A LOOK AT VICTIM EXPERIENCES OF CYBERCRIME IN SOUTH AFRICA AND WHETHER THE CURRENT LEGISLATIVE FRAMEWORK IS EQUIPPED TO DEAL WITH THE ISSUE

Research Proposal Submitted By:

SAVANNAH TUSCANY SMIT

Student Number:

SMTSAV005

Qualification:

MASTER OF LAWS IN CRIMINOLOGY, LAW AND SOCIETY

Supervisor:

ASSOCIATE PROFESSOR KELLEY MOULT

Word Count:

25,379

Research dissertation presented for the approval of the Senate in partial fulfilment of the requirements for the Master of Laws in Criminology, Law and Society in approved courses and a minor dissertation. The other part of the requirements for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of the Master of Laws in Criminology, Law and Society dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

ACKNOWLEDGEMENTS

It has taken me some time to get here, and I would like to express my deepest gratitude to all those who have made this dissertation possible.

First, special thanks to my supervisor, Dr. Kelley Moult, for her guidance and support throughout this project. I appreciate the time and effort you have put in over the years to assist me in finalising my dissertation.

I am also sincerely grateful to my family who have been my principal support system throughout this journey. To my mother, Portia Smit, and my sisters, Imogan Da Rocha and Quiara Smit – your consistent encouragement and moral support have carried me through the past few years. Thank you for listening to my ramblings, talking me through the writer's block and helping me see things differently.

Thank you also to my grandparents, Mabel and John Smit. Their support and weekly questions about my progress encouraged me to keep pushing. I wrote even when I had nothing to say just so I could tell them I was getting there. I wish my grandmother was still here to see the final product.

I am also thankful to all those who participated in my study. Reading through your experiences was eye-opening and indicative that more needs to be done to offer support and assistance to cybervictims. I could not have completed this dissertation without your valuable input.

Thank you to, among others, the South African National Research Foundation for the financial support afforded to me during my studies. This allowed me to focus on my research without the burden of worrying about fees.

Finally, I would like to thank everyone who has reviewed my work. Your insights have been invaluable and have helped to improve my work.

Thank you all.

DEDICATION

In loving memory of my father, Jacquin Steve Smit, and my grandmother, Mabel Smit.

My mantra throughout this journey was Isaiah 41:10.

I know you are both with me every day.

ABSTRACT

Cybercrime has become extremely prevalent in society. It is an indiscriminate form of crime that permeates all levels of society. This is especially true after the COVID-19 pandemic which resulted in individuals becoming increasingly reliant on technology for everyday tasks such as working, shopping and connecting with their loved ones. Cybercriminals have taken advantage of the increased use and reliance on technology and have targeted individuals via various online platforms.

Based on data collected through an anonymous online survey, this research examines victims' experiences of cybercrime and the response to this crime, including whether participants were aware of the legal remedies available to them and how to report that they had been a victim of cybercrime. The data shows that victims are reluctant to approach the authorities to report cybercrime as they are uncertain who to report to. Those who experienced financial crime approached their bank but others, who experienced other forms of cybercrime, were afraid that they would not be taken seriously by the authorities. Furthermore, it became evident that participants were not aware that South Africa has legislation, namely the Cybercrimes Act 19 of 2020, in place to provide for the prosecution of cybercrime. Where participants were aware of the legislation, it was predominantly as a result of being informed about it at their educational institutions.

The study concludes that cybervictims have a lack of confidence in the authorities' ability to deal with cybercrimes and do not feel the current legislative framework in place in South Africa is sufficient to address the issue of cybercrime.

TABLE OF CONTENTS

1. CHAPTER 1 – INTRODUCTION

1.1 Preface

> 'Digital architectures generate an atmosphere of anonymity that protects, promotes, and nourishes new methods of attack against people and institutions.' [1]

Cybercrime is on the rise. It is a growing problem that does not discriminate among its victims. It can happen to anyone at any time provided they utilise some form of technology. The COVID-19 pandemic increased our reliance on technology, making it especially important to create awareness of the problem of cybercrime based on victims' own experiences.

Clicking on online advertisements or entering confidential information on online shopping sites can make individuals wary as they are unsure who has access to their information and whether the cybersecurity systems in place are sufficient to protect their information. This research highlights that people should be aware of risky online behaviours that may result in cybervictimisation and should also understand their rights and the remedies at their disposal.

According to the United Nations Conference on Trade and Development ("UNCTAD") website, 156 countries (80 per cent of countries worldwide) have enacted cybercrime legislation, with Europe having the highest adoption rate (91 per cent) and Africa having the lowest (72 per cent).[2] This is problematic given that "Nigeria was ranked 16th in the world for countries most affected by cybercrime" in 2020.[3] Africa is quickly becoming a hotspot for cybercrime and the lack of effective cybercrime legislation makes Africa more appealing to cybercriminals.

In one minute it is estimated that there are approximately 2 million Twitch views, about US$1,6 million is spent online, there are 2 million Tinder swipes, around 197.6 million emails transmitted, 500 hours of content uploaded onto YouTube, 5 000 TikTok downloads, 69 million WhatsApp messages are sent, 9 132 LinkedIn connections are made, 695 000 Instagram stories are posted and 28 000 Netflix subscribers are streaming content.[4] More and

---

[1] Agustina, Jose 'Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect' (2015) 9:1 *International Journal of Cyber Criminology* at 36.
[2] United Nations Conference on Trade and Development, available at https://unctad.org/page/cybercrime-legislation-worldwide, accessed on 26 February 2022.
[3] AAG 'The Latest 2023 Cyber Crime Statistics (updated March 2023)' available at https://aag-it.com/the-latest-cyber-crime-statistics/, accessed on 8 March 2023.
[4] Jenik, Claire 'Statista' available at https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet- in-one-minute/, accessed on 12 August 2021.

more people are utilising and relying on the internet every day. There is therefore a wealth of opportunity for cybercriminals.

1.2 Existing Studies on Victim Experiences of Cybercrime

In recent years, the amount of research on cybercrime and in particular victims of cybercrime has increased. However, the research appears largely to focus on cyberbullying and its effects on adolescents. In a Google search on "cybervictimisation" the first result will almost always pertain to cyberbullying. While this may be a reflection of the kinds of popular articles or materials accessed when conducting a search on cybervictimisation, it may not be a true reflection on the most common form of cybercrime plaguing the world today.

While cyber harassment is a pertinent issue, in my opinion, one of the more prevalent cybercrimes in society today is phishing which aims to elicit sensitive personal information with the goal of financial gain for the cybercriminal. As stated, there is a wealth of literature on cybercrime and almost all the articles I have read refer to phishing but do not focus solely on the issue or how victims have experienced phishing. Another cybercrime, which is often linked to phishing scams, becoming increasingly frequent is online bank/credit fraud, where cybercriminals gain access to individuals banking information and levy bogus charges to steal funds.

The role of the victim in increasing their risk factors for victimisation is also dealt with extensively in the literature pertaining to cybervictimisation. Essentially, the research considers routine activity theory and whether it is equally applicable to both virtual and physical crimes.

As stated, however, the literature predominantly deals with cyberbullying in children, adolescents and young adults. While dealing with the concepts generally, none of the research focuses on victims' experiences specifically. The research that does focus on victim experiences studies the behaviour that led to their victimisation.

1.3 Unpacking My Research Question

To fill the gaps in the literature, I am interested in victim experiences of cybercrime in South Africa and whether the current legislative framework is equipped to deal with the issue. The literature suggests that Africa is behind other countries when it comes to cybersecurity and the protection of individuals who have the misfortune of becoming victims of cybercrime. To fill

this gap, this dissertation considers the legislative framework and empirical data on South African victims' experiences of cybercrime to determine, *inter alia,* who the victims were, how they were targeted and how the cybercriminals were dealt with. In addition, I consider the role of the authorities, particularly the police, in the reporting process and subsequent investigation of cybercrimes.

My research aims to give victims the opportunity to not only provide insight into the behaviour that may have led to their victimisation but also provides them with an opportunity to elaborate on their experience during and *post*-victimisation. In addition, my research aims to provide insight into how everyday individuals seek to resolve their cybervictimisation. While it may seem that having legislation in place ensures a right of recourse and remedy, this may not be the case. The role the authorities play in victims' willingness to report their cybervictimisation and their treatment of cybercrimes is also an important determinant in how successful the legislative framework will be.

1.4 Overview of Chapters

Chapter 1 introduces the research project by referencing existing studies focusing on victims of cybercrime and expounding on the research project at hand.

Chapter 2 elaborates on the literature pertaining to cybercrime, including the policy documents and legislative framework currently in place in South Africa. Common forms of cybercrime perpetrated in South Africa are discussed and international legislation is also considered.

Chapter 3 outlines the research methodology utilised to conduct this research. The present study is summarised and the sample size, sampling plan and research site are explicated. In addition, the analytical strategy, ethical considerations, and limitations are described.

Chapter 4 presents the research findings and results.

Chapter 5 discusses participants' views on the current legislative framework and reflects on whether they felt it was sufficient to address their victimisation experience. It also provides recommendations, proposing what could be done to better 'police' cybercrime in South Africa and to allow victims to feel a sense of justice after victimisation.

Chapter 6 concludes the research project by highlighting the key contributions of the research, discussing its limitations and providing some direction for future research.

2. CHAPTER 2 – LITERATURE REVIEW

2.1. Definition of Cybercrime

There is no universal definition of "cybercrime". The National Cybersecurity Policy Framework ("NCPF") defines cybercrime as 'illegal acts, the commission of which involves the use of information and communication technologies.'[5] The 2012 Electronic Communications and Transactions Amendment Bill ("Bill"), which aimed to amend the Electronic Communications and Transactions Act 25 of 2002, provides:

> '"Cybercrime" means any criminal or other offence that is facilitated by or involves the use of electronic communications or information systems, including any device or the Internet or any one or more of them'[6]

The Bill was published for comment in 2012 but has never been enacted. Interestingly, the proposed definition was never carried through to the Cybercrimes Act 19 of 2020, nor did the Cybercrimes Act include a definition of "cybercrime". It is unclear why the proposed definition was never included in the Electronic Communications and Transactions Act or the Cybercrimes Act, given that it is sufficiently broad to cover a range of cybercrimes.

There is debate in the literature about the terms that should be used when referring to cybercrime. For example, Steinmetz uses the term "technocrime" as opposed to cybercrime arguing that this term 'acknowledges the often ephemeral, elusive, and ambiguous dimensions of high-technology crime and information security while eschewing the political connotations now attached to "cyber".'[7] According to Steinmetz, the term "cybercrime" is utilised by politicians to create panic in society and 'tends to give us the impression that our conversations concerning high-technology and crime are "closer to the natural laws that gave us computers than to the artificial laws that gave us crimes".'[8] Steinmetz's point is well taken, but it is not clear on why the term cybercrime is deficient. Introducing the novel term "technocrime" may

---

[5] The 'National Cybersecurity Policy Framework for South Africa' (published in *GG* 39475 of 4 December 2015) at 9.

[6] Electronic Communications and Transactions Amendment Bill published in Government Gazette No. 35821 dated 26 October 2012 at 4. The Bill also included definitions of "Cyber Security Hub" and "cybersecurity incident". "Cyber Security Hub" was defined as 'the public body formed in terms of section 85A' and "cybersecurity incident" was defined as 'any event identified as such in terms of the laws and their administration in the Republic, including the National Cyber Security Framework'.

[7] Steinmetz, K 'Technocrime at the Margins: Introduction to the Special Issue on Critical or Marginal Perspectives and Issues in the Study of Technocrime' (2018) 6:2 *Journal of Qualitative Criminal Justice & Criminology* 131.

[8] Ibid at 132. Steinmetz quotes Stéphane Leman-Langlois *Technocrime* (2008).

only serve to confuse individuals who are already familiar with the widely used term "cybercrime".

2.2. Cyber-Enabled versus Cyber-Dependent Crime

Cybercrime can be classified into two sub-categories: cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crimes are '(… "pure" cyber crimes) … that can only be committed using a computer, computer networks or other form of information communications technology (ICT).'[9] These offences can be seen as crimes against computers or networks and often have secondary consequences. Cyber-dependent crimes 'target or require the use of computers or digital technologies' in order to take place.[10]

Cyber-enabled crimes 'are hybrid cybercrimes, which are the outcome of the integration of traditional crimes and networked technologies.'[11] This means that crime can occur with networked technologies but the scale and access to individuals in remote locations are significantly decreased.[12]

In terms of legislation and the common law, cybercrime can be classified into three general categories: 'crimes where the computer is used as the *instrument* of crime; crimes where the computer is *incidental* to the offense, and crimes where the computer is the *target* of crime.'[13]

2.3. Approach to Cybercrime in South Africa

2.3.1. National Cybersecurity Policy Framework for South Africa

The NCPF pertains to Output 8 of the Justice, Crime Prevention and Security ("JCPS") Delivery Agreement. The JCPS Cluster, which comprises the Department of Police, Home Affairs, Justice and Correctional Services and Defence and Military Veterans, is required to develop and implement a 'Cybersecurity Policy' as well as develop the capacity to 'combat

[9] McGuire, M & Dowling, S 'Cyber crime: A review of the evidence – Chapter 1: Cyber-dependent crimes' (2013) 75 *Home Office Research Report* at 4.
[10] Cross, C, Holt, T, Powell, A & Wilson, M 'Responding to cybercrime: Results of a comparison between community members and police personnel' (2021) *Trends and Issues in Crime and Criminal Justice* 635 at 5.
[11] Akdemir, N & Lawless, CJ 'Exploring the human factor in cyber-enabled and cyber-dependent crime victimization: a lifestyle routine activities approach' (2020) 30:6 *Internet Research – Emerald Publishing Limited* 1665 at 1668.
[12] Ibid.
[13] Sarre, R, Yiu-Chung, L & Chang, L 'Responding to cybercrime: current trends' (2018) 19:6 *Police Practice and Research* 515.

and investigate cybercrime.'[14] One of the goals listed in the NCPF pertains to 'Coordination of the promotion of Cybersecurity measures by all role players (State, public, private sector, and civil society and special interest groups) … through interaction …'.[15] This interactive approach is yet to be seen amongst the various role players – either in terms of cybercrime or in terms of crime more generally. All the groups play some role in cybersecurity but there is little evidence to date of a coordinated approach. The NCPF aims to respond to various cybersecurity and online safety issues. It does not, however, appear to have done a good job of reaching those goals.

2.3.2. Electronic Communications and Transactions Act 25 of 2002

The Electronic Communications and Transactions Act 25 of 2002 ("ECTA") was the main source of domestic legislation prior to the commencement of the Cybercrimes Act 19 of 2020 ("the Cybercrimes Act"). ECTA's main objective is 'to provide for the facilitation and regulation of electronic communications and transactions'.[16] ECTA is widely regarded as the first decisive piece of legislation enacted by Parliament in the fight against cybercrime.

Much of the case law dealing with cybercrime stems from contraventions of provisions of ECTA, particularly section 86 of ECTA which pertains to, amongst others, unlawful access, interception and interference with data. The courts have had to address the issue of cybercrime and interpret the legislation, which has resulted in the publication of case law which placed the issue on a larger stage and created some awareness. Section 86 also criminalised cracking and hacking, spamming, extortion, fraud and forgery. ECTA therefore set the stage for the Cybercrimes Act and while it may be unfair to make this assumption at this early stage in the application of the Cybercrimes Act, ECTA appears to be more easily applicable to cybercrimes because of the technicality and lack of available resources to effectively implement the Cybercrimes Act.

[14] NCPF op cit note 5 at 9.
[15] NCPF op cit note 5 at 6.
[16] Cassim, F 'Addressing the challenges posed by cybercrime: A South African perspective' (2010) 5 *Journal of International Commercial Law & Technology* 118 at 119.

2.3.3. Cybercrimes Act 19 of 2020

The Cybercrimes Act was first introduced to the National Assembly on 20 February 2017.[17] After much deliberation and discussion, the Act was assented to on 26 May 2021 and on 1 December 2021, the President of the Republic of South Africa announced that, in terms of section 60 of the Cybercrimes Act, certain sections of the Cybercrimes Act would commence.[18] The Cybercrimes Act amends 11 important pieces of legislation that pertain to cyber or electronic crime.[19] These include the Electronic Communications and Transactions Act, the Criminal Procedure Act, the South African Police Services Act, the Criminal Law Amendment Act, the Criminal Law (Sexual Offences and Related Matters) Amendment Act, the National Prosecuting Authority Act, the Correctional Services Act, the Financial Intelligence Centre Act, the Regulation of Interception of Communications and Provision of Communication-Related Information Act, the Child Justice Act and the Films and Publications Act.[20]

The Cybercrimes Act makes several important changes to the law, including providing more comprehensive definitions of the various types of offences under the general banner of cybercrimes. Part I of Chapter 2 of the Cybercrimes Act lists the following cybercrimes:

> '2. Unlawful access
> 3. Unlawful interception of data
> 4. Unlawful acts in respect of software or hardware tool
> 5. Unlawful interference with data or computer program
> 6. Unlawful interference with computer data storage medium or computer system
> 7. Unlawful acquisition, possession, provision, receipt or use of password, access code or similar data or device
> 8. Cyber fraud
> 9. Cyber forgery and uttering
> 10. Cyber extortion
> 11. Aggravated offences
> 12. Theft of incorporeal property'[21]

[17] Parliamentary Monitoring Group 'Cybercrimes Bill' available at https://pmg.org.za/bill/684/, accessed on 26 March 2021.
[18] The sections that commenced from 1 December 2021 include: Chapter 1, Chapter 2 (excluding Part VI), Chapter 3, Chapter 4 (excluding sections 38(1)(d), (e), (f), 40(3) and (4), 41, 42, 43 and 44), Chapter 7, Chapter 8 (excluding section 54) and Chapter 9 (excluding sections 11B, 11C, 11D and 56A(3)(c), (d) and (e) of the Criminal Law (Sexual Offences and Related Matters) Amendment Act, in the Schedule of laws repealed or amended in terms of section 58).
[19] Mtuze, S 'The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) 43:3 *Obiter* 536 at 545.
[20] Act 25 of 2002, Act 51 of 1977, Act 68 of 1995, Act 105 of 1997, Act 32 of 2007, Act 32 of 1998, Act 111 of 1998, Act 38 of 2001, Act 70 of 2002, Act 75 of 2008, Act 65 of 1996.
[21] Part I of Chapter 2 of the Cybercrimes Act 19 of 2020.

The Cybercrimes Act codifies and criminalises new offences that are not contained in ECTA. Part I of Chapter 2 is therefore not an exhaustive list of offences which is significant given the fast-paced and ever-changing landscape of technology. Although the Cybercrimes Act seems to provide a comprehensive list of offences, it must be fluid and allow for additions and amendments as cybercrimes evolve.

Section 11 of the Cybercrimes Act also recognises certain aggravated offences relating to the unlawful access to and use of data from a 'restricted computer system'. [22]

In practical terms, while the Cybercrimes Act makes useful gains in terms of defining offences, it makes use of technical jargon that can be confusing to a layperson. This makes understanding the various forms of cybercrime and their consequences even more perplexing and overwhelming. Instead of alleviating the concerns of citizens, the technical terminology utilised by lawmakers may serve to feed the 'moral panic' surrounding cybercrimes.[23] Hill and Marion note Cohen's take on a moral panic as 'largely a reaction by the public to a perceived issue'.[24]

Section 19 of the Cybercrimes Act sets out a framework for sentencing under the Act. Depending on the type of offence committed, offenders could be sentenced to a fine or anywhere between three- and fifteen-years imprisonment. Sections 1 to 7 of the Cybercrimes Act address the unlawful and intentional access, interference with, interception of, use of, acquisition of and possession of data or computer programs. Sections 8, 9 and 10 criminalise cyber fraud, cyber forgery and uttering and cyber extortion, respectively. Section 11 deals with aggravated offences, which could attract a sentence of up to 15 years imprisonment. Despite coming into force on 1 December 2021, there is little evidence available on whether these provisions have been applied in criminal prosecutions or courts.

Part VI of Chapter 2 entitled, 'Orders to protect complainants from the harmful effect of malicious communications (ss 20 – 23)' is not yet in effect. This section may prove helpful to cybervictims as it empowers them, where they have laid a charge with the South African Police Service ("SAPS") that an offence contemplated in sections 14, 15 or 16 has been committed,

[22] In terms of section 11(1)(b), a 'restricted computer system' is defined as any data, computer program, computer data storage medium or computer system under the control of or exclusives used by a financial institution or an organ of state, including a court, and which is protected by security measures against unauthorized access or use.
[23] Hill, J & Marion, N 'The Use of Mythic Narratives in Presidential Rhetoric on Cybercrime' (2018) 6:2 *Journal of Qualitative Criminal Justice & Criminology* 170 – 204.
[24] Ibid at 185.

to apply to a magistrate's court for a protection order pending finalisation of criminal proceedings against an offender.[25]

In terms of Chapter 3, comprising section 24 of the Cybercrimes Act, South African courts have extra-territorial jurisdiction in respect of cybercrimes. In other words, South African courts have jurisdiction even in the event the offence occurred outside the Republic of South Africa ("RSA") if the offence affects any natural person, juristic entity incorporated or registered in RSA or a 'restricted computer system' within RSA as contemplated in section 11(1)(b) of the Cybercrimes Act. This could be helpful in cases where cybercriminals outside RSA commit offences against South African citizens. Despite legislative advancement, a question to be addressed is whether SAPS is sufficiently equipped and resourced to undertake cross-border investigations of this nature.

Chapter 4 of the Cybercrimes Act grants SAPS and independent investigators (defined as fit and proper persons who are not members of SAPS) extensive powers to investigate, search, access or seize any computer system, computer data storage medium, database or network. Given that SAPS is already overburdened by cases, affording private investigators the power to investigate cybercrimes will serve to relieve some of the burden placed on SAPS. They may also be better equipped and resourced to investigate cybercrimes as they would have the opportunity to undergo extensive training. It is, however, important that SAPS and private investigators work hand-in-hand in their investigation to ensure an arrest can be made and the cybercriminal prosecuted.

The law, along with policy, political rhetoric and the media all shape how cybercrime and cybercriminals are perceived. While the Cybercrimes Act may have made strides in defining cyber offences and in providing the mechanisms in law to respond to these crimes, cybercriminals are still viewed in the popular imagination as elusive as a result of the contactless crimes they perpetrate. Cybercriminals have a sense of omnipotence because they can strike anywhere at any time; they can be across the world and still target their victims. In addition, while the Cybercrimes Act has updated and strengthened the law, putting these amendments into practice often proves difficult, particularly where cybercrimes are concerned. This creates the impression that cybercriminals will not be apprehended which consequently results in cybervictims not reporting their experiences.

[25] Sections 14, 15 and 16 relate to *'Malicious communications'*. In particular, data messages that incite damage to property or violence (section 14), data messages which threaten persons with damage to property or violence (section 15) and disclosure of data messages of intimate image (section 16).

2.3.4. Case Law

A number of the recent cases deal with technical aspects of the law: the distinction between two types of electronic evidence (*Ndlovu v Minister of Correctional Services and Another*[26]); the admissibility of documentary evidence consisting of computer-generated printouts and the evidential weight of electronic evidence (*S v Ndiki and Others*[27]); the requirement of *'original form'* in terms of section 14 of ECTA (*Barclays Western Bank Ltd v Creser* [28]); and the standard of proof set by section 23 of ECTA (*Jafta v Ezemvelo KZN Wildlife*[29]).

Carolissen v Director of Public Prosecutions deals with the issue of jurisdiction with regard to cybercrime.[30] In this case, the court concluded that the accused was 'liable to be extradited to stand trial in Portland, Maine in the United States of America' for his crimes related to child pornography.[31]

In May 2019, Jabulani 'Cashflow' Ngcobo was 'found guilty of fraud by the specialised commercial crimes court in Durban…for a case that ha[d] been running since 2014.'[32] The accused and his business partner were sentenced to four years in prison 'on several counts of fraud and contravening section 7(1) of the Financial Advisory and Intermediary Services Act.'[33]

In *Msomi v S*, the accused was charged in the Specialised Commercial Court on two counts of fraud, three counts pertaining to ECTA and two counts pertaining to the Prevention of Organised Crimes Act 121 of 1998.[34] The accused committed a financial cybercrime against the Nelson Mandela Metropolitan Municipality when he utilised computer software to obtain confidential bank account information. The court correctly stated that the cybercrimes committed:

> '… have far-reaching consequences for the economy and the public, and the courts must impose sentences that reflect the serious nature of the crimes. ... there is

[26] (2006) 4 All SA 165 (W).
[27] (2008) 2 SACR 252.
[28] 1982 (2) SA 104 (T) at 106.
[29] 2008 (10) BLLR 954 (LC) at para 88.
[30] 2016 (3) All SA 56 (WCC).
[31] Ibid para 67.
[32] Boitumelo Kgobotlo '"Cashflow" Ngcobo appeals jail sentence' *Sowetan Live* 12 May 2019, available at https://www.sowetanlive.co.za/sundayworld/news/2019-05-12-cashflow-ngcobo-appeals-jail-sentence/, accessed on 02 June 2021.
[33] Ibid.
[34] [2019] ZAECGHC 80 (ECG).

