study that focused on the psychological impact experienced by the victims of online victimisation (Schenk, 2011: 25). The following key information was found: nearly half of the respondents (n=30; 46.2%) frequently felt frustrated; two in five (n=27; 40.9%) felt stressed; just less than two in five (n=25; 37.9%) felt sad or hurt and (n=22; 33.8%) felt angry. Additionally, more than a fifth (n=15; 23.4%) indicated that they had difficulties concentrating; (n=14; 21.5%) reported they could not stop crying and (n=14; 21.5%) felt anxious. Other emotional sufferings experienced by the

© University of Pretoria

students, were that less than one in five (n=12; 18.8%) felt embarrassed, or (n=12; 18.8%) thought about it constantly, or (n=12; 18.2%) felt helpless/hopeless or (n=11; 16.7%) felt jumpy and irritable. The study also found that more than a tenth (n=8; 12.1%) reported that their grades dropped and (n=8; 12.1%) that they frequently acted out (Schenk, 2011: 47). An interesting find of the studies was that twenty students experienced suicide ideation and eleven students planned suicide frequently. Additionally, four students attempted to commit suicide, due to their experience of online harassment (Schenk, 2011: 48). Although victims experience the same victimisation, they might all be affected in different ways. Kraft's 2008 study further illustrates how students can have a range of feelings after being victimised online. The study found that nearly three quarters of the victims (73.0%) felt anger; nearly two thirds (63.0%) felt frustration; slightly less than two in five (39.0%) felt humiliated; almost one in five (15.0%) felt depression and a few (2.0%) experienced suicidal thoughts (Kraft, 2010: 83).

Some of the qualities of the internet and electronic devices can increase online victimisation's impact on its victims. For example, online communications can be exceedingly hurtful and aggressive, as offenders feel like they can hide behind their anonymous and sometimes fake profiles online. Furthermore, online victimisation differs from its traditional offline counterpart as such victimisation can be continuous, 24/7. There are no ways of escaping the offenders' actions unless the victims disengage from technologies. However, victims may lose friends or feel even more alone and isolated in their experience. Lastly, any hurtful, intimidating or embarrassing material, even if it is initially sent privately, can be distributed to many others, resulting in the victim feeling embarrassed, criticised and humiliated (Willard, 2007: 3). As a result, online victimisation can lead to depression and suicide ideation, thoughts and eventual attempts (De Wit, 2005: 708). Although there is a lack of research regarding the impacts of online victimisation among university students, research has been carried out to examine its effects on adolescent victims. In some cases, adolescents may commit suicide as a result of being cyberbullied. For example, in 2019, a thirteen-year-old girl from Pretoria committed suicide after a photograph of her went viral around the school, whereby learners then persistently teased the girl (Gous, 2019). Other international examples include in 2010, on the 22nd of September, 18-year-old Tyler Clementi jumped to his death from the George Washington Bridge after his roommate streamed a video of him and another male over the internet (Schenk, 2011: 1).

Furthermore, individuals who have been victimised online may also suffer from physical and social consequences. For instance, in response to specifically being cyberstalked, victims may experience sudden changes in their sleeping and eating patterns, nightmares, hypervigilance, helplessness and fear for their safety. Hypervigilance is often associated with post-traumatic

© University of Pretoria

stress disorder, whereby the victim when in a state of fear, may lash out inappropriately through aggressive and violent behaviour (Pittaro, 2011: 291). Furthermore, the victims may also experience physical effects, such as feeling jumpy or having panic attacks, weakness, fatigue, nausea and headaches (Sissing, 2013: 66). Likewise, Bocij (2004) observed that cyberstalking victims might also suffer feelings of loss of control, isolation and self-blame (Bocij, 2004: 80). In some severe cases, the victims might be vulnerable to developing psychiatric disorders and suicidal tendencies (Drahokoupilová, 2007: 152). Cyberstalking may drive the victim to change their lifestyles; for example, they may change their personal information such as their phone numbers, street and email addresses, and their names in rare cases (Drahokoupilová, 2007: 152). A study conducted in South Africa confirmed such unwanted alterations in victims' lives. The researcher found that one participant who had experienced cyberstalking, feared for her own and her husband's safety, had to relocate and find a new job, were not as active on their social media profiles after the incident, and they refused to post any more pictures of themselves online (Sissing, 2013: 122-123).

2.7 Victims' responses to online victimisation

It is essential to acknowledge that the way online victimisation impacts university students will significantly influence how they respond to such experiences (Hill, 2003: 15). Furthermore, how a victim responds to such victimisation will highlight any shortcomings within existing legislation and policies that combat online victimisation within the university community. However, after reviewing the available literature on responses to online victimisation, a clear gap in the knowledge was identified, highlighting the need for future research.

There are various ways in which a university student responds to online victimisation. For example, a study that focused on examining online harassment experiences of 339 undergraduate students at the University of New Hampshire found the following information: in terms of reporting the online harassment, nearly a third of the respondents (n=7; 30.4%) indicated that they reported it to their internet service provider When the respondents were asked if the situation was resolved to their liking, nearly half (n=11; 47.8%) responded no. Finally, when asked why the respondents did not report the harassment, nearly two in five (37.5%) stated that they believed the problem was not serious enough to report, close to a fifth (19.5%) indicated that they handled it themselves and more than a few (12.5%) said that they did not know whom to report it to (Finn, 2004: 476). Kraft's 2008 study which focused on determining the prevalence rate of cyberbullying and cyberstalking at a public liberal arts college in the USA examined how often university students reported their experiences (Kraft, 2010: 80). The following key information was obtained: a fifth of respondents (20.0%) did not

© University of Pretoria

tell anyone about the incident; however, slightly less than three quarters (72.0%) told their friends, and almost two in five (39.0%) told their parents. Furthermore, only a few (9.0%) sought help from their lecturers and (7.0%) from the counselling centre. The primary reason why the respondents did not tell anyone was because they believed that they could handle it alone (60.0%); more than one in five (22.0%) believed it was not serious enough, and nearly a fifth (18%) indicated that they did not think the university would do anything about it (Kraft, 2010: 87).

Furthermore, a study conducted by Schenk (2011) focused on the online victimisation of 799 students attending West Virginia University. Regarding how the university students responded, the following key information was found: females (n=40) were significantly more likely to tell someone about their experiences than their male counterparts (n=10). Females were also more likely (n=19) to avoid peers or friends than males (n=6). More females (n=13) responded by getting revenge, compared to male victims (n=6) and females (n=10) were more likely to stop going to events than males (n=4) (Schenk, 2011: 53). In the following study, it is important to note that the students who participated were primary and secondary school students. Although they are not university students, how they responded to online victimisation might give researchers a better indication of how university students might respond to such victimisation. Using such a source further highlights the gap in knowledge concerning online victimisation among university students. The study was conducted in Australia, whereby 2 645 students participated in a self-administered survey. The study aimed to examine the relationship between aggressive, assertive and passive students' responses after experiencing online victimisation (Dooley, Shaw & Cross, 2012: 275, 278). The following key information was found: very few participants (13.0%) responded passively, whereby nearly two thirds (n=284; 61.0%) ignored their harasser. Over a third (35.0%) responded aggressively, whereby nearly two in five (n=167; 36,0%) sent nasty words or pictures back to the perpetrator; and just over half (52.0%) responded assertively whereby half (n=235; 50.0%) told their harasser to stop, and two in five (n=179; 39.0%) told a parent or teacher (Dooley, Shaw & Cross, 2012: 280-281).

2.8 Policies and legislation regarding online victimisation

In South Africa, various university policies deal with different forms of online victimisation. Firstly, the University of Cape Town's Sexual Harassment Policy on sexual offences and sexual harassment (University of Cape Town, 2008) will be discussed. The policy was developed in 2008 and states that if a member of the university community experiences sexual misconduct within an online setting, managed or not managed by the university, it falls within

© University of Pretoria

the scope of the policy. The university will investigate the claim and determine whether the conduct impacts the individual's safety within the university community. Part of the policy's definition of sexual harassment includes unwanted non-verbal conduct, which consists of sending sexually explicit pictures. Another form of sexual harassment is defined as unsolicited sexual conduct, which includes direct or indirect conduct via technological devices, images and/or social media platforms. The policy also defines bullying; however, it does not acknowledge bullying that takes place in cyberspace. Thus, there is a gap in such policy, whereby cyberbullies will not be held accountable for their actions. The University of Cape Town has an additional draft policy on disciplinary procedures for sexual misconduct (University of Cape Town, n.d). Firstly, there may be a disciplinary hearing whereby the harasser may receive a sanction, such as community service, suspension or expulsion. The harasser may also receive an interim order as a protective measure for the victim, whereby if a violation of the order occurs, it will result in an automatic suspension (University of Cape Town, 2008).

The second example of a university policy dealing with online victimisation is the University of Pretoria's code of conduct on handling sexual harassment, created in 2008 (University of Pretoria, 2008). The policy defines sexual harassment as unwanted sexual conduct that violates the rights of an employee or student that can result in a barrier to equity in the workplace or within the university community. The definition includes unwanted sexual conduct that can take place within an online environment. For instance, the policy states that unwelcome conduct can include verbal conduct communicated via electronic devices, including sending sexually explicit messages, pictures or objects. If the harasser violates the policy, they may face disciplinary actions such as warnings, suspension or expulsion (University of Pretoria, 2008).

The University of the Witwatersrand does not have a policy explicitly concerning online victimisation; however, they have established a transformation office that implements various projects to improve the institutional culture and uphold the diverse, multicultural university community (University of the Witwatersrand, 2015). Such projects seek to raise awareness and education on issues that affect the community and the country. For example, they have designed an anti-cyberbullying brochure. The brochure defines cyberbullying to include the use of the internet or technological devices to send or post texts or images that intend to hurt, embarrass, discriminate, threaten, torment, humiliate or intimidate an individual or a group of people. It also outlines what constitutes cyberbullying behaviour, for example, sending unwanted sexual or threatening messages or messages that are sexist, derogatory, racist or

© University of Pretoria

homophobic, and online stalking. Lastly, it highlights interventions administered by the university to deal with cyberbullying; for example, mediation takes place through the Wits Transformation and Employment Equity Office (University of the Witwatersrand, 2015).

In South Africa, there is no current legislation that is explicitly aimed at online victimisation. As a result, the legal consequences and remedies to such deviant behaviour rely on a variety of different pieces of legislation (Badenhorst, 2011: 6). Firstly, Section 16(1) of the Constitution of the Republic of South Africa (Republic of South Africa, 1996) grants everyone the right to freedom of expression; however, according to Section 16(2)(b) and (c), such right does not extend to incitement of imminent violence or the promotion of hatred, based on race, ethnicity, gender or religion, that further constitutes incitement to cause harm (Constitution of the Republic of South Africa, 1996). Furthermore, Section 12 grants everyone the right to freedom and security, including Section 12(1)(e), which is to not be treated or punished in a cruel, inhuman or degrading way. Finally, Section 12(2) states that everyone has the right to bodily and psychological integrity (Constitution of the Republic of South Africa, 1996). In terms of civil law responses, a victim can obtain an order to keep the peace. In terms of Section 384 of the Criminal Procedure Act, 1955 (Act 56 of 1955), an individual who has been a victim of violent conduct, has been threatened with injury, or where a person has used language or behaved in a way that is likely to cause a breach of peace or assault. Such a victim may approach the court to obtain an order to keep the peace. Once the court has investigated the victim's claim, the perpetrator may be ordered to pay a fee of R2 000 for six months to keep the peace towards the victim (South African Law Commission, 2004). Secondly, a victim can apply for an interdict to be brought to the High Court for an order to restrain a person from committing or threatening to commit an unlawful act. The victim may also sue for defamation of dignity or their reputation and claim for damages (Hubbard, 2008: 17).

Furthermore, there are four different crimes that a perpetrator of cyberbullying can be charged within South Africa. Firstly, crimen injuria refers to the unlawful, deliberate and serious violation of the dignity and privacy of another person (Badenhorst, 2011: 8). For example, such actions can include vulgar words and disrespectful language (Burchell, 2014: 354). The courts will use both subjective and objective tests to ensure that the victim's dignity was infringed (Pillay & Sacks, 2020: 7). Secondly, assault refers to the illegal, unintentional act or omission that directly or indirectly impairs the victim's bodily integrity, or creates a fear that their integrity may be impaired (Badenhorst, 2011: 8). An example of such behaviour is if an offender had to threaten a victim's well-being through technology. The courts will use a subjective test to determine whether the victim was assaulted (Badenhorst, 2011: 8). Thirdly, criminal defamation, which is linked to denigration. Such defamation can include written or verbal public

© University of Pretoria

communication that intends to harm the victim's reputation (Docherty, 2000: 264). Within the courts, the words must be read by a third party and must intend to damage the victim's reputation. If the defamation goes unnoticed by an audience, then the perpetrator may only be charged with crimen injuria and not criminal defamation (Badenhorst, 2011: 8). Lastly, extortion refers to a perpetrator who illegally obtains personal and compromising information about a victim and threatens to reveal it online if the victim does not comply with the offenders' orders (Pillay & Sacks, 2020: 7).

Various existing Acts in South Africa may assist victims of online victimisation. For example, Section 85 to 89 of the Electronics Communications and Transactions Act 25 of 2002 (Republic of South Africa, 2002) seeks to make the first statutory provisions for cybercrime in South Africa. As the Act deals with all communication, messages and transactions through technology and electronic devices, the Act aims to introduce statutory criminal offences relating to computer-related extortion, fraud and forgery. In addition, the Act wants to develop statutory criminal offences relating to hacking, interception and launching virus attacks, deeming such conduct illegal. In 2012, the Electronic Communications and Transactions Amendment Bill was published, whereby the abovementioned activities are deemed illegal, which can result in the perpetrator receiving a fine of up to R10 million or imprisonment of up to ten years (Republic of South Africa, 2012). Further developments include the enactment of the Cybercrimes Act 19 of 2020 which criminalises additional cyber activities, such as cyber fraud, cyber forgery and cyber uttering; as well as malicious communications, which includes a form of 'hate speech' (Republic id South Africa, 2020). Emma Sadleir, a digital law expert, highlights a paramount development in South African legislation, where for the first time revenge pornography is deemed to be a criminal offence according to the Cybercrimes Act (Zama, 2021). Secondly, one of the newer forms of legislation developed by the Department of Justice and Constitutional Development is the Protection from Harassment Act 17 of 2011, enforced on April 27, 2013 (Republic of South Africa, 2011). Such Act aims to protect individuals being harassed by providing the victim with a court order to prevent the harasser from continuing with the abuse. The victim may even ask for a protection order from the court to protect them from the harasser. The harassment referred to by the Act can include harassment in cyberspace. For example, a peace order was obtained by a girl in high school who was called a derogatory name online by another girl in her school (Badenhorst, 2011: 6).

A third act that a victim of online victimisation may rely on is the Domestic Violence Act 116 of 1998 (Republic of South Africa, 1998), which was implemented to provide protection orders addressing domestic violence and any other matters relating to it. The Act describes a domestic relationship as one in which two people share a relationship in various ways; for

© University of Pretoria

example, it includes people who were once in an intimate or sexual relationship for any duration of time and people related to each other. Domestic violence relates to various abuses such as physical, sexual, economic, emotional, psychological, or intimidation, harassment and stalking. As such, the Act makes provision for any harassment, stalking and intimidation that may take place through electronic means. Victims of such behaviours can apply for a protection order which can include the confiscation of guns and other dangerous weapons belonging to the offender. If an offender breaches the protection order, the police can arrest them (Domestic Violence Act 116 of 1998).

2.9 Summary

In the chapter, a review of the relevant literature was provided. By following the study's objectives, the chapter was able to provide a detailed discussion of the key elements of online victimisation. Typologies of the phenomenon were sub-divided into various categories to better understand the nature of online victimisation, both within a South African and international context. The chapter also examined the extent of online victimisation, whereby a clear gap in knowledge is found regarding crime statistics relating to the phenomenon under investigation. The chapter also described the victims' profiles and highlighted key elements that can assist in predicting and explaining why undergraduate students experienced online victimisation. Lastly, the chapter discussed the impact victimisation has on its victims and the responses to such victimisation, whereby attention was paid to the lack of existing legislation and university policies that focus on online victimisation, locally and internationally. The following chapter (chapter three) will focus on theories applicable to the present student; in addition, the chapter will discuss the development of an integrated theoretical model, which could better understand online victimisation among undergraduate students.

© University of Pretoria

Chapter 3: Theoretical perspectives

3.1 Introduction

The chapter focuses on online victimisation among undergraduate students. The theoretical framework draws primarily on victimology theories, as the study aims to focus on the victims of online victimisation. The chapter will discuss both victim-orientated and perpetrator-orientated theories to understand such a type of victimisation better. However, as there are shortcomings in the existing victimological theories and models used to explain victimisation online, a single comprehensive, integrated model was designed. The integrated model hopes to be useful and applicable in gaining a deeper understanding of how and why university students become victims of crime committed online and what causation factors directly influence an offender to victimise others online. The theoretical application of the integrated model will, however, only take place in Chapter six.

The integrated model uses various victim-orientated and perpetrator-orientated theories to understand the online victimisation of undergraduate students. The victim-orientated theories include the lifestyle/exposure theory (Hindelang, Gottfredson & Garofalo, 1978); routine activities theory (Cohen & Felson, 1979); the opportunity model (Cohen, Kleugel & Land, 1981); the dangerous place theory (Stark, 1987) and the differential risk model (Fattah, 1991). In terms of the perpetrator-orientated theories, the models made use of the cyberbullying model (Barlett & Gentile, 2012), the online disinhibition effect model (Suler, 2005) and the extended control balance theory (Piquero & Hickman, 2003). Each of the theories and models will be discussed, and the chapter will also highlight how each of their influencing factors inter-connect with each other thereby contributing to the development of the integrated model.

3.2 Victim-orientated theories

Victim-orientated theories seek to explain what behaviours or characteristics of the victims increase their own risk of victimisation. Application of such theoretical frameworks include investigating the victim's legal culpability, engagement in deviant lifestyles, having direct or indirect conflict with others and participating in dangerous behaviours, such as having a reckless attitude. Simply put, victim-orientated theories propose that victims are believed to play a role in causing criminal behaviour (Zaykowski & Campagna, 2014: 453).

© University of Pretoria

3.2.1 Lifestyle/exposure theory

The lifestyle/exposure theory, developed by Hindelang, Gottfredson and Garofalo (1978), is based on the idea that the likelihood of individuals being victimised significantly depends on their lifestyle and that if any changes take place within their routine activities, it can either increase or decrease their exposure to risk and provide opportunities for potential offenders and subsequent victimisation to occur (Saponaro, 2019: 15). Hindelang et al. (1978) argued that social role expectations (for example, the responsibilities and behaviours that are typically considered normal for specific ages) and structural constraints (for example, lack of job opportunities) shape people's lifestyles. They further explained that an individual's lifestyle could also refer to their routine activities, which consists of vocational activities, such as work and school responsibilities, and leisure activities, such as visiting family or going to the shops. There are five main elements to the lifestyle/exposure model that can influence an individual's risk of victimisation, such as (Hindelang et al., 1978, 242; Saponaro, 2019: 16-18):

- Role expectations, which are determined by a person's demographic characteristics, such as their age, gender, marital status, education, race, economic status and occupation;
- Structural constraints, which refers to familial, financial, educational and legal structures that can limit and restrict a person's lifestyle, behaviours and opportunities;
- Adaptions, whereby role expectations and structural constraints influence how individuals have to adapt their behaviours and routine activities, which may result in increasing or decreasing their risk of victimisation;
- Exposure, where there is a direct link between a person's lifestyle and routine activities and their risk of being exposed to situations, which may increase or decrease a person's likelihood of being victimised; and
- Associations, where there is an indirect link between a person's lifestyle and their exposure to victimisation, which takes place through associations. For example, individuals who share similar lifestyles are more likely to come into contact with one another, and if such a similar person engages in risky behaviour, it will ultimately increase the victim's exposure to personal victimisation.

Hindelang et al. (1978) also suggests eight propositions regarding being exposed to victimisation, which is influenced by a person's lifestyle. For example, the likelihood that personal victimisation will take place is linked to the amount of time a person spends in public; the amount of time spent in public during the day and night, or the amount of time spent interacting with non-family members (Saponaro, 2019: 17-18).

© University of Pretoria

Although the lifestyle/exposure model is universally accepted and applied, various criticisms have been made about the theory. For instance, the model does not explain personal victimisation within a domestic environment, and it dismisses daily activities that are carried out so routinely by individuals that they are not even aware of their existence. Furthermore, the lifestyle concept can be argued as vague as it does not consider target attractiveness, individual differences and perceptions about and reactions to crime. Lastly, another limitation is that the model suggests that victimisation most likely occurs when an offender is in direct contact with the victim. However, the model needs to consider that direct contact between the two parties is not always necessary for victimisation to take place. Due to the modern times that we live in, victimisation can also take place online where there is physical distance between the offender and the victim (Saponaro, 2019: 18).

3.2.2 Routine activities theory

The routine activities theory, developed by Cohen and Felson (1979) focuses on crimes involving direct contact between the offender and victim. Moreover, the theory explains the influence an individual's routine daily activities can have on criminal opportunities (Coetzee, 2017: 66). Similar to the lifestyle/exposure model, the routine activities theory focuses on how changes in a person's daily activities can increase or decrease the individual's risk of being victimised (Miró-Llinares, 2014: 1). The basic principle of the routine activities theory is that crime takes place when three elements interact with each other; which include (1) the presence of a motivated offender; (2) the availability of a suitable target; and (3) the absence of a capable guardian (Asli, 2013: 61). In terms of a motivated offender, the potential offender may be any person who has a motive to commit a crime, and has the capacity to do so (Miró-Llinares, 2014: 2). The theory further states that offenders are rational human beings who may commit a crime whenever an opportunity arises. Thus, the crime requires the victim and offender to play a role (Coetzee, 2017: 67).

The second element required for a crime to occur is a suitable target, which refers to a person or property that may be considered of value to an offender. The likelihood that a target will be suitable to the motivated offender is heavily influenced by four factors, namely (Miró-Llinares, 2014: 2-3; Coetzee, 2017: 67; Saponaro, 2019: 19):

- Value, which refers to the real (financial) or symbolic value of the target, which influences its desirability from the offender's perspective.

© University of Pretoria

- Physical visibility refers to the opportunity for potential offenders to identify, notice and watch the suitable target.
- Accessibility/attainability refers to the ability of and ease with which the potential offender can approach or gain access to the target, without drawing unwanted attention.
- Inertia refers to the ease and simplicity of acquiring a suitable target. It considers the size, weight and shape, or the physical aspects of the person or property that act as obstacles for the offender.

Felson and Cohen (1980) argued that routine activities significantly affect the suitability of the target, as an individual's lifestyle may increase the chances of the property and/or individuals to be visible and accessible at a specific time (Saponaro, 2019: 19).

The final element described in the routine activities theory is the absence of a capable guardian, which refers to someone who can interfere or deter a crime from taking place. A capable guardian includes anyone who moves through an area or functions as a guard for the person or property, for example, the police, security guards, or residents of a house. In general, a capable guardian is any person who, through their presence or daily activities, can decrease the chances of a crime being committed (Miró-Llinares, 2014: 3). The definition of a capable guardian can go beyond a person and can also include an animal, object, security measures (such as electrical fencing), technological aids (such as CCTV), and even programmes or policies implemented to prevent or discourage violence (Coetzee, 2017: 67).

The routine activities theory is universally accepted and applied and emphasises one of the most important aspects of crime, namely the dynamics of victimisation. However, certain limitations/criticisms have been pointed out, such as the theory shifts the focus from the offender onto the victim, which may result in victim shaming and holding the victim responsible for a crime taking place if they do not change their routine behaviours. Another limitation is that the theory fails to explore further and determine other factors that motivate the potential offender to commit an offence. Finally, various authors have highlighted that a better, more efficient analysis of the underlying link between the three prerequisites for victimisation (namely a motivated offender, suitable target and absence of guardianship) is required (Saponaro, 2019: 20- 21).

3.2.3 The opportunity model

The opportunity model of Cohen, Kleugel and Land (1981) was developed to explain predatory

© University of Pretoria

victimisation and integrate elements of both the lifestyle and routine activities theory. The reader will note the substantial overlap between the opportunity model and the lifestyle/exposure and routine activities theories. The opportunity model is based on the idea that the risk of an individual experiencing personal victimisation significantly depends on their routine pattern of behaviour, which consequently brings them or their property, into direct contact with motivated offenders, in the absence of capable guardians (Saponaro, 2019: 21). According to the model, five factors may increase the likelihood of a person being victimised, namely: exposure, proximity, guardianship, target attractiveness and properties of specific offences. The first element, exposure, refers to the suitable targets' physical visibility and accessibility. The risk of victimisation is influenced by how often the potential offender comes into consistent and direct contact with the potential victim (Booyens, 2009: 95). The more frequent the contact, the more likely victimisation will occur (Saponaro, 2019: 21).

The second element is proximity, which refers to the physical distance between the area where potential targets live and areas where a large population of potential offenders are situated. The closer the potential victims are to the motivated offenders, the greater risk of personal victimisation taking place (Saponaro, 2019: 21). The third element is guardianship, and it refers to the increased amount of time that potential victims spend alone or without people or objects that act as protective measures, as well as the increased risk of victimisation experienced by victims (Finkelhor, 2007: 27). Guardianship refers to individuals, such as neighbours or security guards, or objects such as security fences that prevent crime through their presence or direct or indirect action. The fourth element includes target attractiveness, which refers to the material or symbolic desirability of individuals or property as targets for potential offenders, and the perceived ability or inability of the person to resist such victimisation. The greater the target's attractiveness, the greater the risk of victimisation occurring (Saponaro, 2019: 21). The final element is the properties of specific offences, which refers to the ease of committing crime. The more difficult it is for the offender to commit a crime, the less likely it is for the crime to occur (Booyens, 2009: 96).

The opportunity model is a universally accepted theory used to explain victimisation, as it moves the emphasis from the characteristics of the offender to the characteristics of the situation. However, the model is criticised for its vague interpretation of lifestyle and the fact that victimisation is, according to the model, heightened by exposure and lack of guardianship (Saponaro, 2019: 22). Secondly, the presence of a motivated offender is regarded as the only causation factor that directly influences the occurrence of a crime, and other factors such as online peer group influences, are ignored (Booyens, 2009: 96). Furthermore, the theory does not explain crimes committed in other environments, such as online environments, where no

© University of Pretoria

contact occurs between the two parties (Coetzee, 2017: 70). Lastly, not enough attention is paid to gender differences, and the model does not address the importance of structural variables, such as community context and social inequality, that may act as contributing factors (Saponaro, 2019: 22).

3.2.4 Dangerous place theory

The dangerous place theory, also known as the deviant place theory (Stark, 1987), is an ecological theory of crime, and it argues that there is an underlying link between different community characteristics and the occurrence of crime (Pradubmook-Sherer & Sherer, 2015: 2). The theory suggests that the occurrence of crime does not depend on the victims' lifestyle, but rather it depends on the areas in which the victims reside. For instance, victims who live in socially disorganised high-crime areas have the greatest risk of coming into contact with criminal offenders; thus, they are more vulnerable to experiencing victimisation. Furthermore, the more often victims visit dangerous places, the more likely they will be exposed to crime and violence, which may then be perpetrated against them (Siegel, 2010: 80-81). Deviant places are typically characterised as poor, densely populated and highly transient communities in which commercial and residential property exist. The theory proposed that individuals who live in more affluent neighbourhoods are presumed to take more safety precautions, significantly lowering the chances of an offender committing a crime in that area. However, people who live in poorer areas have a much greater risk of becoming victims as they are closer to motivated offenders, and attempting to protect themselves is more of a challenge. The theory also states that affluent people recognise that by living in an area with greater police presence and lower crime rates, the occurrence of criminal victimisation is reduced (Siegel, 2006: 79-80). Keeping in line with socio-economic approaches to victimisation, the theory explains that low-income households are more likely to be located in or near dangerous areas, and individuals from poor socio-economic backgrounds are less capable of moving away from such areas, thus explaining the reason for their increased risk of being victimised (Grand Canyon University, 2019).