> unfortunately a misguided perception that these crimes are somewhat less morally reprehensible than fraud and theft committed the "old fashioned" way …'[35]

This case shows that the court is aware of the serious and widespread effects of, amongst others, financial cybercrime. It is notable that the court emphasises cybercrimes are not 'less morally reprehensible' than traditional face-to-face crimes. This is a particularly important statement when considering that many cybervictims do not think what happened to them was serious enough to warrant reporting the crime to the authorities. Many cybervictims feel that the police would not take them seriously in the event they reported the cybercrime. The court's statement makes it clear that there should be no distinction between how traditional face-to-face crimes and cybercrimes are viewed. The court goes on to say that cybercrimes are in fact uglier than traditional crimes as they are motivated solely by greed.[36]

Fourie v Van der Spuy and De Jongh Inc. and others is a recent case pertaining to cybercrime.[37] In the opening paragraph, Acting Judge Klein in the Gauteng High Court states, 'This is a judgment on a matter pertaining to cybercrime, it is a matter of innocent people being dragged into cases where emails are hacked and payments are made to unknown hackers.'[38] In this matter, a client sued her attorneys as a result of their failure to adhere to payment instructions. The attorneys held a balance of funds in trust on behalf of their client and erroneously paid the funds over to an account controlled by hackers. This case is particularly important for practising attorneys as the attorneys were liable to pay the full balance back to their client as a result of their failure to verify their client's banking details prior to making payment.

Looking at the case law as a whole shows that the courts are serious about prosecuting cybercrimes and showing the public that cybercrimes are no different to traditional crimes. Although they have not yet dealt extensively with the Cybercrimes Act, their application of other legislation is indicative of their willingness to interpret the law and impose appropriate penalties on cybercriminals.

---

[35] Ibid at paragraph 34.
[36] Ibid.
[37] [2019] JOL 45848 (GP).
[38] Ibid at paragraph 1.

2.3.5. Reporting Cybercrime in South Africa

According to the Microsoft Security Intelligence website, there have been 340 286 malware encounters in South Africa in the 30 days between December 2022 and January 2023 – approximately 11 342 incidents per day.[39] Microsoft is likely aware of these malware encounters because of their Microsoft Defender anti-virus software. Individuals may not have reported these threats to Microsoft as the software includes a layer of defence that entails blocking and reporting any potential threats. This number provides a noteworthy estimate of the scope of the problem. Victims should be made aware, however, that there are a number of websites that allow them to describe their cybervictimisation. There are also websites that provide some guidance on formal routes available to report cybercrimes. These will be discussed in more detail below.

2.3.5.1. Cybercrime.org.za

The first result that appears in a Google search on reporting cybercrime is the website cybercrime.org.za. Clicking on the link takes you to an online reporting form that requests the complainant's full name, phone number, email address, a short description of the incident and full details about the complainant's experience, social media, bank details along with the pecuniary loss suffered by the complainant and the perpetrator's names and contact details.[40] It is unclear where this information is sent or who has access to it.

Cybercrime.org.za is part of an 'independent, non-commercial initiative developed as a result of the needs identified over the past decade for pooling resources to address the criminal exploitation of ICT in South Africa and Africa at large.'[41] While the online reporting form may seem efficient and easy to use, cybervictims may be reluctant to disclose their personal information online due to the fact that they may well have suffered a loss because of predators in cyberspace. At the top of the webpage, a red notification box reads, 'We appreciate your patience as our support team strives to provide you with timely help and advice.'[42] This may be discouraging to cybervictims as it suggests a solution to their problem will not be forthcoming. Instead, they will be provided with advice and, rather than taking immediate

[39] Microsoft Security Intelligence 'Global threat activity' available at https://www.microsoft.com/en-us/wdsi/threats, accessed on 13 January 2023.
[40] Available at https://cybercrime.org.za/reporting, accessed on 6 July 2021.
[41] Ibid.
[42] Ibid.

action against the cybercriminal, the matter will be delayed until such time as it is eventually investigated by the authorities. This is therefore not a formal reporting mechanism. It is unclear whether the victim will be directed to the authorities, whether the people running the website automatically refer the matter to the authorities or whether the victim's information will merely be utilised by the website for statistical purposes. The individuals behind the website are not authorised to investigate the cybercrime so relaying a victimisation experience in this manner may be just that, telling your story with no hopes of taking the matter any further.

2.3.5.2. Internet Service Providers' Association of South Africa

In October 2022, the Internet Service Providers' Association of South Africa ("ISPA") provided an Advisory on the reporting of cybercrime, including a 'suggested process' for reporting cybercrime.[43] The first line of this suggested process provides, 'There is no set process: the advice below is based on ISPA's consultation with senior SAPS personnel.'[44] This initial statement is problematic as it indicates the uncertainty surrounding cybercrime. There is no clarity on who to approach for help or what to do in instances of victimisation.

The reporting process suggested by ISPA places the onus on the cybervictim to prepare a 'short and as simple an affidavit' setting out why they 'believe' a crime has occurred.[45] This is problematic as it creates the impression that a crime may not have taken place and makes this seem like a subjective rather than objective fact. In other words, it suggests a reasonable third party may not believe a crime has occurred. This reinforces the notion that cybercrimes are not "real" crimes and that they will not be taken seriously by the police.

The process instructs victims to 'set out sections of the criminal law which have been breached.'[46] Again, this is problematic. It places the onus on the victim to make out their case against the cybercriminal. It is difficult for law students, who deal with legislation, to understand and interpret the complex wording so it would be even more difficult for a layperson to attempt to make sense of the legislation. It also proposes to treat cybervictims and victims

[43] Internet Service Providers' Association 'Reporting cybercrimes' (2022) available at https://ispa.org.za/wp-content/uploads/2022/10/ISPA-Advisory-Reporting-Cybercrimes-Updated-October-2022.pdf, accessed on 12 December 2022.
[44] Ibid.
[45] Ibid.
[46] Ibid.

of traditional crime differently given that victims of other crimes are not required to research and cite legislation that has been breached by their offender.

The suggested process document tells victims who are lodging the affidavit at the local police station to 'Be patient and polite at all times. Due to their workload and priorities the desk officer may not want to receive your complaint …'.[47] Desk officers should never be entitled to turn a potential victim away because they were impatient or impolite. Their priority should be assisting those who come to report a crime and making them feel safe and assured that the incident will be dealt with. While officers may have substantial caseloads and be stretched thin in terms of capacity, this does not justify telling a victim that they '… will need to accept that it is up to [them] to follow-up and create pressure for the matter to be handled professionally…'.[48] All matters reported to the authorities should be handled as professionally and efficiently as possible. The entire suggested process seems prejudicial and suggests there may be instances where cases of cybercrime may not warrant being investigated by SAPS and prosecuted by the authorities. When reporting a crime, you place your trust in SAPS and believe they will do what is required to obtain justice. ISPA's interpretation and suggested process serves to create more stress for the victim and alludes to the fact that the victim will have to relive their traumatic victimisation experience in order to obtain professional assistance from SAPS.

In addition, the suggested process does not appear to have evolved significantly since 2013, when the first advisory was generated and published, despite the significant increase in the occurrence of cybercrime.

2.3.5.3. Crimeweb.co.za

Crimeweb.co.za is a website that publishes a database of email addresses, telephone numbers, fax numbers, websites and product names that have been linked to fraudulent activity.[49] This site appears to provide individuals who suspect cyber fraud on a specific platform to take matters into their own hands and publicise the names and details of individuals or entities who seem suspicious or may have attempted to defraud them. While this site may not provide cybervictims with a remedy or justice, it empowers them to publicise the cybercriminals details

[47] Ibid.
[48] Ibid.
[49] Available at http://crimeweb.co.za, accessed on 9 July 2021.

and feel as though they have made a difference by preventing some future unsuspecting individual from going through the same experience. This is evidently not a formal reporting mechanism. Other than publicising the names and details of suspected cybercriminals, no criminal sanctions will be imposed on the offenders. They will not be apprehended by the authorities or prosecuted for any crimes they may have committed.

This method of publication will likely pose risks for the cybervictim as they may be liable for defamation. In the event a cybervictim publishes any statement relating to another person that is wrongful and causes injury or demeans their character or reputation, that person may have a right of recourse against the cybervictim. This will only make matters worse for the victim. It is therefore important that victims use designated formal reporting mechanisms to avoid committing an offence themselves.

2.3.5.4. Cybercrimes Act

Section 54 of the Cybercrimes Act, which is not yet in force, imposes an obligation on electronic communication service providers and financial institutions to report an offence in the event it becomes aware that its '… electronic communications service or electronic communications network is involved in the commission of any category or class of offences …'.[50] Should the electronic communication service provider or financial institution fail to report the offence within 72 hours after having become aware of the offence, they shall similarly be guilty of an offence and 'liable on conviction to a fine not exceeding R50 000.'[51] The Cybercrimes Act does not, however, impose an obligation on any other individual or entity to report incidents of cybercrime. They are accordingly left with the discretion to report their cybervictimisation or not. It is likely that the reporting of cybercrime is monitored but it is unclear whether it is monitored by government or private cybersecurity companies.

2.3.5.5. Factors Affecting Reporting of Cybercrimes

Du Toit, Hadebe and Mphatheni refer to a study conducted in 2011 which indicates that cybervictims' failure to report cybercrime 'might be caused by the belief that there is little

[50] Section 54 of the Cybercrimes Act 19 of 2020.
[51] Section 54(3) of the Cybercrimes Act 19 of 2020.

chance of successful prosecution.'[52] There is clear evidence of a lack of trust in authorities' ability to investigate and prosecute cybercrime, which goes back more than a decade. Despite this lack of trust, it seems government has done very little to ensure authorities – in particular, SAPS – are adequately trained and resourced. [53]

Australia has established the Australian Cybercrime Online Reporting Network (ACORN), which is 'a nationally coordinated portal that allows the public to report cybercrime which is triaged to each of the state policing jurisdictions'.[54] Research indicates there is 'a clear imbalance between the growing number of reports since ACORN was introduced and the current number of staff.'[55] More funds should be expended to afford ACORN, and similar networks, the resources they require to ensure their employees have job satisfaction and that their workload is reduced. A South African equivalent of ACORN could be a useful tool. Establishing a team of first responders for cybercrime could help the police in their investigation and it may encourage cybervictims to report, given that there will be a designated office or institution to report to where cybervictimisation is taken seriously. It is important to ensure, however, that the designated team of first responders are not burdened by 'providing a de facto service role to other specialist units seeking advice on various aspects of cyber-crime.'[56] Their responsibility should be to first and foremost provide cybervictims with the guidance and services they require.

2.3.6. Prevention and Apprehension

The prevention and apprehension of cybercriminals has proved difficult, particularly in South Africa. Drafting legislation by drawing from countries with already established cyberlaws is the easy part, actually implementing and prosecuting those offences is the complex part that appears to remain elusive to the authorities. Victims may report their cybervictimisation experience, but authorities are simply not equipped to deal with the issue. In other cases,

---

[52] Du Toit, R, Hadebe, P & Mphatheni, M 'Public perceptions of cybersecurity: A South African context' (2018) 31:3 *Acta Criminologica: Southern African Journal of Criminology* 111 at 126. Also see Leukfeldt, E.R, van de Weijer, S.G.A & Van Der Zee, S 'Reporting cybercrime victimization: determinants, motives, and previous experiences' (2020) 43:1 *Policing: An International Journal of Police Strategies & Management.*
[53] Dlamini, S & Mbambo, C 'Understanding policing of cyber-crime in South Africa: The phenomena, challenges and effective responses' (2019) 5 *Cogent Social Sciences*, available at: https://doi.org/10.1080/23311886.2019.1675404, accessed on 31 March 2023.
[54] Ibid at 523.
[55] Harkin, D, Whelan, C & Chang, L 'The challenges facing specialist police cyber-crime units: an empirical analysis' (2018) 19:6 *Police Practice and Research* 519 at 524.
[56] Ibid at 524.

victims do not even report the cybercrime because they are not confident in the authorities' ability to deal with it and feel that they can handle the matter themselves. Research shows that financial crimes are often reported to financial institutions but the more personal cybercrimes such as cyber harassment or catfishing – which could lead to a financial crime – are not.[57]

As discussed above, only certain sections of the Cybercrimes Act commenced on 1 December 2021, which curtails the prosecution of certain cybercrimes and limits the remedies available, for example obtaining a protection order against someone transmitting malicious messages. Whether South Africa in fact has the tools and infrastructure to detect, investigate and prosecute these crimes remains to be seen. Section 55 of the Cybercrimes Act deals with the capacity to detect, prevent and investigate cybercrimes.[58] In terms of this section, 'The Cabinet member responsible for policing must … establish and maintain sufficient human and operational capacity to detect, prevent and investigate cybercrimes' and 'ensure that members of the South African Police Service receive basic training' in relation to the aforegoing.[59] Despite section 55 coming into force on 1 December 2021, this has evidently not occurred. While reference is made to the 'police cybercrime unit' online, no specific contact details are provided and there is also no detail regarding the composition of this unit.[60] Certain South African case law refers to the 'Cyber Crime and Deep Web Investigations Unit', but it is unclear what exactly the procedure is to report a cybercrime to this Unit. [61]

The National Prosecuting Authority ("NPA") has established a Specialised Commercial Crime Unit. The purpose of the Specialised Commercial Crime Unit is 'to investigate and prosecute commercial crimes and organized commercial crimes.'[62] This included participation in a joint project of the European Union and the Council of Europe known as Global Action on Cybercrime ("GLACY") which was 'aimed at supporting countries worldwide in the implementation of the Budapest Convention.'[63] The project commenced on 1 November 2013

[57] Wall, D 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' (2007) 8:2 *Police Practice and Research* 183 at 194.
[58] Section 55 of the Cybercrimes Act 19 of 2020.
[59] Sections 55(1)(a) and (b) of the Cybercrimes Act 19 of 2020.
[60] Office of the Provincial Commissioner Western Cape 'Media Statement' 19 February 2022, available at https://www.saps.gov.za/newsroom/msspeechdetail.php?nid=38210, accessed on 8 December 2022.
[61] S v Ebrahim [2020] JOL 49106 (KZD). The 'Cyber Crime Investigation and Deep Dark Web unit' is also referred to in the case of S v Mosia [2020] JOL 47966 (FB) at paragraph 49. It is important to note that Lieutenant Colonel Maria Susana Jacoba Beetge of the Cyber Crime Investigation and Deep Dark Web unit of SAPS analysed cell phone numbers in the case of S v Mosia and that this case pertained to a charge of murder. It was not a case relating to a cybercrime.
[62] National Prosecuting Authority of South Africa 'Specialised Commercial Crime Unit' available at https://www.npa.gov.za/specialised-commercial-crime-unit, accessed on 13 December 2022.
[63] Council of Europe Portal 'Global Action on Cybercrime' available at https://www.coe.int/en/web/cybercrime/glacy, accessed on 13 December 2022.

and ended on 31 October 2016.[64] The NPA defines 'commercial crimes' as 'bank fraud … more complex tax schemes to intricate cybercrimes that span the globe.'[65] The fact that the Unit is referred to as the 'Specialised Commercial Crime Unit' makes it seem as though they only deal with commercial or financial crimes. This could be misleading to potential victims seeking assistance for reporting purposes.

The academic and policy literature provides three crime prevention strategies that may be adapted to cybercrime, namely primary prevention, secondary prevention and tertiary prevention.[66] Primary prevention aims to prevent cybercrime from occurring at all with a focus on creating cyber awareness and educating individuals as to the dangers of internet use.[67] Secondary prevention refers to any measures to intervene among individuals who may be at high risk of cybervictimisation. Agustina suggests designing 'concrete policies for correcting prevention deficits in *concrete risk groups* … as much for offenders as for potential victims.'[68] Tertiary prevention deals with actual cybervictims and cybercriminals after an offence has occurred to attempt to avoid and prevent future offences.

In addition, there are also situational prevention techniques that may be employed. 'Situational crime prevention (SCP) focuses on the ways in which crime can be prevented and opportunities for crime can be reduced …'.[69] These kinds of initiatives essentially attempt to prevent cybercriminals from offending by putting measures such as firewalls and malware detection systems in place.[70]

2.3.7. Common Forms of Cybercrime Experienced in South Africa

2.3.7.1. Phishing

Phishing has been defined as 'an internet scam technique' utilised to obtain confidential

[64] Ibid. The primary objective of GLACY is to 'enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime.'
[65] National Prosecuting Authority of South Africa op cit note 62.
[66] Tonry, M & Farrington, D. P 'Strategic Approaches to Crime Prevention' (1995) 19 *Crime & Justice* at 1.
[67] Agustina op cit note 1 at 45.
[68] Ibid.
[69] United Nations Office on Drugs and Crime, 'Situational Crime Prevention' available at https://www.unodc.org/e4j/en/cybercrime/module-9/key-issues/situational-crime-prevention.html, accessed on 18 March 2022.
[70] Ibid.

personal information and is generally considered the initial stage of identity theft.[71] In 2020, the United States Internet Crime Complaint Centre received 241 342 reports of phishing and similar cybercrimes – the most commonly reported cybercrime that year.[72] Studies have shown that legitimate online activities, such as shopping, banking and social networking increase the likelihood of becoming a victim of phishing.[73] There is also an increased chance of becoming a victim of phishing when posting personal information online.[74]

2.3.7.2. Malware

Malware is essentially programs that are designed to damage computers and other electronic devices. It includes programs such as computer viruses, worms, trojan horses and rootkits designed to harm computers.[75] Malware can get onto computers by means of opening malicious email attachments or downloading infected files.

2.3.7.3. Financial Cybercrime

The South African Banking Risk Information Centre's ("SABRIC") mission is 'to contribute to the effectiveness of the partnerships between its members and stakeholders for the benefit of the banking industry' by 'combating banking crime, combating financial crime'.[76] Cybercriminals utilise various methods to obtain confidential personal and banking information which they use to commit some form of identity theft or financial cybercrime. Europol defines financial crime as 'illegal acts committed by an individual or a group of individuals to obtain a financial or professional advantage. The principal motive in such crime is economic gain.'[77]

---

[71] Ezeji, C, Olutola, A & Bello, P 'Cyber-related crime in South Africa: extent and perspectives of state's roleplayers' (2018) 31:3 *Acta Criminologica: Southern African Journal of Criminology* 93 at 96.
[72] Johnson, J 'Most commonly reported types of cyber crime 2020' 18 March 2021 available at https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime/, accessed on 6 April 2021.
[73] Ibid at 1669.
[74] Ibid.
[75] Available at https://cybercrime.org.za/malware/, accessed on 20 January 2023.
[76] South African Banking Risk Information Centre 'Who We Are' available at https://www.sabric.co.za/who-we-are/, accessed on 21 January 2023.
[77] Definition of 'economic crime' available: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime, accessed on 22 January 2023.

2.3.7.4. Cybercrimes Against Children

Children are particularly vulnerable to becoming victims of crime. They are often targeted as they are naïve and too trusting. This is especially true in the arena of cybercrime. Children can easily be lured onto sites portraying toys or games for free online use. Often, they are unsupervised and end up clicking on links that may contain viruses or malware that infect mobile devices such as cell phones and laptops.

In South Africa, there appears to be a wealth of "cyber wellness" literature and campaigns which aim to create awareness and educate individuals, particularly children and their parents, about the pitfalls of cyberspace. This initiative is worthwhile as it seeks to inform individuals about the risks and their vulnerabilities in cyberspace.

Many children have access to cell phones, which often have access to the internet. Cell phones are also at risk of being a site where cybercrime could take place, not just for cyberbullying and phishing, but also for malware attacks. Often, individuals do not think it necessary to have anti-virus software installed on their cell phones. McGuire and Dowling point out that the type of cell phone utilised is an important determinant for whether or not anti-virus software is required to guard against malware attacks.[78] They state:

> '… iPhones are protected from malware through Apple's approval process for code to be included in the App Store (which is the only route for installing software on the phone unless it has been jailbroken). This closed approach limits the potential for malware code to get onto the devices. Android platforms, however, require users to download AV to obtain such protection.'[79]

It is therefore important to educate children on the potential threats they may face when using a cell phone, particularly one that is connected to the internet. It is also important to encourage individuals to install some form of anti-virus software on their cell phone and other devices to mitigate the risk of cybervictimisation.

[78] McGuire & Dowling op cit note 9 at 19.
[79] Ibid at 20.

2.3.7.5. Cyber Harassment

Cyber harassment, in particular 'revenge porn', is fast becoming one of the most common forms of cybercrime experienced globally.[80] Cyber harassment occurs when individuals utilise electronic technology to harass other individuals repeatedly, verbally or psychologically. A simple example of when this occurs is when people leave mean-spirited comments directed at another person on social media. It also often involves rumours transmitted via electronic means such as email, WhatsApp or direct messaging on social media platforms. It may also involve the distribution of intimate or embarrassing images online.[81]

2.3.7.6. Ransomware Attacks

On 6 September 2021, the South African Department of Justice and Constitutional Development fell prey to a ransomware attack on its systems.[82] The ransomware attack resulted in critical systems, including email, bail services, payment of child maintenance, electronic correspondence with magistrates and judges, recording and transcription of court proceeding, being offline for a period of approximately four weeks.[83] This created havoc with court personnel being unable to communicate via email or access important information stored on their computer systems. The Director-General of the Department of Justice acknowledged that 'at least 1,200 files may have been compromised' in the ransomware attack.'[84] It is alleged that the cybercriminals demanded 50 Bitcoin, which amounted to R33 million at the time of the attack.[85] This illustrates that cybercrime can occur at the highest and, what should be, the most secure level of government. A Department that deals with critical work of a highly confidential nature was targeted and essentially left to scramble to regain control of its computer systems.

---

[80] Berasategui, Guillermo 'Cybercrime: Which ones are the most common threats today?' available at https://www.redpoints.com/blog/cybercrime/, accessed on 6 February 2022.
[81] Ibid.
[82] Illidge, Myles 'South African justice department clueless about hacked data' 12 January 2022, available at https://mybroadband.co.za/news/security/429804-south-african-justice-department-clueless-about-hacked-data.html, accessed on 16 February 2022.
[83] Ibid.
[84] Ibid.
[85] Ibid.