The dangerous place theory points out various propositions that increase a person's chances of being victimised. All of the propositions relate to the neighbourhood characteristics of where potential victims may live. The characteristics include: within neighbourhoods that are dense and poor, homes are typically over-crowded with many people, which could drive a potential victim into leaving their homes, and going to high-risk places, where there is an increased chance of being victimised. A crowded house might also result in children being left

© University of Pretoria

unsupervised, which increases their risk of offending or becoming a victim (Stark, 1987: 895-897). Furthermore, poor, dense neighbourhoods with residential houses typically coexist with excessive commercial land use. As a result, it provides more opportunities for offenders to commit crimes due to easy access to suitable targets (Stark, 1987: 898- 900). Lastly, such socially disorganised communities may lack law enforcement presence, which will encourage more crime to occur, as such behaviour may be seen as acceptable and rewarding. As a result, more people are victimised (Stark, 1987: 902-903).

There are a few limitations and criticisms made against the dangerous place theory. For instance, the theory emphasises the link between crime and an area, and forgets to consider the role of opportunity within offending and victimisation (Eck & Weisburd, 1995: 2). Furthermore, by only examining how neighbourhood characteristics increase the likelihood of crime taking place, the theory further overlooks factors that can directly influence an offender to commit a crime, such as the routine activities of a potential victim. Lastly, the theory only considers poor and densely populated areas as crime-hot spots and assumes that criminals only reside in such areas. The theory needs to recognise that crime can occur in different areas and settings where the victims are not in close proximity to the offenders, such as in an online environment (Bouffard & Muftić, 2006: 56).

3.2.5 Differential risk model

Due to the shortcomings of the lifestyle/exposure model (Hindelang, Gottfredson & Garofalo, 1978), the routine activities theory (Cohen & Felson, 1979), and the opportunity model (Cohen, Kleugal & Land, 1981), Fattah (1991) developed the differential risk model of criminal victimisation. The model does not focus specifically on the lifestyle or demographics of the victim. Instead, it consists of an integration of the various theories into a single comprehensive model, which outlines ten categories that could influence the risk of victimisation. The ten broad categories include opportunities, risk factors, motivated offenders and exposure, associations, dangerous times and places, dangerous behaviour, high-risk activities, defensive/avoidance behaviour and structural/cultural proneness (Cinini, 2015: 35).

Firstly, opportunities, where according to Fattah (1991: 341), criminal victimisation is not random, but rather depends on if the offenders are provided with any available opportunities to commit a crime against a victim. A close link can be found between opportunities to victimise and a potential target's characteristics, including their lifestyles, behaviours and routine activities. Fattah (1991: 341) also recognises that lack of guardianship can be an essential opportunity factor. Secondly, an individual's likelihood of being victimised may be determined

© University of Pretoria

by various risk factors in the form of attractiveness, suitability, accessibility and vulnerability. Socio-demographic characteristics of the target, such as age and gender, the area where the individual resides and absence of guardianship, are all viewed as potential risk factors that can increase victim vulnerability (Saponaro, 2019: 22).

The third category suggests that the likelihood of victimisation depends on the number of motivated offenders residing in the same areas as the potential victims. Individuals who live in densely populated and socially disorganised areas, consisting of a large number of male residents between the ages of 12-20 years, are more likely to be victimised (Saponaro, 2019: 22). Fourthly, an individual's exposure to potential offenders and high-risk activities increases their likelihood of being victimised. Variations in the potential victims' characteristics, such as their age, gender and routine activities, for example engaging on social media every day, influences the level and degree of exposure. The fifth category includes differential associations where the model states that individuals in close personal, social or professional contact with potential offenders run a greater risk of being victimised (Saponaro, 2019: 23).

The sixth category, namely dangerous times and places, suggests that an individual's routine pattern of behaviour influences their risk of being victimised; for example, a student walking home at night may increase their likelihood of victimisation. The seventh category includes dangerous behaviours, whereby certain situational variables may increase an individual's risk of victimisation, for instance, behaviours such as negligence, ignorance and provocation (Saponaro, 2019: 23). The eighth category involves high risk-activities, which suggests that offenders and victims may not always be part of two distinct groups (known as the equivalent group hypothesis). Individuals who have high-risk lifestyles, for example, working as illegal sex workers, may increase their risk of victimisation. The ninth category considers a person's attitudes towards risks, influencing their chances of being victimised. For example, individuals who ignore the threat of victimisation increase their chances of being victimised over individuals who fear crime and take the necessary precautions to avoid victimisation (Saponaro, 2019: 23). Lastly, structural/cultural proneness. There is a positive relationship between powerlessness, deprivation and criminal victimisation frequency. Minority groups or individuals who belong to groups that are for example, culturally stigmatised, are more at risk of being victimised (Saponaro, 2019: 23).

Although the model seeks to combine all relevant contributory factors to provide a clearer picture of criminal victimisation, there are some noticeable limitations. For instance, the model has been criticised for differentiating the victim from others by highlighting their personal or behavioural characteristics, thus solely blaming the victim for the crime committed against

© University of Pretoria

them (Walklate, 2003: 126). Another limitation is that the model suggests that an individual's associations specifically refer to whom they come into contact with (Saponaro, 2019: 23); however, some crimes, such as cybercrimes can occur without the two parties ever coming into contact with each other. Finally, the model proposes that individuals who live in poor and densely populated areas run the greatest risk of victimisation (Saponaro, 2019: 23); but the model should not exclude other environments where crime can also occur, for example, online.

3.3 Perpetrator-orientated theories

Perpetrator-orientated theories seek to explain what behaviours, lifestyles, and characteristics of the offender influence the risk of victimisation. Such a theoretical framework will investigate how an offender plays a role in criminal behaviour, for example, by examining how they perceive the actions displayed by the victim. Furthermore, perpetrator-orientated theories will consider the role of situational conditions, offenders' motives and perpetrator dispositions as factors that might increase the likelihood of a crime occurring (Dalal & Sheng, 2018: 103).

3.3.1 Cyberbullying model

In an attempt to understand cyberbullying, various criminological theories were traditionally applied, for example, the theory of reasoned action (Doane, Pearson and Kelley, 2014) and the general strain theory (Agnew, 1992). However, both theories have various criticisms, primarily based on the fact that they do not differentiate between traditional offline bullying and cyberbullying. Therefore, the Barlett and Gentile Cyberbullying Model (BGCM, 2012) was established and is regarded to be the primary theoretical model used to predict cyberbullying perpetration (Barlett, Madison, Heath & DeWitt, 2019: 250). The BGCM suggests that cyberbullying behaviour is a learned process, whereby each time an individual harms a victim online, they recognise that they are (a) more likely to be anonymous and (b) that the online world is an equal playing ground to commit a crime. The reason cyberspace is an equal playground, is due to the fact that characteristics such as a person's stature, looks and status, will not influence whether an individual decides to bully someone online or not (Barlett & Chamberlin, 2017: 444).

The BGCM is based on two aspects: (a) anonymity perceptions and (b) the belief in the irrelevance of physical stature. The two aspects are related to the previously mentioned factors that make cyberbullying behaviour a learned process, which helps predict and identify cyberbullying attitudes. In terms of the perception of anonymity, the BGCM proposes that individuals are more likely to feel anonymous within various social media sites, as the online

© University of Pretoria

platforms provide offenders with the opportunity to conceal their true identities. Online, offenders can create fake social media profiles and pretend to be other people in order to hurt or cause humiliation to the victim. Secondly, it has been found that a reason why many individuals view cyberbullying as an attractive way to cause harm is that anyone with a device connected to the internet (e.g., tablet, computer, cellular phone) can cyberbully others, regardless of their physical stature (Barlett, Chamberlin & Witkower, 2016: 148). The BGCM further expands on predicting cyberbullying behaviour by examining the amount of time an individual spends online and how technology is accessed (Barlett et al., 2019: 251). Although the theory is accepted as a suitable framework to understand cyberbullying, there are various untested assumptions and criticism within the theory, such as whether age influences cyberbullying behaviour development. Lastly, another limitation to the theory can include that the theory dismisses the routine behaviours of the victims, which might influence the likelihood of victimisation.

3.3.2 Online disinhibition effect

Researchers have observed a new phenomenon of how an individual's behaviour online appears quite uninhibited compared to their typical behaviour conducted offline. Such phenomenon is known as the online disinhibition effect (Suler, 2005: 184). Online disinhibition has been recognised as an important factor that influences a person to behave in a correct or deviant way within an online context. Online disinhibition can be described as a psychological state in which individuals feel more comfortable and willing to engage in certain behaviours online that is atypical to what they do or say offline. Research has shown that some individuals take advantage of the freedom provided to them by cyberspace and actively participate in intentional and deviant behaviours that aim to upset, humiliate or hurt other online users (Cheung, Wong & Chan, 2020: 2).

The online disinhibition effect can be defined and conceptualised in three main ways. Firstly, online disinhibition is a behaviour concept consisting of two different types of behaviours namely, benign disinhibition and toxic disinhibition. Benign disinhibition refers to the online environment that encourages and provides a space for individuals to share personal details about themselves and their emotions. Individuals may also use the internet as a way to explore their inner selves and solve interpersonal issues. On the other hand, toxic disinhibition may be equivalent to the modern concept known as being a 'troll', which is illustrated in the form of using rude or derogatory language, harsh commentary, 'hate speech' and threats (Cheung, Wong & Chan, 2020: 2). The second way in which online disinhibition can be conceptualised, is by defining it as a psychological state of mind of online users, where users feel less

© University of Pretoria

restrained and will thus, act in an atypical manner to their offline behaviours (Cheung, Wong & Chan, 2020: 3).

The last way online disinhibition can be conceptualised is by defining it as a collection of various internet characteristics, such as (Cheung, Wong & Chan, 2020: 3-4; Suler, 2005: 184-186, 187-188):

- Dissociative anonymity refers to the individual's opportunity to separate their online behaviour from their offline lifestyle and identity. By dissociating, the individual can behave in any way they want, without facing any consequences of their actions.
- Invisibility and anonymity go hand-in-hand; however, invisibility provides individuals with an opportunity to investigate and monitor other online users' profiles and personal information without the victims ever knowing. Invisibility may also contribute to the disinhibition effect as people do not have to worry about how they look or sound when interacting online.
- Asynchronicity refers to online communication not taking place in 'real time'; therefore, it provides the offenders with a way to avoid the victim's immediate reaction to their behaviour.
- Solipsistic introjection, which refers to how people perceive each other online. However, such introjection may cause individuals to fantasise about their online relationships with other users.
- Dissociative imagination can be defined as the degree to which an individual perceives the online environment as an imaginary world that has no connection to reality. However, as a result, individuals do not take responsibility for their behaviours online as in their minds, it has nothing to do with their reality.
- Finally, minimisation of status and authority, where everyone has an equal opportunity to voice themselves in an online environment, regardless of their offline status, wealth, race and gender.

No criticisms are found regarding the online disinhibition effect; however, based on the criticisms of the above theories and models, it can be said that some may also apply to the model. For example, the model is offender-focused and does not consider the victims' role in criminal behaviour, such as sharing personal information with strangers online. Furthermore, factors such as online group pressure and gender differences are also excluded in the model; however, they might be considered contributory factors that influence the likelihood of victimisation.

© University of Pretoria

3.4 Towards an integrated model of online victimisation

Integrated theories are models that combine the concepts and fundamental propositions from two or more prior existing theories to create a new single integrated model that seeks to provide a more comprehensive explanation of a particular phenomenon (Krohn & Eassey, 2014: 1). The control balance theory (Tittle, 1995) is an example of an integrated model and will be examined below. Following that, the study's integrated model for online perpetration and victimisation will be discussed.

3.4.1 Control balance theory

The control balance theory was originally developed by Tittle (1995) and became the foundation of the general theory of deviance. The extended control balance theory by Piquero and Hickman (2003) is a victimology theory developed from Tittle's control balance theory, and proposes that the amount of control people are subjected to and the amount of control they exercise, influence the likelihood and type of deviant behaviour. Exercising control and being controlled are factors that influence the behaviour and opportunities presented to an individual. Such factors may further be facilitated or limited depending on other people's willingness and ability to help or hinder the individual (Piquero & Hickman, 2003: 283).

An individual's control ratio can be balanced or unbalanced. If the control ratio is balanced, they will be inclined to perform conforming behaviour, whereas if the control ratio is unbalanced, the individual is predisposed toward engaging in deviant behaviour. A control surplus refers to when an individual can exercise more control than she or he is subject to. Such control may result in the individual engaging in deviant behaviours, such as exploiting others. A control deficit refers to when an individual is subject to more control than she or he can exercise. Individuals with a control deficit will typically engage in three types of behaviours in order to restore balance. Firstly, predation, where the individual turns to violence; secondly, defiance, where the individual questions the control but avoids violence; lastly, submission, where the individual accepts the control and submissively obeys the demands of others (Piquero & Hickman, 2003: 284). It is important to note that although certain crimes occur randomly, offenders with a control surplus seek out vulnerable and easy targets with control deficits (Piquero & Hickman, 2003: 285).

Individuals with control deficits do not have the confidence and/or skills to defend themselves against offenders who may victimise them. Individuals with a control surplus can detect individuals who may be weaker and appear more helpless and choose to exploit them for their

© University of Pretoria

own gain. As a result of such behaviour, being an individual with a control deficit becomes a predictor for victimisation as, as their vulnerability increases, so will their risk of being victimised (Piquero & Hickman, 2003: 286). Piquero and Hickman (2003) argued that individuals with control deficits are typically seen as weaker, primarily because of their perceived control disadvantage. The control deficits that individuals experience decreases their desire for autonomy in a way that might create feelings of humiliation (Piquero & Hickman, 2003: 286). As a result of the deficit in control, individuals become passive, withdrawn and submissive (Rothbaum, Weisz, & Snyder, 1982). As a result, individuals are less likely to engage in protective behaviours (Piquero & Hickman, 2003: 285). On the other side of the control balance ratio are individuals with control surpluses. Individuals with a control surplus are also likely to be at risk of victimisation, as they are likely to embrace feelings of impunity, invulnerability, and untouchability. As a result, such individuals will continuously attempt to hold onto such control but engage in behaviours that may place them at risk of being victimised. For example, individuals with a control surplus might participate in thrilling and risky actions, situations and events, such as sharing personal information to strangers online (Piquero & Hickman, 2003: 286).

Only a few limitations are included regarding the control balance theory. Such limitations are the presumption that individuals with a control deficit are more likely to engage in predatory acts more frequently than individuals with a control surplus. Furthermore, the belief that in order to decrease one's control deficit, individuals need to engage in deviant behaviour, so that they can increase their control surplus (Piquero & Hickman, 1999: 336).

3.4.2 Integrated model

Through examining the available literature, it is clear that more attention has been paid to new theoretical understandings of online victimisation, for example, Harris and Steyn (2018) set out to examine the gender differences in adolescent online victimisation and sexting expectancies by collecting data from 83 learners attending two private schools in South Africa. The study also used the theory of reasoned action in order to explain victimisation that took place online (Harris & Steyn, 2018: 25). Furthermore, Jalil and Sinnamon (2019) focused on the risks of online victimisation within their study among 55 college students on mobile social networks within a university in Australia (Jalil & Sinnamon, 2019: 396). However, as the study examines the correlates and predictors of online victimisation among undergraduate students attending a South African university, a single comprehensive, integrated model based on traditional victimology theories, was needed to understand the unique crime phenomenon

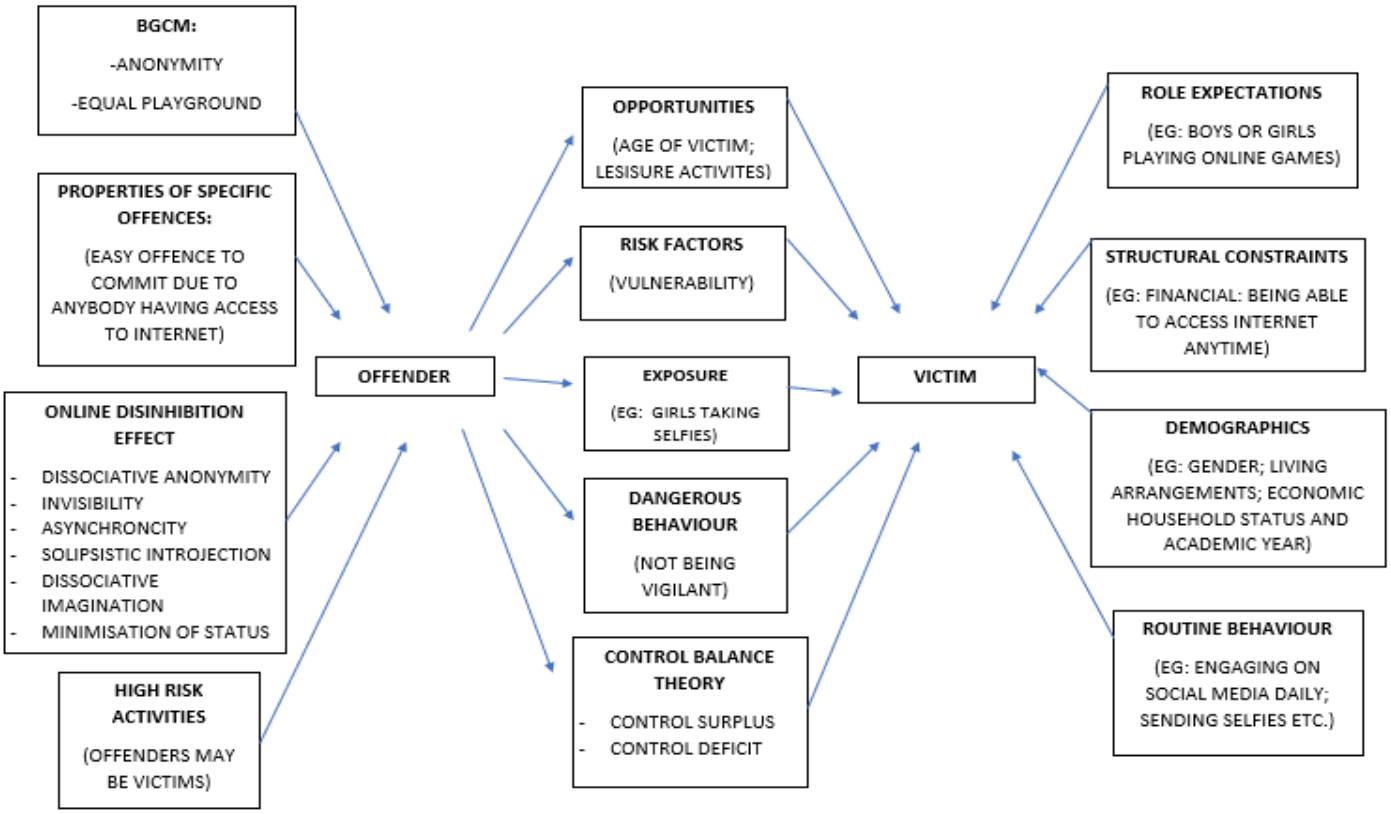
© University of Pretoria

better.

The integrated model consists of various elements from various victimological theories and models that have been combined into a single comprehensive model designed to explain and understand online victimisation. The integrated model is divided into three components, whereby the first component consists of causation factors that directly influence the offender in committing a crime. The component made use of the Barlett and Gentile Cyberbullying Model (2012) as it is based on two aspects: firstly, anonymity perceptions and secondly, the belief that participating in an online platform is an equal playground for all (Barlett, Chamberlin & Witkower, 2016: 148).

In terms of the perception of anonymity, offenders are more likely to commit a crime online, as they can hide their true identities and thus, cause harm without having to face any consequences. Secondly, as the internet is considered an equal playing field, offenders of all ages, gender, race, status, and socio-economic backgrounds can commit a crime. Therefore, online victimisation is considered to be an attractive crime, as anyone with a device that is connected to the internet can be victimised (Barlett, Chamberlin & Witkower, 2016: 148).

Diagram 1: Integrated model of online victimisation



© University of Pretoria

The first component also incorporates an element of the opportunity model developed by Cohen, Kleugel and Land (1981), namely properties of specific offences, whereby such element refers to the ease of committing an offence (Booyens, 2009: 96). Since any person can access the internet, it increases the likelihood of an offender perpetrating an online offence. Thirdly, the first component consists of various internet attributes as mentioned in the online disinhibition effect, such as (Cheung, Wong & Chan, 2020: 3-4; Suler, 2005: 184-186, 187-188):

- Dissociative anonymity refers to offenders feeling a sense of invincibility because no one knows who they are, and thus they can say or do anything they want without having to feel accountable for their actions.
- Invisibility is connected to anonymity and refers to offenders not worrying about what others think about them, as their identities are concealed.
- Asynchronicity refers to the fact that communication online is not in 'real time', which means that an offender can commit a crime and does not have to deal with the immediate reactions experienced by the victim.
- Dissociative imagination, whereby offenders can create a fantasy world online, where the offender can build 'fake' relationships with people and behave in ways different from how they behave in an offline setting. However, some offenders may not be able to keep their dream world and real-world separate, resulting in certain crimes taking place, such as cyberstalking.
- Lastly, the minimisation of authority links to the contributory factor that proposes that the internet is an equal playing ground; therefore, any person can commit a crime.

The first component also includes high-risk activities, as mentioned in the differential risk model, whereby Fattah (1991) states that offenders may have been previous victims themselves. Within the integrated model, it refers to the fact that if offenders were previously victims, they would know the ease of committing an offence and thus would want to commit the crime against somebody else. In addition, the victims may feel vulnerable being on the receiving end of victimisation, therefore, by perpetrating the crime, power can be restored back into their hands.

The second component of the integrated model consists of factors that link the victim and the offender. If the factors are present for the victim, it increases their risk of being victimised by the offender. Such components incorporate various elements from the differential risk model, such as opportunities, which refers to the victims' characteristics and their activities and

© University of Pretoria

behaviours (Booyens, 2009: 97). For example, if a young woman posts a picture every morning on Instagram, it might provide the offender with an opportunity to use her picture for themselves or to harass/insult her. Secondly, risk factors which refer to attractiveness, vulnerability, age and guardianship of the suitable target (Booyens, 2009: 97). In terms of the integrated model, guardianship could refer to the policies developed by various social media platforms, for example, Facebook users are able to report harassment and bullying to the site. Therefore, such policies may safeguard the victims and decrease their risk of victimisation. Thirdly, exposure, however, in terms of the integrated model, it does not refer to the offender coming into contact with the victim, but rather that exposure strengthens the target's attractiveness. For instance, if a victim does not make their account private, it increases their vulnerability to being victimised by an offender. Lastly, dangerous behaviour, whereby offenders are more likely to target individuals who are less vigilant to online crime, compared to people who take safety precautions, such as making their social media settings private, having sufficient antivirus systems installed and having multiple secure passwords (Booyens, 2009: 98). Furthermore, the second component also consists of two values outlined in Picquero and Hickman's extended control balance theory, such as offenders having a control surplus and victims having a control deficit (Van Niekerk & Coetzee, 2020: 21). Such values link to factors such as invisibility and anonymity, in that offenders will have a control surplus due to their identities being concealed. As a result, the victim will be unaware of who is victimising them, which increases their control deficit. The online victimisation may have emotional consequences as the victim is unaware of who committed the crime, their feelings of humiliation or invasion of privacy may have more of a significant impact on them.

The third and last component speaks of factors that directly influence the risk of an individual falling victim to a crime committed online. Such components use two elements from the lifestyle/exposure theory, namely role expectations and structural constraints. In terms of role expectations, individuals can be victimised whilst performing activities that are expected of them by society. Such social roles are determined by age, marital status, gender, occupation and education (Lutya, 2010: 9). For example, in terms of the integrated model, male students might play more online games, compared to their female counterparts. As a result, they may be exposed more to crimes such as online harassment, receiving a virus, repeated messages or identity fraud. Secondly, in terms of structural constraints, such element refers to social and economic structures which restricts a person's behavioural patterns (Lutya, 2010: 10). In terms of the present model, individuals from higher-income households, may have more access to the internet, which increases their risk of being victimised. The third component also indicates that the victims' demographics influence their risk of victimisation. Their demographics include gender, living arrangements, economic household status and their academic year. For

© University of Pretoria

instance, if the victim lives with their families, it could decrease their risk of victimisation as they may, for example, spend less time online or post fewer photos of themselves on social media. Lastly, an individual's routine behaviour can influence their risk of victimisation. For instance, if a victim chooses to leave their 'online status' on within various social media platforms, an offender might be able to monitor their online activities and may cyberstalk them. The author fully acknowledges that the integrated model proposed represents preliminary theorising in an attempt to explain factors that influence online victimisation from occurring.

3.5 Summary

The applicable theoretical framework consists of various victimology theories and models that highlight university students being especially vulnerable to experience online victimisation. Various key features that most of the theories discussed were that a student's routine behaviour and socially expected lifestyles are significant factors influencing their risk of victimisation. In addition, it is not merely the socio-demographic characteristics of students that play a role in victimisation but also their financial, social and familial constraints that contribute to victimisation. A student's attitude towards online crime also significantly influences their risk of victimisation. Students in close proximity to offenders are irrelevant, as any person from around the world can access the internet at any time of the day. Therefore, any person who has access to the internet through a device can commit a crime and/or become a victim of online victimisation.

© University of Pretoria

Chapter 4: Research methods

4.1 Introduction

The following chapter focuses on the research methods used to investigate online victimisation among undergraduate students. Before data collection commenced, the most suitable methodology was selected to accurately gather and analyse data concerning the phenomenon in question. The research methods include the research approach, purpose and type of research and the research design. In addition, the study population and sampling procedure, data collection, data analysis, the pilot study and ethical considerations will also be discussed. Lastly, the limitations and challenges of the methods used will be examined.

4.2 Research paradigm and approach

The positivist paradigm was opted for as the study aimed to investigate the human phenomena of online victimisation by utilising scientific tools to obtain objective and quantifiable results (Rahman, 2016: 106). Positivism is related to the idea of a fact-based investigation and views the world as it is. Thus, it was the most suitable approach as the study required separation between the researcher and the respondents to objectively obtain empirical findings (Wahyuni, 2012: 70-71). The overall aim of positivism is to produce reliable, objective knowledge which could then be used to improve society in the future (O'Reilly, 2012: 164). The study aims to better understand the correlates and predictors of online victimisation among university students, thus becoming a point of reference for future research and theories to develop.

The majority of all positivist studies are quantitative in nature (Neuman, 2014: 62). Thus, a quantitative research approach was opted for, as it was found to be the most suitable approach to achieve the aim of the study. The study required the data to be obtained objectively and without bias whilst focusing on the undergraduate students affected by online victimisation (Burrell & Gross, 2018: 1379). As the researcher needed to numerically count and measure the nature and extent of the phenomenon in question, it further highlighted that a quantitative research approach was most appropriate (Kumar, 2011: 13). In addition, factors such as the time and cost of gathering and analysing data were considered (Burns & Grove, 2005: 22).

A quantitative research approach can be defined as the systematic investigation of a social phenomenon, which is achieved by collecting numerical data that is then statistically analysed and presented (Muijs, 2011: 2). In the context of the study, the quantitative research approach

© University of Pretoria

focused on narrowing down the research problem by examining factors, such as undergraduates' students access to and use of the internet, that appear to be correlates and predictors of online victimisation (Kraska, 2012: 1168). A quantitative research approach was opted for, as it enabled the researcher to produce knowledge and create a better understanding of the social world where undergraduate students are targeted as victims of online victimisation (Burrell & Gross, 2018: 1379). Furthermore, the data obtained by employing a quantitative research approach provided the researcher with insight into what factors influence the likelihood of online victimisation among undergraduate students and the consequences the sample population face as a result of the victimisation (Burrell & Gross, 2018: 1379).