2.3.7.7. Data Breaches and Leaks

N4ughtySecTU, a Brazilian group of hackers, infiltrated a TransUnion fileserver by 'guessing usernames and passwords until they found an account whose password was "password".'[86] The group leaked confidential personal information from a Cell C database and a database containing the personal information of ANC members, including President Cyril Ramaphosa and his wife's identity numbers. The group demanded $15 million, (approximately R222 million) in cryptocurrency to stop them from leaking further data such as the personal data of President Cyril Ramaphosa and other prominent political figures, judges, prosecutors, police officials, attorneys and advocates.[87]

2.3.7.8. Money Laundering and Identity Theft

Seven men were accused of being part of an international group of internet scammers known as 'Black Axe' and were charged with conspiracy to commit wire fraud, money laundering, and aggravated identity theft.[88] A hearing at the Cape Town Magistrates Court for their extradition to the United States was remanded to 30 March 2022. While Black Axe is allegedly headquartered in Nigeria, as a result of transferring money 'across an interstate wire that travelled through New Jersey', the FBI is attempting to extradite the accused to the United States in order that they may be indicted by United States Courts.[89]

2.4. International Approaches to Cybercrime

The Council of Europe's Convention on Cybercrime, also known as the 'Budapest Convention', seeks to harmonise national laws, improve cybercrime investigation techniques, improve international co-operation and provide guidance to signatories on the measures

[86] Vermeulen, Jan 'TransUnion hackers leak Cell C and ANC member databases' 23 March 2022, available at https://mybroadband.co.za/news/security/438560-transunion-hackers-leak-cell-c-and-anc-member-databases.html?utm_source=dlvr.it&utm_medium=twitter, accessed on 25 March 2022.
[87] Ibid.
[88] Bradley Prior 'These are South Africa's top scammers – according to the FBI' 7 March 2022, available at https://mybroadband.co.za/news/security/436352-these-are-south-africas-top-scammers-according-to-the-fbi.html?utm_source=dlvr.it&utm_medium=twitter, accessed on 25 March 2022.
[89] Ibid.

required at national level to deal with the ever-growing issue of cybercrime.[90] In December 2019, the United Nations adopted a resolution to commence the process to draft 'a global comprehensive cybercrime treaty.'[91] This initiative advanced despite 93 states, which included many states that are party to the Budapest Convention, voting against or abstaining from the resolution. Many states appear reluctant to assent to the proposed treaty because of the apparent attempt to restrict individuals' use of the internet together with increased online surveillance.[92] There is a wealth of literature on the fine line between privacy and cybersecurity.[93] The more governments attempt to monitor what is done online, the more they curtail their citizens right to privacy. According to Deborah Brown, a senior researcher and advocate on technology and human rights at Human Rights Watch:

> 'A binding international treaty has the potential to expand government regulation of online content and reshape law enforcement access to data in a way that could criminalize free expression and undermine privacy.'[94]

Brown further suggests that individuals should be protected from criminal activity carried out via the internet by their government, but that protection should not come at the expense of their rights.[95] One should not have to give up their right to privacy or free speech due to governments policing cybercrime. The provisions of the proposed treaty pose a risk of eroding human rights as many of the states pushing for ratification utilise cybercrime as a ploy to clamp down on other rights.[96]

As of 18 June 2020, South Africa had not signed the African Union Convention on Cybersecurity and Personal Data Protection of 2014.[97] Out of the 55 countries that are members of the African Union, fourteen signed the Convention and eight ratified the Convention.

---

[90] Council of Europe's Convention on Cybercrime (Budapest Convention), available at https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html, accessed on 23 May 2021.
[91] Brown, D 'Cybercrime is Dangerous, But a New UN Treaty Could be Worse for Rights' 13 August 2021, available at https://www.justsecurity.org/77756/cybercrime-is-dangerous-but-a-new-un-treaty-could-be-worse-for-rights/, accessed on 29 December 2022.
[92] Ibid.
[93] See for example: Hagen, J & Lysne, O 'Protecting the digitized society – the challenge of balancing surveillance and privacy' (2016) 1:1 *The Cyber Defense Review* 75; Tosoni, L 'Rethinking Privacy in the Council of Europe's Convention on Cybercrime (2018) 34:6 *Computer Law & Security Review* 1197; Valls-Prieto, J 'Fighting Cybercrime and Protecting Privacy: DDoS, Spy Software, and Online Attacks' in Maria Manuela Cruz-Cunha & Irene Maria Portela (eds) *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (2015) 146.
[94] Ibid.
[95] Ibid.
[96] Ibid.
[97] African Union List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cybersecurity and Personal Data Protection, available at https://au.int/sites/default/files/treaties/29560-sl-

The Southern African Development Community Model Law on Computer Crime and Cybercrime of 2012 (the "SADC Model Law") is another tool implemented to provide guidance on the regulation of cybercrime. While the aim of the SADC Model Law is to harmonise cyberlaws across Southern Africa, there may be disadvantages in attempting to create a form of "blanket regulations" when there are varying levels of technological advancement and different political climates in the SADC member states.[98] Each country or state is at its own level of technological advancement and uses different definitions of cybercrime. This makes it difficult to take a "one size fits all" approach, particularly in the African context.

2.5. Effect of COVID-19 Pandemic on the Perpetration of Cybercrime

Cybercrime has always been a looming threat and with the advances in technology, has become more and more prevalent.[99] In March 2020, a National State of Disaster was declared by the President of South Africa as a result of the COVID-19 pandemic. The country went into lockdown and there were major restrictions on, amongst other things, the freedom to move around and interact in public. The world shifted into even more of an "online culture" with people working from home and conducting their day-to-day tasks and work on their personal computers. Because of this increased reliance on technology, South Africa saw a rise in cybercrime and in particular, COVID-related scams. Naidoo states, 'In addition to 18 million daily malware and phishing emails related to COVID-19 in just one week in April, Google's blog reported more than 240 million COVID-related spam messages daily'.[100] This indicates that cybercriminals used the increased reliance on technology to their advantage and attempted to target more individuals, but this time utilised the pandemic, which already instilled fear and uncertainty in individuals. While trying to keep safe during the pandemic, individuals were required to think twice before clicking on a link to purchase face masks or sanitiser online. Cybercriminals took advantage of a time when people were anxious and were predominantly

AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf, accessed on 23 May 2021.

[98] Hove, K 'The SADC Model Law on Computer Crime and Cybercrime: A Harmonised Assault on the Right to Privacy?' 18 July 2017 available at https://www.linkedin.com/pulse/sadc-model-law-computer-crime-cybercrime-harmonised-assault-kuda-hove, accessed on 27 September 2021.

[99] Interestingly, the first cyberattack occurred in France in 1834 – before the internet was even invented – when offenders stole financial market information. See: Arctic Wolf 'A Brief History of Cybercrime' 16 November 2022 available at: https://arcticwolf.com/resources/blog/decade-of-cybercrime/, accessed on 1 April 2023.

[100] Naidoo, Rennie 'A multi-level influence model of COVID-19 themed cybercrime' (2020) 29:3 *European Journal of Information Systems* 306 at 307.

relegated to shopping online. In addition, cybercriminals took advantage of individuals need to obtain information pertaining to the COVID-19 pandemic by launching 'several spam phishing email "saturation" campaigns online'.[101]

The use of home-based networks to remotely access secure networks heightened the risk of phishing scams, denial of service (DDoS) attacks, fake news and applications designed to steal sensitive information from unsuspecting individuals and entities.[102] There was a marked increase, approximately 238 per cent, in cybercrime and threats against financial institutions during February and April 2020, which was the height of the COVID-19 pandemic globally.[103] Throughout the pandemic, the most at risk organisations and institutions included hospitals, governments and businesses because of their increased reliance on technology and remotely accessing secure servers utilising vulnerable home networks.

During the pandemic, cybercriminals targeted a South African commercial bank and demanded a ransomware. In excess of seven million customers' information was leaked by the hackers and the bank itself suffered financially. Furthermore, a South African credit bureau's server was targeted by hackers. More than 24 million consumers' information was exposed and data pertaining to approximately 800 000 businesses was provided to the hackers. Both these financial institutions remained silent as to the severity of the breaches. The main issue, however, is that the financial institutions could not be held liable for the breaches as South African cyberlaw remains 'fragmented and incoherent'.[104]

Cybercriminals therefore exploited an already fragile system and framework by finding new ways to target individuals during the pandemic. People were forced to rely on technology more and cybercriminals took advantage of this. One positive is that people became more aware of potential cyberthreats. People had to learn to be more vigilant and guard their data to decrease their likelihood of becoming targets.

---

[101] Minnaar, Anthony & Herbig, Friedo 'Cyberattacks and the cybercrime threat of ransomware to hospital and healthcare services during the COVID-19 pandemic' (2021) 34:3 *Acta Criminologica: African Journal of Criminology & Victimology* 155 at 156.
[102] Chigada, J & Madzinga, R 'Cyberattacks and threats during COVID-19: A systematic literature review' (2021) 23:1 *South African Journal of Information Management* at 3.
[103] Ibid at 4.
[104] Ibid at 7.

2.6. "Public Policing" and Cybercrime

Another interesting aspect in this digital age is whether civilians play a role in the apprehension of cybercriminals. As a result of the authorities' inability to effectively police cybercrime, civilians have taken it upon themselves to become 'cyber-vigilantes'.[105] There are various online support groups for victims of cybercrime and also online groups that post details of potential scams and fake websites. This seeks to inform potential victims and prevent cybercrime from occurring. In considering the importance and value of these cyber-vigilantes, Huey et al correctly state that 'much of the evidence suggests that they are, as the culture of policing itself seems to dictate the necessity of security networks online.'[106] Cyber-vigilantes have attempted to fill a gap left by traditional police.

One of the major complaints surrounding the policing of cybercrime is a lack of resources. Permitting these cyber-vigilantes to "pick up the slack" and assist in identifying risk factors or fraudulent sites can be helpful. They can assist potential cybervictims by warning them about possible criminal activity online and may be able to assist the police in their investigation by gathering evidence and making links based on the evidence gathered. Once this crucial investigation aspect is attended to by the cyber-vigilantes, the police could attend to the physical aspect of policing cybercrime such as seizure of evidence and making arrests. Research conducted by Huey et al, using Lexis-Nexis and Canadian news databases, has identified three main types of groups, categorised based on the nature of their activity. These groups are:

> '1. "vigilantes", where retributive actions (hacking, harassment and so on) are carried out by members independently of any association with law enforcement;
> 3. "civilian police" who collect and relay information on actual or potential online crimes to law enforcement; and
> 4. "hybrid" organizations that do both.'[107]

While the investigations conducted by these groups have an element of danger attached, vigilantism is particularly dangerous as vigilantes take it upon themselves to not only police cybercrime but also to impose punishment. The fact that law enforcement is not involved may mean that vigilantes are more likely to engage in illegal activities which could make any evidence gathered inadmissible. While the retributive responses that vigilantes offer may be

[105] Huey, L, Nhan, J & Broll, R '"Uppity civilians" and "cyber-vigilantes": The role of the general public in policing cybercrime' (2012) 13:1 *Criminology & Criminal Justice* 81 at 85.
[106] Ibid at 84.
[107] Ibid at 85.

appealing to cybervictims as a means to punish their offender, it could be perilous for the vigilantes and the rule of law. Vigilantism also circumvents the traditional legal frameworks and systems in place which makes it difficult to test the efficacy of these systems. In other words, vigilantes do not abide by the legislation in place to combat cybercrimes and likely effect what they believe to be justice. This makes it difficult to determine whether the legislation and policy in place would have a positive effect on combatting cybercrime. What appears to play a large role in individuals electing to join 'civilian police' groups is what they see on television. Individuals appear to be motivated to join these groups as a result of 'concern over the possibility of victimization of their own children' or 'victimization experienced by relatives or friends'.[108] Being a member of the 'civilian police' is likely not without challenges as they often use a process known as 'scambaiting' to entrap cybercriminals.[109] Members of the 'civilian police' essentially pretend to be potential victims or easy targets for cybercriminals but utilise the information gathered to determine the cybercriminals IP address and possible location. All the information gathered is then provided to the authorities for further investigation. The trick is to remember why you are entrapping the cybercriminal and to remember not to get sucked into their deception. This can be particularly tricky for victims of cybercrime as it could serve to trigger previous trauma. While these groups are not always sanctioned by the authorities, they may assist in breaching a gap and supplementing the existing limited resources available to the authorities.

Situational crime prevention strategies could also be utilised to 'prevent and control the proliferation of cybercrimes.'[110] There are five general situational crime prevention strategies that are utilised to reduce crime, namely '"Increase the Effort, "Increase the Risks," "Reduce the Rewards," "Reduce Provocations" and "Remove Excuses".'[111] Each of the five general strategies include five techniques.[112] It is, however, important to bear in mind that not all the techniques will be directly applicable to cybercrimes.

---

[108] Ibid at 88.
[109] Button, M & Whittaker, J 'Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation' (2022) 66 *International Journal of Law, Crime and Justice* at 4.
[110] Ho, H, Ko, R & Mazerolle, L 'Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review' (2022) 115 *Computers & Security* at 2.
[111] Ibid.
[112] Ibid at 10 to 12. Ho et al elaborate on the various techniques. '"Increase the Effort" comprises "#1 Harden target," "#2 Control access to facilities," "#3 Screen exits," "#4 Deflect offenders" and "#5 Control tools/weapons".' '"Increase the Risks" comprises "#6 Extend Guardianship", "#7 Assist natural surveillance", "#8 Reduce anonymity", "#9 Utilize place managers" and "#10 Strengthen formal surveillance".' '"Reduce the Rewards", consists of "#11 Conceal targets", "#12 Remove targets", "#13 Identify property", "#14 Disrupt markets" and "#15 Deny benefits".' '"Reduce Provocation", is made up of "#16 Reduce frustrations and stress", "#17 Avoid disputes", "#18 Reduce emotional arousal", "#19 Neutralize peer pressure" and "#20 Discourage

2.7. Cybercrime and Routine Activity Theory

> '… cyberspace comprises a new, de-territorialized, dematerialized, and disembodied environment that is in crucial ways discontinuous with the terrestrial world.'[113]

Routine Activity Theory ("RAT") examines crime from an offender's perspective. In terms of RAT, a crime will only be committed if a potential offender believes a target is suitable and a capable guardian is absent. Whether or not the crime takes place is based on the offender's perspective of the situation. Felson and Cohen postulate that changes in individuals' daily routines since the advent of the internet has provided increased opportunities for cybercriminals which could affect the trends observed in various forms of crime. This is applicable to the types of crime that occurred during the COVID-19 pandemic. While violent crimes still occurred – the prevalence of cybercrime increased exponentially as people became more reliant on the internet and technology.[114]

Leukfeldt and Yar confirm that a number of studies utilise RAT to consider and analyse cybercrimes. However, the studies have made it clear that there are various limitations which make it challenging to ascertain whether RAT is in fact a suitable tool to examine cybercrimes.[115] RAT is typically applied to crimes that occur in the "physical" world, not the "virtual" world. There is therefore much debate on whether the same principles apply when the crime occurs online. The elements of RAT make it easily applicable to cybercrimes as the key considerations are whether an offender is motivated by the suitability of a target and the absence of a capable guardian. In the virtual world, there is a plethora of motivated offenders, waiting to take advantage of vulnerable, unsuspecting targets. There are also capable guardians, albeit intangible guardians in some respects. Capable guardians in the virtual world may include 'network administrators, forum moderators … firewalls … anti-virus and anti-intrusion software, and ID authentication and access management systems.'[116] Cybercrime has resulted in theories of criminology evolving as proximity between offenders and targets is not an

imitation".' '"Remove Excuses" comprises "#21 Set rules", "#22 Post instructions", "#23 Alert conscience", "#24 Assist compliance" and "#25 Control drugs and alcohol".'

[113] Leukfeldt, E.R. & Yar, M 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis' (2016) 37:3 *Deviant Behavior* 263 at 264.

[114] Minnaar & Herbig op cit note 101.

[115] Leukfeldt & Yar op cit note 113 at 268.

[116] Ibid at 265.

issue.[117] Cybercrime can occur when offenders and targets are thousands of kilometres apart but the effect on the target, who ultimately becomes the victim, is no less detrimental.

In terms of RAT, crime rates may also be explained by the supply of suitable targets and capable guardians.[118] As a result of working remotely and attending online meetings or classes during COVID-19, individuals spent a lot more time on their cell phones or laptops – which are the primary medium for the perpetration of cybercrime. Consequently, cybercriminals had a spike in vulnerable targets. Knowing that individuals would likely be conducting research on topics related to COVID-19 helped cybercriminals' predating behaviour as they tailored scams and schemes to the pandemic's daily requirements (like masks), which resulted in a higher victim pay-off.

A victim's daily activities in cyberspace, as opposed to the 'physical realm', has a greater influence on the likelihood of victimisation. In other words, the websites and applications utilised by an individual affects how at risk they are for victimisation.[119] Agustina argues that it is more likely an individual will be victimised if they utilise sites on the dark web or sites that have many pop-up advertisements. Studies have shown that individuals who engage in risky online behaviours and activities are significantly more likely to be at risk of online victimisation.[120] These behaviours include utilising free online movie streaming sites, clicking on pop-up messages or advertisements and downloading free music online. It is, however, important to note that merely spending more time on a computer or online does not mean individuals are at an increased risk of victimisation.[121] What does impact victimisation risks are, among other factors, the sites utilised by individuals and the amount of time spent on those sites.[122]

2.8. The General Theory of Crime and General Strain Theory

The General Theory of Crime developed by Gottfredson and Hirschi defined crime as 'acts of force or fraud undertaken in pursuit of self-interest.'[123] Research has shown that individuals

[117] Ibid.
[118] Ngo, F & Paternoster, R 'Cybercrime victimization: An examination of individual and situational level factors' (2011) 5:1 *International Journal of Cyber Criminology* 773 at 775.
[119] Agustina op cit note 1 at 39.
[120] Ngo & Paternoster op cit note 118 at 776.
[121] Ibid.
[122] Ibid.
[123] Gottfredson, M & Hirschi, T *A General Theory of Crime* (1990) *Stanford University Press* at 15.

who lack self-control are more likely to commit criminal offences. According to Gottfredson and Hirschi, 'individuals with low self-control commit deviant acts when presented with the opportunity to do so …'.[124]

In terms of General Strain Theory, 'crime and delinquency are caused by strain.'[125] Agnew posited that strain could fall into three categories, '(a) failure to achieve positively valued stimuli, (b) loss of positively valued stimuli, and (c) actual or anticipated presentation of noxious stimuli.'[126] These strains result in negative emotions which cause individuals to engage in criminal acts to alleviate the emotions or exact revenge. Research has also suggested that past victimisation could be an important source of strain.[127]

While these theories have been applied to cyberbullying, it is unclear whether they have been applied to other forms of cybercrime. However, it is likely that both theories may be relevant when evaluating cybercriminals and the reasons behind their perpetration of crime – be it in the real world or cyberspace. While the General Theory of Crime was developed to evaluate and understand criminal offending, there are aspects of the theory that could be utilised to predict victimisation. It has been argued that a lack of preventative behaviour due to imprudence and risk-taking makes people more susceptible to victimisation.[128] In the context of cybercrime, this means that an individual's failure to utilise passwords or have appropriate security measures in place may lead to an increased likelihood of victimisation. A study conducted by van de Weijer and Leukfeldt considered the relationship between cybervictimisation and what the authors term 'key traits from the Big Five model of personality (i.e. extraversion, agreeableness, conscientiousness, emotional stability, and openness to experience).'[129] The authors compared the responses of non-victims, victims of cybercrime and victims of traditional crime, finding that the same three personality traits, namely conscientiousness, emotional stability, and openness to experience, were significantly related between victims of cybercrime and victims of traditional crime.[130] In other words, these three personality traits can be associated with both cybervictims and victims of traditional crime. As the modus operandi for these crimes are different, one may have expected significant

[124] Lianos, H & McGrath, A 'Can the General Theory of Crime and General Strain Theory explain cyberbullying perpetration' (2018) 64:5 *Crime and Delinquency* 674 at 678.
[125] Ibid at 679.
[126] Ibid.
[127] Ibid at 680.
[128] Van de Weijer, S & Leukfeldt, E.R. 'Big Five Personality Traits of Cybercrime Victims' (2017) *Cyberpsychology, Behavior, and Social Networking* (DOI: 10.1089/cyber.2017.0028) 1 at 2.
[129] Ibid at 1.
[130] Ibid at 5.

differences in the victims' personalities. The only major difference observed by van de Weijer and Leukfeldt pertained to 'openness to experience'. Their research indicated that individuals who are more open to experiences are more likely to become a victim of hacking or computer viruses but not to becoming a victim of cyber-enabled crimes. In other words, individuals who are open to experiences are more likely to click on links and open attachments from unknown sources which could result in falling prey to cyber-dependent crimes.[131]

2.9. Online Disinhibition Effect

> 'Various investigations of the behaviours of habitual internet users indicate that people say and do things in cyber space that they would not ordinarily say or do in their face-to-face relationships …'[132]

One of the main attractions about being online and specifically engaging with people online is that you can be whoever you want to be. Today, chat rooms and virtual reality forums are common, and individuals can be the curator of their virtual mask. People have the courage and freedom to say things or act in a manner they may not act in the physical world. This can be liberating but also very dangerous if used or done for sinister reasons.

Suler developed characteristics of the 'psychology of cyberspace' and noted that the online world creates the space for behaviours that would not take place in real life.[133] People have virtual personas that can be distinguished and distanced from their 'real life' (termed dissociative anonymity), and people have invisibility which allows them to come and go on sites 'anonymously but also secretly,' emboldening them to visit sites which may have consequences to their 'real life'.[134] People can also edit themselves online because the interactions are asynchronous, and do not necessarily occur in real time. In addition, they could act impulsively and then disappear, 'a phenomenon that could be described as an "emotional hit and run"'.[135] Because there is no way to verify information provided by other online users, individuals can ascribe imaginary traits and qualities to other users (termed solipsistic introjection). People may go so far as to use dissociative imagination to view their online persona living in 'another dimension' with the other online users.[136] The online space also

[131] Ibid.
[132] Agustina op cit note 1 at 42.
[133] Ibid.
[134] Ibid at 43.
[135] Ibid.
[136] Ibid.

minimises status and authority, giving everyone the same status online and creating a world where, essentially, nobody is better than anyone else.

These disinhibition effects result in individuals engaging in more risky behaviours online. The anonymity and ability to distance one's real life from their virtual persona allows and even encourages individuals to cross a line, one they would not ordinarily cross if it could easily be linked to their real life. This can be dangerous as individuals may be emboldened to say and do negative things they do not have the freedom to do in real life, where society would hold them accountable for their actions and words. Online trolls post negative and hurtful comments on pictures or videos because their fake usernames give them some sense of security that whatever is said will not be traced back to them.

Suler also describes 'benign disinhibition'.[137] These 'positive manifestations' include efforts to improve self-understanding and personal development.[138] These benign disinhibitions can lead to self-discovery and self-actualisation. Online disinhibition allows individuals the freedom to express themselves and gives them the courage to be whoever they want to be, which can be a positive thing if done in the correct manner. For example, a shy person may be able to express themselves, creating a positive effect. Whether or not the effects and interactions are negative or positive depends on the individual and their intentions.

2.10. Summary of Literature Review

It is evident that there is an abundance of literature dealing with cybercrime, the theories that may be applicable to cybervictims and cybercriminals and more recently, the reporting and prevention of cybercrime. It is clear that many of the theories developed to examine traditional crimes – such as RAT, SCP and the General Theory of Crime and General Strain Theory – can be modified to apply to cybercrimes. With regard to the reporting of cybercrime, the current frameworks in place – both nationally and internationally – need to be revised so that victims feel comfortable approaching the authorities to report their victimisation experience. This may mean police working with other institutions to share the workload and pool available resources.

[137] Lapidot-Lefler, Noam & Barak, Azy 'The benign online disinhibition effect: Could situational factors induce self-disclosure and prosocial behaviors?' (2015) 9:2 *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* at 1.
[138] Ibid.

The current South African legislative and policy frameworks are, on paper, effective documents and have been said to place South Africa on par with its international counterparts.[139] In practice, however, the legislation and policy seems to fall short.

[139] Moyo, A 'Top-notch Cyber Crimes Act ultimately fails to deliver' 2 June 2022 *ITWeb* available at https://www.itweb.co.za/content/PmxVEMKEyOovQY85, accessed on 3 December 2022.

3. CHAPTER 3 – RESEARCH METHODOLOGY

This study examined victims' experiences of cybervictimisation and the response to this crime, including assessing whether the current legislative framework in South Africa adequately addresses the problem. The research also aims to understand whether participants were aware of the legal remedies available to them and whether they knew what to do or where to go to report that they had been victims of cybercrime. Participants were asked to volunteer to consent to take part in an online survey where they were asked to answer a series of questions about their cybervictimisation experience and how the legal system or other institutions were able to assist them.

The research contributes to the literature on cybercrime and cybervictimisation as it provides insight into the forms of cybercrime experienced in South Africa and whether or not these crimes were investigated. The study collected brief biographical information (such as age and gender) and collected information on online behaviours. The study also collected information about common forms of cybercrime experienced together with the social media platform and/or application utilised at the time the cybercrime was perpetrated. The survey also asked participants whether they felt the current South African legislative framework adequately addressed the crime and whether they felt satisfied with the response when they reported the crime.

Because the study is exploratory and uses survey methodology, it is only able to describe trends at the general level. However, it provides an important snapshot of cybercrime in South Africa, showing that just because individuals do not share personal information online does not prevent them from becoming victims of cybercrime; the most common forms of cybercrime experienced by respondents were random, not targeted attacks; more than 50 per cent of respondents did not report their cybervictimisation because they felt SAPS would not have helped; most victims did not receive the services they needed following their cybervictimisation; and majority of participants felt the current laws in South Africa were insufficient or were uncertain as to their effectiveness.

3.1. Methodology

This online survey research utilised a mixture of questions and statements administered anonymously through the SurveyMonkey platform. The questionnaire included a combination

of open-ended and closed-ended questions, although primarily closed-ended questions were utilised to avoid the difficulty that asking open-ended questions in a self-administered questionnaire may introduce, namely the possibility of misunderstanding, which could impact data quality. The questionnaire was modelled on pre-tested measures from existing survey instruments that have been utilised to conduct similar research internationally.[140]

The survey included descriptive and demographic questions and attempted to gauge the factors the participant thought may have led to their victimisation, how they changed their behaviour following the incident and how they responded to the situation. The online survey took between 10 and 15 minutes to complete depending on the level of detail a participant chose to provide in the open-ended response questions. The survey was kept short to ensure it could obtain relevant data without burdening participants with an unnecessarily lengthy survey. To reduce the time burden on participants, the survey also incorporated the use of skip patterns.[141] The survey was edited and tested for approximately one and a half months prior to being distributed via an online flyer, which included a link to the survey. The survey remained open for a period of approximately two months.

3.2. Recruitment

The survey flyer, which included a link to the online survey, was posted on various social media platforms including Facebook (my personal Facebook page, a page called "Cyber Crimes Victims Support Group and a page called "Cyber Crime Investigation"), WhatsApp (my personal status, a neighbourhood watch group called "Ferness Awareness Group", a group for candidate attorneys and attorneys and a church youth group), Telegram (a group for candidate attorneys, attorneys and advocates across South Africa), LinkedIn (my personal page) and Instagram (my personal status). The flyer was also posted on the University of Cape Town Centre for Criminology Facebook page.

---

[140] See for example: Näsi, M, Oksanen, A Keipi, T & Räsänen, P 'Cybercrime victimization among young people: a multi-nation study' (2015) 16:2 *Journal of Scandinavian Studies in Criminology and Crime Prevention* 203; Ngo & Paternoster op cit note 118; Armin, J, Thompson, B & Kijewski, P '2016 – Cybercrime Surveys Report' *Cyber Road – Development of the Cybercrime and Cyber-Terrorism Research Roadmap*, available at www.cyberroad-project.eu, accessed on 23 May 2020; United States Department of Justice, Bureau of Justice Statistics 'National Crime Victimization Survey: Identity Theft Supplement 2012' *Inter University Consortium for Political and Social Research* available at: https://bjs.ojp.gov/library/publications/victims-identity-theft-2012, accessed on 29 May 2020.

[141] Ojanen, T, Boonmongkon, P, Samakkeekarom, R, Samoh, N, Cholratana, M, Payakkakom, A & Guadamuz, T 'Investigating online harassment and offline violence among young people in Thailand: Methodological Approaches, Lessons Learned' (2014) 16:9 *Culture, Health & Sexuality* 1097 at 1101.

When people clicked on the link to the survey, they were directed to the landing page on SurveyMonkey containing the study information, including a description of the risks of participation. The information sheet explained that participation in the survey was completely voluntary, and it informed participants that the information would be utilised for a Master's dissertation as well as for potential future academic publications.

3.3. Sample

Given the study's limited scope as an exploratory, descriptive Master's degree minor dissertation project, it relied on a convenience volunteer sample, aiming for a sample size of at least 300 participants who have experienced cybercrime. The study recognised that relying on a convenience volunteer sample meant that there may be limitations to generalisability introduced but these were deemed acceptable given the scope of the project.

As cybercrime is not age specific, the study aimed to target diverse groups on various social media platforms to ensure participants with a diverse representation of age, socio-economic status, gender and racial diversity were drawn. The sample comprised 87 adult individuals recruited by posting survey flyers on various social media platforms. 80 of the 87 individuals consented to participate in the survey. Participants were asked several questions regarding their gender, age, province of residence and employment status. This information aimed to determine whether cybercriminals disproportionately targeted any one group within society. The responses to these queries are discussed and depicted, hereunder.

The sample comprised of 69.33 per cent females (*n*=52), 26.67 per cent males (*n*=20) and 4.00 per cent of respondents who identified as "Other" (*n*=3). 69.05 per cent of the participants were employed full time (*n*=29). Participants were asked whether they were employed on a full-time or part-time basis to understand whether people who were employed on a part-time basis were more likely to be victimised as one could assume those individuals had more free time to spend online.[142] It also would have been useful to determine whether full-time employees experienced a particular form of cybercrime (such as phishing or financial cybercrime) versus their part-time counterparts. Participants were asked whether they were

[142] In this survey, "Full-time" was defined as four or more hours per day, at least four days per week. "Part-time" was defined as less than three hours per day, up to three days a week. This question was asked to determine whether employment had an effect on the amount of time spent online and subsequently, whether this correlated with routine activities conducted online. One would assume that less time spent working meant more time spent online and a higher chance of being victimised.

students or not. Of the participants, 41.43 per cent confirmed they were students (*n*=29). I asked this question because I was interested to see whether students were more likely to be victims of specific forms of cybercrime and whether they would be more "clued up" on cybercrime and cybersecurity measures.

Figure 1: Age

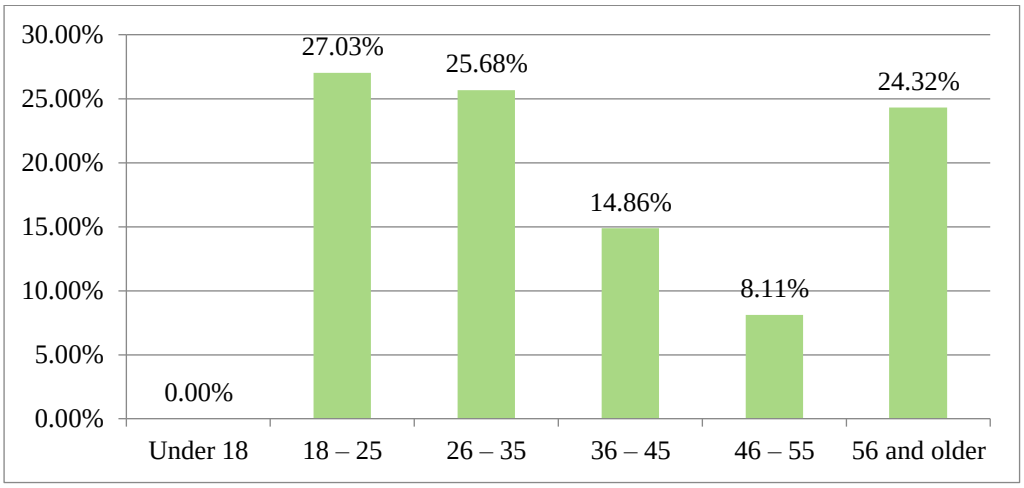


Figure 1 shows that there was a relatively even spread of age among participants, with approximately 25 per cent of the participants falling into the age groups 18 to 25, 26 to 35 and 56 and older respectively.

Figure 2: Province's participants reside in

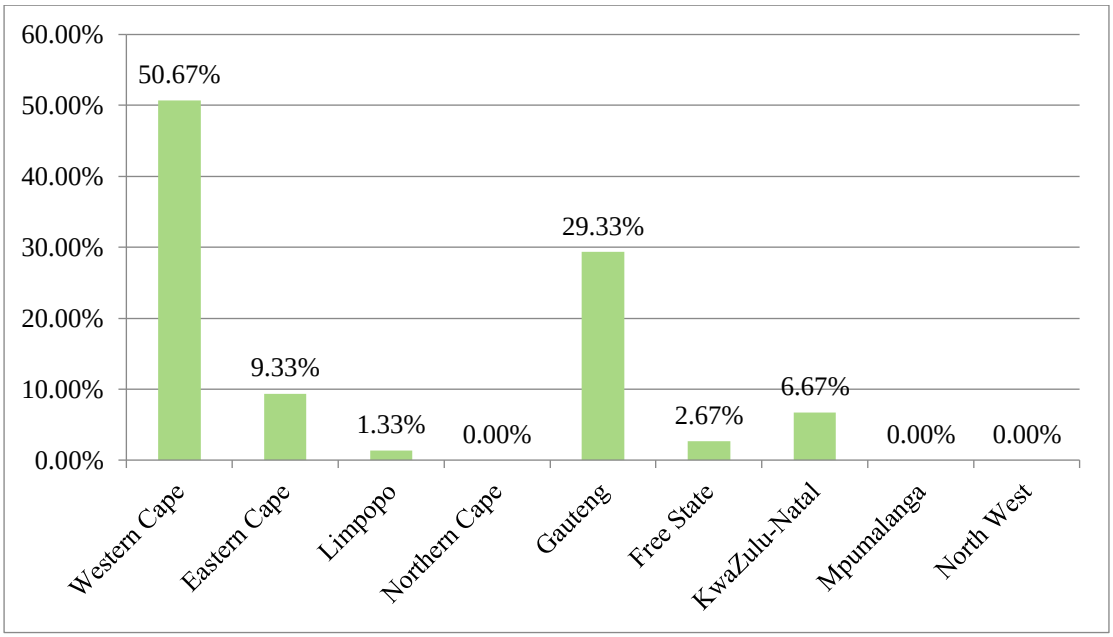


Figure 2 reflects that majority of the sample came from the Western Cape (50.67 per cent) and Gauteng (29.33 per cent). Twelve participants elected not to respond to the question regarding the province they live in.

3.4. Analytical Strategy

A descriptive analysis was employed. This type of data analysis '… helps describe, show or summarize data points in a constructive way such that patterns might emerge …'.[143] Descriptive analysis can further be categorised into four types: frequency, central tendency, dispersion and/or variation.[144] A general overview of responses to the questions are provided and graphs are utilised to depict the frequency of responses.

3.5. Ethical Considerations

Ethical clearance for this study was obtained from the University of Cape Town Faculty of Law Research Ethics Committee (Reference Number: L0208-2022).

I considered several important ethical considerations in preparing the survey. Participants were asked some personal information, but the level of detail required was relatively basic, non-intrusive and general. As the survey did not collect any identifying data such as names or surnames, the participants were able to remain completely anonymous.

It was important to recognise that participants may have felt distressed because they were revealing intimate details of their lives. To deal with this risk, the study warned participants about the kinds of questions they would be asked, that they were able to skip questions and that they were able to stop participating at any time. A positive about doing anonymous research is that participants respond to the survey willingly which means that if they feel uncomfortable at any point, they are free to withdraw.

There was a risk that participants could feel embarrassed or ashamed of what happened to them. This was a difficult element to counteract because the nature of online survey research does not permit any manner to comfort or acknowledge participants feelings and emotions.

---

[143] Rawat, A.S. 'An Overview of Descriptive Analysis" 31 March 2021, available at https://www.analyticssteps.com/blogs/overview-descriptive-analysis, accessed on 5 December 2022.
[144] Ibid.

Best practice is to provide 'contact information for questions during the consent process'.[145] Participants were therefore provided with the researcher and supervisor's contact information, as well as information on free telephone and online counselling resources they could utilise in the event they experienced any distress as a result of the survey.

A major concern relating to conducting research on social media is that of informed consent. Two potential issues that could arise include 'the lack of face-to-face contact with participants' and 'how to obtain parental consent in the case of a minor participant.'[146] The second issue is particularly important in relation to research conducted via Facebook and Twitter because by posting a link to the survey interview, one is unable to control who accesses it. This risk was, however, mitigated by the fact that the landing page provided an overview of the survey and set out that only individuals over the age of 18 years old were permitted to participate in the survey, participants were also requested to provide their informed consent prior to answering any survey questions. In addition, none of the participants indicated they were under the age of 18 in response to the question about age and the fact that 42 participants responded they were employed indicates that the survey was successful in restricting access to people under the age of 18 years old.

Another key concern is the protection of confidentiality.[147] This means participants should have the right to know how their data will be used and who will have access to it.[148] The participants were not deceived in any manner as they were informed exactly what the survey was about and what the aim was. Linked to the concept of confidentiality is that of privacy. Privacy refers to the participant's ability to decide what they want others to know and what information they want to withhold.[149] Something that must be taken into account when using an online survey is the issue of internet tracking tools.[150] These tracking tools are used by websites to store an individual's preferences which can be used to tailor the user's web experience to their liking. The "Anonymous Responses Collector" feature on SurveyMonkey was utilised to ensure identifiable respondent information was not tracked or stored.

---

[145] Ibid at 712.
[146] Moreno, M, Goniu, N, Moreno, P & Diekema, D 'Ethics of social media research: Common concerns and practical considerations' (2013) 16:9 *Cyberpsychology, Behaviour and Social Networking* 708 at 711.
[147] Ibid at 711.
[148] Toepoel, V 'Online survey design' in Nigel G. Fielding, Raymond M. Lee & Grant Blank (eds) *The SAGE Handbook of Research Methods* (2017) 184, available at https://dx.doi.org/10.4135/9781473957992, accessed on 15 May 2019.
[149] Siegel, Max 'Privacy, ethics, and confidentiality' (1979) 10:2 *Professional Psychology* 249 available at http://dx.doi.org/10.1037/0735-7028.10.2.249, accessed on 14 May 2019.
[150] Toepoel op cit note 148 at ch 3 p 4.

Informed consent is another ethical consideration to be aware of. In order to respect this right insofar as possible, participants were provided with 'a description of the study, … the purpose of the study, what the participant [was] expected to do and why the study is important.'[151] Informed consent is especially difficult to obtain for online surveys but one way to obtain participant consent is 'by requesting they click an 'I agree' button.'[152] In this survey, participants were provided with information about the study and requested to confirm their consent to participate in the survey.

3.6. Limitations

The data collected is not generalisable as it is not representative of the South African population at large. Participants from various provinces did, however, access and participate in the survey. Individuals from five of the nine provinces in South Africa namely, Western Cape, Eastern Cape, Limpopo, Gauteng and KwaZulu-Natal, participated in the survey. The survey flyer was published on various social media platforms, but it is important to remember that not everyone has access to the internet or the social media platforms the flyer was posted on. The data may therefore not be utilised to make inferences about the population as a whole.

Survey research is typically plagued with issues of high non-response rates.[153] Participants, particularly those from neighbourhood watch and cybervictims groups invited to participate on Facebook, may have been reluctant to participate as the survey was not posted by someone in their group. One way to mitigate this would be to post the survey results on the group page, but this does not pre-emptively improve response rates.[154] The survey results are therefore limited by its relatively small size.

Another limitation is that individuals may have been reluctant to come forward with their experiences of cybercrime because they feel embarrassed. I tried to mitigate this by assuring individuals that their personal information will remain confidential and by informing them that

[151] Toepoel op cit note 148 at ch 3 p 4.
[152] Keller, Heidi & Lee, Sandra 'Ethical issues surrounding human participants research using the internet' (2003) 13:3 *Ethics and Behaviour* 211.
[153] Wright, Kevin B 'Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services' (2005) 10:3 *Journal of Computer-Mediated Communication* available at https://doi.org/10.1111/j.1083-6101.2005.tb00259.x, accessed on 16 May 2019
[154] Ibid.

their names would not be used in the dissertation. I also tried to encourage participation by informing participants that their experiences may help future cybervictims.

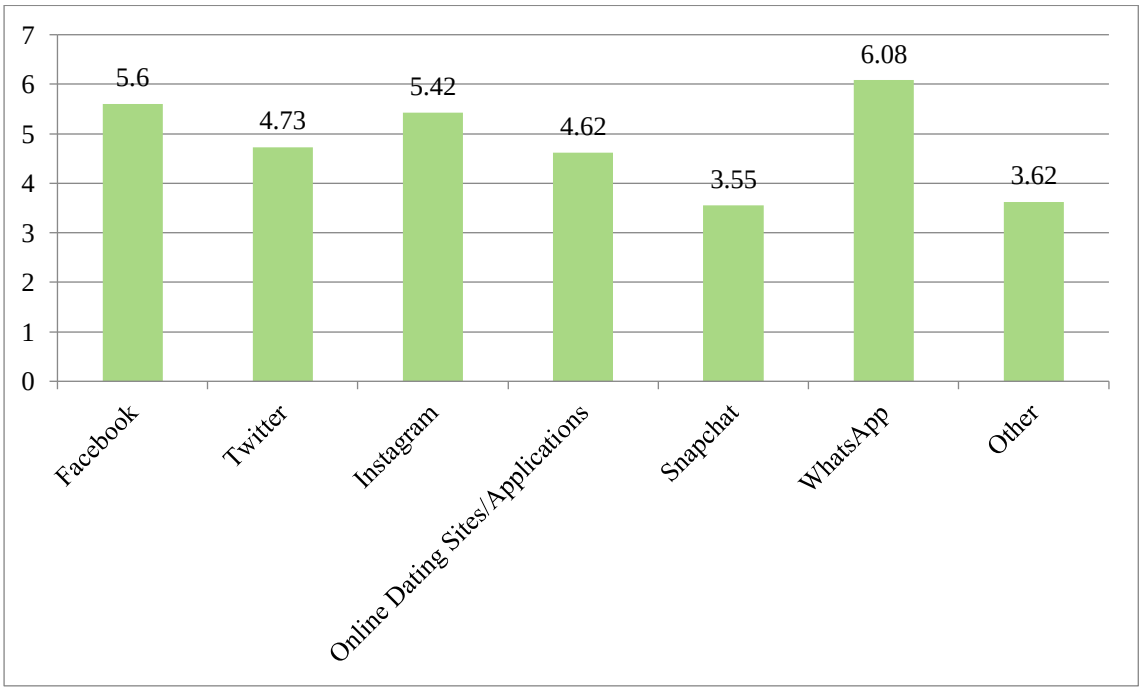
A final possible limitation is that there may be a language barrier for the participants as the survey was presented in English. I attempted to mitigate this by using simple language, providing explanations as far as possible and by avoiding jargon.

4. CHAPTER 4 – RESULTS

4.1. Social Media Platforms Utilised

The three most utilised social media platforms include WhatsApp, Facebook and Instagram (Figure 3 below). This is to be expected as WhatsApp is widely utilised as a primary and efficient means of communication. Phishing scams have also become more common via WhatsApp, which means that users are vulnerable because scammers can contact individuals via their mobile numbers. A popular cybercrime experienced on Instagram and Facebook is social media fraud, also known as catfishing.[155] Research has found that 'Cybercriminals are also using Facebook, Instagram, WhatsApp, and other legitimate platforms to communicate with each other and sell stolen identities, credit card and … other hacked data.'[156] Participants did not elaborate on the "Other" platforms used.

Figure 3: Online/Social media platform/s used most frequently

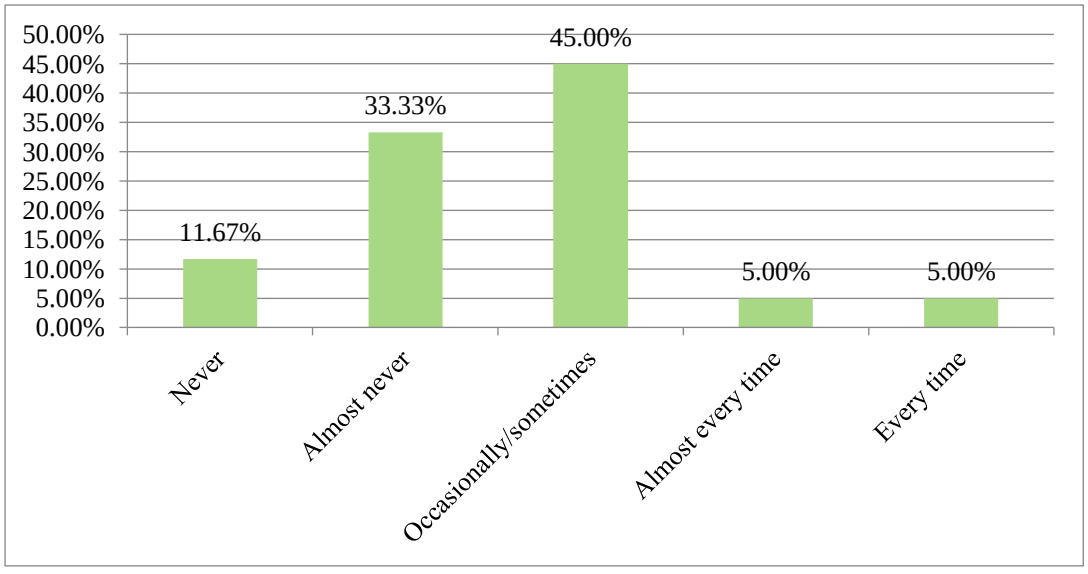


[155] Baron, Jessica 'Social Media Platforms Increasingly Popular With Cybercriminals' 30 April 2019 available at https://www.forbes.com/sites/jessicabaron/2019/04/30/social-media-platforms-increasingly-popular-with-cybercriminals/?sh=3eccd94f7324, accessed on 2 December 2022.
[156] Ibid.

4.2. Sharing of Personal Information

Figure 4 shows that participants sometimes share personal information about themselves online. The data indicates that participants were more likely not to share personal information online (45 per cent of respondents selected this option). This is interesting as a small percentage of people shared information freely (around 10 per cent) which suggests it is more likely that respondents were targeted by savvy scammers. In other words, it seems unlikely respondents were targeted because of their risky online behaviours but rather that they were targeted by knowledgeable cybercriminals running complex scams. Interestingly, some participants never shared any personal information online but still fell prey to cybercriminals. This suggests that cybercriminals may have targeted these individuals randomly. This indicates that the availability of information is not the sole factor utilised by cybercriminals when targeting potential victims. It is, however, prudent to remain vigilant and share as little personal information online as possible.

Figure 4: Sharing of personal information online

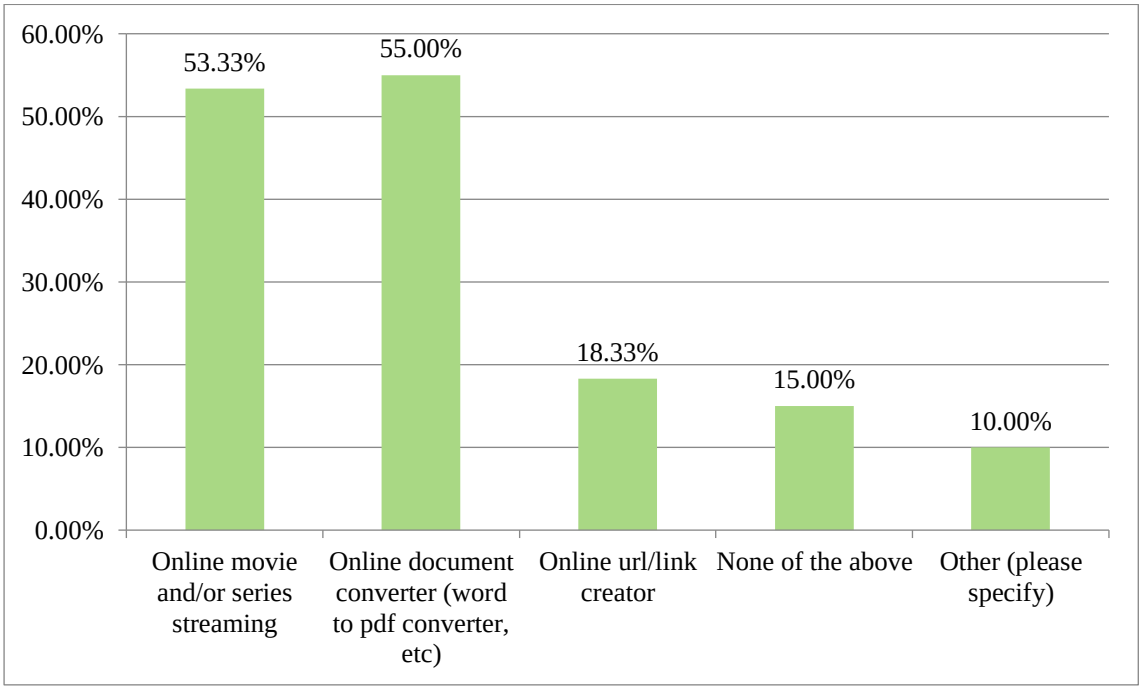


4.3. Participants Online Behaviours

Most people reported making use of various “free” software/apps as is depicted in Figure 5 below. The types of free software/apps included in “Other” were EskomSePush, Canva, YouTube Music, AVG Anti-Virus, Twitch, Discord, Spotify, Steam and Epic Games.