4.3 Purpose of research

The study was descriptive in nature, as it aimed to determine the experiences of online victimisation among undergraduate students attending a South African university. Descriptive research describes the existence of a social phenomenon whilst focusing on discovering new facts, for instance, information relating to the undergraduate students' responses to online victimisation, which has previously been neglected and ignored by existing research (Blanche, Durrheim & Painter, 2006: 44). The study systematically describes a phenomenon or attitudes towards an issue rather than examining any cause-and-effect relationships (Kumar, 2011: 383). Furthermore, descriptive research, also known as statistical research, describes situations and events in detail through scientific observation. The key purpose of the study was to identify and obtain precise information regarding the extent of online victimisation, which was achieved by collecting data that accurately represents the online experiences of undergraduate students. Therefore, focusing on obtaining the answers to questions such as: what, who, where, how and when (Akhtar, 2016: 75-76).

4.4 Type of research

Basic research, also known as pure research, was carried out in the study, as the study focused on gaining a better understanding of online victimisation among undergraduate students, which existing research has previously neglected (Miller & Salkind, 2011: 3). The research was guided by the researcher's curiosity in seeking more knowledge about the unique crime typology, purely for the sake of gaining insight and expanding on what is already known, rather than to solve any practical problems (Salkind, 2011: 74). Basic research was carried out in the hopes of developing general principles and theories that can better explain online victimisation (Miller & Salkind, 2011: 2). It also focuses on capturing, recording and

© University of Pretoria

measuring the nature of the relationships between the variables in the study (Gaber, 2012: 38). Through gaining new knowledge, the researcher can make recommendations to guide policies and future research into discovering ways to prevent undergraduate students from falling victim to online victimisation (Salkind, 2011: 74). Basic research starts with a research question: what are the experiences of online victimisation among undergraduate students? Such a question is typically based on victimology theories and previous empirical investigations, where the researcher must, through the basic research, either confirm or disprove previous findings (Gaber, 2012: 37-38). Simply put, the purpose of basic research is to find out the way in which a social phenomenon comes into existence and how victims respond to it (Lewis- Beck, Bryman & Liao, 2011: 54).

4.5 Research design

Once the research question has been established, a research design must be selected to guide the direction of the study. A research design acts as a blueprint for the study and outlines the process of collecting, measuring and analysing the data in the most logical way (Mishra & Alok, 2017: 7-8). Within the study, a non-experimental research design was chosen, namely a survey design. A survey study was found to be the most appropriate design to use because the study focused on gaining knowledge regarding university students, who make up a large percentage of a society's total population. Thus, a survey design was needed as it is typically used when researchers need to ask a large number of willing individuals questions about their behaviours, attitudes, previous experiences and opinions (Marczyk, DeMatteo & Festinger, 2005: 151, 154). Still keeping the aim of the study in mind, survey research examines various measurable characteristics of the undergraduate students, such as how often they use the internet for social media, and determine whether it relates to their experience of online victimisation (Marczyk, DeMatteo & Festinger, 2005: 151). In the study, once the questions were asked by means of administering a questionnaire, the responses were summarised in order to draw inferences about the social phenomenon (Leedy & Ormrod, 2016: 141).

There are many advantages when utilising a survey study. For instance, the survey was instrumental in investigating the profile and characteristics of undergraduate students, as it made sampling practical and provided greater flexibility during data analysis (Babbie & Mouton, 2003: 263). In addition, as the study intended to determine online victimisation experiences among undergraduate students, surveys can assist the researcher by producing numerical information (Neuman, 2011: 309). Such statistical information can determine whether any relationships exist between variables (Muijs, 2011: 10). A survey design proved to be more efficient as it could gather large amounts of data concerning undergraduate

© University of Pretoria

students by asking many questions at once, at reasonably low costs and effort (Muijs, 2011: 10). Finally, a survey made it easier for the researcher to ensure that the respondents remained anonymous, thus safeguarding one of the ethical considerations applicable to social science research. However, there are some limitations to survey research. For example, the surveys may restrict the researcher's control over the environment, as the students are responsible for completing the questionnaire independently. Furthermore, it can also be difficult for the researcher to gain a deeper understanding of the phenomenon and contextual differences, as surveys are standardised and limited in length, thus not providing opportunities for in-depth responses (Muijs, 2011: 10).

A correlational survey was conducted, which examines the extent to which differences in one variable are associated with differences in one or more other variables. A correlation, therefore, exists when one variable has different outcomes for dissimilar sample groups, in a somewhat foreseeable way. In the study, there are many advantages to using a correlational study. For instance, as the researcher gathered quantitative data about various characteristics, such as living arrangements and household economic statuses, relating to the undergraduate students (Leedy & Ormrod, 2016: 137-138), the correlational survey design did not manipulate any of the characteristics, as its aim was to rather identify and explore whether the variables were interrelated and showed meaningful differences (Wilson & Joye, 2019: 2).

Furthermore, correlational surveys allow the researcher to study the undergraduate student's behaviour, as it occurs every day (Stangor, 2011: 177). Therefore, it enables the researcher to achieve part of the studies objectives, which was to construct a profile of undergraduate students who are more likely to be victimised online. However, there are some disadvantages to using correlational surveys; namely, correlations do not mean causation, in that no cause-and-effect relationships can be determined. As a result, the researcher may uncover relationships between variables that may not have been previously known, but the correlational study cannot provide a conclusive reason why that connection exists (Stangor, 2011: 178). Lastly, the outcomes of the correlational surveys can be significantly impacted by the nature of the questions asked to the undergraduate students. For example, if the survey questions did not ask the respondents how they access the internet, it could severely harm the researcher's aim of determining the predictors of online victimisation (Gaille, 2020).

4.6 Research methods

The discussion below provides an overview of the study population and sampling method, the methods used in data gathering, data analysis, data quality and any ethical considerations.

© University of Pretoria

4.6.1 Study population and sampling

Sampling is defined as the process of selecting a portion of a population to be included in a study (Fitzgerald & Fitzgerald, 2014: 32). A non-random, convenience sampling procedure was applied to the research. Non-random, also referred to as non-probability sampling, is a sampling method of selecting participants from a population using a subjective (non-random) method. Within the sampling procedure, the participants are included with unknown probabilities, or probabilities known to be zero (Vehovar, Toepoel & Steinmetz, 2017: 2). Simply put, non-probability sampling is a sampling procedure that does not provide all of the participants in the population the same chance to be in the sample (Daniel, 2012: 67). Another limitation of non-probability sampling includes the researcher's lack of control over who responds to the questionnaire; thus, they may not be able to control how seriously the participants take the study, which may result in false responses (Bourque & Fielder, 2011: 15). Advantages of non-probability sampling include that it is quick and convenient, which assists researchers in collecting and analysing the results in a shorter time-frame and it is inexpensive as respondents are typically individuals within close physical proximity to the researcher, for example, the respondents of the study attended the same university as the researcher. Finally, it reduces the burden placed on the respondents, as they are not asked personally to participate, but rather if they are willing and available, they will agree to engage in the study (Statistics Canada, 2021).

Convenience sampling forms part of non-probability sampling and is applied on a 'first-come, first-served' basis (Luborsky & Rubinstein, 1995: 104). Also known as availability sampling, it refers to a method of selecting participants who are readily available and who volunteer on the days of data collection. Their availability typically relates to the physical proximity and ease of accessibility (Waterfield, 2018: 403). The advantages of using convenience sampling are that it is the most useful sampling procedure to use when there are limited resources available, such as time and money (Marston, 2010: 107). Additionally, it is the most suitable sampling method to use when the research does not aim to generate results to create generalisations relating to the total population (Etikan, Musa & Alkassim, 2016: 1). However, such an advantage can be seen as a limitation of the study, as further discussed. Limitations to convenience sampling include, the sample is not representative of the entire population, as it only includes students who were available and willing to participate; thus, the sampling procedure provides an opportunity for selection bias (Taherdoost, 2016: 23).

A total of 1 695 students were registered for undergraduate Criminology modules. Of the 1 695 registered undergraduate students, 1 001 participated in the study, amounting to a response

© University of Pretoria

rate of 59.1%. According to the literature, a response rate of 50% is adequate for reporting and analysis, a response rate of 60% is regarded as good, and a response rate of 70% is considered very good (Babbie & Mouton, 2001: 261). A total of 1 100 questionnaires were printed, 1 001 completed questionnaires and 99 blank questionnaires were recorded, resulting in 91.0% of the questionnaires being adequately completed and returned. Consequently, 9.0% of the distributed questionnaires were handed back to the data gatherers unanswered. It is important to note that prior to the distribution of the questionnaire, arrangements were made with the three Criminology lecturers to ensure that minimal disruption would take place during class. Furthermore, the sampling criteria did, however, exclude graduate students. The reason being was because there were more undergraduate students, which allowed for the sample population to be larger, thus getting more accurate and thorough results. Finally, the researcher only selected undergraduate students registered for Criminology modules, due to the ease of access to such students.

4.6.2 Data collection instrument and method

The most suitable technique to collect the data from the sample population was through a self-administered questionnaire. The questionnaire, which consisted of two-pages with a total of 26 closed-ended questions, was set up using pre-existing questionnaires which was compiled from Finn (2004), Sticca, Machmutow, Stauber, Perren, Palladino, Nocentini, Menesini, Corcoran and McGudin (2015) as well as Cetin, Yaman and Peker (2011). The questionnaire consisted mostly of closed-ended and matrix-type questions. The closed-ended questions were used as they are more easily understood and it also allowed the researcher to make more effective comparisons between the respondent's answers after all the data was gathered (Babbie, 2007: 246).

A questionnaire can be defined as a formalised set of questions used to obtain information from the respondents of a study, in order to achieve the research objectives. A questionnaire enables quantitative data to be collected in a standardised way so that the data can remain internally consistent for analysis (Malhotra, 2011: 83). Standardisation, with regards to data collection, means that all of the respondents were asked the same questions in the same manner (Clow & James, 2014: 324). A self-administered questionnaire refers to a questionnaire that has been designed to be self-explanatory and independently completed by the participants. As no intervention or assistance is provided by the researcher, how the questions are worded and the structure of the questionnaire, needs to be carefully designed, to avoid measurement error (Wolf, 2011: 804).

© University of Pretoria

The self-administered questionnaires were distributed within a group setting, for instance, in a lecture hall. In such group administration, each person is expected to complete the questionnaire without consulting other persons in the group. Students were informed about the purpose of the study, and introductory instructions were communicated about the instrument (Bourque & Fielder, 2011: 2). There are various advantages when employing a self-administered questionnaire; for instance, it allows for an easier analysis which is thus less time-consuming. Secondly, as the study is dealing with a sensitive topic, self-administered questionnaires are useful as the respondents may feel more comfortable in answering questions about their experience as interviews are not involved (Bourque & Fielder, 2011: 10). Lastly, as no interviewer is present to insert bias in the way that they ask the questions, and because the same questionnaire is administered to all respondents, it further ensures that the researcher will obtain a more accurate representation of the phenomenon (Readex Research, 2021).

In terms of disadvantages, although the self-administered questionnaires were distributed to 1 001 undergraduate students, the obtained data may not necessarily represent the total sample population (the disadvantage will be discussed in the limitations of the study). Furthermore, as the researcher lacks control over how the respondents answer the questionnaire, the researcher cannot prevent the respondents from lying about their background information or online victimisation experiences. The researcher also does not have control over whether the students leave some questions unanswered. Therefore, inaccurate data may be collected, which may affect the study's validity (Bourque & Fielder, 2011: 15).

As mentioned, the self-administered questionnaire consisted of 26 structured and closed-ended questions. Structured questions direct the questionnaire format and specifically set out the responses required by the researcher (Malhotra, 2011: 88). Structured questionnaires typically make use of closed-ended questions, whereby the researcher used dichotomous questions, which consists of only two response options, multiple-choice questions, which provide the respondents with three or more answers to choose from (Clow & James, 2014: 332), and scale questions, which refers to several statements or questions that are rated by the respondents (Blanche et al., 2006: 489).

An example of a dichotomous question presented in the self-administered questionnaire is:

© University of Pretoria

Section 1 – Background information

1. How old are you?	years

2. Are you:	Male		Female	

Additionally, an example of a multiple-choice question used in the study is:

8. How many hours per day do you spend on the internet?	Less than 1 hour	
	1 – 2 hours	
	2 – 3 hours	
	3 – 4 hours	
	More than 4 hours	

Lastly, an example of a scale question within the self-administered questionnaire is:

10. How often do you use the internet for the following activities?				
	Often	**Sometimes**	**Seldom**	**Never**
Social media (e.g. Whatsapp, FB)				
Studies (e.g. assignments)				
Blogs / blogging				
Entertainment (e.g. music, gaming)				

In closed-ended questions, the researcher makes prior assumptions about what the relevant categories are so that the respondents can immediately reply to the questions (Lewis-Beck, Bryman & Liao, 2011: 129). The most useful closed-ended questions are the ones that offer response options that accurately reflect the respondents' attitudes and thoughts towards the phenomenon in question. Additionally, the researcher must ensure that the respondents can only select the most applicable response option (Keeter, 2011: 134). There are various advantages to closed-ended questions; for instance, they provide respondents who may lack communication skills an opportunity to answer the questions as best as possible. Thus, ensuring more accurate data is collected. Respondents may be more willing to participate in the study, as they do not have to provide long responses to the questions, therefore encouraging them to be more honest about their experiences. Lastly, it is less time-consuming for the researcher to analyse and code all of the data (Hyman & Sierra, 2016: 2). However, disadvantages include: the researchers will be unable to obtain in-depth insights (this limitation of the study will be discussed further); if the categories do not reflect the thoughts of a respondent, and the categories may hint at the 'right' answer, thus, both resulting in inaccurate data being obtained (Hyman & Sierra, 2016: 3).

© University of Pretoria

4.7 Data analysis

Quantitative data analysis was conducted to interpret and understand the numerical data obtained from the survey study, namely from the structured questionnaire. The data were manually coded and reduced into standardised and manageable numerical forms (Dantzker, Hunter & Quinn, 2018: 372, 375) in order for the researcher to analyse the data by utilising a statistical test, namely the Statistical Package of the Social Sciences (SPSS) (IBM Corp, 2021). SPSS is a valuable tool for managing and accurately interpreting data in order to identify any trends or relationships; make inferences about the results (Grotenhuis & Matthijssen, 2021: 2), and examine how the results relate to other aspects of reality (Hilbe, 2015: 1). Following that, the data was then presented in a table format, as the research followed a quantitative approach.

Once the data has been entered into the dataset, the quantitative analysis begins. The study uses three types of data analyses: bivariate, multivariate, and descriptive analyses (Dantzker et al., 2018: 384). A univariate analysis uses descriptive statistics and is typically conducted to gain information about the data before bivariate and multivariate analyses are completed. Such analysis focuses on examining the characteristic of a single variable at one point in time and may involve the use of frequency distribution tables and measures of central tendency and variability (Dantzker et al., 2018: 400). Secondly, bivariate analysis is the examination of the relationship between two variables. Such analysis typically involves determining how an independent variable influences a dependent variable. Assessing the relationship between two variables will address the strength of the relationship, the direction of the relationship and the degree of significance (Dantzker et al., 2018: 413). Lastly, multivariate analysis examines the relationship between three or more variables. Typically, such analysis determines how a dependent variable is influenced by more than one independent variable. Such analysis offers more insight than bivariate analysis, as it can study the relationships among several variables simultaneously (Dantzker et al., 2018: 418).

The study used logistic regression, which refers to a model that analyses the relationship between multiple independent variables and a categorical dependent variable. The model then predicts the likelihood of an event occurring by fitting the data into a logistic curve (Hyeoun-Ae, 2013: 155). Logistic regression provides an indicator of the adequacy of the model by assessing the ‘goodness of fit’ (Pallant, 2007: 169). In order to assess the adequacy, the study utilised the Hosmer-Lemeshow test, a goodness of fit test for logistic regression, particularly for risk prediction models. The test informs the researcher how well the data fits the model.

© University of Pretoria

Specifically, the test calculates if the observed event rates match the expected event rates in the population subgroups (Statistics How To, 2021). The Nagelkerke R2 value indicates the amount of variation in the dependent variable explained by the model (with a minimum value of 0 to a maximum of approximately one) (Pallant, 2007: 211). In addition to statistics regarding the goodness of fit and R2 values, logistic regression models commonly create classification tables, to illustrate the predicted and observed values of the dependent variable for the cases in the analysis (Menard, 2013: 64). Simply meaning, the table informs the researcher how well the model can predict the correct category for each case (Pallant, 2007: 211).

In order to run the logistic regression, the study required the following: one or more of the independent variables had been on a continuous or categorical scale, for example, asking how often the respondents had experienced rumours being spread about them over social media or the internet. Secondly, it required one dependent variable to be dichotomous, for example, either answering male or female when asked about gender (Pallant, 2007: 166). Furthermore, logistic regression can handle relationships between variables, whereby if one changes, the other is unaffected (known as non-linear relationships) (Hyeoun-Ae, 2013: 156). Lastly, it is required that the categories of both the dependent and independent variables reflect the respondents' experiences and thoughts about the phenomenon, and the response options should ensure that the respondents can only choose one option (Quantemna, s.a).

The study made use of two measures of association, namely the odds ratio (OR) – presented as part of the logistic regression – and the Chi-square test. Firstly, the odds ratio (OR) represents the change in odds of being in one of the outcome categories when the value of a predictor increases by one (Pallant, 2007: 213). It is important to note that the odds ratio value is only an estimate at the true value, based on the sample data. As within the study, the sample consisted of a large population (1 001 students), therefore it is more likely that the odds ratio will be an accurate representation of the true value (Pallant, 2007: 214). The Chi-square test, which is a non-parametric statistic, is also known as a distribution free test (McHugh, 2013: 143) or the Pearson's chi-square test (Salkind, 2011: 138). The Chi-square test of independence is one of the most useful statistics for analysing group differences when the dependent variable is measured at a nominal level. The test informs the researcher about the significance of any observed differences between the variables and provides specific information on which categories account for any of the differences found (McHugh, 2013: 143). There are various requirements to be completed before the commencement of the Chi-square test; for instance, none of the categories may contain only a few items, preferably not less than five, but no less than one, and the number of the total items must be significant (at least 50) (McHugh, 2013: 144). In addition, the study groups are to be independent of each other, whereby if the two

© University of Pretoria

groups are related, a different test must be used, and lastly, the categories of the variables must ensure that the respondents can only choose one of the response options (McHugh, 2013: 144). Once the Chi-square results were obtained, the test used Crammer's *V* strength test. Cramer's *V* is an effect size measurement that investigates how strongly two categorical fields are associated (Kearney, 2017: 1). The greater the difference between the observed and the expected variables, the greater the effect size will be; therefore, the more likely the observed frequencies will differ significantly (Cramer & Howitt, 2011: 24). Cramer's V varies between 0 and 1 without any negative values. Values that are close to 0 means no association, however, a value larger than 0.25 is found to have a very strong relationship for the Cramer's V. Furthermore, values between 0.05 to 0.10 indicate a weak to moderate effect size, 0.10 to 0.15 denotes a moderate to strong, and 0.15 to 0.25 indicates a strong to very strong effect size (Akoglu, 2018: 92-93). The effect sizes are indicated for results that show a statistically significant association.

4.8 Data quality

Quantitative researchers must continuously keep in mind and ensure that the study meets two quality measurement standards: reliability and validity. A lack of both might result in the study being criticised and deemed of little use (Hagen, 2014: 431). Reliability is concerned with issues of consistency and unchanging replications of the findings. Measures of reliability evaluate the extent of individual differences between scores across the groups of respondents (Hagen, 2014: 431). Reliability consists of the following area of focus, namely, how similar the measurements are at any given time (Golafshani, 2003:598). Furthermore, a study's reliability can be determined through triangulation. Triangulation is used to better understand the topic under investigation and assumes that if the researcher uses various sources and employs different methods, the researcher's bias will be avoided (Flick, 2004: 179). However, a shortfall to using triangulation is that if the different sources produce conflicting results, it might cause confusion and lead to inaccurate results generated by the study (Cutcliffe & McKenna, 1999: 379).

Reliability can be subdivided into two categories, one of which is internal reliability. Within the study, the internal reliability of the questionnaire was measured by calculating Cronbach's alpha coefficient. The Cronbach's alpha coefficient is commonly used when a quantitative study uses a questionnaire with a scale as the research instrument to collect data (McNeish, 2018: 414). The calculation of Cronbach's alpha will result in a computed alpha co-efficient that varies between one and zero. A result of one (1.00) indicates that the study has perfect internal consistency, while a result of zero (0.00) indicates that the study has no internal

© University of Pretoria

consistency (Jonker & Pennink, 2010: 157). Within the study, the Cronbach's alpha coefficient for the scale relating to how often the respondents used the internet for each of the four activities was 0.199. Although the outcome is fairly low, it is generally accepted that scales with less than ten items often reveal low coefficients. The alpha coefficient for the victimisation scale (section three of the questionnaire) was 0.781, and the coefficient for the frequency of the victimisation scale (section four of the questionnaire) was 0.702, both of which were above the acceptable minimum level of 0.7 (Field, 2018: 823).

The study's validity may also measure the quality of the study, whereby it will employ measurements to assess the extent to which a study and the study's key components are valid (Given, 2012: 716). A study is valid if the measures are observed to actually measure what they claim to and if there are no logical errors when drawing conclusions from the data (Garson, 2013: 8). The concept of validity can be subdivided into internal and external validity. A study has internal validity when the instrument used in a study, measures what it intends to measure (Given, 2012: 716). In the study, the validity of the research must have face validity and predictive validity. A study has face validity when without the researcher knowing all of the facts, the study appears to measure the targeted concept (Horne, 2018: 34). In simple terms, it means that the test appears to test what is intended to be tested (Cohen, Manion & Morrison, 2007: 163). Within the study, determining the face validity was necessary, as the study's constructs were conceptually hard to separate from each other (Bhattacherjee, 2012: 59). Finally, the study must ensure predictive validity, which entails the test's usefulness to predict a future performance (Kothari, 2004: 74) that is theoretically expected (Bhattacherjee, 2012: 60). As discussed above, statistical procedures were used to predict the possibility of falling victim to different types of online victimisation.

4.9 Pilot study

A pilot study can refer to a small-scale version of a full-scale study or a trial run conducted before the study as a form of preparation. A pilot study enhances the reliability of the research instrument and enables the researcher to identify any problems within the study, for example, if the questionnaire does not make sense or is too complicated for respondents to complete accurately. Although the pilot study might predict possible errors, the researcher needs to be aware that a pilot study cannot guarantee that no problems will arise when the major study is conducted (Van Teijlingen & Hundley, 2002: 33-34). Furthermore, a pilot study can assist the researcher in developing, refining, and testing the measurement tools and processes (Kumar, 2011: 11). With the objective of improving the quality of the data in mind, a pilot study was

© University of Pretoria

conducted using 50 questionnaires that were distributed to undergraduate students who were not registered for undergraduate Criminology modules. The students were asked to complete the questionnaire and were, upon completion, questioned about the structure and wording of the questionnaire. Based on the pilot study, a few minor shortfalls in terms of wording and question construction were identified, and adjustments were made before the full-scale survey was conducted (Van Teijlingen & Hundley, 2002: 33-36).

4.10 Ethical considerations

Various ethical considerations were made when conducting the study. Firstly, the respondents received an informed consent form. An informed consent form is useful as it communicated the researcher's expectations for the study and described the phenomenon under investigation. It was also used to explain why the research was being conducted, what was expected of the respondents, the purpose and aim of the study, voluntary participation, expected duration, compensation issues, potential harm and how the findings will be distributed. The informed consent form is meant to protect the respondent and provide both the participant and the researcher with a mutual understanding of both parties' responsibilities and roles. Finally, it provided the researcher with an opportunity to address any questions or concerns at the beginning of the study (Gaiser & Schreiner, 2011: 33). The informed consent letter of the study is provided as Annexure D.

A second ethical consideration was that the participation in the study was voluntary. The participants must have been aware of any potential risks and benefits of participating and consent was needed in order to partake in the study. The respondents needed to understand that they could refuse to answer any specific questions and may withdraw from the study at any time. Such consideration represents the principle of autonomy, whereby individuals are free to volunteer and choose to participate in the study (Patten & Newhart, 2018: 74). Students had the right to decide whether they wanted to participate in the study or not, and they could withdraw from the survey without any penalty brought against them.

Thirdly, the study ensured anonymity and maintained confidentiality by reassuring the respondents that they did not need to share any personal information, such as their name or address, and that after the data would be collected, they would not be able to be identified (Kumar, 2011: 246). All of the data will be kept confidential, whereby only the researcher has access to the completed questionnaires, and the questionnaires will be kept safe at all times.

A fourth ethical consideration included the respondent's understanding that they would not be

© University of Pretoria

compensated for their voluntary participation in the study, and such consideration was explained in the letter of informed consent. Sharing information should be voluntary and not coerced (Babbie, 2014: 79).

A fifth ethical consideration stated that the participants were to be protected from physical and psychological harm, which also referred to the principle of beneficence. Beneficence means that the research attempted not to harm the participants, maximised any possible benefits and minimised any potential risks (Patten & Newhart, 2018: 73).

Although the researcher avoided to cause harm or emotional distress, a sixth consideration was that the respondents were provided with the contact information of a debriefing service in case they experienced secondary victimisation. The respondents were also informed that they were able to directly contact the researcher if any issues came about (Babbie, 2014: 71).

A seventh consideration made was that the researcher's bias was avoided. The researcher analysed and presented the findings without fabrication or falsification. All shortcomings, failures, limits, negative findings and methodological constraints were reported (Babbie, 2014: 76).

Lastly, permission to conduct the research was given by the Faculty of Humanities Ethics Committee and the Head of the Department of Social Work and Criminology. The research was neither funded by the University of Pretoria nor by an outside agency. The completed questionnaires will be safely stored in the Department of Social Work and Criminology for fifteen years.

4.11 Limitations and challenges

It is essential to identify and acknowledge the research methods' limitations and shortfalls. Although there are many advantages to employing a quantitative research approach, a major shortfall was that the researcher could not acquire in-depth information from the undergraduate students. Therefore, a limitation to the study was that the undergraduate's feelings, attitudes, thoughts and personal experiences concerning online victimisation would not be available, as no discussion took place to collect such data (Ivankova, Creswell & Plano Clark, 2007: 265). Secondly, as the quantitative data entailed secondary data, it limited the researcher's choice in designing the survey and what type of questions were asked in the questionnaire (Mahoe, 2004: 36). Thirdly, due to the research being basic in nature, the

© University of Pretoria

researcher could not apply the findings to solve any practical problems of the phenomenon. At most, the findings can be used to make recommendations that can guide policies, future research and theory building (Salkind, 2011: 74).

A fourth limitation identified in the study was that as the study's purpose was descriptive in nature, it was only able to describe the phenomenon and could not explain why undergraduate students experienced online victimisation (Kumar, 2011: 383). A fifth limitation can be found as the study employed a non-probability, convenience sampling procedure which may result in the possibility of undercoverage occurring. Undercoverage refers to certain participants in the population of interest being excluded from the sample (Waterfield, 2018: 403). A sixth limitation of the study was that as a self-administered questionnaire was distributed to the undergraduate students, it resulted in the researcher losing control over how the respondents answered the questions, which refers to the possibility that respondents purposely falsified their answers or responded incorrectly as they may not have understood what the question is asking them. As a result, it may cause inaccurate results to be obtained (Bourque & Fielder, 2011: 15). Lastly, although 1 001 undergraduate students completed the self-administered questionnaire, the obtained data cannot be generalised to the total population because a random sample of university students was not drawn (Bourque & Fielder, 2011: 11).