When utilising free software such as an online document converter, individuals are not typically required to input their personal information, neither are they required to do so when utilising an online streaming service. Whether or not the free software/apps resulted in the collection of personal information and subsequent perpetration of cybercrimes is accordingly not determinable. Free sites are known to utilise pop-up advertisements which, when clicked on, may result in computer viruses. Research conducted by Full Fact, a registered charity in the United Kingdom, found that '[m]alware can be a huge issue when streaming online and it's a problem that should not be ignored. … criminals behind digital piracy often make the content freely available illegally to "bait" a large number of visitors'.[157]

Figure 5: Use of "free" software/apps

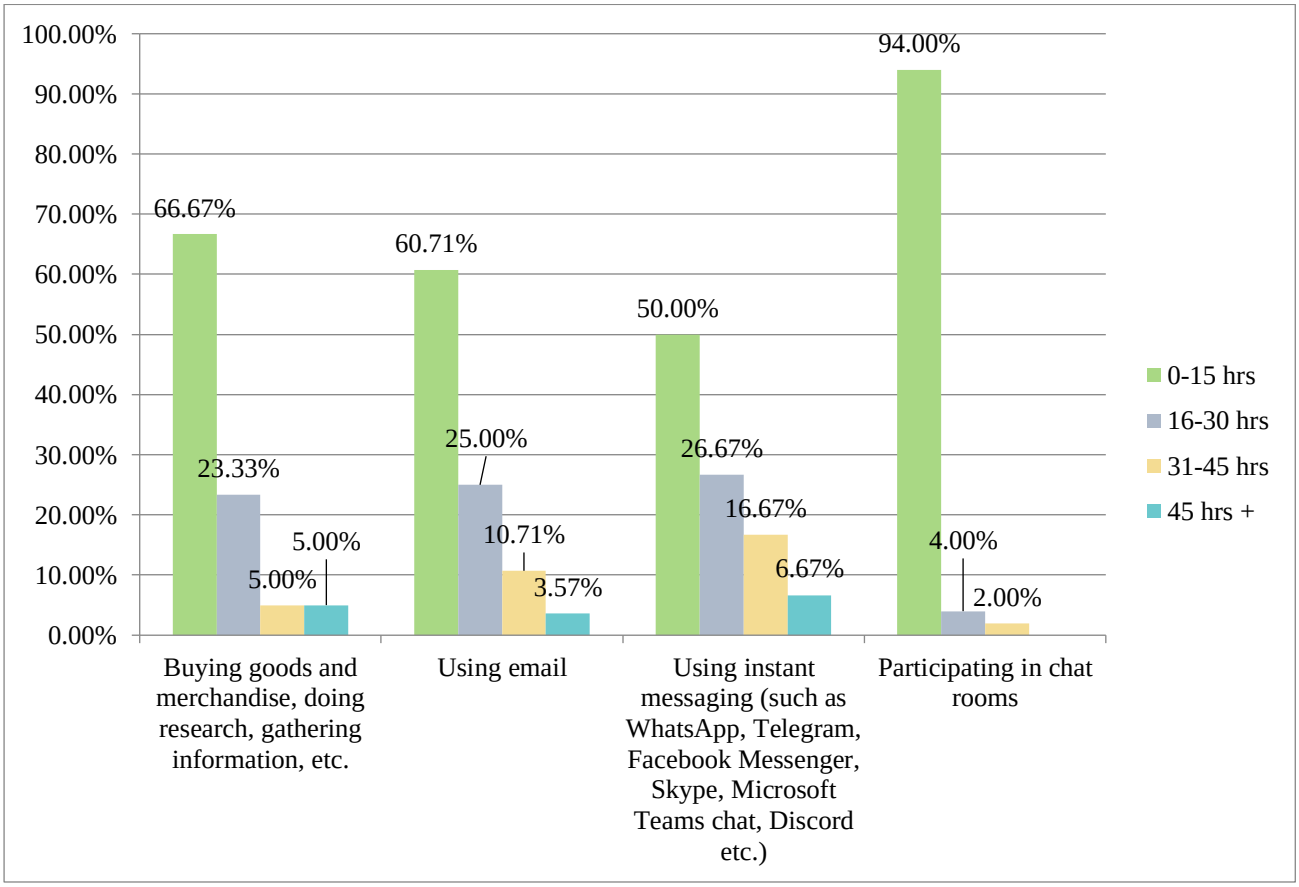


I was interested in whether the number of hours spent engaging in online activities may be linked to cybervictimisation and further, whether specific online activities increased the likelihood of cybervictimisation. Figure 6 indicates that individuals spend more time utilising instant messaging (*n*=60) than they do using email (*n*=56). Ninety-four per cent of the 60 participants who responded indicated that they spent 0 to 15 hours per week engaging in chatrooms (*n*=50). The data indicates that participants engaged in "Buying goods and

[157] BlockSite '5 Ways to Avoid Malware While Streaming Content Online' 18 July 2022 available at https://blocksite.co/blog/5-ways-to-avoid-malware-while-streaming-content-online, accessed on: 2 December 2022.

merchandise, doing research, gathering information, etc" (*n*=60) and "Using instant messaging (such as WhatsApp, Telegram, Facebook Messenger, Skype, Microsoft Teams chat, Discord, etc" (*n*=60) for the most time per week. This evidences that victims may have been targeted as a result of activities conducted in their personal time and not while performing work-related activities. This may be because victims are more relaxed and not as vigilant to threats when conducting their personal business. Engaging in potentially harmful activity utilising work resources would be more detrimental as it would affect them in their professional capacity. This could indicate that individuals have their guard down more when browsing the internet for personal reasons, engaging in online shopping or chat rooms.

Figure 6: Hours per week engaging in online activities



Of the 60 participants that responded, 78.33 per cent have anti-virus or protective software installed on their computer (*n*=47) and 21.67 per cent do not have any anti-virus or protective software installed (*n*=13). This suggests that having anti-virus software installed on a device may not be a sufficient mechanism to deter cybercriminals. Most participants have anti-virus software installed, yet they still fell prey to cybercriminals. Research has indicated, however,

that even where individuals have anti-virus software installed on their devices, they remain vulnerable to cyber-attacks – especially on their personal devices – as they are required to make sure the software remains up to date.[158] There is no team of IT specialists or a protected system to monitor their use or potential breaches of cybersecurity on their personal devices.

It is unclear whether these participants installed the software prior to or after their cybervictimisation. Perhaps future research could be done on this aspect to determine whether or not anti-virus software is a sufficient deterrent and whether it blocks certain forms of cyber-attacks. In addition, it would be interesting to consider whether paid anti-virus software was indeed better at protecting computer systems than free anti-virus software.

4.4. Cybervictimisation

Participants were requested to select all the behaviours they had experienced online. Of the 56 participants who responded to this question, 42 confirmed they had experienced phishing (75.00 per cent). Phishing is defined as 'a technique for attempting to acquire sensitive data, … through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.'[159] This was followed by 32 participants confirming they received unwanted messages or emails to personal devices without consent (57.14 per cent).

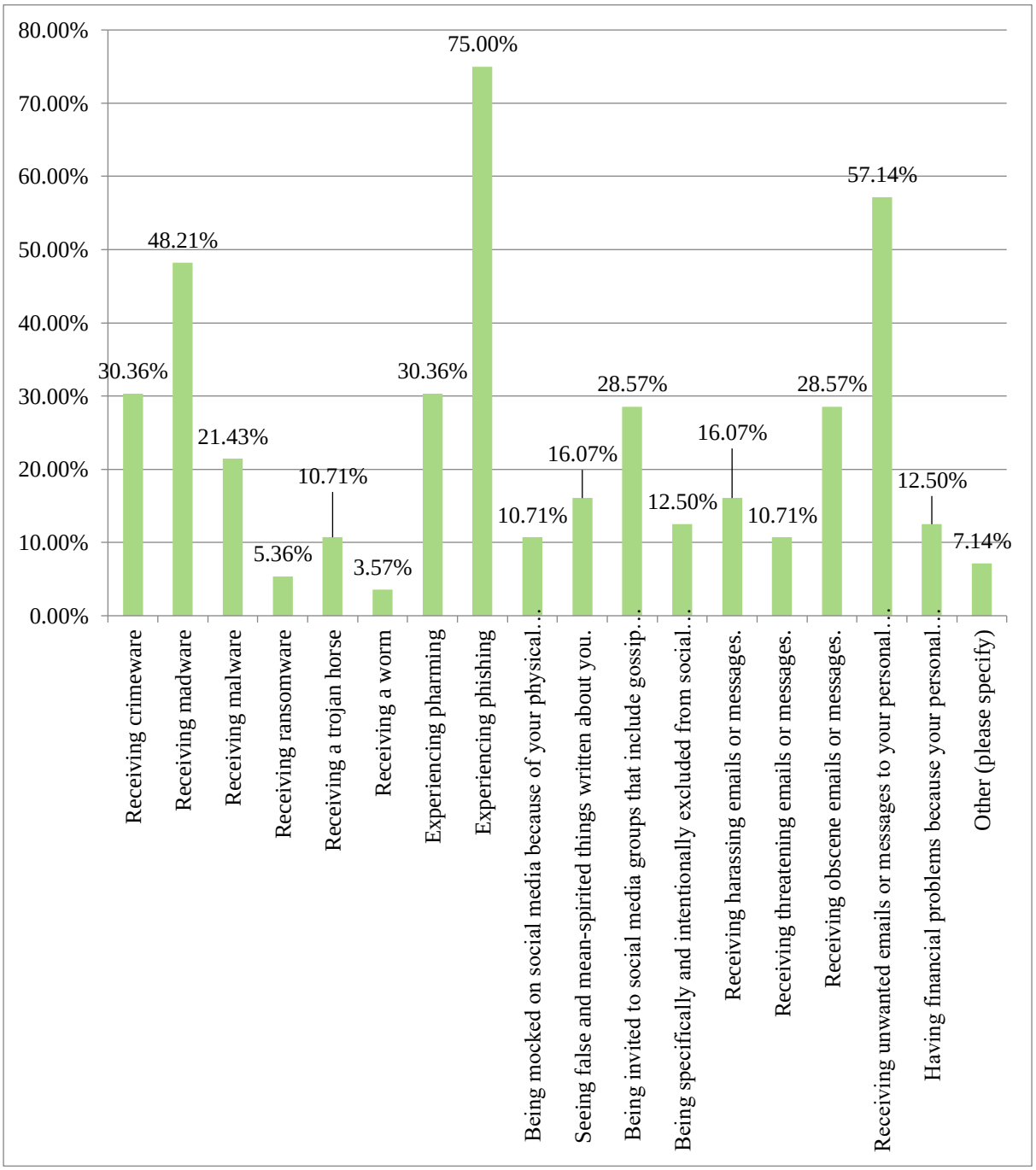
The "Other" behaviours experienced online included email addresses being hacked, intimate nude photographs being leaked and receiving an email that they had won something with a request to pay an amount for delivery, which delivery fee was subsequently deducted from their account. One participant felt that they were being "mocked" online as a result of targeted advertisements and/or memes that would appear on their social media timeline or newsfeed. Targeted advertisements have become a common occurrence as when downloading mobile or computer apps, individuals allow – whether knowingly or unknowingly – apps to access the device microphone and collect cookies. This essentially allows the app to track users' online activity and personalise the user experience.[160]

---

[158] Du Toit, Hadebe & Mphatheni op cit note 52 at 118.
[159] Information Technology Laboratory Computer Security Resource Centre 'Definition of phishing' available at https://csrc.nist.gov/glossary/term/phishing, accessed on 2 December 2022.
[160] Stouffer, Clare 'Is my phone listening to me? Yes, here's why and how to stop it' 15 August 2022 available at https://us.norton.com/blog/how-to/is-my-phone-listening-to-me#, accessed on 2 December 2022.

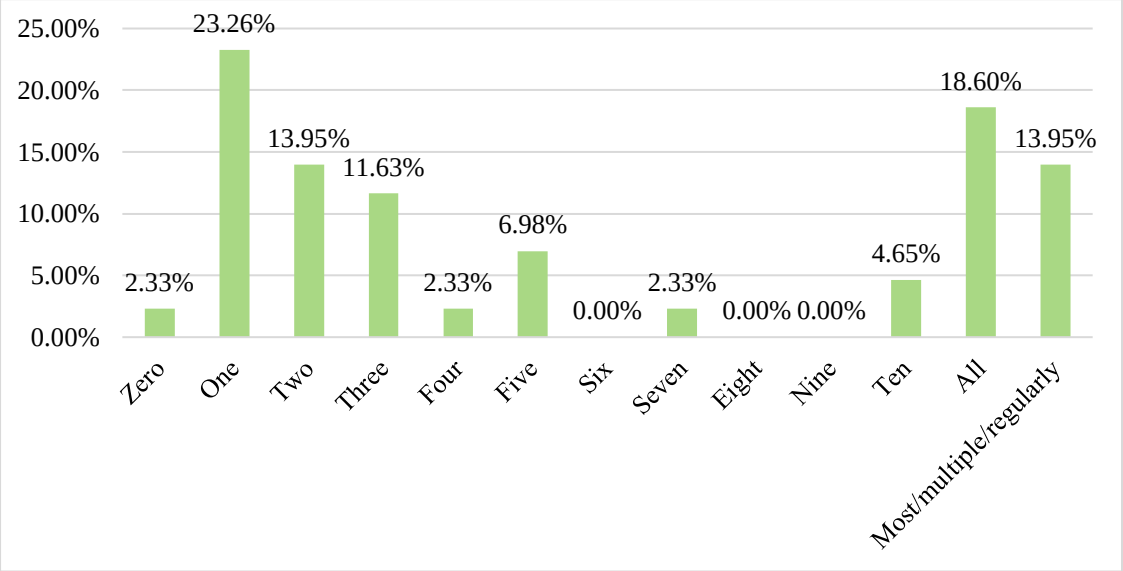
The forms of cybercrime most commonly experienced by the participants are random and not targeted attacks on a specific individual. In other words, the most frequently reported forms of cybercrime were not specific to an individual in that it could happen to anyone. It was not an instance of revenge porn, for example, that targeted a specific individual in the hopes of causing damage. Although, as stated above, there was one participant who indicated that their nude images had been leaked.

Figure 7: Behaviours experienced online



Most of the participants (*n*= 42) experienced cybercrime within the last two years. The majority of respondents confirmed they experienced at least one cybercrime in the last two years (23.26 per cent). Only one respondent indicated that their cybervictimisation experience/s occurred more than two years ago. Whether this number is a result of the increased reliance on technology pursuant to the COVID-19 pandemic is uncertain, but it does indicate that people are being targeted online. This type of inference cannot be made from the data gathered as cybercrime has been increasing exponentially in the past few years and it is likely that this surge in cybercrime would have continued, notwithstanding the COVID-19 pandemic.

Figure 8: How many cybercrimes took place in the last 2 years?



4.5. Type of Technology Used

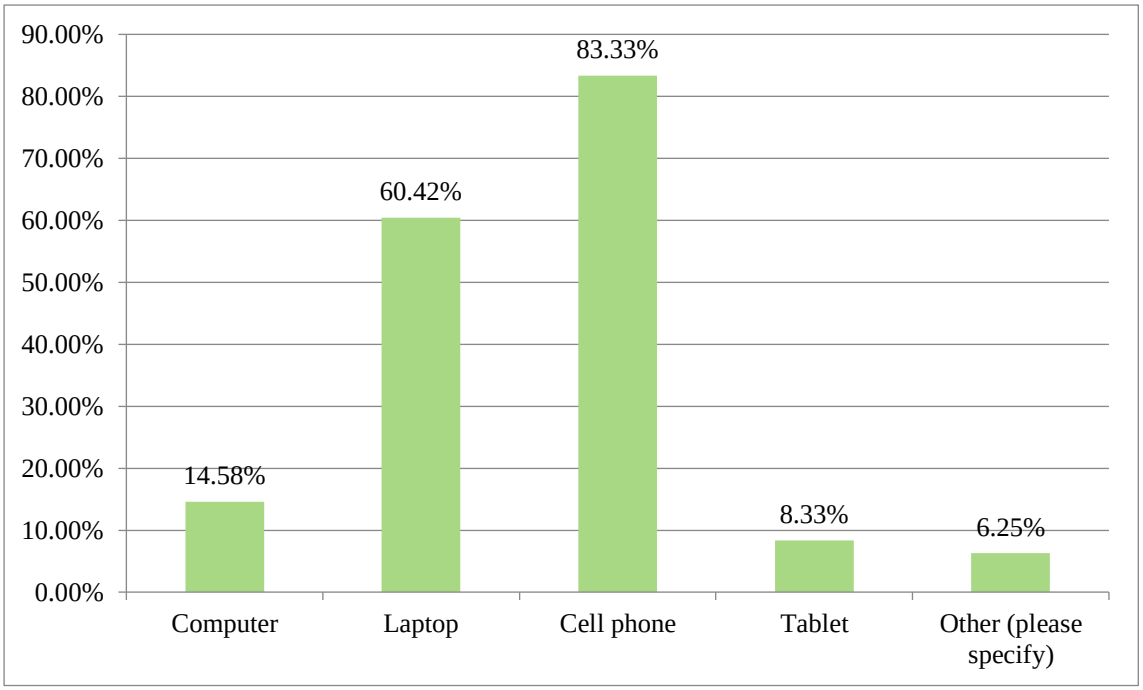
Most participants utilised their cell phones or laptops at the time the cybercrime was committed. This is to be expected as these are the main forms of technology used on a day-to-day basis, be it for work, personal use, or both. It, therefore, makes sense that cybercrime would have been experienced and perpetrated via these devices, although it is impossible to tell from this study whether one form of technology makes a person more vulnerable to cybercrime.

For many, a cell phone is the first thing they reach for in the morning. It can essentially be used to run their lives – an alarm wakes them up in the morning, they use it to check the weather and read the news, they may set reminders for various meetings or appointments, and it has fast become one of the easiest ways to bank. It is important to remember that cell phones are

mobile devices, that are typically always switched on. This means they are accessible to cybercriminals who may be lurking and waiting for their opportunity. A cybercriminal could wreak havoc on a person's life if they were to hack and take control of their cell phone, which may also contain personal images and passwords. In addition, cell phones are used by individuals of various ages and often the very young and old do not understand what they are doing or posting for everyone to see, which may also increase their risk of victimisation.

The 6.25 per cent using "Other" devices included using a gaming console. This indicates that cybercriminals utilise any form of technology they may gain access to. Minors, who use such devices, may be particularly vulnerable as they are not always aware they are being taken advantage of and would be more likely to disclose confidential personal information. Parents should therefore be particularly vigilant of their minor children who use gaming consoles connected to the internet.

Figure 9: Type of technology utilised



4.6. Activities Preceding Victimisation

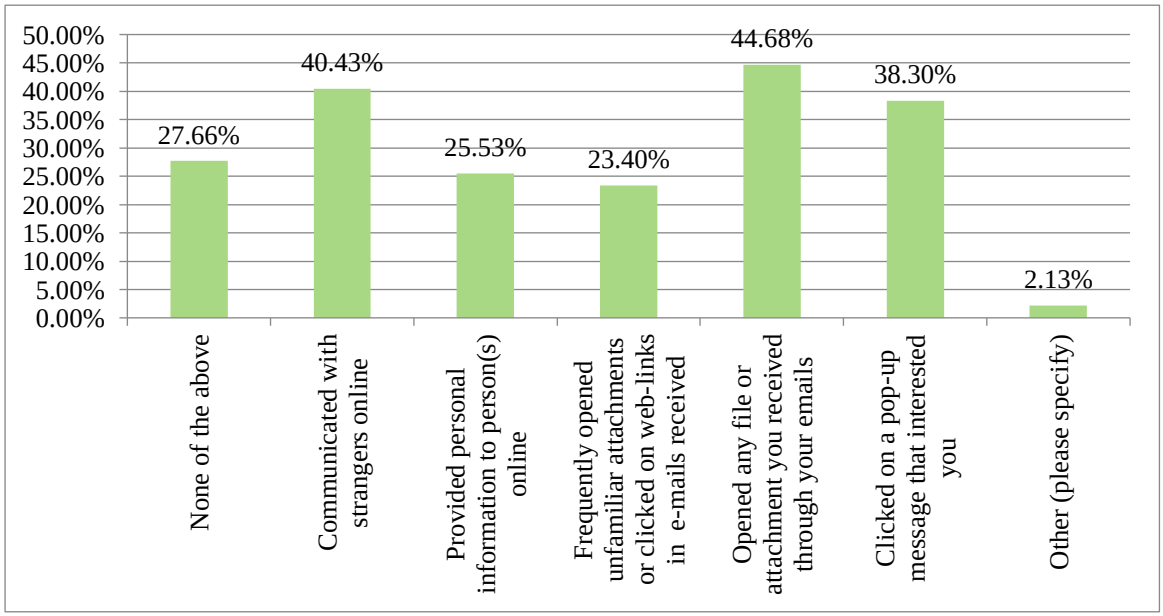
Participants engaged in a range of activities in the twelve months preceding their cybervictimisation that may have put them at increased risk of victimisation. Almost 45 per cent of the respondents confirmed they opened any file or attachment received via email

(*n*=21). As email is one of the main ways individuals communicate, in particular for work purposes, it is therefore surprising that this figure is not higher. Individuals assume the emails received are from trusted sources and do not suspect they may be targeted by cybercriminals by means of an email attachment. Often emails are sent from sources purporting to be bankers with attachments such as monthly statements or other confidential information that require you to input a password, usually your identity number. These types of phishing emails have become more and more common in recent years.

Approximately 40 per cent of respondents communicated with strangers online prior to their cybervictimisation (*n*=19). Cybercriminals often utilise social media and chat rooms to conduct reconnaissance on unsuspecting individuals. Engaging with individuals online is also dangerous as one can never really be sure who is on the receiving end of the information. In other words, cybercriminals could pretend to be a distant relative or a potential romantic connection to gather information which could be used to perpetrate cybercrimes.

Both of the activities referred to above required a form of engagement and participation from the participant. Participants either engaged directly with someone via a chatroom or via an email they received. Whether this made them more trusting of the individual or attachment and opened them up to cybervictimisation is unclear. Individuals should be more vigilant when it comes to divulging personal information and be sure to check email addresses when opening attachments annexed to emails received. This could serve to guard against becoming a victim of cybercrime.

Figure 10: Activities prior to cybervictimisation



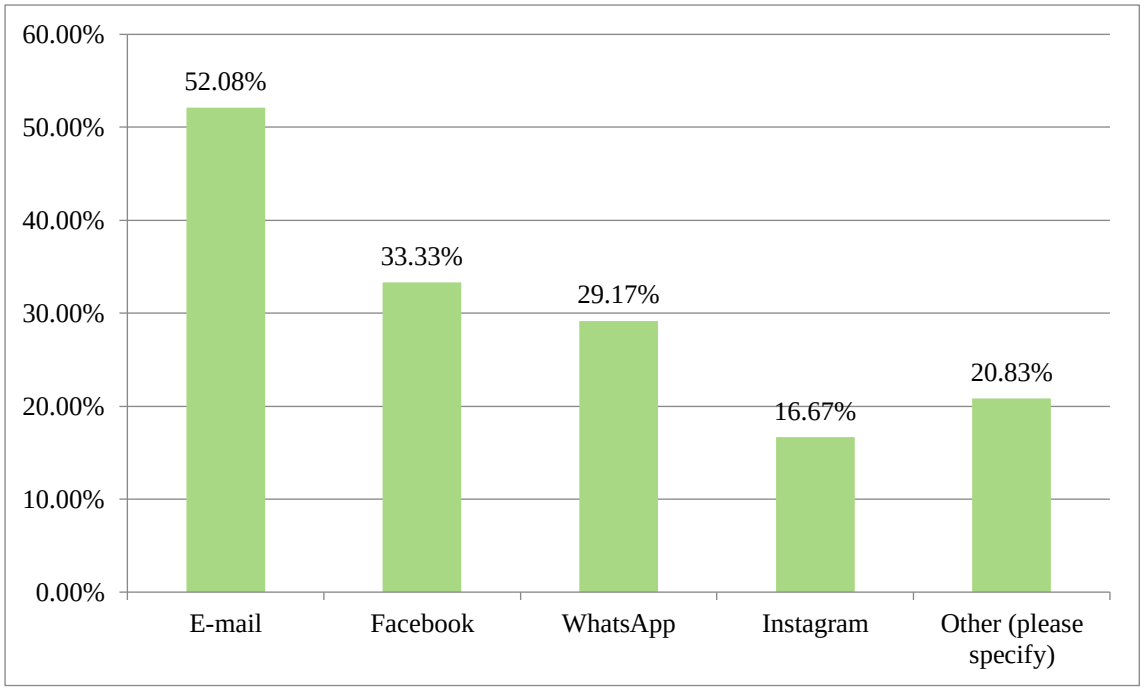
4.7. Site of Victimisation

It appears that participants were predominantly victimised via email. Given that approximately 45 per cent of participants confirmed they opened any file or attachment received via email (see Figure 10 above) it is likely that a sizeable portion may have been victimised as a result of opening attachments to emails.

The "Other" forms of media included a gaming console, Tinder and other dating apps, Telegram, Twitter, streaming websites and Discord. According to the State of Email Security 2022 Report, 'more than three out of every four South African organisations are receiving an increased number of email-based threats…'.[161]

It is unclear whether participants were victimised via their work email or their personal email. Individuals will usually use their personal email addresses when engaging in online behaviours that might be risky. For example, when using free online software, certain websites may require individuals to supply their email address to create a free account.

Figure 11: Where cybervictimisation took place

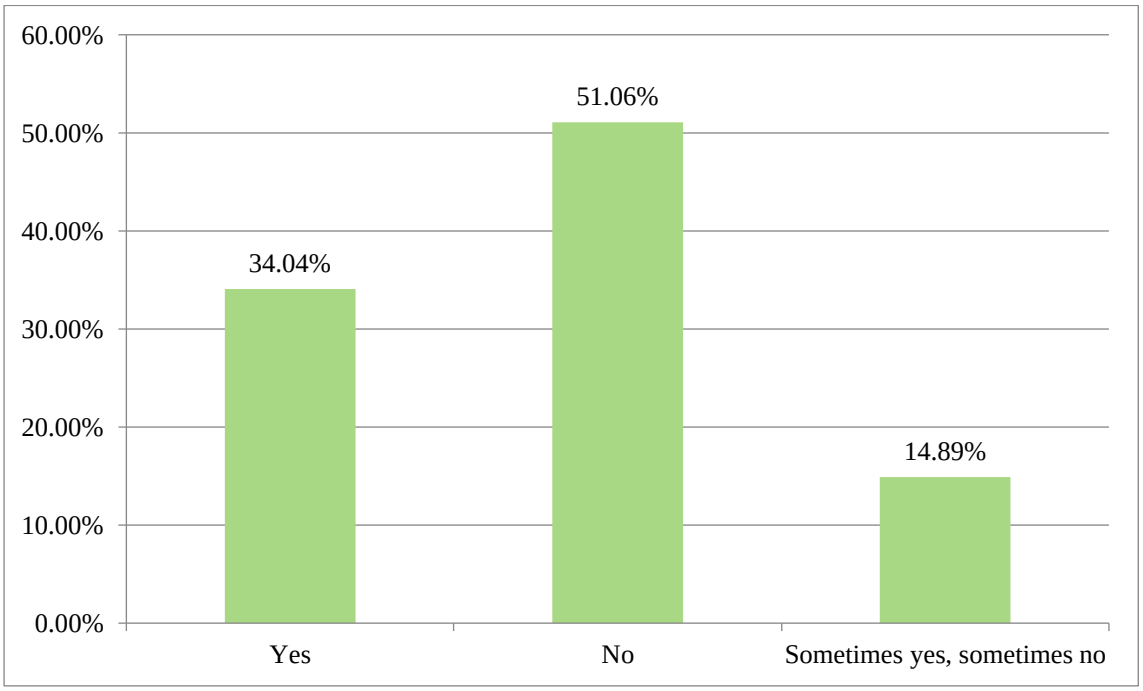


[161] Gondwe, Moss 'South Africans must up their game against cybercrime' *Mail & Guardian* 12 October 2022 available at https://mg.co.za/opinion/2022-10-12-south-africans-must-up-their-game-against-cybercrime/, accessed on 12 December 2022.

4.8. Reporting Victimisation

Forty-seven participants responded to the question about reporting cybercrime. Approximately 34 per cent reported the cybercrime (*n*=16), while 51.06 per cent did not report the crime (*n*=24). The remaining 14.89 per cent reported the cybercrime on certain occasions but not others (*n*=7). This is in line with estimates from previous research that indicate under-reporting amongst the public and businesses. Studies have shown that, in comparison to traditional crimes, the levels of reporting cybercrimes to the police are low.[162] Cybervictims are reluctant to report incidents of victimisation for a range of reasons, including that authorities do not treat cybercrimes as serious offences, that victims are embarrassed to report their victimisation or that victims feel they can deal with the incident themselves.

Figure 12: Reporting of cybercrime



4.9. Reported Cases

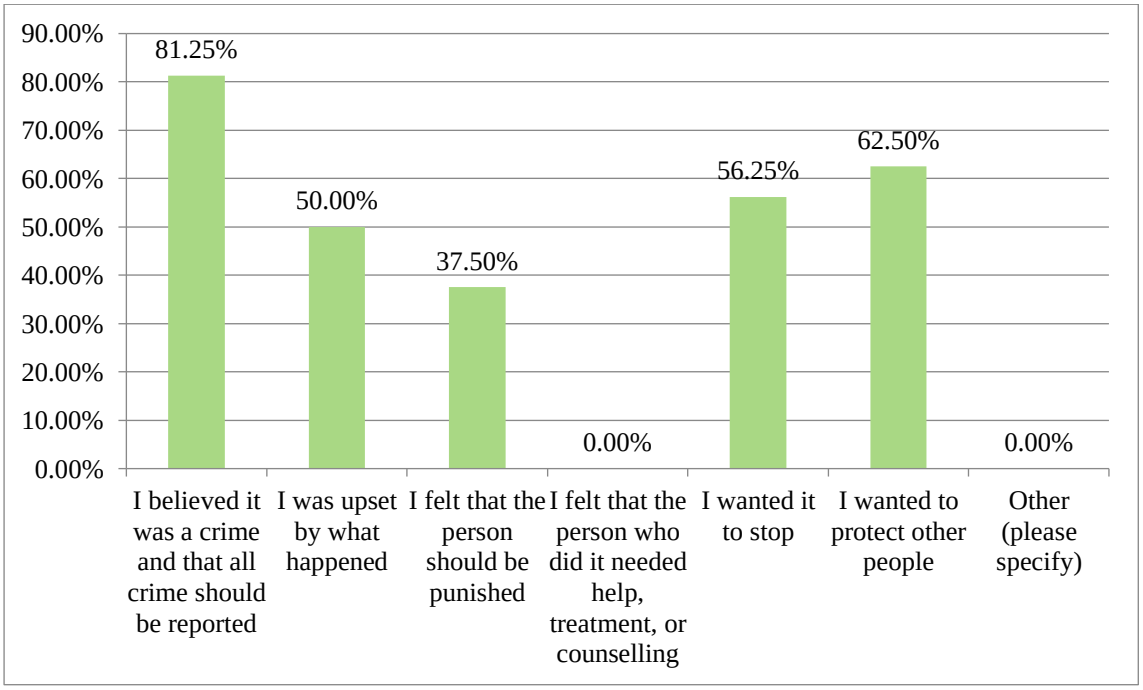
Only 16 participants answered that they reported the cybercrime. Participants were requested to select all reasons that lead them to report the cybercrime. Most people reported because they believed the incident was a crime and that all crime should be reported (81.25 per cent). This

[162] McGuire & Dowling op cit note 9 at 11.

outcome is interesting because existing research suggests that victims often feel that their victimisation – in particular cybervictimisation – is not serious enough to warrant reporting the incident to the authorities. This was evidently not the case for the victims who participated in this survey. Many of them felt compelled to report their cybervictimisation because they believed it was a crime that warranted investigation and prosecution. The positive is that this suggests some form of awareness as to what constitutes a cybercrime.

Interestingly, none of the participants selected "I felt that the person who did it needed help, treatment or counselling". This suggests the participants did not report the cybercrime to allow the perpetrator to be rehabilitated, they reported the cybercrime to benefit themselves or other potential victims. Research suggests victims are more likely to select the rehabilitation option in instances where the perpetrator has a face.[163] Cybercriminals may be perceived as faceless perpetrators as they never come face-to-face with their victims, cybervictims therefore do not have feelings of compassion or empathy towards the cybercriminal.

Figure 13: When victim did report to authorities



[163] O'Hear, Michael & Wheelock, Darren 'Public Attitudes Toward Punishment, Rehabilitation, and Reform: Lessons from the Marquette Law School Poll' (2016) 29:1 *Federal Sentencing Reporter* 47 at 51.

4.10. Where Did Victims Report?

Information on where to report the cybercrime is available, but not widely known. Fifteen participants responded to the question about where they found information on who to report the cybercrime to. Four found information on the internet, two found information on Instagram, three obtained information from the bank, one obtained information from their employer, two obtained information from family or friends, one person stated it was general knowledge, one participant obtained information from their service provider and two participants found information on Facebook.

Navigating the internet or other platforms after being a victim of cybercrime can be daunting. It may be difficult for victims to know who to approach to report a cybercrime. Participants were asked to select all of the places they had reported, and because victims may have tried to resolve a victimisation in more than one way, they were able to select more than one response. Most of the respondents reported the cybercrime to the bank which suggests the cybercrime experienced was a form of financial crime. According to an article by Chigada and Madzinga, 'cyberattacks and threats on [financial institutions] increased by more than 238% globally' between February and April 2020.[164] This is because of the increased use of online banking as opposed to face-to-face banking. Ransomware attacks also increased utilising phishing emails as the primary source.[165] It therefore follows that cybervictims of financial crime would approach their bank where they fell victim to financial cybercrimes.

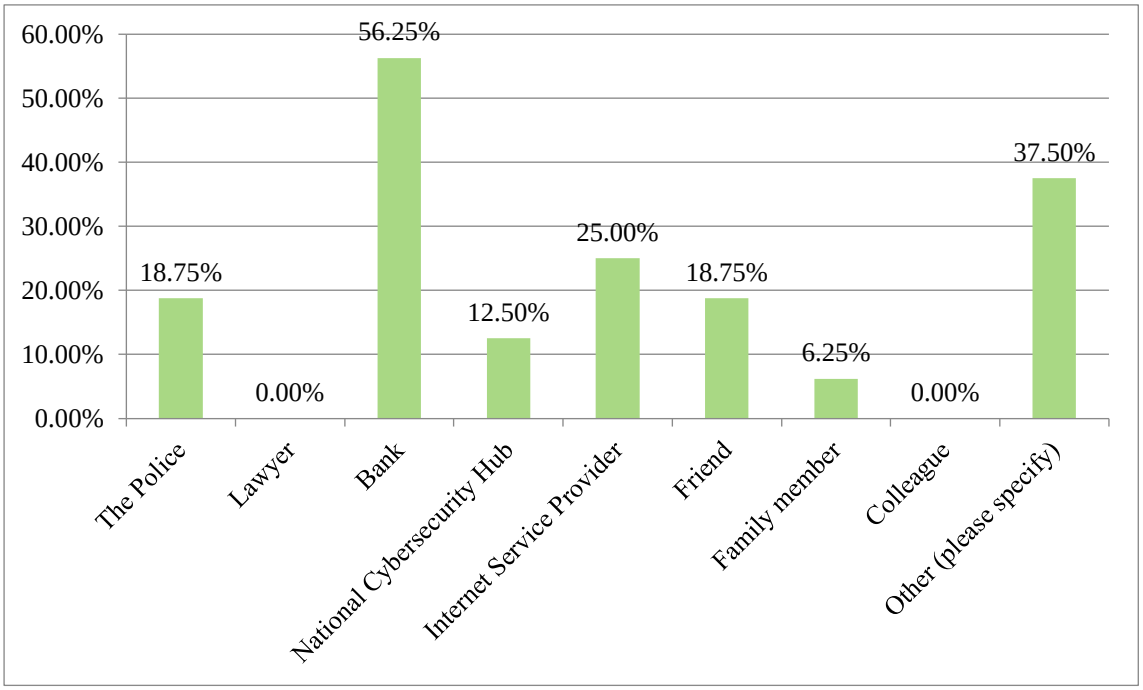
Only 19 per cent of the respondents reported the incident to the police. This, again, suggests that victims may not feel the police are well-equipped to deal with cybercrime or that the police would not treat the cybercrime as a serious offence. This appears to be a common thread with reporting cybercrime and is important because if victims do not feel comfortable reporting their cybervictimisation, there will be no cybercrimes to investigate and prosecute. In other words, the Cybercrimes Act will not be tested and we will not know whether the legislation is effective or not.

Although banks are well-placed to investigate financial cybercrimes that affect their customers, there are a host of other cybercrimes that do not necessarily have a financial impact. It is therefore important that victims see reporting to the police as a viable option. It is also

[164] Chigada & Madzinga op cit note 102 at 4.
[165] Ibid.

important to create awareness, at all levels of society, to designate who to turn to once a cybercrime has occurred.

Figure 14: Who cybervictims reported cybercrime to



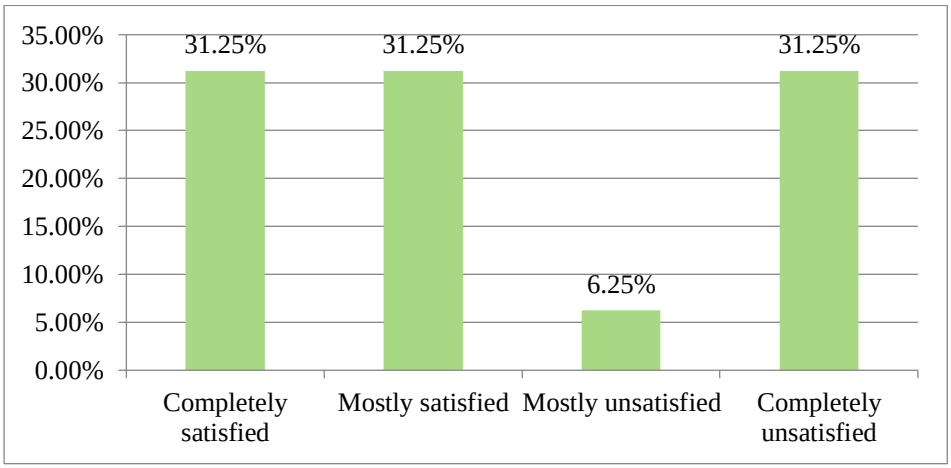
4.11. Did Authorities Take Incidents Seriously?

Equal numbers of participants answered "Yes" (*n*=7) and "No" (*n*=7) in response to the question about whether the authorities viewed the incident as a serious crime worth investigating. One participant felt the bank viewed the incident as a serious crime, but Facebook did not. In instances of financial crime, the cybervictims are likely to approach their bank which would take any form of financial fraud seriously as it could be a result of a breach of their systems. In other instances, however, cybervictims may approach the police for assistance and may not be satisfied with the response they elicit. This may be because police officers are insufficiently trained to deal with cybercrimes. The approach to a cybercrime is not necessarily the same as the approach to a face-to-face crime – there are no physical wounds which makes, for example, gathering evidence difficult. It is, however, important to remember that whether something is serious or not is subjective. What is serious to one person is not necessarily serious to another.

4.12. Satisfaction with Authorities and Reporting Future Cybercrimes

Sixteen participants responded to the question as to whether they were satisfied when they reported the crime to the authorities. The results indicate that most of the participants who responded to this question found some form of satisfaction in reporting cybercrime to the authorities. This may suggest that the authorities who investigated these cybercrimes were partially successful in responding to and remedying the cybercrime. This is important as it generates some positive feelings towards the authorities and indicates that some of them are equipped to deal with certain forms of cybercrime.

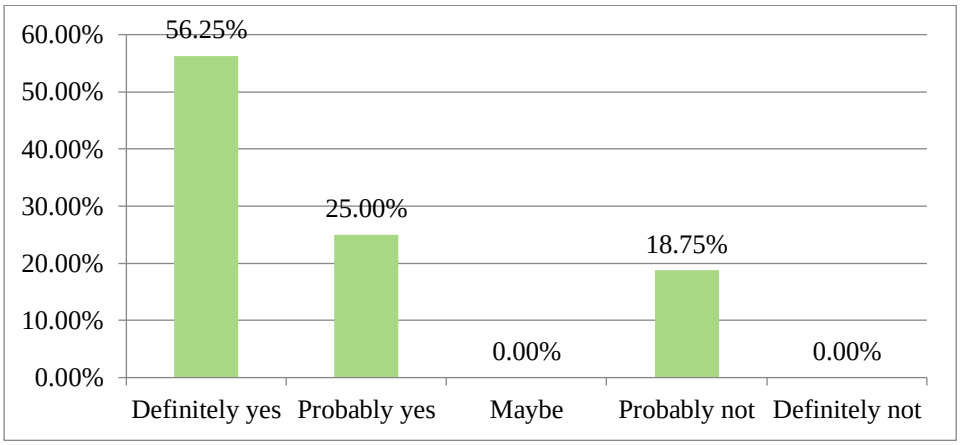
Figure 15: Satisfaction with authorities



Participants were asked whether they would report to the authorities in the future in the event they fell prey to cybercrime. It is important to be aware that this does not necessarily mean they will report to the police. In this study, "authorities" included banks, lawyers, internet service providers and the like. Of the 16 participants that responded, 81.25 per cent responded in the affirmative (*n*=13). However, as Figure 15 above shows, only 68.75 per cent responded that they found some form of satisfaction when reporting to the authorities (*n*=11). It appears that even where participants were completely unsatisfied with the results after reporting to the authorities, they would nevertheless report future cybercrimes to the authorities.

Research also shows that while people intend to report to the authorities after a victimisation, they may not actually follow through with doing so when an incident has occurred.

Figure 16: Reporting future cybercrimes



4.13. Cases That Were Not Reported

Figure 17 shows the range of reasons participants had for not reporting their cybervictimisation experience. The responses again indicate that the participants elected not to report to the authorities for reasons that would benefit themselves or prevent other individuals from becoming cybervictims. None of the participants indicated they did not report the crime because they did not want to get the cybercriminal in trouble – which is often the case in certain face-to-face crimes between family members or friends.

Most participants did not report as they felt, amongst other things, the police would not have helped (*n*=12). Only 18.75 per cent of the participants who reported to authorities elected to report to the police. Of the participants, 36.00 per cent responded they did not report as they dealt with the incident themselves (*n*=9). What comes through strongly in the research is that people are not confident in the police's ability to respond to or investigate their cybervictimisation experience. Almost half of the participants (48.00 per cent) said that the "police would not have helped". This comports with findings by Cross et al which showed that even members of the Australian federal and state police 'consistently reported lower confidence in their capabilities to respond to cybercrime.'[166]

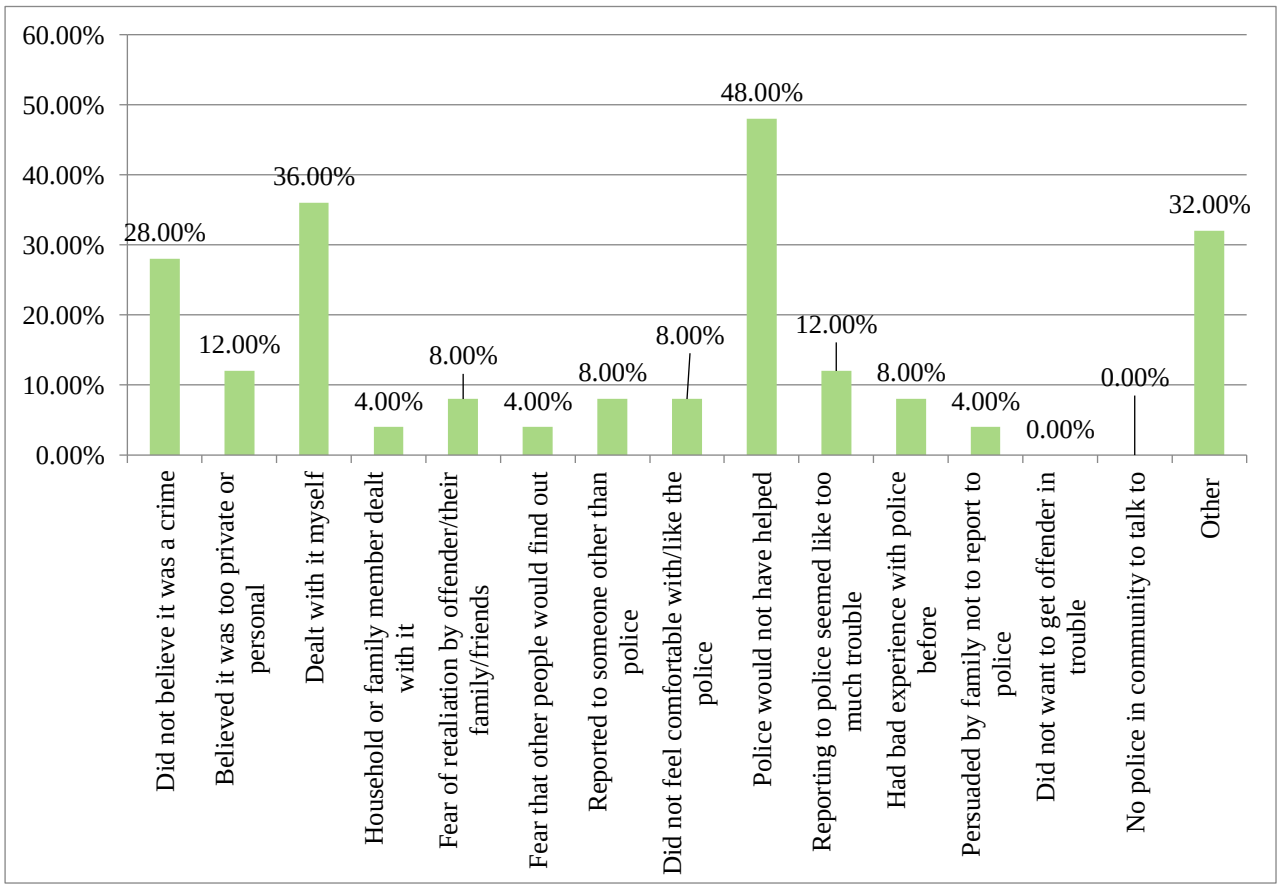
A number of participants did not report because they did not believe what had happened was a crime (*n*=7). This is not surprising as there are a variety of cybercrimes, and most people are not aware they exist. There are insufficient cyber-awareness programs in South Africa to alert people to the various forms of cybercrime and potential means of perpetration. While

[166] Cross, Holt, Powell & Wilson op cit note 10 at 13.

people may see things as scams, they may not realise they are in fact crimes in terms of legislation.

The "Other" reasons for not reporting included: the crime was not serious, police officers located in police stations did not know how to deal with cybercrimes, nothing came of the cybercrime, fear of consequences and conducting research to determine the cybercrime was a scam. The lack of confidence in the police and authorities was selected by almost half the respondents as a reason for not reporting and was also mentioned under "Other". This links back to the literature and indicates that the feeling in South Africa regarding confidence in the police corresponds with the feeling of cybervictims internationally. The comment that "police officers located in police stations do not know how to deal with cybercrimes" is problematic given the suggested process put forward by ISPA. The suggested process was discussed in more detail above, but it essentially places the onus on victims to prepare an affidavit outlining their victimisation experience and instructs them to liaise with the police officer on duty at the police station. Another interesting response was "fear of consequences". This could encompass fear of retaliation, fear of humiliation or fear of what others may think. This is not an uncommon feeling among victims of crime. Victims often feel that others may judge them or may even feel concerned that the criminal will retaliate if they are reported.

Figure 17: Reasons for not reporting



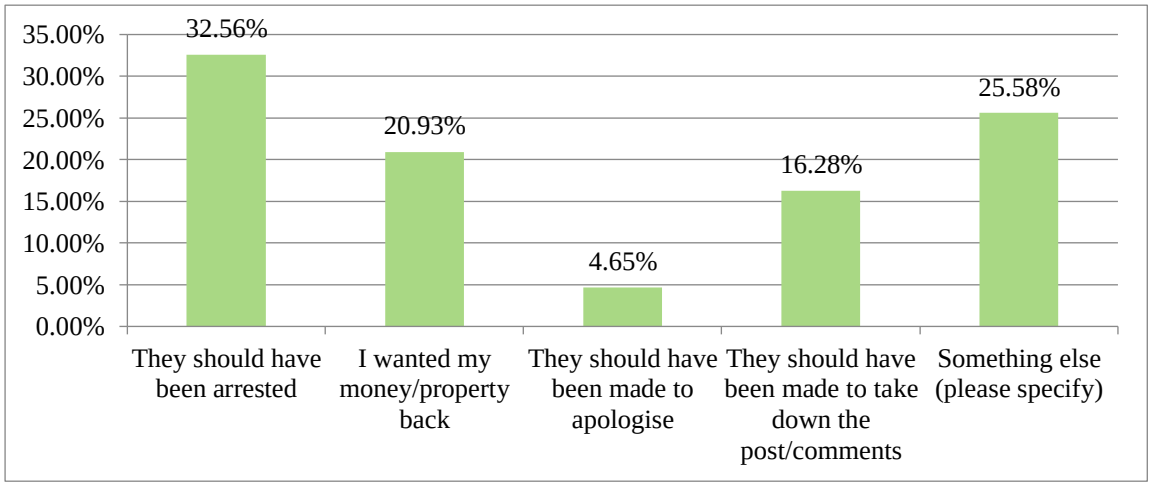
4.14. Recourse After Victimisation

Of the 44 participants who responded to the question about whether they wanted the offender to be punished, 79.55 per cent indicated the offender should be punished (*n*=35).