4.12 Summary

In the chapter, the researcher provided a detailed discussion of the research methodologies used in the study. The study employed a quantitative research approach that was basic in nature and descriptive in purpose. The research design was a correlational survey, and data was collected by distributing self-administered questionnaires completed by 1 001 students who were registered for undergraduate Criminology modules. A non-probability, convenience sampling procedure was utilised and was established on a 'first-come, first-served' basis. Once the necessary quantitative results were obtained, the data was recorded, coded and analysed by two statistical tests. Validity and reliability were the two measurements of the study's quality, which was further assisted by conducting a pilot study. Various ethical considerations were acknowledged, and any limitations and shortfalls to the study were identified. The following chapter will discuss the empirical results obtained from the questionnaires.

© University of Pretoria

Chapter 5: Empirical results

5.1 Introduction

The current chapter presents the empirical results gathered from the questionnaire completed by each respondent. The chapter is divided into three main sections: respondents' profiles, their experiences of online victimisation, and their reactions to such victimisation. The results are presented in tables, where the key findings are highlighted above the table figure. The descriptive results are presented first, followed by the bivariate results and the significant differences with their respective effect sizes. The Hosmer and Lemeshow test of the logistic regression results are explained directly after the respondents' experiences and responses to the online victimisation sections (in other words, after the individual bivariate tables). It should be noted that the logistic regressions mostly confirm the bivariate analyses.

5.2 Profile of respondents

The respondents' ages ranged from 18 to 50 years old, with a mean of 20.5 years and a standard deviation of 2.5 years. Nearly two-thirds of respondents were between the ages of 19 and 21 years. The majority of the respondents (n=821; 82.6%) were female[1]. More than half of the respondents were White (n=456; 46.0%), and slightly more than two in five (n=432; 43.5%) were Black. Two in five (n=407; 40.9%) were in their first academic year; more than three quarters (n=783; 79.2%) had a middle-income household status and nearly two in five (n= 388; 38.9%) lived in a commune/own apartment (Table 1).[2]

Table 1: Background information of respondents

	n	%
Age:		
18	83	8.4
19	222	22.5
20	254	25.8
21	215	21.8
22	120	2.2
≥ 23	91	9.2
Gender:[3]		
Male	173	17.4
Female	821	82.6

[2] Due to the missing values, the total number will not always equal 1001. This can be seen throughout the entire chapter.
[3] The questionnaire did not provide for non-binary gender categories.

© University of Pretoria

Table 1 continued

	n	%
Population group:		
Black	432	43.5
White	456	46.0
Coloured	46	4.6
Indian/Asian	58	5.8
Academic year:		
1st year	407	40.9
2nd year	283	28.4
3rd year	306	30.7
Household economic status:		
Low-income	106	10.7
Middle-income	783	79.2
High-income	100	10.1
Residential arrangements:		
Residence	265	26.6
Family	343	34.4
Commune/own apartment	388	38.9

5.3 Respondents' internet use

Nearly all of the respondents (n=934; 93.7%) used the internet daily, and only 6.3% used the internet a few times per week.

Table 2 shows that there was a weak to moderate effect size (*V*=0.08) within respondents' household economic status, whereby more respondents (n=13; 12.4%) from a low-income economic status used the internet weekly compared to those from high-income status (n=6; 6.0%). No significant differences were featured for the frequency of internet use in gender, academic year, and respondents' living arrangements (Table 2).

Table 2: Bivariate results of how often respondents used the internet

	Daily		Weekly		*p*	*V*
	n	%	n	%		
Gender:						
Male	165	95.9	7	4.1	0.193	-
Female	764	93.3	55	6.4		
Academic year:						
First	381	93.6	26	6.4	0.928	-
Second	264	93.3	19	6.7		
Third	285	94.1	18	5.9		

© University of Pretoria

Table 2 continued

	Daily		Weekly		*p*	*V*
	n	**%**	**n**	**%**		
Household economic status:						
Low-income	92	87.6	13	12.4	0.024	0.08
Middle-income	738	94.5	43	5.5		
High-income	94	94.0	6	6.0		
Living arrangements:						
Residence	245	92.8	19	7.2	0.628	-
Family	320	93.3	23	6.7		
Commune/own apartment	365	94.6	21	5.4		

More than a third of the respondents (n=364; 36.5%) spent more than four hours per day on the internet, while very few (n=178; 17.8%) spent between one to two hours on the internet per day (Table 3).

Table 3: Descriptive results of the hours per day respondents spent on the internet

	n	**%**
< 1 hour	49	4.9
1 – 2 hours	178	17.8
2 – 3 hours	236	23.6
3 – 4 hours	171	17.1
> 4 hours	364	36.5
Total	**998**	**100.0**

A moderate to strong effect size (*V*=0.11) was found, which indicates a significant difference within the living arrangements of the respondents. Slightly more than two in five respondents (n=160; 41.2%) living in a commune/own apartment used the internet for more than four hours per day, compared to nearly a third (n=104; 30.5%) living with their families. No significant differences in the time respondents spent on the internet according to gender, academic year or household economic status were found (Table 4).

© University of Pretoria

Table 4: Bivariate results of the hours per day respondents spent on the internet

	< 1 hour		1 – 2 hours		2 – 3 hours		3 – 4 hours		> 4 hours		*p*	*V*
	n	%	n	%	n	%	n	%	n	%		
Gender:												
Male	8	4.6	34	19.7	49	28.3	30	17.3	52	30.1	0.321	-
Female	40	4.9	143	17.5	186	22.7	140	17.1	310	37.9		
Academic year:												
First	15	3.7	76	18.7	98	24.1	65	16.0	152	37.4	0.468	-
Second	17	6.0	43	15.2	61	21.6	50	17.7	112	39.6		
Third	17	5.6	59	19.3	76	24.8	56	18.3	98	32.0		
Household economic status:												
Low-income	10	9.5	22	21.0	18	17.1	17	16.2	38	36.2	0.310	-
Middle-income	34	4.3	135	17.3	190	24.3	133	17.0	290	37.1		
High-income	5	5.0	18	18.0	26	26.0	20	20.0	31	31.0		
Living arrangements:												
Residence	16	6.0	58	21.9	55	20.8	37	14.0	99	37.4	0.001	0.11
Family	16	4.7	73	21.4	93	27.3	55	16.1	104	30.5		
Commune/own apartment	17	4.4	47	12.1	86	22.2	78	20.1	160	41.2		

© University of Pretoria

Nearly all of the respondents (n=868; 90.4%) accessed the internet through their mobile phones, while very few (n=32; 3.3%) accessed it through the library (Table 5).

Table 5: Descriptive results for where respondents accessed the internet

	n	%
Mobile device	868	90.4
Computer at home	60	6.3
Library	32	3.3
Total	**960**	**100.0**

In terms of where the respondents accessed the internet, a moderate effect size (*V*=0.10) between the two genders was found, whereby nearly all of the female respondents (n=721; 91.6%) accessed the internet via their mobile devices, compared to only four in five (n=141; 84.4%) males. The bivariate results also illustrated that first-years (n=20; 5.2%) were more likely than third years (n=5; 1.7%) to access the internet via the library; and respondents living with their family (n=27; 8.2%) were more likely to use the computer at home to access the internet compared to those living in a commune/own apartment (n=19; 5.1%) and in residence (n=14; 5.4%). However, only weak to moderate effect sizes (*V*=0.07) were featured. Finally, a strong effect size (*V*=0.18) was found between the household economic statuses of the respondents, whereby respondents from low-income households (n=16; 16.5%) were significantly more likely than those from high-income households (n=1; 1.0%) to access the internet via the library (Table 6).

© University of Pretoria

Table 6: Bivariate results for where respondents accessed the internet

	Mobile device		Computer at home		Library		*p*	*V*
	n	**%**	**n**	**%**	**n**	**%**		
Gender:								
Male	141	84.4	20	12.0	6	3.6	0.004	0.10
Female	721	91.6	40	5.1	26	3.3		
Academic year:								
First	337	88.0	26	6.8	20	5.2	0.026	0.07
Second	250	89.9	21	7.6	7	2.5		
Third	279	94.3	12	4.1	5	1.7		
Household economic status:								
Low-income	78	80.4	3	3.1	16	16.5	0.000	0.18
Middle-income	693	91.7	50	6.6	13	1.7		
High-income	89	91.8	7	7.2	1	1.0		
Living arrangements:								
Residence	232	90.3	14	5.4	11	4.3	0.022	0.07
Family	301	90.9	27	8.2	3	0.9		
Commune/own apartment	333	90.2	19	5.1	17	4.6		

© University of Pretoria

Nearly all of the respondents (n=922; 92.4%) often used the internet for social media; two thirds (n=657; 66.4%) often used the internet for studies, and over half (n=553; 55.7%) often used the internet for entertainment (Table 7).

Table 7: Descriptive results for respondents' activities on the internet

	Often		Sometimes		Seldom		Never	
	n	%	n	%	n	%	n	%
Social media	922	92.4	59	5.9	13	1.3	4	0.4
Studies	657	66.4	291	29.4	33	3.3	8	0.8
Entertainment	553	55.7	295	29.7	116	11.7	28	2.8

The following three tables provide the bivariate results for the respondents' use of the internet relating to their gender, academic year level, household economic status and living arrangements. As explained in the previous chapter, the four response categories have been reduced to two in order to facilitate the bivariate analyses.

Table 8 demonstrates a strong effect size (*V*=0.16) between internet use and the two genders, whereby fewer males (n=161; 93.6%) compared to females (n=814; 99.3%) often/sometimes used the internet for social media purposes. A weak to moderate effect size (*V*=0.07) was recorded that illustrated a significant difference between the use of the internet and living arrangements, whereby respondents living in a commune/own apartment (n=376; 97.2%) were less likely to often/sometimes use the internet for social media compared to those living in residence (n=262; 99.2%) (Table 8).

Table 8: Bivariate results for respondents' activities on the internet – social media

	Often/ sometimes		Seldom/ Never		*p*	*V*
	n	%	n	%		
Gender:						
Male	161	93.6	11	6.4	0.000	0.16
Female	814	99.3	6	0.7		
Academic year:						
First	399	98.3	7	1.7	0.993	-
Second	278	98.2	5	1.8		
Third	300	98.4	5	1.6		
Household economic status:						
Low-income	104	98.1	2	1.9	0.403	-
Middle-income	768	98.2	14	1.8		
High-income	99	100.0	0	0.0		
Living arrangements:						
Residence	262	99.2	2	0.8	0.048	0.07
Family	340	99.1	3	0.9		
Commune/own apartment	376	97.2	11	2.8		

© University of Pretoria

No significant differences were featured for academic year levels, economic status and the living arrangements of the respondents. However, a weak to moderate effect size (*V*=0.09) was found between the two genders, whereby fewer males (n=157; 91.8%) than females (n=786; 96.8%) often/sometimes used the internet for their studies (Table 9).

Table 9: Bivariate results for respondents' activities on the internet – studies

	Often/ sometimes		Seldom/ Never		*p*	*V*
	n	%	n	%		
Gender:						
Male	157	91.8	14	8.2	0.003	0.09
Female	786	96.8	26	3.2		
Academic year:						
First	389	95.8	17	4.2	0.813	-
Second	269	96.4	10	3.6		
Third	287	95.3	14	4.7		
Household economic status:						
Low-income	99	96.1	4	3.9	0.307	-
Middle-income	747	96.1	30	3.9		
High-income	91	92.9	7	7.1		
Living arrangements:						
Residence	246	94.3	15	5.7	0.313	-
Family	327	96.2	13	3.8		
Commune/own apartment	371	96.6	13	3.4		

In terms of using the internet for entertainment, the bivariate results indicated a weak effect size (*V*=0.06) regarding the gender of the respondents, whereby nearly all of the males (n=154; 90.6%) often/sometimes used the internet for entertainment, compared to four in five females (n=688; 84.3%). There were no significant differences in the respondents' use of the internet for entertainment according to academic year level, household economic status and living arrangements (Table 10).

Table 10: Bivariate results for respondents' activities on the internet – entertainment

	Often/ sometimes		Seldom/ Never		*p*	*V*
	n	%	n	%		
Gender:						
Male	154	90.6	16	9.4	0.035	0.06
Female	688	84.3	128	15.7		
Academic year:						
First	238	86.6	54	13.4	0.179	-
Second	245	87.2	36	12.8		
Third	252	82.4	54	17.6		

© University of Pretoria

Table 10 continued

	Often/ sometimes		Seldom/ Never		*p*	*V*
	n	%	n	%		
Household economic status:						
Low-income	85	81.7	19	18.3	0.109	-
Middle-income	663	58.1	116	14.9		
High-income	90	91.8	8	8.2		
Living arrangements:						
Residence	227	86.3	36	13.7	0.309	-
Family	282	83.2	57	16.8		
Commune/own apartment	336	87.0	50	13.0		

5.4 Respondents' experiences of victimisation

The following section describes the respondents' experiences of victimisation. Similar to the order followed thus far, a descriptive table for each typology is first presented, followed by the bivariate results, regression analysis and when the victimisation took place.

5.4.1 Having had rumours spread on the internet/social media

Slightly more than two-thirds of the respondents (n=674; 68.8%) never had rumours spread about them on the internet/social media, just under a quarter (n=243; 24.8%) experienced it between one to two times and very few (n=38; 3.9%) experienced rumours being spread about them between three to five times (Table 11).

Table 11: Descriptive results for how often respondents had rumours spread

	n	%
Never	674	68.8
1 – 2 times	243	24.8
3 – 5 times	38	3.9
5 times or more	25	2.6
Total	**980**	**100.00**

The bivariate analysis shows that respondents who came from high-income households (n=42; 42.9%) were significantly more likely than those from low-income households (n=26; 26.0%) to have had rumours spread about them on the internet/social media. However, the effect size of the significant difference was weak to moderate (*V*=0.08). No other significant differences were found regarding gender, academic year level and the respondents' living arrangements (Table 12).

© University of Pretoria

Table 12: Bivariate results for having had rumours spread about the respondents

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	121	72.0	47	28.0	0.320	-
Female	549	68.1	257	31.0		
Academic year:						
First	278	69.5	122	30.5	0.782	-
Second	190	69.1	85	30.9		
Third	202	67.1	99	32.9		
Household economic status:						
Low-income	74	74.0	26	26.0	0.021	0.08
Middle-income	537	69.6	234	30.4		
High-income	56	57.1	42	42.9		
Living arrangements:						
Residence	180	70.3	76	29.7	0.302	-
Family	220	65.5	116	34.5		
Commune/own apartment	270	70.3	114	29.7		

The Hosmer and Lemeshow test of the logistic regression confirmed the bivariate analysis which indicated that the model was not a poor fit, $\chi2(8)=5.173$, $p>0.05$. The model explained 2.5% (Nagelkerke R2) of the variance in the tendency to have had rumours spread on the internet/social media and correctly classified 68.6% of cases. Respondents from high-income households were more likely than those from low-income households to have had rumours spread about them on the internet/social media (OR=2.271, $p=0.009$).

The majority of the respondents (n=242; 84.0%) reported that rumours had been spread about them at school, and only a very few said that they experienced it at university (n=22; 7.6%) (Table 13).

Table 13: Descriptive results for when rumours were spread

	n	%
At school	242	84.0
At university	22	7.6
Both school and university	24	8.3
Total	**288**	**100.0**

5.4.2 Having had social media used as a slandering tool

Slightly more than three-quarters of the respondents (n=746; 76.3%) never experienced social media being used as a slandering tool against them; however, just less than a fifth (n=182; 18.6%) experienced it between one to two times. In addition, very few (n=34; 3.5%) experienced it between three to five times (Table 14).

© University of Pretoria

Table 14: Descriptive results for how often social media was used as a slandering tool

	n	%
Never	746	76.3
1 – 2 times	182	18.6
3 – 5 times	34	3.5
5 times or more	16	1.6
Total	**978**	**100.0**

No significant differences were found regarding respondents having fallen victim to slandering through social media; however, respondents from high-income households (n=31; 31.3%) were more likely to have experienced social media used as a slandering tool than those from low-income households (17; 17.0%). Furthermore, respondents living with family (n=88; 26.2%) were more likely to have experienced slandering compared to those living in residence (n=50; 19.8%) (Table 15).

Table 15: Bivariate results for social media being used as a slandering tool

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	127	74.7	43	25.3	0.606	-
Female	614	76.6	188	23.4		
Academic year:						
First	317	79.4	82	20.6	0.133	-
Second	202	73.5	73	26.5		
Third	223	74.3	77	25.7		
Household economic status:						
Low-income	83	83.0	17	17.0	0.058	-
Middle-income	589	76.6	180	23.4		
High-income	68	68.7	31	31.3		
Living arrangements:						
Residence	203	80.2	50	19.8	0.189	-
Family	248	73.8	88	26.2		
Commune/own apartment	293	76.1	92	23.9		

In terms of social media used as a slandering tool, the Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi2(8)=7.978$, $p>0.05$. The model explained 2.4% (Nagelkerke R2) of the variance in the tendency to have experiences of the media being used as a slandering tool against respondents and correctly classified 76.4% of cases. Respondents from high-income households were more likely than those from low-income households to have experiences of the media being used as a slandering tool against them (OR=2.242, $p=0.023$).

© University of Pretoria

Nearly three-quarters of the respondents (n=161; 73.9%) were at school when social media was used as a slandering tool, and only fewer than one in five (n=33: 15.1) was at university when the victimisation took place (Table 16).

Table 16: Descriptive results for when social media was used as a slandering tool

	n	%
At school	161	73.9
At university	33	15.1
Both school and university	24	11.0
Total	**783**	**100.0**

5.4.3 Being harassed by a stranger

Nearly two-thirds of the respondents (n=595; 60.7%) have never experienced harassment by a stranger, but over a quarter (n=275; 28.0%) experienced it between one to two times, and a few (n= 71; 7.2%) experienced it between three to five times (Table 17).

Table 17: Descriptive results for how often a stranger harassed the respondents

	n	%
Never	595	60.7
1 – 2 times	275	28.0
3 – 5 times	71	7.2
5 times or more	40	4.1
Total	**981**	**100.0**

The bivariate analysis shows that female respondents (n=330; 40.9%) were more likely than males (n=53; 31.4%) to have experienced harassment by a stranger, but the effect size of the significant difference was weak to moderate (V=0.07). There were no other significant differences in being harassed by a stranger regarding the respondent's academic year, household economic status and living arrangements. However, respondents from high-income households (n=47; 47.5%) reported experiencing harassment from a stranger more than those from middle-income households (n=289; 37.5%) (Table 18).

© University of Pretoria

Table 18: Bivariate results for how often a stranger harassed the respondents

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	116	68.6	53	31.4	0.020	0.07
Female	476	59.1	330	40.9		
Academic year:						
First	239	59.3	164	40.7	0.448	-
Second	161	59.0	112	41.0		
Third	191	63.5	110	36.5		
Household economic status:						
Low-income	57	56.4	44	43.6	0.103	-
Middle-income	481	62.5	289	37.5		
High-income	52	52.5	47	47.5		
Living arrangements:						
Residence	156	60.9	100	39.1	0.888	-
Family	208	61.5	130	38.5		
Commune/own apartment	229	59.8	154	40.2		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=5.887$, $p>0.05$. The model explained 2.0% (Nagelkerke R2) of the variance in the tendency to have been harassed by a stranger and correctly classified 61.2% of cases. Female respondents were more likely than male respondents to have been harassed by a stranger (OR=1.601, $p=0.011$).

Table 19 illustrates that over half of the respondents (n=163; 54.3%) were harassed by a stranger whilst at school, while a quarter (n=77; 25.7%) experienced it at university (Table 19).

Table 19: Descriptive results for when a stranger harassed the respondents

	n	%
At school	163	54.3
At university	77	25.7
Both school and university	60	20.0
Total	**300**	**100.0**

5.4.4 Harassed by someone the respondents knew

Just over half of the respondents (n=520; 53.9%) never experienced harassment by someone they know but, slightly less than one in three (n=310; 32.1%) experienced it between one to two times (Table 20).

© University of Pretoria

Table 20: Descriptive results for frequency of being harassed by someone known

	n	%
Never	520	53.9
1 – 2 times	310	32.1
3 – 5 times	80	8.3
5 times or more	55	5.7
Total	**965**	**100.0**

No significant differences were found regarding the respondents' experiences of falling victim to harassment by someone they knew. However, respondents from second-year (n=138; 51.3%) were more likely to have experienced harassment by someone they knew than first-year respondents (n=169; 42.8%). In addition, respondents from low-income households (n=51; 51.5%) experienced such victimisation more than those from middle-income households (n=338; 44.7%) (Table 21).

Table 21: Bivariate results for how often respondent was harassed by someone known

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	94	56.3	73	43.7	0.556	-
Female	426	53.8	366	46.2		
Academic year:						
First	226	57.2	169	42.8	0.097	-
Second	131	48.7	138	51.3		
Third	159	53.5	138	46.5		
Household economic status:						
Low-income	48	48.5	51	51.5	0.412	-
Middle-income	418	55.3	338	44.7		
High-income	52	52.5	47	47.5		
Living arrangements:						
Residence	131	52.4	119	47.6	0.650	-
Family	187	56.0	147	44.0		
Commune/own apartment	201	53.3	176	46.7		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=6.911$, $p>0.05$. The model explained 1.0% (Nagelkerke R2) of the variance in the tendency to have been harassed by someone known to the respondent and correctly classified 55.0% of cases. Female respondents were more likely than male respondents to have been harassed by someone they knew (OR=1.375, $p=0.049$).

In terms of when the respondent experienced harassment by someone they knew, slightly less than two-thirds of the respondents (n=223; 65.4%) experienced such victimisation whilst at

© University of Pretoria

school, while just under one in five (n=67; 18.8%) experienced it both at school and university (Table 22).

Table 22: Descriptive results for when respondents were harassed by someone known

	n	%
At school	223	65.4
At university	56	15.7
Both school and university	67	18.8
Total	**356**	**100.0**

5.4.5 Had someone use the respondents' identity

Table 23 demonstrated that the majority of the respondents (n=837; 85.5%) had never experienced someone using their identity; however, more than a tenth (n=120; 12.3%) experienced such victimisation between one to two times (Table 23).

Table 23: Descriptive results for how often someone used the respondents' identity

	n	%
Never	837	85.5
1 – 2 times	120	12.3
3 – 5 times	12	1.2
5 times or more	10	1.0
Total	**979**	**100.0**

The bivariate analysis shows that a weak to moderate effect size (*V*=0.08) was observed regarding the respondents' household economic statuses. Respondents who came from high-income households (n=22; 22.2%) were significantly more likely than those from middle-income households (n=100; 13.0%) to have experienced their identities used by someone else. Although no other significant differences were found regarding the respondents' gender, academic year and living arrangements; those living in a commune/own apartment (n=64; 16.7%) were found to have more likely experienced such victimisation than those living with their family (n=43; 12.8%) (Table 24).

© University of Pretoria

Table 24: Bivariate results for how often someone used the respondents' identity

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	148	87.6	21	12.4	0.424	-
Female	685	85.2	119	14.8		
Academic year:						
First	342	86.1	55	13.9	0.398	-
Second	230	83.0	47	17.0		
Third	261	86.7	40	13.3		
Household economic status:						
Low-income	81	81.8	18	18.2	0.026	0.08
Middle-income	670	87.0	100	13.0		
High-income	77	77.8	22	22.2		
Living arrangements:						
Residence	221	86.7	34	13.3	0.270	-
Family	294	87.2	43	12.8		
Commune/own apartment	319	83.3	64	16.7		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=4.479$, $p>0.05$. The model explained 2.5% (Nagelkerke R2) of the variance in the tendency to have fallen victim to identity theft and correctly classified 85.6% of cases. Of the four predictor variables, none were significant.

In terms of where the respondents experienced identity theft, over a quarter (n=33; 26.8%) indicated that it had taken place whilst at university, and nearly a fifth (n=21; 17.1%) experienced it whilst both at school and university (Table 25).

Table 25: Descriptive results for when the respondents' identity was used

	n	%
At school	69	56.1
At university	33	26.8
Both school and university	21	17.1
Total	**123**	**100.0**

5.4.6 Had someone hacked the respondents' private accounts

Nearly three in four respondents (n=730; 74.6%) never experienced someone hacking into their private accounts, but just over a fifth (n=213; 21.3%) experienced it between one to two times. Furthermore, less than a few (n=23; 2.4%) experienced it between three to five times (Table 26).

© University of Pretoria

Table 26: Descriptive results for how often someone hacked the respondents' accounts

	n	%
Never	730	74.6
1 – 2 times	213	21.3
3 – 5 times	23	2.4
5 times or more	12	1.2
Total	**978**	**100.0**

Table 27 illustrates no significant differences in respondents falling victim to their private accounts being hacked. However, respondents from high-income households (n=30; 30.6%) were more likely to have experienced their accounts being hacked than those from low-income households (n=22; 22.0%). In addition, second-years (n=77; 28.1%) were more likely than first-years (n=88; 22.0%) to experience such victimisation (Table 27).

Table 27: Bivariate results for how often the respondents' accounts were hacked

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	127	75.1	42	24.9	0.861	-
Female	599	74.5	205	25.5		
Academic year:						
First	312	78.0	88	22.0	0.116	-
Second	197	71.9	77	28.1		
Third	217	72.3	83	27.7		
Household economic status:						
Low-income	78	78.0	22	22.0	0.358	-
Middle-income	576	74.9	193	25.1		
High-income	68	69.4	30	30.6		
Living arrangements:						
Residence	183	72.0	71	28.0	0.467	-
Family	254	74.9	85	25.1		
Commune/own apartment	291	76.4	90	23.6		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=1.992$, $p>0.05$. The model explained 1.6% (Nagelkerke R2) of the variance in the tendency to have fallen victim to identity theft and correctly classified 74.6% of cases. Of the four predictor variables, none were statistically significant.

Less than half of the respondents (n=88; 45.6%) experienced their private accounts being hacked whilst at school and one in three (n=65; 33.7%) experienced it whilst at university (Table 28).

© University of Pretoria

Table 28: Descriptive results for when the respondents' accounts were hacked

	n	%
At school	88	45.6
At university	65	33.7
Both school and university	40	20.7
Total	**193**	**100.0**

5.4.7 Had someone repeatedly send the respondent messages

Once examining the frequency of respondents' experiencing repeated messages sent to them, the descriptive results revealed that more than a quarter of respondents (n=303; 30.8%) experienced such victimisation between one to two times. Furthermore, slightly less than a fifth received repeated messages between three to five times (n=171; 17.4%) and between five times or more (n=167; 17.0%) (Table 29).

Table 29: Descriptive results for how often someone repeatedly sent messages

	n	%
Never	344	34.9
1 – 2 times	303	30.8
3 – 5 times	171	17.4
5 times or more	167	17.0
Total	**985**	**100.0**

A strong to very strong effect size (*V*=0.18) was found that demonstrates a significant difference between the two genders and receiving repeated messages. The bivariate analysis shows that female respondents (n=559; 68.9%) were considerably more likely to have received repeated messages from someone than males (n=76; 45.2%). Furthermore, the analysis also shows that respondents living in a commune/own apartment (n=265; 69.0%) were more likely than those living with their families (n=204; 59.8%) to have experienced such victimisation. However, the effect size was weak to moderate (*V*=0.08). The two remaining predictors, namely the respondents' academic year and household economic status, had no significant statistical differences (Table 30).

© University of Pretoria

Table 30: Bivariate results for how often someone repeatedly sent messages

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	92	54.8	76	45.2	0.000	0.18
Female	252	31.1	559	68.9		
Academic year:						
First	140	34.7	263	65.3	0.998	-
Second	96	34.9	179	65.1		
Third	105	34.7	198	65.3		
Household economic status:						
Low-income	30	29.7	71	70.3	0.217	-
Middle-income	269	34.8	505	65.2		
High-income	41	41.4	58	58.6		
Living arrangements:						
Residence	87	34.0	169	66.0	0.033	0.08
Family	137	40.2	204	59.8		
Commune/own apartment	119	31.0	265	69.0		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=10.772$, $p>0.05$. The model explained 5.6% (Nagelkerke R2) of the variance in the tendency to have fallen victim to someone repeatedly sending messages and correctly classified 66.3% of cases. Female respondents were more likely than male respondents to have someone repeatedly sending them messages (OR=2.666, $p=0.000$).

Roughly a third of the respondents received repeated messages from someone whilst at school (n=170; 35.5%) and at university (n=151; 31.5%) (Table 31).

Table 31: Descriptive results for when someone repeatedly sent messages

	n	%
At school	170	35.5
At university	151	31.5
Both school and university	158	33.0
Total	**479**	**100.0**

5.4.8 Had unwanted sexual messages sent to the respondent

Table 32 examines how often the respondents received unwanted sexual messages. Over half of the respondents (n=531; 54.1%) never received unwanted sexual messages; however, more than one in four (n=281; 28.6%) experienced such victimisation between one to two times (Table 32).

© University of Pretoria

Table 32: Descriptive results for how often someone sent unwanted sexual messages

	n	%
Never	531	54.1
1 – 2 times	281	28.6
3 – 5 times	82	8.4
5 times or more	87	8.9
Total	**981**	**100.0**

A strong effect size (*V*=0.15) was found that illustrates a significant difference between receiving unwanted sexual messages and gender. The bivariate analysis shows that female respondents (n=398; 49.3%) were considerably more likely than males (n=49; 29.3%) to have received unwanted sexual messages. No other significant differences for receiving unwanted sexual messages were found regarding the respondents' academic year, household economic status and living arrangements (Table 33).

Table 33: Bivariate results for how often someone sent unwanted sexual messages

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	118	70.7	49	29.3	0.000	0.15
Female	410	50.7	398	49.3		
Academic year:						
First	216	54.0	184	46.0	0.821	-
Second	153	55.4	121	44.6		
Third	159	52.8	142	47.2		
Household economic status:						
Low-income	54	54.0	46	46.0	0.792	-
Middle-income	422	54.7	350	45.3		
High-income	50	51.0	48	49.0		
Living arrangements:						
Residence	138	54.3	116	45.7	0.893	-
Family	188	55.3	152	44.7		
Commune/own apartment	205	53.5	178	46.5		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=2.126$, $p>0.05$. The model explained 3.2% (Nagelkerke R2) of the variance in the tendency to have received unwanted sexual messages and correctly classified 54.4% of cases. Female respondents were more likely than male respondents to have received unwanted sexual messages (OR=2.322, $p=0.000$).

Two in five of the respondents (n=138; 40.1%) experienced someone repeatedly sending them messages at school and over a quarter (n=103; 29.9%) experienced it at university (Table 34).

© University of Pretoria

Table 34: Descriptive results for when someone sent unwanted sexual messages

	n	%
At school	138	40.1
At university	103	29.9
Both school and university	103	29.9
Total	**344**	**100.0**

5.4.9 Had someone share respondents' personal photos

In terms of how often the respondents experienced someone sharing their photos, slightly less than two in three respondents (n=643; 65.6%) never experienced such victimisation, but over a fifth (n=231; 23.6%) experienced it between one to two times (Table 35).

Table 35: Descriptive results for how often someone shared respondents' photos

	n	%
Never	643	65.6
1 – 2 times	231	23.6
3 – 5 times	58	5.9
5 times or more	48	4.9
Total	**980**	**100.0**

The bivariate analysis shows that respondents living in residence (n=99; 38.7%) were significantly more likely than those living with their families (n=96; 28.5%) to have had someone sharing their personal photos. The effect size of the significant difference was weak to moderate (*V*=0.09). Although no other significant differences were found in terms of gender, academic year and household economic status, first-year respondents (n=150; 37.2%) were found to have had someone share their photos more than third-years (n=88; 29.7%). Furthermore, respondents from a low-income household (n=42; 41.6%) were more likely to have experienced such victimisation compared to respondents from high-income households (n=31; 31.3%) (Table 36).

Table 36: Bivariate results for how often someone shared respondents' photos

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	105	62.5	63	37.5	0.352	-
Female	534	66.3	272	33.7		
Academic year:						
First	253	62.8	150	37.2	0.106	-
Second	178	64.3	99	35.7		
Third	208	70.3	88	29.7		

© University of Pretoria

Table 36 continued

	No		Yes		*p*	*V*
	n	%	n	%		
Household economic status:						
Low-income	59	58.4	42	41.6	0.241	-
Middle-income	509	66.2	260	33.8		
High-income	68	68.7	31	31.3		
Living arrangements:						
Residence	157	61.3	99	38.7	0.017	0.09
Family	241	71.5	96	28.5		
Commune/own apartment	243	63.3	141	36.7		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=3.955$, $p>0.05$. The model explained 2.5% (Nagelkerke R2) of the variance in the tendency to have received unwanted sexual messages and correctly classified 65.7% of cases. Respondents who lived with their families were less likely than those living in residences to have had someone sharing their personal photos (OR=0.679, $p=0.034$).

Table 37 illustrates that slightly less than half of the respondents (n=120; 49.0%) experienced someone sharing their personal photos whilst at school and more than a fifth (n=56; 22.9%) experienced it whilst at university.

Table 37: Descriptive results for when someone shared respondents' personal photos

	n	%
At school	120	49.0
At university	56	22.9
Both school and university	69	28.2
Total	**245**	**100.0**

5.4.10 Had someone sent the respondents a virus

Nearly all of the respondents (n=876; 89.0%) indicated that they had never experienced receiving a virus from someone, whereas only a few (n=87; 8.8%) experienced it between one to two times (Table 38).

Table 38: Descriptive results for how often someone sent a virus

	n	%
Never	876	89.0
1 – 2 times	87	8.8
3 – 5 times	11	1.1
5 times or more	10	1.0
Total	**984**	**100.0**

© University of Pretoria

The bivariate analysis shows that male respondents (n=27; 16.0%) were significantly more likely than females (n=80; 9.9%) to have had a virus sent to them. The effect size of the significant difference was weak to moderate (*V*=0.07). The analysis also shows that third-years (n=46; 15.4%) were considerably more likely than first-years (n=31; 7.7%) to have had experienced such victimisation, whereby the effect size was moderate (*V*=0.10). The two other predictors of receiving a virus, namely household economic status and living arrangements, had no significant differences (Table 39).

Table 39: Bivariate results for how often someone sent a virus

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	142	84.0	27	16.0	0.021	0.07
Female	729	90.1	80	9.9		
Academic year:						
First	374	92.3	31	7.7	0.005	0.10
Second	245	88.8	31	11.2		
Third	253	84.6	46	15.4		
Household economic status:						
Low-income	92	91.1	9	8.9	0.813	-
Middle-income	688	89.0	85	11.0		
High-income	88	88.9	11	11.1		
Living arrangements:						
Residence	231	89.5	27	10.5	0.737	-
Family	298	87.9	41	12.1		
Commune/own apartment	343	89.6	40	10.4		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=3.955$, $p>0.05$. The model explained 2.5% (Nagelkerke R2) of the variance in the tendency to have had a virus sent and correctly classified 89.2% of cases. Male respondents were more likely than female respondents to have received a virus (OR=0.542, $p=0.014$).

Slightly less than two in five respondents (n=35; 36.8%) experienced someone sending them a virus whilst at university, and roughly the same proportion (n=34; 35.8%) experienced such victimisation whilst both at school and university (Table 40).

Table 40: Descriptive results for when someone sent a virus

	n	%
At school	26	27.4
At university	35	36.8
Both school and university	34	35.8
Total	**95**	**100.0**

© University of Pretoria

5.4.11 Having had someone pretend to be someone they are not

Slightly less than a third of respondents (n=312; 31.7%) experienced someone pretending to be someone they are not between one to two times, more than a tenth (n=110; 11.2%) experienced it between three to five times, and very few (n=67; 6.8%) experienced such victimisation five times or more (Table 41).

Table 41: Descriptive results for how often someone pretended to be someone different

	n	%
Never	494	50.3
1 – 2 times	312	31.7
3 – 5 times	110	11.2
5 times or more	67	6.8
Total	**983**	**100.0**

Although the bivariate analysis found no significant differences regarding having fallen victim to someone pretending to be someone they are not, respondents from third-year (n=158; 52.7%) experienced such victimisation more than those from second-year (n=128; 46.5%). Furthermore, respondents from low-income households (n=58; 59.2%) were more likely to have experienced such victimisation than those from middle-income households (n=375; 48.4%) (Table 42).

Table 42: Bivariate results for how often someone pretends to be someone they are not

	No		Yes		*p*	*V*
	n	%	n	%		
Gender:						
Male	87	51.8	81	48.2	0.684	-
Female	405	50.1	404	49.9		
Academic year:						
First	201	49.8	203	50.2	0.337	-
Second	147	53.5	128	46.5		
Third	142	47.3	158	52.7		
Household economic status:						
Low-income	40	40.8	58	59.2	0.113	-
Middle-income	400	51.6	375	48.4		
High-income	47	47.5	52	52.5		
Living arrangements:						
Residence	128	50.0	128	50.0	0.769	-
Family	176	51.8	164	48.2		
Commune/own apartment	188	49.1	195	50.9		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=3.118$, $p>0.05$. The model explained 1.4% (Nagelkerke R2) of the variance in

© University of Pretoria

the tendency to pretend to be someone they are not and correctly classified 52.6% of cases. Respondents from middle-income households were less likely than those from lower-income households to have dealt with someone pretending to be someone they are not (OR=0.632, *p*=0.045).

In terms of when the respondent experienced someone pretending to be someone, they are not, nearly half of the respondents (n=174; 47.0%) experienced such victimisation whilst at school and over a quarter (n=101; 27.3%) experienced it whilst at university (Table 43).

Table 43: Descriptive results for when someone pretends to be someone they are not

	n	%
At school	174	47.0
At university	101	27.3
Both school and university	95	25.7
Total	**370**	**100.0**

5.5 Respondents' reactions to online victimisation

The following section discusses the respondents' responses to online victimisation. Similar to the order followed thus far, a descriptive table for each response is provided. The analysis of the bivariate results then follows it, ending with the results from the regression tests.

In examining the overall responses to online victimisation, over two-thirds of the respondents (n=557; 69.5%) did not ask why the perpetrator did it. Furthermore, over half (n=432; 53.5%) did tell the harasser to stop, and (n=426; 52.1%) ignored all of the messages. The majority of the respondents (n=700; 88.1%) did not write mean things to the harasser, and slightly less than a fifth (n=156; 19.7%) informed an authority figure (Table 44).

Table 44: Descriptive results for respondents' reactions to online victimisation

	Yes		No	
	n	%	n	%
Asked why they did it	244	30.5	557	69.5
Told the harasser to stop	432	53.5	376	46.5
Ignored all messages	426	52.1	391	47.9
Wrote mean things to the harasser	95	11.9	700	88.1
Informed an authority figure	156	19.7	637	80.3

© University of Pretoria

5.5.1 Asked the harasser why they were doing it

A strong to very strong effect size (*V*=0.18) was found, indicating a significant difference between the respondent's academic year levels and asking the harasser why they did it. The bivariate analysis shows that respondents from third-year (n=86; 45.3%) were considerably more likely than those from second-year (n=65; 23.8%) to have asked the harasser why they did it. Although no other significant differences were found in terms of gender, household economic status, and living arrangements, respondents from low-income households (n=38.3%) were more likely to have responded in such a way than those from high-income households (n=23; 27.1%) (Table 45).

Table 45: Bivariate results for asking the harasser why they did it

	n	%	*p*	*V*
Gender:				
Male	41	30.1	0.907	-
Female	202	30.7		
Academic year:				
First	93	27.7	0.000	0.18
Second	65	23.8		
Third	86	45.3		
Household economic status:				
Low-income	31	38.3	0.245	-
Middle-income	188	30.1		
High-income	23	27.1		
Living arrangements:				
Residence	67	31.2	0.819	-
Family	88	31.1		
Commune/own apartment	87	29.0		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi2(7)=3.880$, $p>0.05$. The model explained 5.2% (Nagelkerke R2) of the variance in the tendency to ask the harasser why they were doing it and correctly classified 69.1% of cases. Respondents in their second (OR=2.219; $p=0.000$) and third (OR=2.772; $p=0.000$) academic years were more likely to ask the harasser why they were doing it than respondents in their first academic year.

5.5.2 Told the harasser to stop

In terms of the respondents asking the harasser to stop, the bivariate analysis shows that female respondents (n=368; 55.1%) were more likely than males (n=59; 44.0%) to have told the harasser to stop; however, the effect size of the significant difference was weak to

© University of Pretoria

moderate (*V*=0.08). The analysis also shows a very strong effect size (*V*=0.23), indicating a significant difference between the respondents' academic year levels. Third-years (n=144; 73.5%) were significantly more likely than second-years (n=117; 42.7%) to have told the harasser to stop. No significant differences were found in the other two predictors, namely household economic status and living arrangements (Table 46).

Table 46: Bivariate results for telling the harasser to stop

	n	%	*p*	*V*
Gender:				
Male	59	44.0	0.019	0.08
Female	368	55.1		
Academic year:				
First	171	50.9	0.000	0.23
Second	117	42.7		
Third	144	73.5		
Household economic status:				
Low-income	43	54.4	0.648	-
Middle-income	336	53.0		
High-income	49	58.3		
Living arrangements:				
Residence	111	50.9	0.624	-
Family	157	55.3		
Commune/own apartment	161	53.3		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=4.816$, $p>0.05$. The model explained 8.9% (Nagelkerke R2) of the variance in the tendency to tell the harasser to stop and correctly classified 59.6% of cases. Female respondents (OR=1.617; *p*=0.017) were more likely than their male counterparts to tell the harasser to stop. In addition, respondents in their second (OR=2.676; *p*=0.000) and third (OR=3.760; *p*=0.000) academic years were more likely to tell the harasser to stop compared to respondents in their first academic year.

5.5.3 Ignored messages

The bivariate analysis shows that female respondents (n=375; 55.5%) were significantly more likely than males (n=46; 34.1%) to have responded to the victimisation by ignoring all of the messages. The effect size of the significant difference was strong (*V*=0.16). Third-years (n=132; 67.7%) were also considerably more likely than second-years (n=114; 41.3%) to have ignored all messages. The effect size of the significant difference was strong to very strong (*V*=0.19). Furthermore, the analysis also shows that respondents from high-income households (n=50; 58.1%) were significantly more likely than those from low-income

© University of Pretoria

households (n=30; 35.7%) to ignore all messages. Finally, respondents living with their families (n=160; 56.3%) were more likely than respondents living in residence (n=96; 43.2%) to respond to victimisation in such a way. The effect sizes of both of the significant differences were moderate (*V*=0.11) (Table 47).

Table 47: Bivariate results for respondents ignoring all of the messages

	n	%	*p*	*V*
Gender:				
Male	46	34.1	0.000	0.16
Female	375	55.5		
Academic year:				
First	180	52.3	0.000	0.19
Second	114	41.3		
Third	132	67.7		
Household economic status:				
Low-income	30	35.7	0.004	0.11
Middle-income	341	53.6		
High-income	50	58.1		
Living arrangements:				
Residence	96	43.2	0.007	0.11
Family	160	56.3		
Commune/own apartment	168	54.7		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(7)=9.536$, $p>0.05$. The model explained 11.0% (Nagelkerke R2) of the variances in the tendency to ignore messages and correctly classified 60.5% of cases. Female respondents (OR=2.372; $p=0.000$) were more likely than male respondents to ignore messages. Further, respondents in their second (OR=1.819; $p=0.002$) and third (OR=2.950; $p=0.005$) academic years were more likely to ignore messages compared to respondents in their first academic year. Also, respondents from middle-income households (OR=2.577, $p=0.005$) were more likely to ignore messages than those from low-income households. Finally, respondents who lived with their families (OR=1.533, $p=0.041$) were more likely to ignore all messages than respondents who lived in residences.

5.5.4 Wrote mean things to the harasser

A moderate to strong effect size (*V*=0.12) was found, which indicated a significant difference between the two genders and writing mean things back to the harasser. The bivariate analysis found that male respondents (n=28; 20.9%) were significantly more likely than females (n=66; 10.1%) to write mean things to the harasser. A moderate to strong effect size (*V*=0.13) was found regarding the respondents' academic year levels. The analysis found that third-years

© University of Pretoria

(n=37; 19.9%) were considerably more likely than first-years (n=28; 8.4%) to respond to the harasser in such a way. Although no other significant differences were found regarding the respondents' household economic status and living arrangements, the bivariate analysis shows that those living with their family (n=38; 13.5%) were more likely to have written something mean back to the harasser, compared to those living in a commune/own apartment (n=29; 9.8%) (Table 48).

Table 48: Bivariate results for writing mean things to the harasser

	n	%	*p*	*V*
Gender:				
Male	28	20.9	0.000	0.12
Female	66	10.1		
Academic year:				
First	28	8.4	0.000	0.13
Second	30	11.0		
Third	37	19.9		
Household economic status:				
Low-income	10	12.5	0.993	-
Middle-income	75	12.1		
High-income	10	11.9		
Living arrangements:				
Residence	26	12.0	0.383	-
Family	38	13.5		
Commune/own apartment	29	9.8		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi 2(8)=4.816$, $p>0.05$. The model explained 8.9% (Nagelkerke R2) of the variance in the tendency to write mean things to the harasser and correctly classified 59.6% of cases. Male respondents (OR=0.394; $p=0.000$) were more likely to write mean things to the harasser than their female counterparts. Further, respondents in their second (OR=3.114; $p=0.000$) and third (OR=2.178; $p=0.005$) academic years were more likely to write mean things to the harasser than respondents in their first academic year.

5.5.5 Informed an authority figure

The bivariate analysis shows that female respondents (n=144; 22.0%) were significantly more likely than males (n=10; 7.6%) to inform an authority figure. The effect size of the significant difference was moderate to strong ($V=0.13$). The analysis also shows that third-years (n=48; 25.9%) were considerably more likely than second-years (n=40; 14.7%) to inform an authority figure, whereby the effect size of the significant differences was moderate ($V=0.10$). Although no other significant differences were found regarding the respondents' economic income

© University of Pretoria

status and living arrangements, the analysis shows that those from high-income households (n=21; 24.7%) were more likely to respond in such a way compared to those from low-income households (n=14; 17.5%). Finally, respondents living with family (n=59; 21.3%) were more likely to inform an authority figure than those living in a commune/own apartment (n=52; 17.4%) (Table 49).

Table 49: Bivariate results for informing an authority figure

	n	%	*P*	*V*
Gender:				
Male	10	7.6	0.000	0.13
Female	144	22.0		
Academic year:				
First	68	20.4	0.011	0.10
Second	40	14.7		
Third	48	25.9		
Household economic status:				
Low-income	14	17.5	0.436	-
Middle-income	119	19.3		
High-income	21	24.7		
Living arrangements:				
Residence	44	20.5	0.476	-
Family	59	21.3		
Commune/own apartment	52	17.4		

The Hosmer and Lemeshow test of the logistic regression indicated that the model was not a poor fit, $\chi2(8)=5.574$, $p>0.05$. The model explained 6.4% (Nagelkerke R2) of the variance in the tendency to inform an authority figure and correctly classified 80.4% of cases. Female respondents (OR=3.312; $p=0.001$) were more likely to inform an authority figure than male counterparts. In addition, respondents in their third academic year (OR=2.017; $p=0.005$) were more likely to inform an authority figure about the harassment than respondents in their first academic year.

5.6 Summary

The data in the chapter, which was obtained by administering a questionnaire to undergraduate students attending a South African university, was presented both as text and in tables to understand the key findings highlighted in the study easily. The results were categorised into three main sections, the respondents' profile, the respondents' experiences of online victimisation, and their reactions to such victimisation. After analysing the descriptive and bivariate results and running regression tests on the data, various significant differences

© University of Pretoria

were revealed. It is important to note that the logistic regressions mostly confirmed the bivariate results.

© University of Pretoria

Chapter 6: Discussions and recommendations

6.1 Introduction

The final chapter will discuss the empirical results presented in chapter five. The chapter will focus on the similarities and differences to the extant literature and studies conducted internationally and locally, making comparisons. The chapter is structured according to the objectives of the study, which were: to describe the undergraduate students' access to and use of social media and other electronic platforms through which online victimisation can take place, to identify correlates and predictors to construct a profile of undergraduate students who are more likely to experience online victimisation and to determine the nature and extent of and responses to online victimisation among undergraduate students. The purpose of the last chapter is to use the objectives to answer the study's research question, which was to determine the correlates and predictors of online victimisation among undergraduate students attending a South African university. Finally, the theoretical application and recommendations for practice, policy, theory and future research will be discussed.

6.2 Socio-demographic characteristics of respondents

As the study focused on online victimisation among undergraduate students, six socio-demographic characteristics were examined to construct a profile of students who were more likely to experience online victimisation. The first characteristic was age, whereby the students' ages ranged between 18 to 50 years old. However, nearly two-thirds of the students were between 19 and 21 years. The age range of the respondents makes sense, as students typically complete high school at eighteen years old and start university from nineteen years old. Secondly, gender was investigated, whereby the majority of the students (82.6%) were female, and nearly a fifth (17.4%) were male. Similar findings were identified in a study conducted in the USA which examined the prevalence, psychological impact, and coping strategies of American college students who had experienced online victimisation. The study found that almost three-quarters of the students (72.5%) were female, and only over a quarter (27.5%) were male victims (Schenk, 2011: 45). The reason for such disproportion between genders is that more females enroll in the Humanities Faculty compared to males, which can be seen in other studies conducted at the same university. For example, a local study focusing on substance abuse among undergraduate students found that the bulk of the students were female (77.3%) whilst only slightly more than a fifth (22.7%) were male (Steyn, 2016: 2). In terms of gender, such similarity found between the two studies could also point to the results

© University of Pretoria

having a generalisation value.

The study looked at the students' race in terms of the third characteristic. The study found that more than half of the respondents (46.0%) reported to be White, and just over two in five (43.5%) identified as Black. The observation indicates that the student profile of the study does not match the country's profile, whereby the majority of the people are Black (47.4 million) and only 4.4 million are White (Statista Research Department, 2021). A possible reason for the discrepancy is that the study was conducted at a traditionally privileged university with a history of exclusively catering for only White students under apartheid rule (1948-1994). Thus, racial diversification has not yet been achieved at the university where the study took place. The fourth aspect investigated the academic year levels of the students, whereby two in five (40.9%) indicated to be in the first year, and over a quarter (28.4%) were in their second year. More first-year students were found in the sample, which is expected, given the increase in attrition/dropout rates towards the third academic year. Another possible reason is that Criminology 110 is an elective module for many programmes in the Humanities and Law faculties, at the university where the study was conducted. Research that focused on the high university dropout rates in South Africa confirmed such observation, as they found that over a fifth of university students (20.0%) drop out from their second and third year of university (Letseka & Maile, 2008: 5). Thus, the reader should keep the proportions in mind when valuing the results.

The fifth aspect looked at the respondent's household economic status. The study found that nearly four in five (79.2%) had a middle-income status, and very few had a low-income (10.7%) and high-income (10.1%) status. The university is a public entity that the government partially funds; the fees are lower and more affordable than private universities that cost substantially more, thus explaining why there was a greater proportion of middle-income students compared to those who had a high-income status. The last socio-demographic characteristic examined was the students' living arrangements, whereby nearly two in five (38.9%) lived in a commune/own apartment; a third (34.4%) lived with their family, and just over a quarter (26.6%) lived in residences. The living arrangements of the students may ultimately influence their risk of victimisation. Students living on their own may be exposed to more potential victimisation as they may actively spend more time online and engage in risky behaviours as they may not have the same levels of daily social interaction with friends and family, and can use the internet in private. The matter will be discussed in more depth below.

© University of Pretoria

6.3 Access to and use of the internet

Each year, the number of university students in South Africa using the internet for academic, social and professional reasons increases (Lama, 2020). Therefore, it is not surprising that the majority of the students (93.7%) reported that they use the internet daily, and only very few (6.3%) use it a few times per week. The finding is supported by a study conducted in the USA which examined cyberstalking experiences of undergraduate and graduate students. The study found that all 302 student participants responded 'yes' to using the internet every day (Paullet, Rota & Swan, 2009: 645). After reviewing the use of the internet in terms of the student's household income status, a weak to moderate effect size (V=0.08) was found. A greater proportion of students from a low-income household status (12.4%) used the internet every week, compared to individuals from a middle-income (5.5%) and high-income (6.0%) household status. Therefore, the results suggest that nearly all students use the internet daily; however, those from lower-income backgrounds only do so on a weekly basis potentially due to the cost of data. South Africa has amongst the most expensive mobile data available in Africa. Research points out that data is only affordable if an individual purchases mobile data in large bundles; however, the majority of South Africans cannot afford to buy in bulk, which then makes the cost per megabyte very expensive (Bottomley, 2020).

Students who live alone typically have less face-to-face interaction with others on a daily basis. Such observation was especially true when lockdown restrictions were enforced, as the COVID-19 pandemic spread throughout the world. As students living alone were even further isolated from others, the only way to connect with people was to spend an increased amount of time on the internet to alleviate their loneliness (Boursier, Gioia, Musetti & Schimmenti, 2020: 1-2). For that reason, it is of no surprise that a moderate effect size (V=0.11) was found, whereby more than two in five students (41.2%) who lived in a commune/own apartment used the internet for more than four hours per day, compared to students living with their families (30.5%).[4] Furthermore, as smartphones are increasingly becoming more affordable (Popovac & Leoschut, 2012: 1), it explains why the study found that nearly all students (n=868; 90.4%) accessed the internet primarily through their mobile phones. The finding is further confirmed in a local study that focused on cyberstalking victimisation of university students, as cell phones and laptops were the most commonly used devices to access the internet (Sissing, 2013: 94). A moderate effect size (V=0.10) was also found whereby nearly all female students

[4] Although the data was not collected during the COVID-19 lockdown, the reason still applies. Students who lived in a commune/own apartment were isolated from others, which may have driven them to spend more time on the internet to alleviate their loneliness.

© University of Pretoria

(91.6%) accessed the internet through their mobile phones compared to only four in five (84.4%) male students. However, males (12.0%) accessed the internet through their home computer more than females (5.3%). A study in the USA investigating the internet use of college students confirmed that males used the computer more, and the reason was because more than two in five (43.6%) male students used the computer to play online games, compared to only a quarter (26.9%) of females (Odell, Korgen, Schumacher & Delucchi, 2000: 857). Therefore, the results show that a large population of students spend substantial time on the internet, mainly using their mobile phones, although male students are more likely to use their computers to access the internet, for online gaming purposes. Although males are found to more likely use their computers to access the internet, due to the lack of overall evidence, it cannot be suggested that males or females are more at risk of online victimisation.

In recent times, feminist commentators praise the rise of social media, as they believe that through various online platforms, women are provided with a space to have a voice and are empowered to challenge mainstream media stereotypes. Women outnumber men on social media (Webb & Temple, 2015: 641). The study confirmed such observation as a strong effect size (V=0.16) was found, indicating a significant difference between gender and the use of social media. Female students (99.3%) were more likely to often/sometimes use the internet to access social media than male students (93.3%). An Australian study that focused on students' attitudes towards online risk-taking behaviour found a similar result, as the majority of their female students (85.4%) had three or more social media accounts, and over a third (34.1%) had at least five personal profiles. On the other hand, three in four male students (78.6%) had three or more social media accounts, and nearly a third (28.6%) had five (Jalil & Sinnamon, 2019: 403). Therefore, the results show that female students have a more prominent online social media presence compared to male students, as women are taking it as an opportunity to express themselves and fight the norms and stereotypical gender roles that have previously been expected and placed upon them.