About a third of the 43 participants who answered the question regarding how the cybercriminal should be punished (*n*=14) responded that they wanted the offender to be arrested. About 25 per cent of the respondents provided other ways they wanted the cybercriminal to be punished, which included: "…to withdraw the bug", "stop contacting me on my number via WhatsApp", "restorative justice …", "funds be repayed, perpetrators should be sent to prison, with no access to any pc [sic]" and "they should be banned from accessing the site". Many participants simply wanted the cybercriminal to stop committing the cybercrime, while other participants felt the cybercriminal should be fined. Some simply wanted an acknowledgement of wrongdoing in the form of an apology. Interestingly, one participant responded, "… what happened does not seem serious or personal enough to warrant punishment".

The responses indicate a mixture of restorative and retributive justice. Some participants wanted things to go back to the way they were before the cybercrime, others wanted the cybercriminal to be punished. Some participants wanted both restoration and retribution.

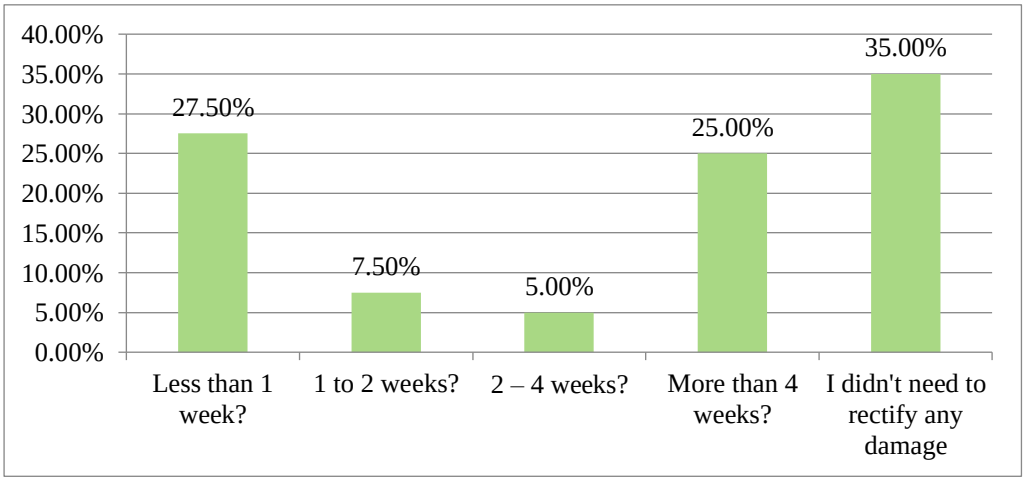
Figure 18: How should cybercriminals be punished



Depending on the type of cybercrime, victims may be plagued by the consequences for varying amounts of time. Participants were requested to indicate how long it took them to rectify the damage caused by the cybercrime. Most participants responded that they did not

need to rectify any damage (*n*=14). Where participants experienced a form of financial crime, it is likely that their bank would attempt to remedy the situation by reversing any fraudulent transactions. In other instances, however, cybercrimes may result in psychological trauma which could take months or even years to alleviate. This could mean a lack of trust in other individuals or deeper trauma where individuals were victims of cyberbullying. Where participants experienced phishing, they may not have responded or acted on the scam which meant they would not have suffered any damage. People either spent less than one week or more than four weeks rectifying the damage caused by cybercrime. This is, however, largely dependent on the type and severity of the cybercrime experienced. It may also be regarded as subjective. Some victims care more and would therefore expend more time and energy into rectifying the damage, dealing with the authorities to lodge a complaint and the like.

Figure 19: Rectification of damage caused by cybercrime

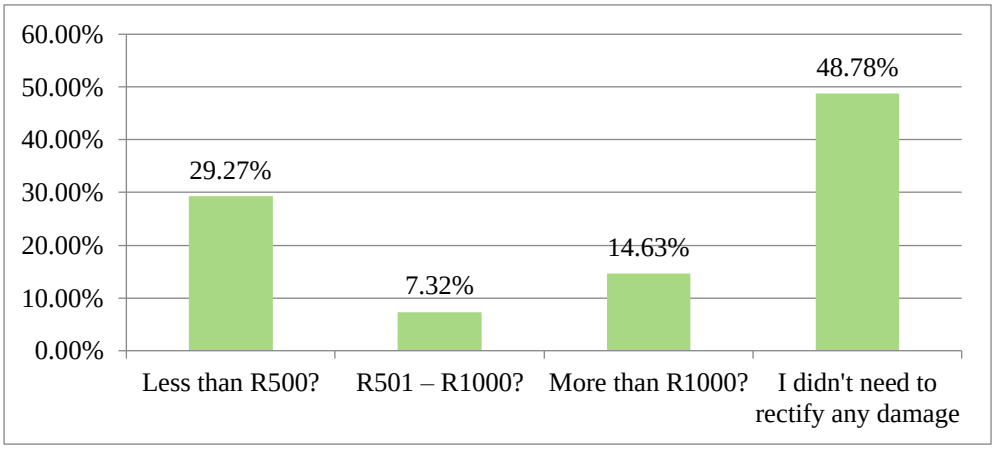


The cybercrime may also have had financial implications for the victim. This question does not pertain only to victims who suffered financial crimes, but also to those who were required to enlist the help of specialists to remedy the damages suffered. These specialists may include internet service providers or psychologists. None of the participants required the help of lawyers which suggests none of the cybercrimes were prosecuted.

Where victims incurred monetary costs, they either expended less than R500 or more than R1000 to rectify the damage caused by the cybercrime. As with the time spent rectifying the damage, the type and severity of the cybercrime would likely dictate how much money would need to be spent on remedying the situation. The cost would also differ depending on who the

cybercrime was reported to as some people or entities would charge money for the time spent investigating and assisting in remedying the cybercrime.

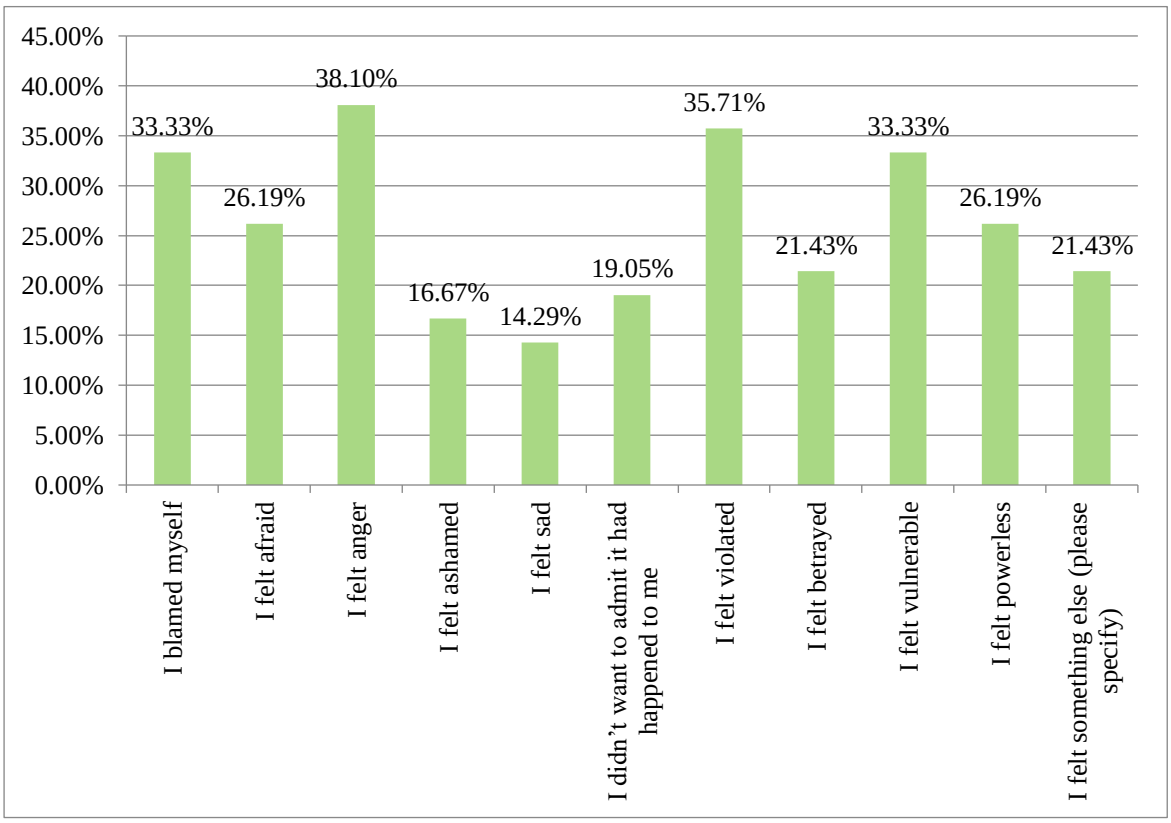
Figure 20: Cost to rectify damage caused by cybercrime



4.15. Post-Victimisation Experience

Participants were asked how they felt after they became aware they were a victim of cybercrime. Figure 21 shows that most people felt anger (*n*=16) and felt that they had been violated (*n*=15). Naturally, some participants felt that they were to blame (*n*=14).

Figure 21: Feelings after realising victim of cybercrime



Of the 42 participants who responded to the question about how they felt after they became aware they were a victim of cybercrime, 21.43 per cent felt "something else" (*n*=9). Of the participants that responded, "something else", four participants felt annoyed, two participants did not have any feelings about their cybervictimisation, one participant felt disappointed in humanity and one participant felt empowered that they were able to uncover the phishing scam.

The feelings expressed by the participants are not uncommon amongst victims of crime – be it face-to-face or virtual. Victims may have a sense that they could have done something to prevent their victimisation. They may also feel vulnerable, especially in the context of cyberspace and the fact that they may not know what to do or who to turn to for assistance to remedy the situation. It is also difficult to know what to do to prevent the incident from occurring again. There is, however, one upside to realising one has been a victim and having the feelings associated therewith – one is determined to ensure it does not happen again. This allows a victim to regain some sense of control after an experience of victimisation as they are able to put measures in place and shift their focus from the negative feelings.

4.16. Post-Victimisation Behaviour Change

Participants were asked whether they noticed any changes in their behaviour since their cybervictimisation and 42 responded. Most participants became more protective of their belongings/information/family/friends as they wished to protect them from experiencing the same thing and to prevent future incidents from occurring.

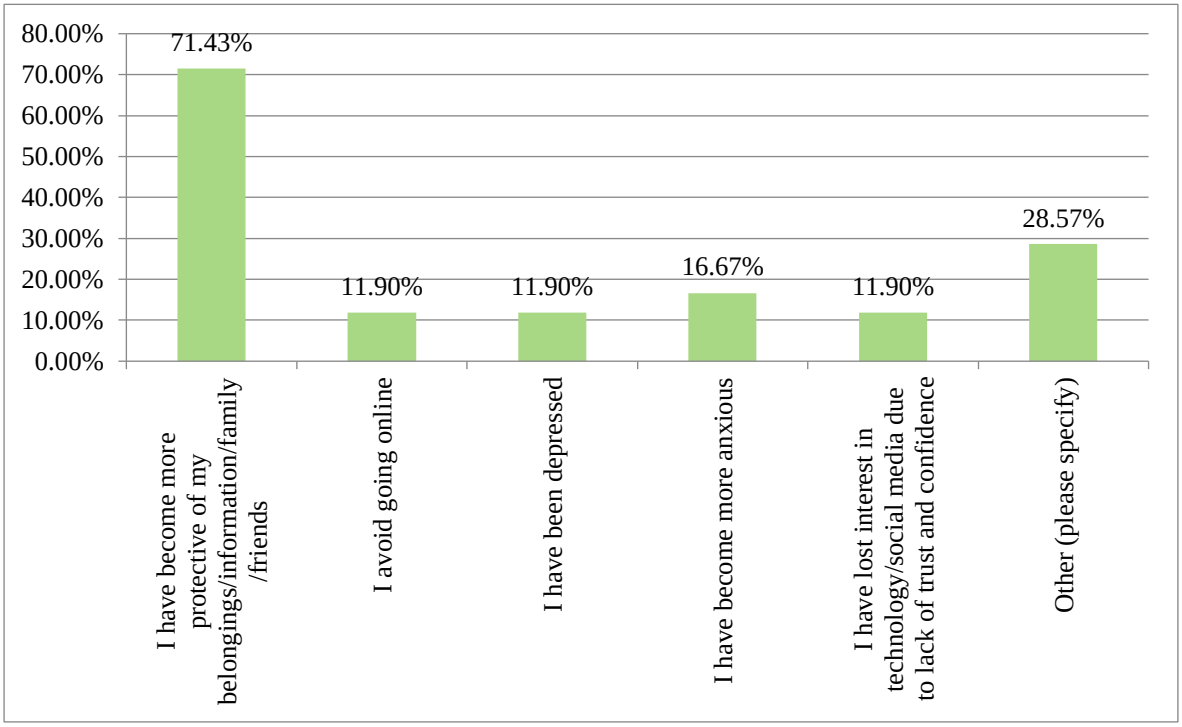
Of the 12 participants (28.57 per cent) that responded "Other", five participants did not experience any behavioural changes. The remainder said that they have become more guarded and no longer respond and/or immediately block potential scams. One participant reported they have become completely reclusive, another reported they became much less active online and one participant reported they utilised cybersecurity more frequently. These are all natural responses to victimisation.

There is not a wide range of literature on the effect of cybercrime on victims and the recovery time associated with cybercrime. Previous studies indicate that 'victims suffered from psychological and financial harm even years after the incident.'[167] In addition, 'anecdotal

[167] Jansen, J & Leukfeldt, E.R. 'Coping with Cybercrime Victimization: An Exploratory Study into Impact and Change' (2018) 6:2 *Journal of Qualitative Criminal Justice & Criminology* 205 at 208.

evidence is provided by Cross et al.'s (2016) study that reported long-term emotional effects of some of the victims they interviewed.'[168] This is indicative that the effects of cybercrime differ from victim to victim and that they are no less serious than the effects of face-to-face crimes. Victims who experience the same form of cybercrime may have different reactions and recovery times.

Figure 22: Changes in behaviour after cybervictimisation



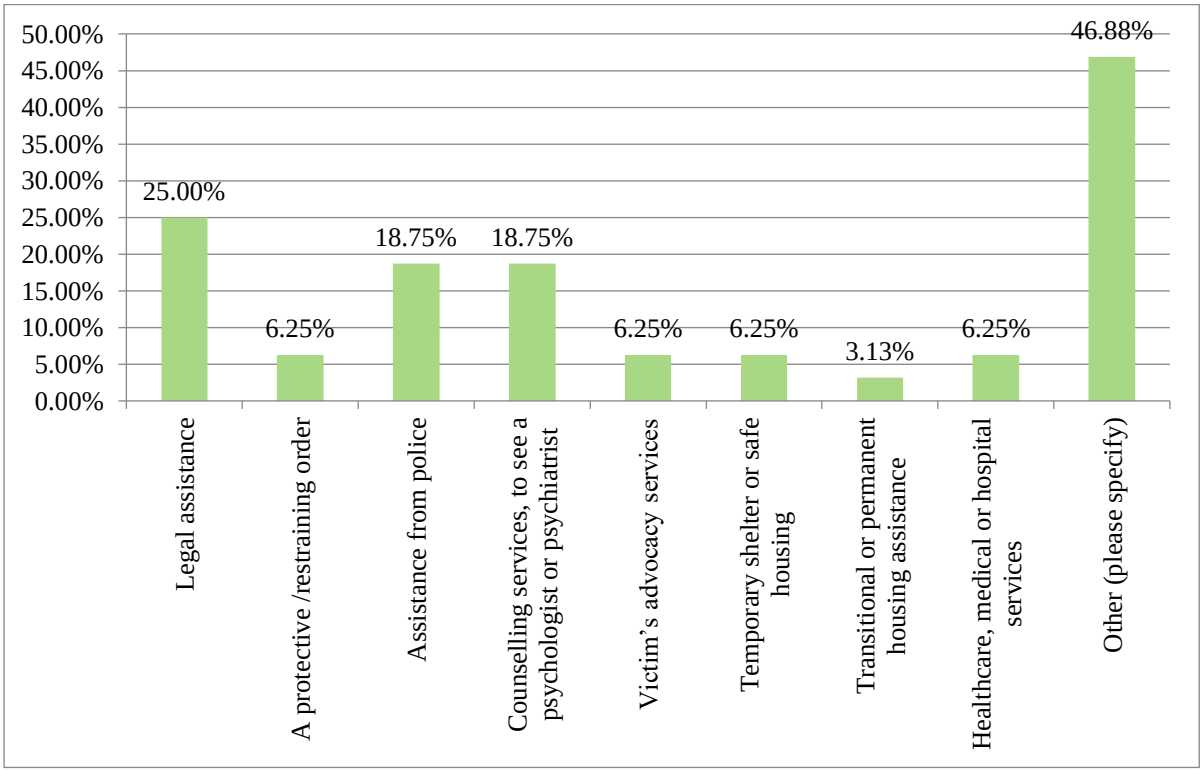
Victims may need some form of support to recover after a victimisation. One quarter of participants said that they needed legal assistance, however, none approached a lawyer to report the cybercrime, nor did they spend in excess of R1000 on legal services to rectify the damage caused. Roughly 6 per cent of respondents required a protective or restraining order pursuant to their cybervictimisation. It is unclear whether or how these orders were granted given that the provision of the Cybercrimes Act that provides for protective orders in instances of digital intimate partner violence is not yet in force.

Of the 32 participants that responded to this question, 46.88 per cent responded "Other" (*n*=15). Seven of these participants did not require any assistance, two responded they required better cybersecurity or anti-virus software, one responded they required police assistance and

[168] Ibid.

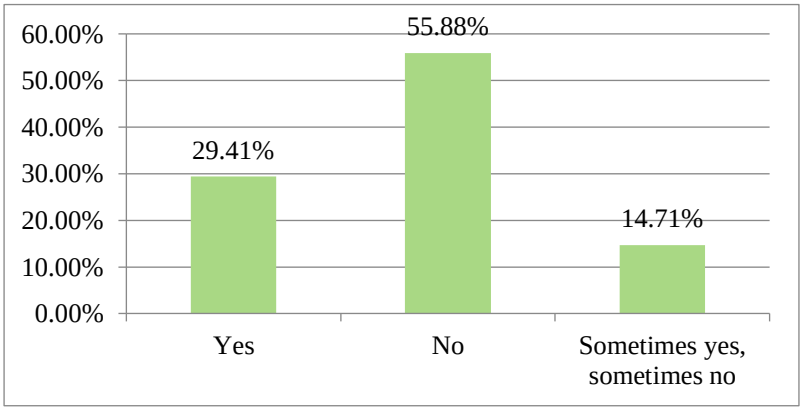
one responded they required a paid email address. One participant also stated they did not access any services as they questioned whether their victimisation was their fault. Research indicates that it is quite common that victims elect not to report or seek assistance in instances of self-blame as they feel that others will say the incident was their fault and will not be prepared to help.

Figure 23: Services required because of cybercrime



I was interested in whether participants received the services they needed after their cybervictimisation experience. Of the 34 participants that responded to this question, one participant responded that their mobile network provider refused to assist and they did not wish to approach the police, one participant stated they had nowhere supportive to report their experience to discuss realistic options available to them, three participants did not require any services, one participant responded that they did not seek out any services, another responded they did not wish their experience on anyone else and another responded that education is vital as jurisdictional issues make cybercrimes extremely complex.

Figure 24: Did cybervictims receive the services needed

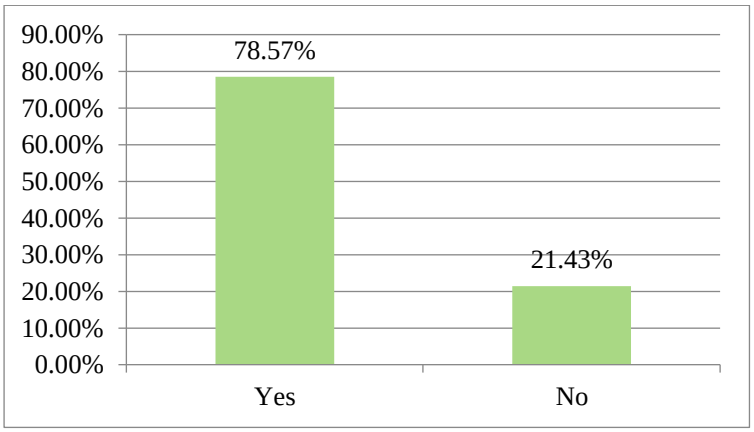


Overall, it seems that participants either did not require any services after their experience or were unable to access the relevant services as they did not know who to approach for help. This again comes back to the lack of cyber-awareness in South Africa. There are insufficient resources to assist victims of cybercrime and what makes these scarce resources harder to access is the lack of publicity surrounding them. People fail to understand that just because the victim was not physically assaulted, does not mean the experience had any less of an impact on them. They still require assistance from the state or private institutions to work through and recover from their experience. It would also be helpful to teach them ways to safeguard themselves from further incidents as opposed to victims feeling the need to isolate themselves on social media.

4.17. Awareness of Other Cybervictims

Almost 79 per cent of participants confirmed they know someone else who has been a victim of cybercrime (*n*=33). This speaks to the prevalence of cybercrime. More and more people are becoming aware of others who have had brushes with cybervictimisation. This may also mean that people are starting to talk about their victimisation experience. This is a positive as it suggests they are dealing with the incident by talking about it with others and getting their feelings out into the open – which is a form of support for victims.

Figure 25: Aware of any other victims of cybercrime



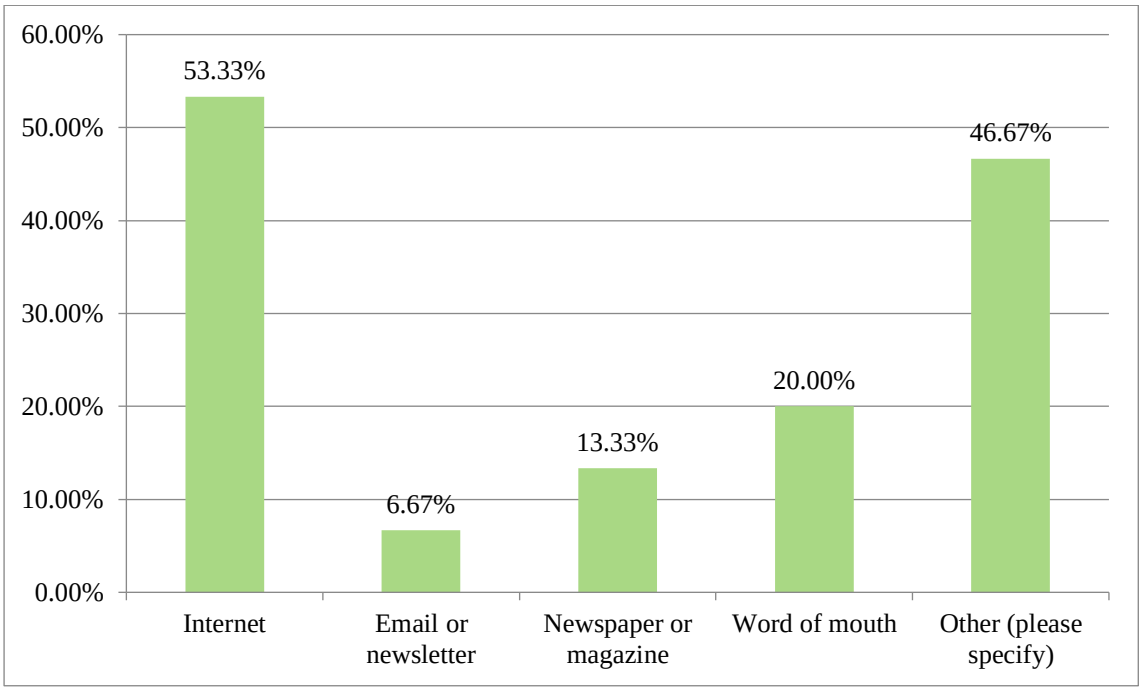
A sizeable proportion of the respondents knew more than one other victim of cybercrime. The most common response to this question was "multiple" or "too many to recall". This speaks to the prevalence and lack of safeguards in place to protect individuals from cybercrime. Seventeen participants confirmed they knew between one and five other cybervictims and twelve participants confirmed they knew more than five other cybervictims.