As technology advances, teaching and learning techniques are changing, as students can now participate in online learning and obtain their degrees through universities online. Such transition can especially be seen after the COVID-19 pandemic spread throughout South Africa, as universities were forced to shut down and operate online (Sadiki & Steyn, 2020: 149). As the survey was administered pre-Covid, it is not surprising that the study only found that two-thirds of the students (66.4%) often used the internet for their studies. Since March of 2020, all contact lessons and consultations have stopped; thus, 66.4% of students would probably increase to 100% as the university transitioned into online learning (Sadiki & Steyn,

© University of Pretoria

2020: 151-152). Furthermore, a weak to moderate effect size (*V*=0.09) was found, indicating a significant difference between genders. Fewer male students (91.8%) often/sometimes used the internet for studies than female students (96.8%). A reason that might explain the finding is that female students are presumed to be more focused and goal-oriented in their academics than their male counterparts (Fouladchang, Marzooghi & Shemshiri, 2009: 968) thus explaining why a slightly bigger proportion of female students use the internet for their studies. Finally, the study reported that over half of the students (55.7%) often used the internet for entertainment. As undergraduate students participated in the study, such observation is expected. It has become more accessible for students to stream movies or series, play online games, or download various apps through the internet in recent times. A study that was conducted in the USA, focusing on university students' experiences with online victimisation confirmed such observation by reporting that over half (53.7%) of the students used the internet for online gaming (Marcum 2011: 257, 260).

6.4 Nature and extent of online victimisation among university students

The section below aims to provide a more comprehensive representation of the nature and extent of online victimisation among undergraduate students. The section contains an analysis of the various types of online victimisation experienced by the students. The types of online victimisation are clustered into three themes in order to prevent duplication of arguments.

6.4.1 Identity fraud, hacking, viruses and offenders pretending to be someone else

Through the evolution of technology, cybercriminals continuously adapt and better their techniques to successfully commit crimes, such as identity theft, where university students are at particular risk (Norum & Weagley, 2007: 45-46). In the study, the majority of the students (85.5%) had never been a victim of identity theft, and one in eight (12.3%) indicated that it happened to them once or twice. Furthermore, more than a quarter (26.8%) of students experienced identity fraud[5] at university. A weak to moderate effect size (*V*=0.08) found a significant difference between household income statuses of the students and identity fraud. A greater proportion of students from high-income households (22.2%) experienced someone else using their identities than those from middle-income households (13.0%). The reason might be because students from higher-income backgrounds have fewer financial constraints;

[5] Identity theft is the theft or acquisition of a pre-existing identity, with or without consent, and whether in the case of an individual, the person is living or deceased. Identity fraud can be defined as the obtaining of money, goods, services, or other benefits or the avoidance of obligations through the use of a false identity, a manipulated identity or a stolen identity (Seda, 2014: 462).

© University of Pretoria

for example, they can afford to make more online purchases than those from lower-income backgrounds. As such, it might result in offenders having an increased opportunity to commit identity theft. However, a slight anomaly was observed in a study conducted in the USA focusing on the extent to which selected internet activities could minimise university students' risk of victimisation. The study found that students from lower-income brackets had their identities stolen more frequently than students from higher-income households (Norum & Weagley, 2007: 57). Such disparity might indicate that household income statuses, as a risk factor of online victimisation, may differ according to the context in which it is interpreted. Overall, the results found that university students are at particular risk of experiencing someone else using their identities, and such risk might be escalated depending on the students' online activities and lack of prevention techniques applied, for example, downloading a preventative app called identity guard (Seda, 2014: 463, 465).

Due to university students' behaviours online, they are also at an increased risk of falling victim to their accounts being hacked. Although the study found that nearly three in four students (74.6%) never experienced someone hacking into their account, just over a fifth (21.3%) indicated that it has happened to them once or twice. If the students experienced their accounts being hacked, one in three (33.7%) experienced it at university. Similarly, a study in South Africa found that one participant had their social media profile hacked, whereby the offender sent repeated messages to the victim's friends and family (Sissing, 2013: 102). Social networking is a growing trend in South Africa, with many students growing their social media presence. As a result, it increases the offenders' opportunity to hack into the victims' accounts. Students can be hacked by receiving a virus, such as a file-infecting virus attached to executable files, for example, when they run a file ending in .com (i.e., www.facebook.com) (Ubarhande, 2011: 2). However, sometimes, the offenders will use a virus to spy on the victims without them knowing. For instance, the national crime victimisation survey in the USA found that less than a fifth of participants (19%) had an offender monitor their activities using listening devices (Stalking Victimisation, 2016: 1). In the study, a weak to moderate effect size (V=0.07) indicated a considerable difference between genders and receiving a virus. Male students (16.0%) were more likely than females (9.0%) to have experienced such victimisation. A reason to explain the finding could be that men are presumed to play more online games than women, thus, it increases the opportunity for offenders to send the victims viruses. Moreover, nearly two in five (36.8%) students experienced such victimisation at university. Overall, the results indicate that some university students are at particular risk of having their accounts hacked and receiving a virus. The regression analysis showed that male students are more vulnerable than females to receiving a virus, possibly because online gaming crosses borders,

© University of Pretoria

in that they play with people from around the world.

As social media has become the primary means of communication for university students, such advancement in interaction has opened a flood-gate for criminals to engage in deviant behaviours, such as creating false accounts on various social networking platforms (Smith, Smith & Blazka, 2017: 33). Through creating false accounts, students may be connecting with a person who is pretending to be someone else. Half of the students (50.3%) reported that they had never experienced such victimisation; however, slightly less than a third (31.7%) experienced it once or twice, and roughly one in nine (11.2%) students experienced it between three to five times. A noteworthy observation is that over a quarter of the students (27.3%) experienced it at university, and (25.7%) at both school and university. Such findings could confirm that there may be an increase in the trend of students being 'catfished', which is slang for someone impersonating another individual (Siemer, 2013). Victims who experience being catfished can face emotional harm. For instance, victims can feel humiliated or have regret or develop mental illnesses such as anxiety and depression (The Cybersmile Foundation, 2020). Finally, the regression analysis confirmed no significant difference between males (48.2%) and females (49.9%) experiencing someone pretending to be someone else, which indicates that university students as a whole are more at risk of being victimised. Overall, the results indicate that offenders may be provided with more opportunities to pretend to be someone they are not, as more students, for example, are downloading dating apps on their phones or accepting strangers on their social media accounts or online gaming profiles (Vogels, 2021).

6.4.2 Harassment and cyberbullying

Logging onto, viewing and posting on social media is engrained into the routine behaviours of university students. Engaging on various online platforms on a daily basis has significantly influenced the likelihood of students experiencing online harassment (Zhong, Zheng, Huang, Mo, Gong, Li & Huang, 2021: 1). Online harassment can be conducted by a stranger or somebody the students know. A study in the USA that investigated online harassment of university students reported that 10% to 15% of the students experienced online harassment either from strangers, acquaintances or their significant others (Finn, 2004: 473). The study found that students were more commonly harassed by somebody they knew than a stranger. For instance, more than a quarter of the students (28.0%) experienced being harassed once or twice by a stranger, whereas nearly a third (32.1%) were harassed by someone they knew between one to two times. Online harassment perpetrated by somebody the students knew was experienced by a quarter (25.7%) of students whilst being at university. Although social

© University of Pretoria

media pages might have policies for reporting online harassment, students can still experience such victimisation, as it may go unnoticed by social media websites (The Cybersmile Foundation, 2020). As a result, friends, family members, colleagues or former partners are provided with an opportunity to harass the students online. Two other studies can confirm such observation. Firstly, a study, conducted in the USA focusing on determining the prevalence rate of cyberbullying and cyberstalking within a university found that most of the students knew their harassers, whereby more than a quarter (28.0%) were ex-partners, and 26.0% were students from the same university (Kraft, 2010: 81). Secondly, a local study further confirmed such results, as six out of the twelve students knew their harassers, who were either their friend, former roommate, landlord or someone who mistook their friendship as something romantic (Sissing, 2013: 99).

Although the phenomenon of online harassment is relatively new, researchers in the USA who focused on online harassment of university students, have identified that one of the most commonly experienced forms of harassment is receiving repeated messages, which is mainly perpetrated against university students (Brown & Krysik, 2011: 7, 9). In the study, nearly a third of the students (30.8%) experienced it once or twice, and slightly less than a fifth (17.0%) experienced it five times or more. Of the times that the students experienced online harassment, nearly a third (31.5%) reported that it took place while at university. Similarly, a study in the USA found that more than a tenth (12.6%) of the students received repeated messages from someone they did not know, who threatened, insulted or harassed them (Finn, 2004: 473). Furthermore, a strong effect size (V=0.18) indicated a statistically significant difference between gender and receiving repeated messages. The regression test confirmed that female students (68.9%) were more likely to experience such harassment than males (45.2%). A reason that might explain why a greater proportion of females experienced such form of harassment could be due to several factors. For instance, women are vulnerable to violence and are regarded as an easy target, as patriarchal and sexist views within society have legitimised violence against women to ensure men's dominance and control (Council of Europe, 2021). Interpersonal violence in the real world is found to intersect with technology. Therefore, as there is a general acceptance of violence in an offline setting, such as women being harassed on the street, violence exists in an online environment too, such as women repeatedly receiving messages (Brown & Krysik, 2011: 6). Overall, university students are at a higher risk of online victimisation in the form of receiving repeated messages, which could be due to a combination of them gaining more independence, forming new identities and having a near-constant technological connection (Brown & Krysik, 2011: 2).

© University of Pretoria

In South Africa, gender-based violence is an overwhelming and widespread problem in the country, whereby women in South Africa are being harassed and victimised daily (Safer Spaces, 2021). One example of gender-based violence is online sexual harassment, whereby a victim can receive unwanted sexual messages. The study found that over a quarter (29.9%) of the students reported that when they received unwanted sexual messages, such victimisation took place while at university. Similarly, a study conducted in Jordan that aimed to investigate cyberstalking found that nearly two-thirds (64.6%) of the students experienced being sent unwanted sexual materials (Abu-Ulbeh et al., 2021: 25). The study also found a strong effect size (V=0.15), which illustrated a significant difference between genders and receiving unwanted sexual messages. The logistic regression confirmed that female students (49.3%) were considerably more likely than males (29.3%) to be sexually harassed online. Research in the USA confirms that female students are at significant risk of falling victim to receiving unwanted sexual messages, as survey results from a study that investigated the state of online harassment observed that the extent of female university students experiencing online sexual harassment has doubled since 2017 (Pew Research Centre, 2021). Overall, the results indicate that university students are at risk of receiving unwanted sexual messages, especially female students, which shows that gender-based violence is a pressing matter in South Africa. Confusion over what constitutes consent (Rainn, 2021) might be the reason behind students experiencing such victimisation. Whilst expressed consent is not given, offenders might perceive that as an opening to send unwanted messages.

Online victimisation is significantly interrelated with victims having limited control over the actions of their offenders (Ben-Joseph, 2021). One typology acknowledged in the study are students experiencing their personal photos being shared, which is often done without consent or knowledge. The study found that over a fifth (23.6%) of the students had someone share their photos between one to two times, whereby one in five (22.9%) reported that it took place while at university. Furthermore, a weak to moderate effect size (V=0.09) was found, which indicated that students living in a residence (38.7%) were significantly more likely than individuals living with their families (28.5%) to experience such victimisation. Overall, the logistic regression confirmed such a finding, therefore illustrating that where a person lives while at university might predict their likelihood of having their photos shared. As students move away from home and live in a residence, they gain a sense of freedom and independence, resulting in them engaging in riskier behaviour, as their family cannot deter them from doing so. An example of risky behaviour is students participating in sexting, which refers to the sending, receiving and/or forwarding nude or sexually suggestive photographs and/or sexually explicit messages across social media platforms (Harris & Steyn, 2018: 15).

© University of Pretoria

However, once the photo is sent to someone, the student loses control over what the offender will do with the personal photo.

6.4.3 Rumours and social media used as a slandering tool

Due to some of the many characteristics of the internet and Section 16(1) of the Constitution of the Republic of South Africa (1996), people have been provided a nearly unrestricted platform to enforce their right to freedom of speech and expression, which enables them to say whatever they want, about whomever they want, even if it may be untrue. Such action is known as spreading rumours; however, it may not be as commonly experienced as one might expect. In the study, slightly more than two-thirds of the students (68.8%) never had rumours spread about them. Similarly, a study in the USA which focused on the differences in online bullying behaviours between men and women confirmed such observation by reporting that very few males (8.0%) and female (13.0%) students experienced someone posting gossip about them online (Marcum et al., 2014: 544). In the study, if the students experienced rumours being spread about them, the majority (84.0%) indicated that it only happened while at school. A survey conducted in the USA focusing on cyberbullying, found that nearly a third (32.0%) of American high schoolers experienced false rumours being spread about them (Pew Research Center, 2018). Therefore, the results might indicate that being a university student does not increase the likelihood of rumours being spread about them; however, learners in high school appear to be more at risk of such victimisation.

Bullying is no longer limited to physical acts, such as hitting somebody. As technology grows, bullying can now consist of cyberbullying and online harassment, such as an offender using the media as a slandering tool against a student (Stopbullying, 2021). The study found that under a fifth (18.6%) of the students experienced the media being used as a slandering tool. Such type of victimisation can occur in different forms, for example, a study in the USA, investigating the prevalence of online victimisation of university students found that nearly a quarter (23.2%) of the students reported that offenders would post derogatory statements about them online (Kennedy & Taylor, 2010: 11). Evidence of another form of victimisation was found e in a local study which focused on the experiences of cyberbullying among undergraduate students. A student in the study described her experience of denigration, where a former partner posted rude comments on their Facebook status about the victim (Pillay & Sacks, 2010: 10). Although the logistic regression found no significant differences, the study observed that students from high-income households (31.3%) were more likely to experience the media being used as a slandering tool than students from low-income backgrounds

© University of Pretoria

(17.0%). The finding could point to the presumption that their victimisation risk increases due to their heightened status and wealth. Overall, university students commonly experience the media used as a slandering tool, whereby students from higher-income backgrounds are targeted more, possibly due to the power imbalance between the offender and victim. Offenders who feel as if they have a control deficit due to having a lower-income background will hurt or retaliate against those who are perceived to have a control surplus (students from a higher- income background) as a way to restore the power (Piquero & Hickman, 2003: 285)

The study's main objective was to determine the correlates and predictors of online victimisation of undergraduate students. After examining the empirical results obtained by the study, various key observations regarding the profile of victims emerged. Firstly, the type of personal victimisation that both females and males were subjected to, such as being harassed by a stranger or receiving a virus, indicates that gender is a major correlate and predictor of online victimisation (Table 50). Females, in particular, have the greatest risk of becoming a victim of many crimes linked to online harassment, cyberstalking and cyberbullying. Such offences have the potential for severe emotional and psychological distress for female students, given their personal nature. Secondly, students' economic household status appeared to correlate and predict online victimisation, especially for students from a high-income background. Such observation may link to the causation factors discussed in the integrated model, such as the minimisation of status, equal playing ground and control deficit. Finally, an interesting finding was that both the academic year levels and the living arrangements of the undergraduate students did not feature as recurring correlates and predictors of online victimisation. Nevertheless, students in their third academic year and those living in a residence appear to be more vulnerable to particular types of victimisations.

Table 50: Correlates and predictors of students' experiences of online victimisation

Gender		**Academic year**	
Correlates: Harassed by a stranger (female) Repeatedly received messages (female) Unwanted sexual messages (female) Received virus (male)	**Predictors:** Harassed by a stranger (female) Harassed by someone known (female) Repeatedly received messages (female) Unwanted sexual messages (female) Received virus (male)	**Correlates:** Received virus (third-year)	**Predictors:** -

© University of Pretoria

Household economic status		Living arrangements	
Correlates: Rumours spread (high-income) Used identity (high-income)	**Predictors:** Rumours spread (high-income) Media as slandering tool (high-income)	**Correlates:** Someone shared personal photos (residence)	**Predictors:** Someone shared personal photos (residence)

6.5 Responses to online victimisation

One of the main objectives of the study was to examine five responses showcased by undergraduate students after being victimised online. Doing so will help identify South Africa's current legislation problems and guide and adapt university policies that deal with online victimisation. The first response included nearly a third (30.5%) of the students asking why the harasser victimised them. The finding might be explained by looking at how online victimisation impacts students. For instance, the student may feel shocked and immediately wonder why they were chosen to be victimised (Pillay & Sacks, 2020: 9). If the self-blame continues, it could push the student to respond to the offender by asking them why they did it. Similarly, a local study that examined the prevalence of online sexual harassment of female students further confirmed such observation. The study reported that some students attempted to confront their harassers by asking them why they sexually harassed them online (Sehlule, 2018: 88). Such response might form part of their coping mechanism into raising their self-confidence after they have been victimised, by feeling like they have played an active role in overcoming the victimisation (Herrera, Herrera & Expósito, 2014: 45).

The second type of response to online victimisation was an assertive response, where the students asked the harasser to stop. In the study, students were more likely to ask the harasser to stop (53.5%) than students who did not (46.5%). Similarly, a study in Australia that examined the relationship between aggressive, assertive and passive responses to online victimisation found that over half of the students (52.0%) told the harasser to stop immediately after being victimised (Dooley, Shaw & Cross, 2012: 280). In modern times, students may be more encouraged to voice their opinions and boundaries than in the past. Such freedom of expression can further be seen in the study as the logistic regression found a very strong effect size (V=0.23), thus, illustrating a significant difference between students' academic year levels. Students in their third-year (73.5%) were considerably more likely than second-year students (42.7%) to ask the harasser to stop. Such observation could point to the fact that students in third-year may have more confidence and less patience due to being older and having more university experience. Therefore, the results indicate that university students can

© University of Pretoria

be assertive in their responses, especially senior students, as they may be less afraid to confront their harasser and tell them to stop, compared to those in lower academic year levels. The students' coping strategy to being victimised online can be defined as their behavioural, emotional, and cognitive responses to stress (Machackova, Cerna, Sevcikova, Dedkova & Daneback, 2013: 1). One of the most common responses to victimisation is to ignore the harasser, which is the third response to online victimisation examined by the study. Over half of the students (52.1%) ignored all of the messages sent by the harasser. Within that, a strong effect size (V=0.16) was confirmed by the logistic regression, which found a significant difference between the two genders. The female students (55.5%) were considerably more likely than the male students (34.1%) to have ignored all messages. A similar finding was observed in another local study, which reported that out of the twenty female student victims, the majority of them ignored or blocked their harasser (Sehlule, 2018: 88). These findings might relate to traditional societal norms, where women are expected to remain passive, soft and non-aggressive. Therefore, if more women responded in other ways, it might be considered unnatural, unacceptable and as if they had broken society's norms (Dittman, 2003: 52). It is important to note that societal norms and expected gender roles apply to women and men. For instance, in terms of informing an authority figure regarding victimisation, female students (22.0%) were more likely than male students (7.6%) to do so. The logistic regression confirmed that an effect size of the significant differences between gender was illustrated to be moderate to strong (V=013). Furthermore, a South African study reported a similar finding, where six females out of ten students reported the incident and were more inclined to seek help. In contrast, the four male students did not tell anyone about what happened to them. Such findings could point out that men are expected to "take it like a man" and be quiet otherwise they may be considered weak or feminine-like (Dittman, 2003: 52). Additionally, they may have chosen to have not reported it as they might have felt that no one would take the matter seriously enough (Finn, 2004: 473), especially if a female victimised them. Therefore, the results found that females were more likely to ignore their harassers, and male students were less likely to inform an authority figure. Such observations could be explained by the fact that gender roles and expectations significantly influence the way students respond to online victimisation (Dittman, 2003: 52).

The fourth response examined is considered an aggressive response, where the students retaliate against their harasser and write mean things back to them. The study found that the majority of the students (88.1%) did not respond in such a manner, and only a few (11.9%) did. Similarly, a local study that focused on cyberstalking victimisation of university students, found that out of the twelve undergraduate students, only two students stated that they retaliated

© University of Pretoria

by messaging their cyber stalker back (Sissing, 2013: 113-114). Retaliation is found to be the least common response, as students may feel that they do not want to swoop down to the same level as the offender, by behaving in the same manner as they did. Moreover, it could also be that when growing up, children are often taught to never fight back but to rather ignore the offender (Neaville, 2017: 84, 168). The logistic regression confirmed that a moderate effect size (V=0.12) was found, illustrating a significant difference between the two genders. The study found that male students (20.9%) were more likely than female students (10.1%) to write mean things to the harasser. Such a finding is not a surprise, as males are presumed to be more aggressive than females (Staniloiu & Markowitsch, 2012: 1032). Furthermore, although the logistic regression did not find any more significant differences, the study indicated that students living with their family (13.5%) were more likely to write mean things back to the harasser than those living in a commune/own apartment (9.8%). Such difference could be that those living with family have more social support and might encourage the students to stand up for themselves. Overall, the results indicate that there are gender differences, where males are more likely than females to respond to online victimisation by writing mean things back.

6.6 Theoretical application

The integrated model consists of a range of elements from various victimological theories that have been combined into a single comprehensive model to explain and understand online victimisation. The first component of the model focused on explaining what factors may influence the likelihood of an offender committing a crime. Firstly, around the world, any person can have access to the internet at any time of the day, every day of the week. As of January 2021, there were 4.66 billion active internet users worldwide, more than half (59.5%) of the global population (Johnson, 2021). The same goes for students in university, as the study observed that nearly all of the students (93.7%) used the internet daily. Due to the ease of accessing the internet, the ease of committing an offence increases the likelihood of an individual victimising somebody online. Secondly, the model used the Barlett and Gentile Cyberbullying Model (2012). As cyberspace offers offenders an opportunity to conceal their identity and behave in specific ways that may be atypical to their offline conduct, any person can commit an offence. Furthermore, the victims may believe that they are getting harassed by a stranger; for example, over a quarter of the students (28.0%) experienced harassment once or twice without knowing who the offender was. However, a study conducted in the USA found that the most frequent type of perpetrator was a friend or former friend of the victim (Schenk, 2011: 28). Therefore, the findings highlight that anonymity provided by the internet makes online victimisation an attractive crime to commit. In line with the perception of

© University of Pretoria

anonymity, offenders of any age, economic status and background may commit a crime against the victim of their choice. Cyberspace also allows for an equal playing ground, where students from high-income households (42.9%) were more likely than students from low-income households (26.0%) to have had rumours spread about them. Within an equal playing field, a minimisation of status can be awarded to offenders, as regardless of their income and class status, they may target anyone who has a device connected to the internet (Barlett, Chamberlin & Witkower, 2016: 148).

The model also makes use of various factors of the online disinhibition effect. As previously mentioned, cyberspace offers the perception of anonymity. Such concept is further expanded into the offender feeling a sense of invincibility, and having the choice to behave in any way, as cyberspace offers identity flexibility and dissociative anonymity (Jalil & Sinnamon, 2019: 398). The offender can avoid being held accountable for their actions, by concealing their identities. For instance, nearly a third of the students (30.8%) experienced someone repeatedly sending them messages between one to two times. In a study conducted in the USA, although the victims told the harassers to stop (10.1%), they repeatedly sent messages (Finn, 2004: 473). Such a finding further illustrates that people's online behaviours differ from their offline behaviours, as the offender is more likely to stop when asked in a face-to-face interaction. The offender may also feel that through their invisibility of no one knowing who they are or by pretending to be someone they are not; they can exploit such a factor and harm who they want as many times as they want. For instance, slightly less than a third of students (31.7%) experienced someone pretending to be someone else between one to two times. Another factor of the online disinhibition effect that can be used is asynchronicity, where online communication does not take place in real-time. Offenders may then commit an offence without having to face immediate consequences, as cyberspace lacks nonverbal cues such as facial expressions and tone of voice (Kraft, 2010: 77) thus allowing the offender not to see the victim's response to the victimisation and the impact it has on them. For instance, as half of the students (52.1%) responded to the victimisation by ignoring the harasser, the harasser could get away with their actions, as they did not witness the impact of their behaviour on the victim.

In addition, cyberspace allows offenders to create a fantasy world online, where they can build 'fake' relationships with people who might not share the same feelings. Slightly less than one in three students (32.1%) experienced being harassed by someone they knew between one to two times. South African research confirms that when victims are harassed by someone they know, frequently, it is perpetrated by someone who mistook the relationship for something

© University of Pretoria

romantic (Sissing, 2013: 99). Such dissociative imagination links with another factor known as solipsistic introjection, when an offender fantasises about the relationship. The last element considered in the first component of the model suggests that offenders who victimise others online have typically been victims themselves. In a study conducted in the USA, individuals who were found to have cyberbullied others over Facebook had personally been cyberbullied in the past. The finding was important, as it shows that bullying can cause a person to act out in a similar way, to retaliate as a result of the hurt and loss of control. While being bullied can be hurtful, bullying someone else can cause the same individual to feel powerful and vindicated (Marcum et al., 2014: 545).

The second component of the integrated model consists of factors that link to the victim and the offender. If the factors are present within the victim, it increases their chances of being victimised by an offender. Firstly, various opportunities may present themselves to the offender; for instance, students' routine behaviour may consist of using their devices for their studies, entertainment, or social media. The study found that a third of the students (36.5%) reported spending more than four hours per day on the internet. It creates an opportunity for offenders to target university students and victimise them online. In addition, the students may lack guardianship, which can be considered as a risk factor. For example, nearly all of the students (92.4%) often used the internet for social media. Sites such as Twitter or Facebook may not have enough policies that focus on monitoring the online victimisation of students. Just less than a fifth of students (18.6%) experienced media being used as a slandering tool between one to two times. In line with risk factors, students may increase their vulnerability by engaging in dangerous behaviour. For example, a study from the USA found that over a fifth of students (23.7%) reported that they post personal information online for any person to see (Jalil & Sinnamon, 2019: 400). Reasons for not being vigilant could range from being impulsive to being unconcerned with the privacy status of their online profiles (Acquisti & Gross, 2006: 3). As a result, students who are not vigilant will be more likely to be victimised online by offenders. In addition, the students may have other characteristics that increase their exposure to being victimised, such as taking selfies and sharing them with other individuals. Consequently, the student loses control over what happens to such photos. Nearly a quarter of the students (23.6%) experienced someone sharing their personal photo between one to two times. Having a control deficit increases the offender's control surplus, resulting in an emotional consequence for the victim, where the victim may feel powerless and humiliated. The third and last component speaks of factors that directly influence the risk of an individual falling victim to a crime committed online. The third component uses two elements from the lifestyle/exposure theory, namely role expectations and structural constraints. Firstly, male

© University of Pretoria

students more readily used the internet for entertainment compared to the female students. Males may be expected more to play online gaming; however; as a result, they can fall victim to certain crimes. In terms of structural constraints, students from high-income households (22.2%) were significantly more likely than students from low-income households (13.0%) to have their identities stolen. As students from higher-income brackets have fewer financial constraints, their leisure activities may include making online purchases. However, it results in them being more likely to be victimised by offenders. Furthermore, the component examines how students' demographics could influence their victimisation risk. In terms of gender, the study observed that female students (49.3%) were significantly more likely than male students (29.3%) to receive unwanted sexual messages. As gender-based violence increases in South Africa, the simple characteristic of being female increases their vulnerability to experience harm and harassment online. Secondly, individuals who are not living at home but instead at a residence or in a commune may have an increased risk of being victimised. For example, students living in a residence (38.7%) were significantly more likely than those living with their families (28.5%) to have had someone share their personal photos. The reason being may be because students who leave home have gained newly-found independence, which may cause them to engage in risky behaviour, which as a result, ends in more of a chance of being victimised. The last factor of the third component consists of an individual's routine behaviour and how it can influence their risk of victimisation. The study found that two thirds (66.4%) of the students used the internet for their studies. Checking emails from lecturers or attending online classes, has become a routine activity for university students, which has especially been true for the past two years due to COVID-19 (Sadiki & Steyn, 2020: 149). However, an offender may be able to monitor a university student's routine of using the internet for their studies. Thus, university students have an increased risk of being victimised due to their routine activities.

6.7 Recommendations

The study presented an overview of existing knowledge and delivered new information regarding online victimisation among undergraduate students attending a South African university. The chapter highlighted that university students are at risk of experiencing online victimisation, and as such, their experiences need to be recognised on a national and local level. There is no denying that future research is required, thus, the researcher recommends the following:

- In terms of future research, there is a clear gap in research of online victimisation not only

© University of Pretoria

among university students but also within the context of South Africa. More research needs to be conducted in order to gain a better understanding of the phenomenon.

- An explorative study on online victimisation towards the development of legal definitions, targeted at South African policy should be considered.
- Future research should focus on the differences between traditional victimisation and online victimisation. Understanding the differences between the two may guide future policymaking.
- As the study was quantitative and basic in nature, future researchers might consider conducting qualitative research that is applied in nature (with a smaller sample population), in order to gain a more in-depth understanding of online victimisation, whilst thinking of ways to practically solve the problem.
- Furthermore, as the sample consisted of only undergraduate students, future research might consider expanding the sample population to include graduate students as they too can experience online victimisation. It might indicate a wider variety of predictors of online victimisation of university students.
- Future research might consider focusing on the responses to online victimisation among university students in South Africa, as the researcher identified a clear gap in such knowledge.

In terms of universities, the researcher recommends the following:

- University staff members should be trained on how to effectively and respectfully deal with university students who have been victimised online.
- Universities should consider conducting an orientation day where students are taught how to behave properly online, for instance, that their personal information should remain personal; to not accept friend requests from strangers; to apply caution when clicking on links that may lead to websites that are unsecured; to use strong and different passwords; re- consider sending and posting personal photos and setting their social media profiles on private.
- Awareness campaigns can be brought into the university where students are taught what signs to look out for and what to do if their friends (or themselves) are being victimised online.

In terms of adaption of policies, the researcher recommends the following:

- Universities should aim to redress and adapt their policies that focus on harassment, bullying and stalking, and ensure that they clearly outline that such types of victimisations

© University of Pretoria

that occur in an online setting are prohibited.

- Universities should consider separating policies that focus on online victimisation from traditional offline victimisation, as they have different meanings and implications for their victims.
- University policies need to clearly describe how students can report the incident, who they can report it to and what support will be provided to them after they have experienced online victimisation.
- Social media sites should consider looking at their own policies and aim to improve their monitoring and security systems, in order to ensure that any hateful, degrading, inappropriate and hurtful posts are identified and immediately removed.
- In South Africa, there are no clear guidelines, legislation or policies that solely focus on identifying online victimisation among university students, and until there is something, offenders will continue to commit the crimes as there are limited sanctions for their actions
- There is a need for government to create awareness programmes to educate the general public on issues related to crime and victimisation in cyberspace

6.8 Conclusion

After comparing the study's empirical results with the existing local and international literature, a few key observations were found. The study identified that university students who spend an increased time online, namely four hours or more per day, were more vulnerable to being victimised online. Gender differences were observed that influenced the likelihood of online victimisation. In terms of how students accessed the internet, male students were more likely to use their computers than females. However, females were more likely to use social media, presumably as a platform to express their opinions and use their voices to fight against gender norms. Furthermore, the researcher examined that based on the four factors that could influence the likelihood of online victimisation, students from high-income backgrounds were more likely to experience identity fraud, rumours being spread about them and offenders using social media as a slandering tool against them. In terms of gender, women were more likely to experience crimes linked to emotional and psychological sufferings, for example, receiving unwanted sexual messages. On the other hand, men were more likely to receive a virus, and students in third-year were also more susceptible to such victimisation. Lastly, students living in a residence had their personal photos shared more commonly due to an increased sense of freedom, or simply because they lived with more individuals who could take and share their photos by accident. Subsequently the researcher examined how the students responded to online victimisation. The most common response was that respondents ignored the harasser,

© University of Pretoria

Moreover, the shortfalls in both South Africa's current legislation and the university's existing policies were highlighted. Subsequently, various recommendations were made to use the study as a point of reference for adaptions to be made to address the occurrence of online victimisation among university students.

© University of Pretoria

List of references

Abu-Ulbeh, W., Altalhi, M., Abualigah, L., Almazroi, A.A., Sumari, P. & Gandomi, A.H. 2021. Cyberstalking victimisation model using criminological theory: A systematic literature review, taxonomies, applications, tools, and validations. *Electronics*, 10(1670): 1-45.

Acquisti, A. & Gross, R. 2006. *Imagined communities: Awareness, information sharing, and privacy on the Facebook.* Paper presented at the International Workshop on Privacy Enhancing Technologies. Available: https://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf (Accessed 2021/11/24).

Adams, B. 2021. South African teen commits suicide after bullied by schoolgirl in viral video. Available: https://news.yahoo.com/south-african-teen-commits-suicide-150237292.html?guccounter=1 (Accessed 2021/11/24).

Aftab, P. 2010. Stop cyberbullying: What is cyberbullying, exactly? Available: www.stopcyberbullying.org/what_is_cyberbullying_exactly.html (Accessed 2021/11/07).

Akbulut, Y. & Eristi, B. 2011. Cyberbullying and victimisation among Turkish university students. *Australasian Journal of Educational Technology*, 27(7): 1155-1170.

Akhtar, I. 2016. *Research design. In research in social science: Interdisciplinary perspectives*. New Delhi: Rawat Publication.

Akhter, S. 2020. *Cyber victimisation of adult women: A systematic review*. Sweden: Malmo University (MA Dissertation).

Akoglu, H. 2018. User's guide to correlation coefficients. *Turkish Journal of Emergency Medicine,* 18: 91-93.

Alemu, S.K. 2018. The meaning, idea and history of university/higher education in Africa: A brief literature review. *Forum for International Research in Education,* 4(3): 210-227.

Alhaboby, Z.A., Barnes, J., Evans, H. & Short, E. 2017. Cyber-victimisation of people with chronic conditions and disabilities: A systematic review of scope and impact. *Trauma, Violence*

© University of Pretoria

& Abuse, 2(1): 1-18.

Asli, M.R. 2013. Introducing general theory of victimology in criminal sciences. *International Journal of Humanities,* 20(3): 53-79.

Babbie, E. & Mouton, J. 2001. *The practice of social research*. Cape Town: Oxford University Press.

Babbie, E. & Mouton, J. 2003. *The practice of social research*. Cape Town: Oxford University Press.

Babbie, E. 2007. *The practice of social research*. 3rd ed. Belmont, CA: Thomson Wadsworth.

Babbie, E. 2014. *The Basics of Social Research*. 6th ed. Australia: Wadsworth Cengage Learning.

Badenhorst, C. 2011. Legal responses to cyberbullying and sexting in South Africa. *Centre for Justice and Crime Prevention CJCP Issue Paper, No. 10*. August 2011. Available: https://www.childlinesa.org.za/wp-content/uploads/issue-paper-10-legal-reponses-to-cyberbullying-and-sexting-in-sa.pdf (Accessed 2021/11/07).

Barlett, C., Chamberlin, K. & Witkower, Z. 2016. Predicting cyberbullying perpetration in emerging adults: A theoretical test of the Barlett Gentile Cyberbullying Model. *Aggressive Behaviour*, 43(2): 147-154.

Barlett, C.P. & Chamberlin, K. 2017. Examining cyberbullying across the lifespan. *Computers in Human Behaviour*, 71: 444-449.

Barlett, C.P., Madison, C.S., Heath, J.B. & DeWitt, C.C. 2019. Please browse responsibly: A correlational examination of technology access and time spent online in the Barlett Gentile Cyberbullying Model. *Computers in Human Behaviour*, 92: 250-255.

Bayer, J.B., Triệu, P. & Ellison. N.B. 2019. Social media elements, ecologies and effects. *Annual Review of Psychology*, 71: 1-27.

Ben-Joseph, E.P. 2021. Cyberbullying. Available:

© University of Pretoria

https://kidshealth.org/en/teens/cyberbullying.html (Accessed 2021/11/27).

Bhattacherjee, A. 2012. *Social Science Research: Principles, Methods, and Practices*. 2nd ed. Tampa, Florida: Global Text Project.

Blanche, M.T., Durrheim, K. & Painter, D. 2006. *Research in practice: applied methods for the social sciences*. 2nd ed. Cape Town: University of Cape Town Press.

Bocij, P. & McFarlane, L. 2003. Seven fallacies about cyber stalking. *Prison Service Journal*, 149: 37-42.

Bocij, P. 2004. *Cyberstalking: Harassment in the internet age and how to protect your family*. Wesport: Praege.

Bocij, P. 2005. Reactive stalking: A new perspective on victimisation. *The British Journal of Forensic Practice*, 7: 23-45.

Booyens, K. 2009. *The sexual assault and rape of male offenders and awaiting trial detainees*. Pretoria: University of Pretoria (DPhil Thesis).

Bossler, A.M. & Holt, T.J. 2011. Malware victimisation: A routine activities framework. In Jaishankar, K. *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*. United States: Taylor & Francis Group.

Bossler, A.M., Holt, T.J. & May, D.C. 2012. Predicting online harassment victimisation among a juvenile population. *Youth & Society*, 44(4): 500-523.

Bottomley, E.J. 2020. SA has some of Africa's most expensive data, a new report says – but it is better for the richer. Available: https://www.businessinsider.co.za/how-sas-data-prices-compare-with-the-rest-of-the-world-2020-5#:~:text=South%20Africa%20ranks%20at%20148,t%20afford%20bulk%20data%20packages (Accessed 2021/11/26).

Bouffard, L.A. & Muftić, L.R. 2006. The "rural mystique": Social disorganisation and violence beyond urban communities. *Western Criminology Review,* 7(3): 56-66.

Bourque, L.B. & Fielder, E.P. 2011. Overview of self-administered questionnaires. In *how to*

© University of Pretoria

conduct self-administered and mail surveys. Thousand Oaks: SAGE.

Boursier, V., Gioia, F., Musetti, A. & Schimmenti, A. 2020. Facing loneliness and anxiety during the COVID-19 isolation: The role of excessive social media use in a sample of Italian adults. *Frontiers in Psychiatry,* 11: 1-10.

Brown, M.L. & Krysik, J. 2011. Online harassment among college students: A replication study incorporating new internet trends. *SSRN Electronic Journal,* 15(5): 1-21.

Burchell, J. 2014. Protecting dignity under common law and the Constitution: the significance of crimen injuria in South African criminal law. *South African Journal of Criminal Justice*, 27(3): 250-271.

Burns, N. & Grove, S.K. 2005. *The practice of nursing research: conduct, critique and utilisation.* 5th ed. Saint Louis: Elsevier Saunders.

Burrell, N.A. & Gross, C. 2018. Quantitative research, "purpose of quantitative research". In *The SAGE Encyclopedia of Communication Research Methods*. Thousand Oaks, CA: SAGE.

Burton, P. & Mutongwizo, T. 2009. Inescapable violence: Cyber bullying and electronic violence against young people in South Africa. *Centre for Justice and Crime Prevention, CJCP Issue Paper, No. 8*. December 2009.

Business Software Alliance. 2004. Types of cybercrime. Available: http://www.playitcybersafe.com/cybercrime/ (Accessed 2021/10/20).

Business Tech. 2019. These are the biggest social media and chat platforms in 2019. Available: https://businesstech.co.za/news/internet/296752/these-are-the-biggest-social-media-and-chat-platforms-in-2019/ (Accessed 2021/11/08).

Carr, C.T. & Hayes, R.A. 2015. Social media: Defining, developing and divining. *Atlantic Journal of Communication*, 23: 46-65.

Carter, M.A. 2013. Protecting oneself from cyber bullying on social media sites – a study of undergraduate students. *Social and Behavioural Sciences*, 93: 1229-1235.

Casey, E. 2000. *Digital evidence and computer crime*. London, UK/CA: Academic Press.

© University of Pretoria

Cetin, B., Yaman, E. & Peker, A. 2011. Cyber victim and bullying scale: A study of validity and reliability. *Computers and Education,* 57: 2261-2271.

Cheung, C.M.K., Wong, R.Y.M. & Chan, T.K.H. 2020. Online disinhibition: conceptualization, measurement, and implications for online deviant behaviour. *Industrial Management & Data Systems*, 10: 1-17.

Choi, K.S. 2008. Computer crime victimisation and integrated theory: an empirical assessment*. International Journal of Cyber Criminology*, 2(1): 308-333.

Choi, K.S. 2011. Cyber-Routine activities: Empirical examination of online lifestyle, digital guardians, and computer-crime victimisation. In Jaishankar, K. *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*. United States: Taylor & Francis Group.

Cilliers, L. 2021. Perceptions and experiences of cyberbullying amongst university students in the Eastern Cape province, South Africa. *The Journal for Transdisciplinary Research in Southern Africa*, 17(1): 1-6.

Cinini, S.F. 2015. *A Victimological exploration of the victimisation vulnerability of a group of foreign nationals in the city of Durban*. KwaZulu-Natal: University of KwaZulu-Natal (MA Dissertation).

Clow, K.E. & James, K.E. 2014. *Essentials of marketing research: putting research into practice*. Thousand Oaks: SAGE Publications, Inc.

Coetzee, A. 2017. *Workplace violence against educators in private and public secondary schools in Pretoria, Gauteng: a comparative investigation*. Pretoria: University of Pretoria (MA Dissertation).

Cohen, L., Manion, L. & Morrison, K. 2007. *Research methods in education*. 6th ed. Abingdon, UK: Routledge.

Constitution of the Republic of South Africa, 1996.

Council of Europe. 2021. What causes gender-based violence? Available:

© University of Pretoria

https://www.coe.int/en/web/gender-matters/what-causes-gender-based-violence (Accessed 2021/12/05).

Cramer, D. & Howitt, D. 2011. Chi-Square or Chi-Squared (x2). In *The SAGE Dictionary of Statistics*. London, UK: SAGE Publications.

Crosslin, K. & Golman, M. 2014. "Maybe you don't want to face it" – College students' perspectives on cyberbullying. *Computers in Human Behaviour*, 41: 14-20.

Cutcliffe, J. R. & McKenna, H.P. 1999. Establishing the credibility of qualitative research findings: the plot thickens. *Journal of Advanced Nursing*, 30(2): 374-380.

Dalal, R.S. & Sheng, Z. 2018. Mistreatments in organisations: towards a perpetrator-focused research agenda. *Industrial and Organisation Psychology,* 11(1): 101-106.

Daniel, J. 2012. Sampling and probability sampling. In *Sampling Essentials: Practical Guidelines for Making Sampling Choices*. Thousand Oaks: SAGE.

Dantzker, M.L., Hunter, R.D. & Quinn, S.T. 2018. *Research methods for Criminology and criminal justice*. 4th ed. City of Massachusetts, United States: Jones & Barlett Learning.

Davis, A., Wladkowski, S.P. & Mirick, R.G. 2017. Lessons learned for successful dissertation completion from social work doctoral graduates. *Journal of Teaching in Social Work,* 37(2): 107-120.

Davis, J.L. & Jurgenson, N. 2014. Context collapse: Theorising context collusions and collisions. *Information, Communication and Society*, 17(4): 476–485.

De Vos, A.S., Strydom, H., Fouché, C.B & Delport, C.S.L. 2021. *Research At Grass Roots - For The Social Sciences And Human Services Profession.* 5th Ed. Cape Town: Van Schaik Publishers.

Department of Justice and Constitutional Development. 2008. Understanding the South African Victims' Charter- A Conceptual Framework. Pretoria: Government printers.

Department of Justice. 2004. Computer crime and intellectual property section (CCIPS).

© University of Pretoria

Available: https://www.justice.gov/criminal-ccips (Accessed 2021/10/20).

Department of Social Development. 2020. *Victim Empowerment Programme*. Western Cape: The Department of Social Development Victim Empowerment Programme. Available: https://www.westerncape.gov.za/service/victim-empowerment-programme (Accessed 2021/11/07).

Dittman, M. 2003. Anger across the gender divide. *Monitor on Psychology*, 34(3): 52-53.

Dlamini, S. & Mbambo, C. 2019. Understanding policing of cybercrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences,* 5(1): 1-13.

Docherty, B. 2000. Defamation law: Positive jurisprudence. *Harvard Human Rights Journal*, 13: 263–268.

Dooley, J.J., Shaw, T. & Cross, D. 2012. The association between the mental health and behavioural problems of students and their reactions to cyber-victimisation. *European Journal of Developmental Psychology*, 9(2): 275-289.

Drahokoupilová, J. 2007. Cyberstalking. Available: https://journals.muni.cz/mujlt/article/view/2495/2059 (Accessed 2021/11/08).

Dyer, H.T. 2020. *Designing the social: Unpacking social media design and identity*. Singapore: Springer.

Eck, J.E. & Weisburd, D. 1995. *Crime places in crime theory*. Washington D.C: University of Maryland.

Etikan, I., Musa, S.A. & Alkassim, R.S. 2016. Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1): 1-4.

Finkelhor, D. 2007. Developmental Victimology: the comprehensive study of childhood victimisations. In Davis, R.C., Luirigio, A.C. & Herman, S. 3rd ed. *Victims of Crime*. Thousand Oaks: SAGE.

Finn, J. 2004. A survey of online harassment at a university campus. *Journal of Interpersonal*

© University of Pretoria

Violence, 19(4): 468-483.

Fire, M., Kagan, D., Elyashar, A. & Elovici, Y. 2014. Friend or foe? Fake profile identification in online social networks. *Social Networking Analysis and Mining,* 4(194): 1-23.

Fitzgerald, J. & Fitzgerald, J. 2014. *Statistics for criminal justice and Criminology in practice and research: An introduction*. London: SAGE.

Flick, U. 2004. Triangulation in qualitative research. In Flick, U., von Kardorff, E. & Steinke, I. (Eds). *A Companion to Qualitative Research*. Trans. B. Jenner. London: SAGE.

Fouladchang, M., Marzooghi, R. & Shemshiri, B. 2009. The effect of gender and grade level differences on achievement goal orientations of Iranian undergraduate students. *Journal of Applied Sciences,* 9(5): 968-972.

Gaber, J. 2012. Applied Research. In Salkind, N.J. *Encyclopedia of Research Design*. Thousand Oaks: SAGE.

Gaillie, L. 2020. 12 advantages and disadvantages of correlational research studies. Available: https://vittana.org/12-advantages-and-disadvantages-of-correlational-research-studies (Accessed 2021/11/25).

Gaiser, T.J. & Schreiner, A.E. 2011. Research standards and ethical considerations. In *A Guide to Conducting Online Research.* London: SAGE.

Garson, G.D. 2013. *Validity and Reliability*. Asheboro, NC: Statistical Associates Publishing.

Gibb, S.G. & Devereux, P.G. 2014. Who does that anyway? Predictors and personality correlates of cyberbullying in college. *Computers in Human Behaviour*, 38: 8-16.

Given, L. M. 2012. Quantitative research. In *The SAGE Encyclopedia of Qualitative Research Methods.* Thousand Oaks, CA: SAGE.

Golafshani, N. 2003. Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4): 597-607.

Golbeck, J. 2018. *Online harassment (Human computer interaction series).* New York:

© University of Pretoria

Springer.

Goodno, N. H. 2011. How public schools can constitutionally halt cyberbullying: A model cyberbullying policy that considers first amendment, due process, and fourth amendment challenges. *The Wake Forest Law Review*, 46: 641–700.

Gous, N. 2019. Pretoria girl commits suicide allegedly after cyberbullying. Available: https://www.timeslive.co.za/news/south-africa/2019-02-19-pretoria-girl-commits-suicide-allegedly-after-cyberbullying/ (Accessed 2021/11/11).

Grand Canyon University. 2019. Three modern theories of victimology. Available: https://www.gcu.edu/blog/criminal-justice-government-and-public-administration/3-modern-theories-victimology (Accessed 2021/07/19).

Grigg, D.W. 2010. Definitional constructs of cyber-bullying and cyber-aggression from a triangulatory overview: A preliminary study into elements of cyberbullying. *Journal of aggression, conflict and peace research*, 4(4): 202-215.

Grotenhuis, M.T. & Matthijssen, A. 2021. Statistics program SPSS. In *Basic SPSS Tutorial*. Thousand Oaks: SAGE.

Hagan, T.L. 2014. Measurements in quantitative research: How to select and report on research instruments. *Oncology Nursing Forum,* 41(4): 431.

Harris, T. & Steyn, F. 2018. Gender differences in adolescent online victimisation and sexting expectancies. *Child Abuse Research: A South African Journal*, 19(1): 15-29.

Hendricks, K., Tsibolane, P. & Van Belle, J.P. 2020. *Cyber-harassment victimisation among South African LGBTQIA + Youth*. Cape Town: Springer Nature Switzerland.

Henson, B., Reyns, B.W. & Fisher, B.S. 2016. Cybercrime Victimisation. In Blackwell, W. *The Wiley Handbook on the Psychology of Violence*. London, UK: John Wiley & Sons.

Herrera, M.C., Herrera, A. & Expósito, F. 2014. Stop harassment! Men's reactions to victims' confrontation. *The European Journal of Psychology Applied to Legal Context,* 6: 45-52.

Hilbe, J.M. 2015. *Practical Guide of Logistic Regression*. Boca Raton, United States: CRC

© University of Pretoria

Press.

Hill, J.K. 2003. *Victims' response to trauma and implications for interventions: A selected review and synthesis of the literature*. Ottawa: Department of Justice Canada (Victims of crime research series). Available: https://www.justice.gc.ca/eng/rp-pr/cj-jp/victim/rr03_vic2/index.html (Accessed 2021/11/08).

Hinduja, S. & Patchin, J.W. 2007. Offline Consequences of online victimisation: school violence and delinquency. *Journal of School Violence*, 6(3): 89-112.

Horne, C.S. 2018. *A quick, free, somewhat easy-to-read introduction to empirical social science research methods*. Chattanooga: University of Tennessee at Chattanooga.

Hubbard, D. 2008. Stalking: Proposed New Legislation for Namibia. *Monograph No. 3*, Gender Research & Advocacy Project, Legal Assistance Centre, Windhoek, Namibia.

Hyeoun-Ae, P. 2013. An introduction to logistic regression: From basic concepts to interpretation with particular attention to nursing domain. *Journal of Korean Academy of Nursing,* 43(2): 154-64.

Hyman, M.R. & Sierra, J.J. 2016. Open-versus close-ended survey questions. *Business Outlook*, 14(2): 1-5.

Ivankova, N.V., Creswell, J.W. & Plano Clark, V.L. 2007. Foundations and approaches to mixed methods research. In Maree, K. *First steps in research*. Pretoria: Van Schaik Publishers.

Jalil, J. & Sinnamon, G. 2019. Risks of Online Victimisation Among College Students on Mobile Social Networks. *International Journal of Cyber Criminology*, 13(2): 396-417.

Johnson, J. 2021. Statista: Global digital population as of January 2021. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed 2021/11/19).

Johnston, M.P. 2014. Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries,* 3: 619-626.

Jones, L.M. & Mitchell, K.J. 2016. Online harassment. In Blackwell, W. *The Wiley Handbook*

© University of Pretoria

on the Psychology of Violence. London, UK: John Wiley & Sons, Ltd.

Jonker, J. & Pennink, B. 2010. *The essence of research methodology: A concise guide for Master's and PhD students in management science*. Heidelberg: Springer.

Kaplan, A.M. & Haenlein, M. 2010. Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53: 59-68.

Kearney, M.W. 2017. Cramer's V. In *SAGE Encyclopedia of Communication Research Methods*. Thousand Oaks: SAGE.

Keeter, S. 2011. Survey research. In Druckman, D. 2005. *Doing Research*. Thousand Oaks, CA: SAGE.

Kennedy, M.A. & Taylor, M.A. 2010. Online harassment and victimisation of college students. *Justice Policy Journal*, 7(1): 1-21.

Kent, M.L. 2010. Directions in social media for professionals and scholars. In Heath, R.L. *Handbook of Public Relations*. 2nd ed. Thousand Oaks: SAGE.

Khalid, F. 2012. *Psychosis and aggression in childhood & adolescence: investigations in clinically referred, inpatient and general population samples*. Kings College London (PhD Thesis).

Kokkinos, C.M., Baltzidis, E. & Xynogala, D. 2016. Prevalence and personality correlates of Facebook bullying among university undergraduates. *Computers in Human Behaviour*, 55(Part B): 840-850.

Kota, R., Schoohs, S., Benson, M. & Moreno, M.A. 2014. Characterising cyberbullying among college students: hacking, dirty laundry and mocking. *Societies,* 4: 549-560.

Kothari, C.R. 2004. *Research Methodology: Methods and Techniques*. 2nd ed. New Delhi: New Age International Publishers.

Kraft, E. 2010. An exploratory study of the cyberbullying and cyberstalking experiences and factors related to victimisation of students at a public liberal arts college. *International Journal*

© University of Pretoria

of Technoethics, 1(4): 74-91.

Kraska, M. 2012. Quantitative research. In *Encyclopedia of Research Design*. Thousand Oaks, CA: SAGE.

Krohn, M.S. & Eassey, J.M. 2014. Integrated theories of crime. In Miller, J.M. *The Encyclopedia of Theoretical Criminology*. Hoboken, New Jersey, United States: Blackwell.

Kumar, R. 2011. *Research Methodology: a step-by-step guide for beginners*. 3rd ed. London: SAGE.

Kunz, M. & Wilson, P. 2004. *Computer crime and Computer fraud.* Maryland: University of Maryland (MA dissertation).

Lama. 2020. Social Media Statistics and usage in South Africa. Available: https://www.talkwalker.com/blog/social-media-stats-south-africa# (Accessed 2021/11/10).

Law Insider. 2021. Student definition. Available: https://www.lawinsider.com/dictionary/student (Accessed 2021/11/24).

Lazic, M. 2021. 39 Worrying cybercrime statistics by Legaljobs. Available: https://legaljobs.io/blog/cyber-crime-statistics/ (Accessed 2021/11/10).

Leedy, P.D. & Ormrod, J.E. 2016. *Practical Research: Planning and Design*. 11th ed. New York City, United States of America: Pearson.

Letseka, M. & Maile, S. 2008. High university drop-out rates: A threat to South Africa's future, HSRC Policy Brief. In *HSRC Policy Brief*. Bloemfontein, South Africa: HSRC Press. Available: http://wwwdocs.hsrc.ac.za/uploads/pageContent/1088/Dropout%20rates.pdf (Accessed 2021/11/07).

Lewis-Beck, M.S., Bryman, A. & Liao, T.F. 2011. Basic Research. In T*he SAGE Encyclopedia of Social Science Research Methods*. Thousand Oaks, CA: SAGE.

Lewis-Beck, M.S., Bryman, A. & Liao, T.F. 2011. Close-ended questions. In The SAGE

© University of Pretoria

Encyclopedia of Social Science Research Methods. Thousand Oaks, CA: SAGE.

Lewis-Beck, M.S., Bryman, A. & Liao, T.F. 2011. Mann-Whitney U Test. In *the SAGE Encyclopedia of Social Science Research Methods.* Thousand Oaks, CA: SAGE.

Lindsay, M. & Krysik, J. 2012. Online harassment among college students. *Information, Communication & Society*, 15(5): 703-719.

Lindsay, M., Booth, J.M., Messing, J.T. & Thaller, J. 2016. Experiences of online harassment among emerging adults: Emotional reactions and the mediating role of fear. *Journal of Interpersonal Violence*, 31(19): 3174-3195.

Luborsky, M.R. & Rubinstein, R.L. 1995. Sampling in qualitative research: Rationale, issues, and methods. *Research on Aging,* 17(1): 89-113.

Lutya, T.M. 2010. *Lifestyles and routine activities of South African teenagers at risk of being trafficked for involuntary prostitution*. Pretoria: University of Pretoria (Research Articles).

MacDonald, C.D. & Roberts-Pittman, B. 2010. Cyberbullying among college students: prevalence and demographic differences. *Social and Behavioural Sciences*, 9: 2003-2009.

Machackova, H., Cerna, A., Sevcikova, A., Dedkova, L. & Daneback, K. 2013. Effectiveness of coping strategies for victims of cyberbullying. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 7(3): 1-12.

Mahoe, R. 2004. Reflections on the dissertation process and the use of secondary data. *Educational Perspective,* 37(2): 34-37.

Malhotra, N.K. 2011. Questionnaire design and scale development. In *The Handbook of Marketing Research*. Thousand Oaks, CA: SAGE.

Manning, J. 2014. Social Media, Definition and Classes of. In Harvey, K. *Encyclopedia of social media and politics*. Thousand Oaks, CA: SAGE.

Marcum, C.D. 2011. Adolescent Online Victimisation and Constructs of Routine Activities Theory. In Jaishankar, K. *Cyber Criminology: Exploring Internet Crimes and Criminal*

© University of Pretoria

Behaviour. New York, United States: Taylor & Francis.

Marcum, C.D., Higgins, G.E., Freiburger, T.L. & Ricketts, M.L. 2014. The American Journal of Criminal Justice, 39: 538- 548.

Marston, L. 2010. *Introductory statistics for health and nursing using SPSS*. London: SAGE.

Mason, K.L. 2008. Cyberbullying: A preliminary assessment for school personnel. *Psychology in the Schools*, 45: 323-348.

McFarlane, L. & Bocij, P. 2005. An exploration of predatory behaviour in cyber-space: Towards a typology of cyber stalkers. *First Monday*, 26(10): 1-12.

McHugh, M.L. 2013. The Chi-square test of independence. *Biochemia Medica,* 23(2): 143-9.

McNeish, D. 2018. Thanks Coefficient Alpha, We'll Take It from Here. *Psychological Methods*, 23(3): 412-433.

Meadows, R.J. 2007. *Understanding violence and victimisation*. Upper Saddle River, New Jersey, United States: Pearson/Prentice Hall.

Menard, S. 2013. Prediction Tables and Qualitative approaches to explained variation. In Menard, S. 2010. *Logistic Regression: From Introductory to Advanced Concepts and Applications*. Thousand Oaks, CA: SAGE.

Merriam-Webster. 2021. Definition of gender. Available: https://www.merriam-webster.com/dictionary/gender (Accessed 2021/11/24).

Merriam-Webster. 2021. Definition of university. Available: https://www.merriam-webster.com/dictionary/university (Accessed 2021/11/24).

Meyers, C.A. & Cowie, H. 2017. Bullying at university: The social and legal contexts of cyberbullying among university students. *Journal of Cross-Cultural Psychology,* 48(8):1172–1182.

Miller, B.N. & Morris, R.G. 2012. Cyber-related violence. In DeLisi, M. &. Conis, P.J. 2nd ed.

© University of Pretoria

2012. *Violent offenders: Theory, research, policy and practice*. London: Jones & Bartlett.

Miller, D.C. & Salkind, N.J. 2011. Defining the characteristics of basic, applied, and evaluation research. In *The Handbook of Research Design & Social Measurement*. Thousand Oaks, CA: SAGE.

Miller, D.C. & Salkind, N.J. 2011. The orientation and commitment of the basic researcher. In Miller, D.C. & Salkind, N.J. *The Handbook of Research Design & Social Measurement*. Thousand Oaks, CA: SAGE.

Miró-Llinares, F. 2014. Routine activity theory. In *The Encyclopedia of Theoretical Criminology Online*. Hoboken, New Jersey, United States: Blackwell Publishing.

Mishra, S.B. & Alok, S. 2017. *Handbook of Research Methodology: A Compendium for Scholars & Researchers*. New Delhi: Educreation Publishing.

Morin, A. 2019. Cyberbullying statistics everyone should know: From threats to rumours, cyberbullies use a variety of tactics. Available: https://www.verywellfamily.com/cyberbullying-statistics-4589988#citation-1 (Accessed 2021/11/10).

Mosley, M.A., Lancaster, M., Parker, M.L. & Campbell, K. 2020. Adult attachment and online dating deception: a theory modernised. *Sexual and Relationship Therapy,* 35(2): 1-17.

Muijs, D. 2011. Designing Non-Experimental Studies. In *Doing Quantitative Research in Education with SPSS.* London: SAGE.

Muijs, D. 2011. Introduction to Quantitative Research. In *Doing Quantitative Research in Education with SPSS*. London: SAGE.

Mullen, P.E., Pathé, M. & Purcell, R. 2009. *Stalkers and their victims*. 2nd ed. London: Cambridge University Press.

Muller, J. *The influence of Harm Avoidance and Novelty Seeking temperament traits on emotional processing*. University of Pretoria (MA Dissertation).

National Crime Prevention Council. 2010. Cyberbullying FAQ for Teens. Available:

© University of Pretoria

http://www.ncpc.org/topics/cyberbullying/cyberbullyingfaq-for-teens (Accessed 2021/11/07).

National Supplemental Victimisation survey (NSVS). 2018. Victims of Identity Theft. Available: https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (Accessed 2021/11/10).

Ndubueze, P.N. & Abdullahi, A.S. 2019. Awareness of cyber victimisation among internet-active undergraduate students in selected Nigerian universities. *Journal of Sociological Studies*, 3(1): 19-26.

Neaville, S. 2017. *Investigating the Efficacy of the Coping Strategies Adolescents Use to Handle Cyberbullying*. Washington: Walden University (PhD Dissertation).

Neuman, W.L. 2011. *Social research methods: qualitative and quantitative approaches*. 7th Ed. Boston: Pearson Education.

Neuman, W.L. 2014. *Basics of social research: qualitative and quantitative approaches*. 3rd Ed. Harlow: Pearson Education.

Ngo, F.T., Piquero, A.R., LaPrade, J. & Duong, B. 2020. Victimisation in cyberspace: Is it how long we spend online, what we do online, or what we post online? *Criminal Justice Review,* 45(4): 430-451.

Norum, P.S. & Weagley, R.O. 2007. College students' internet use, and protection from online identity theft. *Educational Technology Systems*, 35(1): 45-59.

O'Reilly, K. 2012. Positivism. In O'Reilly, K. 2009. *Key concepts in Ethnography*. London: SAGE.

Odell, P.M., Korgen, K.O., Schumacher, P. & Delucchi, M. 2000. Internet use among female and male college students. *Cyber Psychology & Behaviour,* 3(5): 855-862.

Osborne-Gowey, J. 2014. What is social media? *Fisheries*, 39(2): 55.

Pallant, J. 2007. *SPSS Survival Manual: A step by step guide to data analysis using SPSS for Windows*. 3rd ed. England: Open University Press.

Patten, M.L. & Newhart, M. 2018. *Understanding Research Methods: An Overview of the*

© University of Pretoria

Essentials. 10th ed. New York: Routledge.

Paullet, K.L., Rota, D.R. & Swan, T.T. 2009. Cyberstalking: An exploratory study of students at a mid-Atlantic university*. Issues in Information Systems*, 10(2): 640–648.

Pew Research Center. 2018. A majority of teens have been the target of cyberbullying, with name-calling and rumour-spreading being the most common forms of harassment. Available: https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/pi_2018-09-27_teens-and-cyberbullying_0-01/ (Accessed 2021/11/27).

Pew Research Centre. 2021. The state of online harassment. Available: https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/ (Accessed 2021/11/09).

Pillay, R. & Sacks, G. 2020. Cyberbullying- A shrouded crime: Experiences of South African undergraduate students. *The Oriental Anthropologist*, 1-17.

Pineiro, C.R. 2016. *Social Media Use and Self-esteem in Undergraduate Students*. New Jersey: Rowan University (MA Dissertation).

Piquero, A.R. & Hickman, M. 1999. An empirical test of Tittle's control balance theory. *Criminology,* 37(2): 319-340.

Piquero, A.R. & Hickman, M. 2003. Extending Tittle's control balance theory to account for victimisation. *Criminal Justice and Behaviour*, 30(3): 282-301.

Pittaro, M.L. 2011. Cyber Stalking: Typology, Etiology and Victims. In Jaishankar, K. *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour*. New York City, United States: Taylor & Francis.

Poirier, G. n.d. What is Foursquare & How does it work? Available: https://smallbusiness.chron.com/foursquare-work-28728.html (Accessed 2022/02/03).

Popovac, M. & Leoschut, L. 2012. Cyberbullying in South Africa: Impact and responses. *Centre for Justice and Crime Prevention, CJCP Issue Paper, No. 13*. June 2012.

© University of Pretoria

Pradubmook-Sherer, P. & Sherer, M. 2015. Victimisation among high school students in Thailand. *Australian & New Zealand Journal of Criminology*, 0(0): 1-19.

Prakash, Y.G. & Rai, J. 2017. The generation Z and their social media usage: A review and a research outline. *Global Journal of Enterprise Information System,* 9(2): 110–116.

Quantemna, s.a. *Advanced SPSS Training manual*. [SI; sn].

Rahman, S. 2016. The advantages and disadvantages of using qualitative and quantitative approaches and methods in language “testing and assessment” research: A literature review. *Journal of Education and Learning*, 6(1): 102-112.

Rainn. 2021. What consent looks like. Available: https://www.rainn.org/articles/what-is-consent (Accessed 2021/11/27).

Readex Research. 2021. A brief overview of the benefits of self-administered surveys. Available: https://www.readexresearch.com/advantages-of-self-administered-surveys/ (Accessed 2021/05/14).

Reddick, M.A. 2018. *Social media use and its relationship with anxiety and depression*. Virginia: Ferrum College (MA Dissertation).

Republic of South Africa. 1998. Department of Justice. Domestic Violence Act 116 of 1998. Published in the Government Gazette, (20601) Pretoria: Government Printer.

Republic of South Africa. 2002. Department of Justice. Electronics Communication and Transactions Act 25 of 2002. Published in the Government Gazette, (23708) Pretoria: Government Printer.

Republic of South Africa. 2011. Department of Justice. Protection from Harassment Act 17 of 2011. Published in the Government Gazette, (34818). Cape Town: Government Printer.

Republic of South Africa. 2012. Department of Communications. Electronic Communications and Transactions Amendment Bill, 2012. Published in the Government Gazette, (35821). Pretoria: Government Printer.

© University of Pretoria

Republic of South Africa. 2020. Department of Justice and Correctional Services. Cybercrimes Act 19 of 2020. Published in the Government Gazette, (44651). Pretoria: Government Printer.

Sadiki, L. & Steyn, F. 2020. 'All hands-on deck!': Responding to undergraduate criminology teaching and learning in a time of pandemic pedagogy. *African Journal of Criminology & Victimology,* 33(3): 149-168.

Safer Spaces. 2021. Gender-based violence in South Africa. Available: https://www.saferspaces.org.za/understand/entry/gender-based-violence-in-south-africa (Accessed 2021/11/18).

Salkind, N.J. 2011. Basic research. In *The Encyclopedia of Measurement and Statistics*. Thousand Oaks, CA: SAGE Publications.

Salkind, N.J. 2011. Chi-Square Test for Independence. In *The Encyclopedia of Measurement and Statistics*. Thousand Oaks, CA: SAGE.

Saponaro, A. 2019. Theoretical approaches and perspectives in victimology. In Peacock, R. 3rd ed. *Victimology in Africa*. Pretoria: Van Schaik Publishers.

Schenk, A.M. 2011. *Psychological impact of cyberbully victimisation among college students*. West Virginia: West Virginia University (MA Dissertation).

Seda, L. 2014. Identity theft and university students: do they know, do they care? *Journal of Financial Crime,* 21(4): 461-483.

Sehlule, T. 2018. *Assessing the online sexual harassment experiences of female students at a South African Institution of Higher Learning*. Limpopo: University of Venda (MA Dissertation).

Siddiqui, S. & Singh, T. 2016. Social media: Its impact with positive and negative aspects. *International Journal of Computer Applications Technology and Research*, 5(2): 71-75.

Sissing, S.K. 2013. *A Criminological exploration of cyber stalking in South Africa*. Pretoria, SA: University of South Africa (MA Dissertation).

Smith, L.R., Smith, K.D. & Blazka, M. 2017. Follow me, what's the harm? Considerations of

© University of Pretoria

catfishing and utilising fake online personas on social media. *Journal of Legal Aspects of Sport,* 27: 32-45.

South African Government. 2021. Coronavirus COVID-19 Alert Level 1. Available: https://www.gov.za/covid-19/about/coronavirus-covid-19-alert-level-1 (Accessed 2021/11/24).

South African Law Reform Commission. 2004. Stalking. *Discussion Paper, Project 130*, September 2004. Available: https://www.justice.gov.za/salrc/dpapers/dp108.pdf (Accessed 2021/11/24).

South African Police Service: Department of Police. Available: https://www.saps.gov.za/services/july_to_september_2020_21_crime_situation.pdf (Accessed 2021/11/08).

Stangor, C. 2011. *Research methods for the behavioural sciences*. Boston: Laureate Education, Inc.

Staniloiu, A. & Markowitsch, H. 2012. Gender differences in violence and aggression- a neurobiological perspective. *Social and Behavioural Sciences,* 33: 1032-1036.

Stark, R. 1987. Deviant Places: A theory of the ecology of crime. *Criminology*, 25(4): 893-909.

Statista Research Department. 2021. Total population of South Africa 2019, by ethnic groups. Available: https://www.statista.com/statistics/1116076/total-population-of-south-africa-by-population-group/ (Accessed 2021/11/26).

Statistics Canada. 2021. Non-probability Sampling. Available: https://www150.statcan.gc.ca/n1/edu/power-pouvoir/ch13/nonprob/5214898-eng.htm (Accessed 2021/11/25).

Statistics How To. 2021. Hosmer-Lemeshow Test: Definition. Available: https://www.statisticshowto.com/hosmer-lemeshow-test/ (Accessed 2021/12/02).

Statistics South Africa. 2014. *Victims of Crime Survey 2013/14*. Pretoria: Statistics South

© University of Pretoria

Africa.

Steyn, F. 2016. Methylphenidate use and poly-substance use among undergraduate students attending a South African university. *South African Journal of Psychiatry,* 22(1): 1-4.

Sticca, F., Machmutow, K., Stauber, A., Perren, S., Palladino, B.E., Nocentini, A., Menesini, E., Corcoran, C. & McGudin, C. 2015. The coping with cyberbullying questionnaire: Development of new measurements. *Journal of Societies,* 5: 515-536.

Stopbullying. 2021. What is Cyberbullying. Available: https://www.stopbullying.gov/cyberbullying/what-is-it#logo (Accessed 2021/11/27).

Suler, J. 2005. Contemporary media forum: The online disinhibition effect. *International Journal of Applied Psychoanalytical Studies*, 2(2): 184-188.

Taber, K.S. The use of Cronbach's alpha when developing and reporting research instruments in science education. *Research in Science Education,* 48: 1273-1296.

Taherdoost, H. 2016. Sampling methods in research methodology: How to choose a sampling technique for research. *International Journal of Academic Research in Management,* 5(2): 18-27.

The Cyberbsmile Foundation. 2020. Social media and apps. Available: https://www.cybersmile.org/advice-help/category/social-networks (Accessed 2021/11/27).

Thomas, D. & Loader, B. 2000. Introduction-cybercrime: Law enforcement, security and surveillance in the information age. In Thomas, D. & Loader, B. *Cybercrime: Law enforcement, security and surveillance in the information age*. London, United Kingdom: Routledge.

Turan, N., Polat, O., Karapirli, M., Uysal, C. & Turan, S.G. 2011. The new violence type of the era: cyber bullying among university students: violence among university students. *Neurology, Psychiatry and Brain Research*, 17(1): 21-26.

Turenne, N. 2018. The rumour spectrum. *Plos One*, 13(1): 1-27.

Ubarhande, S.D. 2011. Computer viruses. *International Journal of Scientific & Engineering*

© University of Pretoria

Research, 2(12): 1-4.

UCSD Center on Gender Equity and Health. 2019. Measuring #MeToo: A National Study on Sexual Harassment and Assault. Available: https://www.raliance.org/wp-content/uploads/2019/04/2019-MeToo-National-Sexual-Harassment-and-Assault-Report.pdf (Accessed 2021/11/10).

Underwood, M., Galen, B. & Paquette, J. 2001. Top ten challenges for understanding gender and aggression in children: why can't we all just get along? *Social Development*, 10(2): 248-266.

University of Cape Town. 2008. Policy on Sexual Misconduct: Sexual Offences and Sexual Harassment. Available: https://www.uct.ac.za/sites/default/files/image_tool/images/328/about/policies/Policy_on_Sexual_Misconduct_2021.pdf (Accessed 2021/11/09).

University of Cape Town. N.D. University of Cape Town Disciplinary Procedure for Sexual Misconduct: Sexual offences and Sexual Harassment. Available: https://www.uct.ac.za/sites/default/files/image_tool/images/328/about/policies/Disciplinary_Procedure_for_Sexual_Misconduct_2021.pdf (Accessed 2021/11/09).

University of Pretoria. 2008. Code of Conduct on the handling of sexual harassment. Available: https://www.up.ac.za/media/shared/409/code-of-conduct-on-the-handling-of-sexual-harrasment.zp85249.pdf (Accessed 2021/12/04).

University of Witwatersrand. 2017. Transformation Projects. Available: https://www.wits.ac.za/transformationoffice/programmes-and-projects/ (Accessed 2021/11/09).

Van Niekerk, S. & Coetzee, L. 2020. Secondary victimisation of child victims in the criminal justice system. *Child Abuse Research: A South African Journal*, 21(1): 20-31.

Van Teijlingen, E.R. & Hundley, V. 2002. The importance of pilot studies. *Nursing Standard,* 16(40): 33-36.

Vehovar, V., Toepoel, V. & Steinmetz, S. 2017. Non-probability Sampling. In Wolf, C., Joye,

© University of Pretoria

D., Smith, T.W. & Fu, Y.C. *The SAGE Handbook of Survey Methodology*. London: SAGE.

Vogels, E.A. 2021. Pew Research Center: Online Harassment occurs most often on social media, but strikes in other places too. Available: https://www.pewresearch.org/fact-tank/2021/02/16/online-harassment-occurs-most-often-on-social-media-but-strikes-in-other-places-too/ (Accessed 2021/11/10).

Wahyuni, D. 2012. The research design maze: understanding paradigms, cases, methods and methodologies. *Journal of Applied Management and Advanced Research,* 10(1): 69-78.

Walklate, S. 2003. *Understanding Criminology: Current theoretical debates*. 2nd ed. Buckingham: Open University Press.

Waterfield, J. 2018. Convenience Sampling. In *The SAGE Encyclopedia of Educational Research, Measurement, and Evaluation*. Thousand Oaks, CA: SAGE.

Webb, L.M. & Temple, N. 2015. Social media and gender issues. In Guzzetti, B. & Lesley, M. 2015. *Handbook of Research on the Societal Impact of Digital Media.* Hershey, Pennsylvania, United States: IGI Global.

Webster Dictionary. 2021. Definition of student. Available: http://webstersdictionary1828.com/Dictionary/student (Accessed 2021/11/24).

White, W.E. & Carmody, D. 2018. Preventing online victimisation: College students' views on intervention and prevention. *Journal of Interpersonal Violence*, 33(14): 2291-2307.

Willard, N. 2007. Educator's guide to cyberbullying, cyberthreats & sexting. Center for safe and responsible use of the internet. Available: https://cdn.ymaws.com/www.safestates.org/resource/resmgr/imported/educatorsguide.pdf (Accessed 2021/11/07).

Wilson, J.H. & Joye, S.W. 2019. Research designs and variables. In Wilson, J.H. & Joye, S.W. *Research Methods and Statistics: An Integrated Approach*. Thousand Oaks, CA: SAGE.

Wolak, J., Finkelhor, D., Mitchell, K.J. & Ybarra, M.L. 2008. Online "predators" and their victims. *American Psychological Association,* 63(2): 111-128.

© University of Pretoria

Wolf, J. 2011. Self-Administered questionnaire. In *Encyclopedia of Survey Research Methods*. Thousand Oaks, CA: SAGE.

Working to Halt Online Abuse (WHO@). 2013. Online harassment/cyberstalking statistics. Available: http://www.haltabuse.org/resources/stats/ (Accessed 2021/11/10).

Xiao, B. & Wong, R.Y.M. 2013. Cyberbullying among university students: an empirical investigation from the social cognitive perspective. *International Journal of Business and Information*, 8(1): 34-69.

Ybarra, M.L. & Mitchell, K.J. 2008. How risky are social networking sites? A comparison of places online where youth sexual solicitation and harassment occurs. *Paediatrics*, 12(2): 350-357.

Zama, Z. 2021. Understanding what the Cyber Crimes Act entails. Available: https://www.702.co.za/articles/434022/understanding-what-the-cyber-crimes-act-entails (Accessed 2022/02/04).

Zaykowski, H. & Campagna, L. 2014. Teaching theories of Victimology. *Journal of Criminal Justice Education*, 25(4): 452- 467.

Zhong, J., Zheng, Y., Huang, X., Mo, D., Gong, J., Li, M. & Huang, J. 2021. Study of the influencing factors of cyberbullying among Chinese college students incorporated with digital citizenship: From the perspective of individual students. *Frontiers in Psychology,* 12: 1-16.

© University of Pretoria

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Faculty of Humanities

Researcher: Prof F Steyn
Contact details: francois.steyn@up.ac.za, 012-420 3734

Dear Respondent

6.8.1 Title of the study

Correlates of online victimisation among undergraduate students attending a South African university

6.8.2 Purpose of the study

The purpose of the study is to determine students' experiences of online victimisation. The study sets out to describe undergraduate students' access to and use of social media and other electronic platforms through which online victimisation can occur.

6.8.3 Procedures

You are kindly requested to participate in a rapid self-administered survey among undergraduate students. The questionnaires will be handed out in class after which you are requested to answer the questions without discussing your answers with a fellow student. It should take you between five and ten minutes to answer all the questions. Please do not write your name, student number or any information that could identify you on the questionnaire.

6.8.4 Possible risks

No risks are foreseen in completing the questionnaire. However, if you experience any emotional distress while answering the questions, or you are reminded of a negative personal experience that involves online victimisation, please alert the data gatherers immediately or as soon as possible after the survey. Arrangements will be made to assist you.

6.8.5 Benefits of participation

No compensation is tied to participating in the survey. However, your participation will provide valuable information that can assist in better understanding the phenomenon of online victimisation among undergraduate students. The study will make recommendations on how to address online victimisation in student populations.

6.8.6 Rights as a participant

Your participation in the survey is voluntary. You have the right not to participate in the survey and you have the right to withdraw from the research at any time, without any negative consequences.

6.8.7 Anonymity and confidentiality

The information you share is completely anonymous since you are requested to not provide any information (name or student number) that could identify yourself. This step is needed since you are kindly requested to answer all the questions as honest and truthful as possible. After returning the completed questionnaires to the data gatherers, no one will know who completed which questionnaire.

Room 4-1.7, Level 4, Building
University of Pretoria, Private Bag X20
Hatfield 0028, South Africa
Tel +27 (0)12 420 1234
Fax +27 (0)12 420 5678
Email name.surname@up.ac.za
www.up.ac.za

Fakulteit Geesteswetenskappe
Lefapha la Bomotho

© University of Pretoria

6.8.8 Contact details

If you need more information about the study, you are more than welcome to contact the researcher at his e-mail (francois.steyn@up.ac.za) or on his office number (012-420 3734/2030).

6.8.9 Data storage

The completed questionnaires will be stored for 15 years at the Department of Social Work and Criminology, University of Pretoria, as stipulated in their policy, for archiving purposes.

6.8.10 Data usage

The results of the study will be presented in a research report and may be disseminated by means of professional publications and conferences.

6.8.11 Permission for participation in the research study

I understand the information provided above and all my questions have been addressed satisfactorily. I understand what the research is about and why it is being done. I understand my rights as a participant and give my permission to voluntarily participate in the research study.

Please indicate your consent to participate in the survey by ticking the box below.

I have read this letter and understand what is requested. I hereby consent to participate in the survey.	

© University of Pretoria

ONLINE HARASSMENT QUESTIONNAIRE

Please indicate your answers clearly with an **X**

Section 1 – Background information

1. How old are you?	years

2. Are you:	Male		Female	

3. To which population group do you belong?	Black	
	Indian/Asian	
	Coloured	
	White	

4. In what academic year are you?	1st		2nd		3rd	

5. What is the economic status of the household you grew up in?	Low income	
	Middle income	
	High income	

6. During the academic term, where do you live?	University residence	
	Family	
	Commune	
	Own apartment	

Section 2 – Internet use

7. How often do you use the internet/social media?	Daily	
	A few times a week	

8. How many hours per day do you spend on the internet?	Less than 1 hour	
	1 – 2 hours	
	2 – 3 hours	
	3 – 4 hours	
	More than 4 hours	

9. Where/how do you **mostly** access the internet?	Mobile device (phone / tablet)	
Select only one option.	Computer at home	
	University library	
	Internet café	

10. How often do you use the internet for the following activities?

	Often	**Sometimes**	**Seldom**	**Never**
Social media (e.g. Whatsapp, FB)				
Studies (e.g. assignments)				
Blogs / blogging				
Entertainment (e.g. music, gaming)				

© University of Pretoria

Section 3 – Online victimisation

Please read the statements below. If they apply to you, indicate with an X how often it happened, and then indicate whether it happened while you were enrolled at school or at university, or both.

Have you been victimised by…	Never	1 – 2 times	3 – 5 times	5 or more times		At school	At varsity		
11. Someone spreading rumours about you on the internet/social media									
12. Someone using the internet/social media as a slandering tool against you									
13. Receiving insults or harassment from a stranger									
14. Receiving insults or harassment from someone you know									
15. Someone using your identity without your permission on the internet									
16. Someone hacking your private accounts on the internet									
17. Someone repeatedly sending messages after you told them to stop contacting you									
18. Someone sending you unwanted sexual messages or images									
19. Someone sharing your personal photos/videos without your permission									
20. Someone who sent you a virus or malicious software on purpose									
21. Someone pretending to be someone they are not									

Section 4 – Response to harassment

If you have been harassed online, what did you do? (If not, please skip the questions)

	Yes	No	
22. Asked the harasser why he or she is doing it			
23. Told the harasser to stop			
24. Ignored all messages / pictures so that the harasser would lose interest			
25. Wrote mean and threatening things to the harasser			
26. Informed an authority figure (e.g. parent, teacher or police)			

Thank you for participating in the survey!

© University of Pretoria

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Faculty of Humanities
Fakulteit Geesteswetenskappe
Lefapha la Bomotho

Humanities 100
Since 1919

1 December 2021

Dear Miss SA Parsons,

Project Title:	Correlates and predictors of online victimisation among undergraduate students attending a South African university
Researcher:	Miss SA Parsons
Supervisor(s):	Prof F Steyn
Department:	Social Work and Criminology
Reference number:	17001596 (HUM010/0321 Line 2) (Amendment)
Degree:	Masters

Thank you for the application to amend the existing protocol that was previously approved by the Committee.

The revised / additional documents were reviewed and **approved** on 01 December 2021 along these guidelines, further data collection may therefore commence (where necessary).

Please note that this approval is based on the assumption that the research will be carried out along the lines laid out in the amended proposal. Should your actual research depart significantly from the proposed research, it will be necessary to apply for a new research approval and ethical clearance.

We wish you success with the project.

Sincerely,

Prof Karen Harris
Chair: Research Ethics Committee
Faculty of Humanities
UNIVERSITY OF PRETORIA
e-mail: tracey.andrew@up.ac.za

Research Ethics Committee Members: Prof KL Harris (Chair); Mr A Bizos; Dr A-M de Beer; Dr A dos Santos; Dr P Gutura; Ms KT Govinder Andrew; Dr E Johnson; Dr D Krige; Prof D Maree; Mr A Mohamed; Dr I Noomé, Dr J Okeke; Dr C Puttergill; Prof D Reyburn; Prof M Soer; Prof E Taljard; Ms D Mokalapa

© University of Pretoria