4.18. Knowledge of the Law

One of the survey questions enquired whether participants were aware of which laws protect people from cybercrime. Of the 42 participants that answered, just over a third answered "Yes" (*n*=15) and 64.29 per cent answered "No" (*n*=27). The participants who knew about the law mostly reported they found out about it at their previous workplace, as a result of their education – either at university or at school. One participant seemed to have information from the "Act" itself.

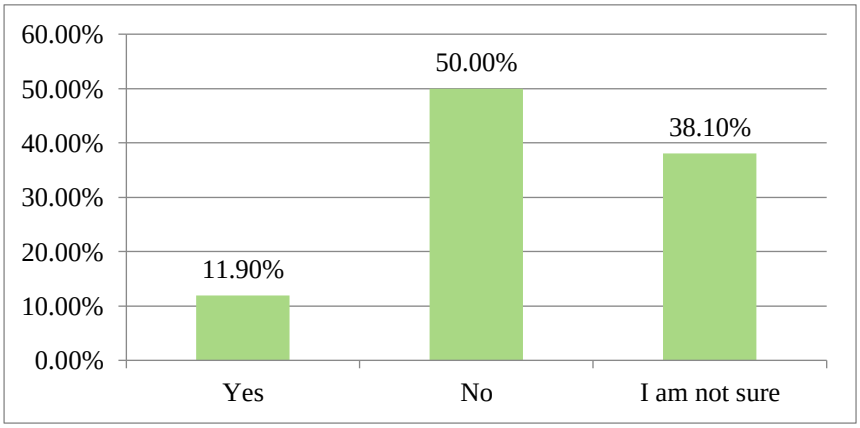
While many companies appear to have some form of cybersecurity in place to protect their data and systems, many do not educate their employees as to the threat cybercrime poses or the risky behaviours that may result in cybercrime. Schools and tertiary education institutions in South Africa facilitate cyber-awareness workshops for their educators and employees and it seems the educators pass this knowledge on to their students. Most South African universities also offer courses in Cyber Law to educate students on cybersecurity and the legislation currently in place. This is relevant given the number of students who were in the sample.

Figure 26: Knowledge of laws that regulate cybercrime



Most of the participants did not think that the existing South African laws were sufficient to deter and/or punish cybercriminals (*n*=21). A sizeable portion (*n*=16) responded that they were unsure, and only five participants felt that the laws were sufficient.

Figure 27: Are existing laws sufficient to regulate cybercrime



It is likely that those who were unsure do not know the laws in place to regulate cybercrime. Even if the legislation is sufficient to regulate cybercrime, not enough is being done to prosecute these crimes, which automatically renders the legislation ineffectual. As many of the participants felt unsatisfied with the authorities after reporting the crime, it is unsurprising that

many of them deem the legislation insufficient. Notwithstanding the fact that there is a framework to govern and regulate cybercrimes, participants still appear to be unsatisfied with the resulting remedies. Whether this issue lies with the legislation, or with its implementation (in the initial investigation of the crime or the subsequent prosecution) is unclear.

4.19. Summary of Data

The data gathered confirms much of what was discovered in previous studies. There are, however, aspects that are particularly important in respect of cybercrime victimisation in South Africa. These aspects will be summarised below.

It is important that people understand that just because you do not share any personal information online, does not mean you will not be targeted by cybercriminals. In other words, even though participants shared very little to no information online they evidently still became cybervictims.

It is difficult to definitively say that participants were targeted by cybercriminals because they utilised free online software or apps. While this may have comprised part of their risky online behaviours, one cannot confirm there was a correlation between their use of the software and their subsequent victimisation.

People spend the most time per week engaging in instant messaging and the least time per week engaging in chat rooms. Instant messaging could be utilised for personal or professional use which explains why it is engaged in most frequently. People often assume they will be safe utilising instant messaging platforms because they can control and manage who they interact with. They are therefore unlikely to have their guard up when engaging with individuals via these platforms and will likely be more willing to disclose personal or confidential information even though they cannot verify who is on the receiving end of the information. This can be dangerous.

The most common types of cybercrime were random and not targeted attacks. In other words, the cybercrime was not aimed at disrupting a specific individual's life. This is not to say that targeted attacks do not occur. One respondent in this survey was the victim of a targeted attack in which intimate nude photographs were leaked. It is important to mention that the provision of the Cybercrimes Act that would permit the victim to obtain a protection order

against the offender, the cybercriminal, is not yet in force. The legislative measures currently in place would therefore not be sufficient to deter or punish the offender.

People are always "connected". When at work, they are likely on computers for most of the day and when they get home, they are likely on their cell phones. Cell phones are the most frequently used form of technology, which is unsurprising. People are always "switched on" as they seldom shut down or switch off their cell phones – which carry so much of their lives. They are therefore constant targets for cybercriminals.

Participants engaged in various activities before their victimisation. The top two activities were opening any file attached to emails and communicating with strangers online. The former is typically associated with their professional life and the latter with their personal life. One may assume that communicating with strangers online is a sure-fire way to becoming a victim of cybercrime, but this is not necessarily the case. Many emails contain attachments or links to infected sites or require you to input a password before accessing a document. As previously stated, individuals may be more trusting of emails because they purport to be from trusted sources. It is therefore important to double check the details of the sender before acting on any email.

More than 50 per cent of participants did not report the cybercrime. Based on the literature, this response was to be expected. There are a range of reasons why victims do not report, the main reason being that the "Police would not have helped". When victims did report to the authorities, the main reason was "I believed it was a crime and that all crime should be reported". These reasons link to the most common reasons selected by participants in other studies.[169] Approximately 82 per cent of victims reported the incident because they believed it was a crime. This indicates that there is some form of awareness as to what constitutes a cybercrime.

More than 56 per cent of victims reported the incident to their bank which indicates they likely suffered some form of financial cybercrime. Only 18.75 per cent reported the incident to the police. This is likely because of the overwhelming feeling that the police would not have helped.

[169] Leukfeldt, E.R, van de Weijer, S.G.A & Van Der Zee, S 'Reporting cybercrime victimization: determinants, motives, and previous experiences' (2020) 43:1 *Policing: An International Journal of Police Strategies & Management* 17.

Most participants found information on who to report to on the internet or social media. People tend to look for answers at the site of victimisation. For example, if it was a financial cybercrime that occurred it is likely that the victim approached their bank for assistance.

There was an equal split as to whether the authorities viewed the incident as serious or not. This is, however, subjective which means that perceptions of the treatment received may differ from victim to victim. A majority of participants experienced some form of satisfaction when they reported the incident to the authorities. It is important to be cognisant that in this survey, "authorities" included police, banks, internet service providers and the National Cybersecurity Hub. Most participants (81 per cent) confirmed they would report cybercrimes in future. Whether this is true, however, remains to be seen. The vignette studies conducted by Leukfeldt et al indicated that while people intend to report incidents of victimisation, they do not always follow through.[170]

Most respondents felt that the offender should have been arrested. Many respondents also wanted the cybercrime perpetrated against them to stop.

Most respondents indicated that they did not need to rectify any damage caused by the cybercrime. A large number indicated they required less than one week while others indicated they needed more than four weeks. These results were reflected in the costs expended to rectify the damage caused by the cybercrime. While most participants stated they did not need to rectify any damage, others indicated they spent less than R500 or more than R1000. It is likely that the time needed to recover and the costs expended to rectify the damage are largely dependent on the form of cybercrime suffered.

Upon realisation that they had been victims of cybercrime, victims reported a host of emotions. The most common emotions were anger, feeling violated, feeling vulnerable and feelings of self-blame. De Kimpe et al state that feelings of self-blame are often linked to control and that although 'self-blame is traditionally considered to be a negative reaction, it is also recognized as beneficial to some extent.' [171] Essentially, victims feel confident about ensuring they minimise the behaviours that led to their victimisation in the first place. They feel empowered that they have some sense of control again. The downside to self-blame, however, is that victims are reluctant to report their victimisation.

---

[170] Ibid at 16.
[171] De Kimpe, L, Ponnet, K, Walrave, M Snaphaan, T & Pauwels, L 'Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims' (2020) 108 *Computers in Human Behavior* 106310 at 4.

The main change in behaviour after victimisation is that victims become more guarded and protective of their personal information to mitigate the risk of future victimisation.

Most victims responded that they did not receive the services they needed pursuant to their cybervictimisation. This may be because of a lack of access or not knowing who to approach. In any event, more should be done to create awareness of the services and support available to victims of cybercrime.

Almost 80 per cent of the participants knew other people who were victims of cybercrime. The most common response was that they "knew too many to recall". This is not a good thing as it indicates that incidents of cybercrime are on the rise. On the other hand, however, it may show that there is a wider conversation on the topic of cybercrime and that victims were seeking support by confiding in others.

Most respondents were not aware of the laws regulating cybercrime but those that were aware predominantly obtained their information from the internet, the workplace or their educational institutions. Overwhelmingly, participants either felt the laws were insufficient or were uncertain as to their efficacy (cumulative total of 88.10 per cent). This response essentially answers the second part of the research question. The results seem to indicate that the current legislative framework in South Africa is not equipped to deal with the issue of cybercrime.

5. CHAPTER 5 – DISCUSSION

Overall, participants felt that more should be done to create awareness about how cybercrimes are perpetrated, and more services should be offered to victims. One participant stated "Getting scammed is fast. Rectifying the effect is very slow if at all. … Laws protect the perpetrators more than the victims." There is a sense of anger and resignation in this statement. The victim is left to pick up the pieces after their experience and often feels that it is impossible to get justice. It is evident that more should be done to assist them at every stage of their experience.

There is a wealth of information online, but this is only accessible when searching for specific phrases or material. Even then, the volume of information is likely to overwhelm individuals who have already been traumatised by their experience. The fact that information is not simply presented and readily ascertainable makes finding resources on, among other things, who to report to another daunting aspect for cybervictims.

The survey results suggest that where individuals are victims of financial crime, they can approach their bank which attends to most of the investigation and attempts to remedy the situation by reversing fraudulent transactions, where possible. However, it is remarkably clear that the same is not applicable to victims of other forms of cybercrime. Individuals do not know who to approach to investigate and resolve their issues, which makes an already traumatic experience even more demoralising. People do not appear to have faith in the police to investigate cybercrime and seem to believe they would be turned away as a result of their cybercrime experience not being deemed "serious enough". This needs to be addressed as people should be aware of the institutions they can appeal to for help. Even if they do not approach the correct institution from the outset, they should be pointed in the direction of someone who will be able to assist.

The response to cybercrime also appears to be fairly uniform amongst the participants. Most block the potential scammer immediately and become more protective of their information. This is to prevent further attempts by offenders and to safeguard their family or friends from experiencing the same thing. In severe cases, individuals may become completely reclusive and stay off all forms of social media. Another way individuals try to safeguard themselves and others is by reporting any scams they come across on the various social media platforms. Further research would be required to ascertain whether reporting the scammer has a positive effect on reducing cybercrime on platforms or whether it simply results in a new fake account popping up to attempt to scam users.

Whether the current legislative framework in South Africa is actually equipped to deal with the issue of cybercrime also warrants further research. The findings from the study are not sufficient to determine whether the current legislative framework in South Africa is sufficient to regulate cybercrime, whether it provides for prosecution and whether the legislation deters cybercriminals from offending. These are important questions.

This study shows that most people are not aware that there are laws to protect people from cybercrime. It therefore makes it difficult to determine whether the laws have a positive effect on the regulation of cybercrime. Where individuals were aware of the legislation, they found out about it on the internet. While it is useful to have this information on the internet, many individuals will not understand the different forms of cybercrime criminalised in terms of the Cybercrimes Act, nor will they understand the penalties associated with these crimes. This needs to be explained to them in a manner that is easy to understand and free from legal and technical jargon. It is important to note, however, that cybervictims may be reluctant to engage in online activities such as researching various forms of cybercrime and penalties, when they have already been victimised online. Other methods should therefore be utilised to create awareness.

Section 52(1) of the Cybercrimes Act empowers the National Commissioner to 'establish or designate an office within existing structures of the South African Police Service to be known as the designated Point of Contact …'.[172] Despite certain sections of the Cybercrimes Act commencing on 1 December 2021, the commencement date for section 52 is yet to be proclaimed. This creates further uncertainty as the Act, which is supposed to provide guidance on what to do and where to report in instances of cybercrime, fails to adequately inform individuals of their rights. The fact that this section of the Cybercrimes Act is not yet in force speaks to the insufficient capacity, resources and training available to SAPS when dealing with cybercrimes. Ahmore Burger-Smidt, Director and Head of Data Privacy and Cybercrime practice at Werksmans, notes that 'some of these crimes are difficult to investigate because the perpetration of the illegal act is "by no means computer-dependent but merely computer-

[172] Section 52(1)(a) of the Cybercrimes Act 19 of 2020. In addition, section 52(3) provides that the "designated Point of Contact must ensure the provision of immediate assistance for the purpose of proceedings or investigations regarding the commission or intended commission" of various offences under the Cybercrimes Act.

enabled".'[173] In other words, many of the crimes use computers to carry out other crimes.[174] They do not depend on computers or networks but utilise the internet or technology to take these crimes to another level. Cyber-dependent and cyber-enabled crimes can occur anywhere to anyone who has access to and makes use of technology. An important aspect in the fight against cybercrime is to ensure police officers are adequately trained and resourced to detect, investigate and combat cybercrime. This should be a first step when it comes to implementing the legislation. The absence of appropriately trained and resourced personnel defeats the purpose of (what is said to be) world class legislation.

The perception that the police are not equipped to fight crime, including cybercrime is not new, yet little has been done to change the public's views. This should be priority as without investigation and evidence, there can be no prosecution. This does nothing to demonstrate that cybercrimes are serious crimes worthy of punishment that will be treated as such by the authorities. Perhaps, as an alternative to SAPS being solely responsible for the investigation of cybercrimes, other government organisations independent of SAPS should be established to assist SAPS with the reporting and investigation aspects of cybercrime. Partnering with other organisations or quasi-governmental bodies, may alleviate concerns regarding SAPS capabilities to adequately deal with cybercrime and could result in increased reporting of cybercrimes. Collaborating with other entities will increase the manpower and resources available to investigate cybercrime. There are some private companies that offer cybersecurity services such as G4S, IBM, Symantec and PWC.[175] These cybersecurity services are, however, generally provided to companies, not individuals.

Du Toit, Hadebe and Mphatheni point out that 'more than two-thirds of countries in Europe report sufficient legislation, the picture is reversed in Africa, the Americas, Asia and Oceania, where more than two-thirds of countries view laws as only partly sufficient or not sufficient at all.'[176] This sentiment is echoed by this study's data which shows only 12 per cent of participants thought South Africa's existing laws are sufficient to deter cybercriminals.

Research indicates that cybercriminals are more likely to target people who are easily deceived and those who are inexperienced or trusting. Research conducted by Joseph Aghatise

---

[173] Moyo op cit note 139.
[174] Alvarez, R 'Cyber Enabled Crime vs. Cyber-Dependent Crime' 2 September 2021 *IP Probe* available at https://ipprobe.global/2021/09/02/cyber-enabled-crime-vs-cyber-dependent-crime/, accessed on 6 December 2022.
[175] Button, M 'The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions' (2020) 36:1 *Journal of Contemporary Criminal Justice* 39 at 44.
[176] Du Toit, Hadebe & Mphatheni op cit note 52 at 112.

found that older people were more trusting of content – such as websites and spam emails – which could make them more susceptible to cybercrime.[177] This is also true of younger children. A sizeable portion of respondents who had been victimised in this study (roughly 25 per cent) were 56 years of age or older. It is therefore important to implement cyber-awareness campaigns that target all ages in society – in particular the younger and older individuals. These campaigns should alert individuals what to look out for when utilising online platforms and provide ways to improve cybersecurity. Previous research has indicated that young and old internet user groups are more vulnerable to cybercriminals because they are too trusting and are less likely to have sufficient cybersecurity measures in place.[178] This is akin to traditional crimes where the youngest and oldest members of society are targeted because they are viewed as soft targets and easier to manipulate than other individuals.

The data collected in this study echoes the results of a vignette study conducted by Leukfeldt, van de Weijer and Van Der Zee showing that the most common reasons for not reporting cybercrime to the police were that people thought they would solve it themselves or that there was no point in reporting because the police would not do anything about the crime.[179]Although this study did not interrogate the reasons people did not report, it is likely that this may stem from people's previous negative interactions with the police and a general lack of legitimacy for the police. Respondents may also be unaware that the police have been tasked with investigating cybercrime in terms of the Cybercrimes Act. The fact that respondents felt more comfortable to deal with the incident themselves as opposed to getting police assistance shows that there is important work to be done in bridging the victim-police relationship.

Prevention initiatives that target cybercrimes are important. These activities include internet-based campaigns raising awareness about the risks of cybercrime. Another approach is to focus on detection and investigation. This entails working to identify victims of cybercrime and bringing the cybercriminals to justice. A third approach is to focus on victim support. Many participants stated they did not feel there was enough support for cybervictims. Public and private institutions should be more vocal about the help and support available to victims of cybercrime. This would also serve to bolster the notion that cybercrimes are serious crimes that should be reported and prosecuted. A multi-pronged approach which covers the

[177] Aghatise, J 'Cybercrime definition' (2014) available at https://www.researchgate.net/publication/265350281_Cybercrime_definition, accessed on 8 December 2022.
[178] McGuire & Dowling op cit note 9 at 19.
[179] Leukfeldt, van de Weijer & Van Der Zee op cit note 169.

diverse strategies listed above would be most effective in combatting cybercrime. Lipton argues:

> 'In global online communities, laws must interact with other regulatory modalities to achieve a comprehensive approach to combating abuses. … Legislators and judges will learn much from observing the development of market solutions, technological solutions, and emerging social norms that impact online behavior. … Public education, through news stories, and publicly or privately funded education initiatives, is also an important part of the framework.'[180]

It is important that all spheres of society work together to find means to guard against cybercrime and, where unable to do so, implement justifiable sanctions to appropriately remedy the issue. This could have a positive effect on deterring cybercriminals and may be the key to a notable decrease in the perpetration of cybercrime.

There are a number of tips individuals can utilise to protect themselves and guard against cybercrime:

i. Individuals should be wary of unsolicited electronic communications, particularly requests for personal information.
ii. Do not click on unfamiliar links or download unknown attachments in emails.
iii. Do not share passwords or access public Wi-Fi networks.
iv. Before making any online purchases or payments, conduct research to verify the merchant site and bank details.
v. Ensure all electronic devices have anti-virus software – which should be updated regularly to avoid breaches.
vi. Do not believe offers that seem too good to be true, conduct research to ascertain authenticity before acting.

In the light of developments in, particularly, the cryptocurrency and fintech space, it is important to ensure the Cybercrimes Act can be implemented effectively by the relevant authorities. Failure to do so will likely result in, amongst others, egregious financial crimes being committed by bold cybercriminals.

[180] Lipton, J 'Combating Cyber-Victimisation' (2011) 26 *Berkeley Technology Law Journal* 1103 at 1141.

It is evident that more resources are required to effectively tackle the issue of cybercrime. Kshetri states:

> '… organizations must increase investment in cybersecurity technologies, provide cybersecurity-related training to employees and appoint professionals such as CISOs. It is also important to create cybersecurity awareness among consumers.'[181]

Cyber awareness should start at school level. Learners should do mandatory cyber-wellness courses or modules to ensure learners – where each learner is likely to have a cell phone – are aware of the pitfalls of the internet and potential scams. Future research should consider cybercrime amongst minor children, specifically primary (grades 4 to 7) and high school (grades 8 to 12) learners, as well as the elderly (65 and older). These are vulnerable groups of society who probably do not have the best cyber practices in place to guard against cybercrime. Cyber-wellness should also be a focus at all levels of society. In other words, more should be done to create awareness about the common pitfalls of cyberspace, how to prevent the likelihood of becoming a cybervictim and what to do in the event you have fallen prey to a cybercriminal.

In addition, perhaps the police – who are mandated by the Cybercrimes Act to investigate cybercrimes – should work alongside private institutions to investigate cybercrime and apprehend cybercriminals. The private institutions will have access to more resources and personnel who would have the skills to assist the police in their tasks. This may serve to boost confidence in their ability to investigate cybercrime, which may result in increased rates of reporting. It is important to remember that cybervictims need to report their victimisation as the police will not be in a position to investigate when they are not aware a crime has occurred. Moreover, perhaps a hotline dedicated to victims of cybercrime should be established so they feel they have a place to turn to and someone to report to in the event of an incident. This may serve to increase reporting rates and will offer the cybervictims a modicum of support.

The cybercrime landscape is constantly evolving. We learn more and more about the methods cybercriminals may use to commit an offence and we accordingly have to adapt the existing cybersecurity strategies in place to counteract these new methods. The only way to effect major change in the statistics is to ensure all levels of society are informed and do their part to combat cybercrime. This means that governments should afford the authorities in charge of policing cybercrime more resources. It means that cybervictims should come forward and

---

[181] Kshetri, N 'Cybercrime and Cybersecurity in Africa' (2019) 22:2 *Journal of Global Information Technology Management* 77 at 80.

report their victimisation. Only in doing so, will the current legislative framework be useful. Until there is co-operation, the incidents of cybercrime will continue to rise and the current legislative framework will remain insufficient in tackling the growing spectre of cybercrime.

6. CHAPTER 6 – CONCLUSION

6.1. Key Contributions of the Research

This research provides valuable insights into the cybercrimes most commonly suffered by South African victims of cybercrime, victims' feelings towards the authorities and whether victims think the legislation actually helped them and provided them with a remedy pursuant to their cybervictimisation. This research complements the existing research on cybercrime victimisation both nationally and internationally by providing South African victims' perspectives, which is something that has not really been dealt with before.

6.2. Limitations of this Study

One of the main limitations was that the sample was fairly small. While individuals from five out of the nine provinces participated in the survey, it is important to note that the results cannot be used to generalise and make assumptions about the population of South Africa as a whole. Perhaps there would have been a higher response rate and sample if the survey had been conducted online and in person. While some people might have felt embarrassed to share their experiences face-to-face, others might have felt more comfortable knowing who was handling their data. Some people are also more forthcoming when telling a story in person. Given that the participants already experienced a form of trauma online, they may have been reluctant to click on a link especially when they did not know the person who would be handling their sensitive data. While this may have had implications for the confidentiality aspect of the research, there are mechanisms available to address this.

6.3. Recommendations for Future Research

There is so much more that needs to be done in relation to cybercrimes, cybervictims and cybercriminals in South Africa. One of the main aspects I picked up while conducting this research is that there is not much literature on the long-term effects of cybercrimes on victims, particularly victims of targeted cyber-attacks. Future research should also consider cybercrimes from SAPS perspective – do they feel equipped to tackle the issue of cybercrime and are they aware of the offences contained in the legislation.

The nature of cybercrime is that it is constantly evolving which means there are constantly new avenues and perspectives to explore and consider. To be effective in combatting cybercrime, we need to interrogate these different perspectives so that we can have a holistic view of the ever-changing cyber landscape.

BIBLIOGRAPHY

Primary Sources

Cases

Barclays Western Bank Ltd v Creser 1982 (2) SA 104 (T).

Carolissen v Director of Public Prosecutions 2016 (3) All SA 56 (WCC).

Fourie v Van der Spuy and De Jongh Inc. and others [2019] JOL 45848 (GP).

Jafta v Ezemvelo KZN Wildlife (2008) (10) BLLR 954 (LC).

Msomi v S [2019] ZAECGHC 80 (ECG).

Ndlovu v Minister of Correctional Services and another (2006) 4 All SA 165 (W).

S v Ebrahim [2020] JOL 49106 (KZD).

S v Mosia [2020] JOL 47966 (FB)

S v Ndiki and others (2008) 2 SACR 252.

Statutes

South African

Child Justice Act 75 of 2008.

Correctional Services Act 111 of 1998.

Criminal Law (Sexual Offences and Related Matters) Amendment Act 32 of 2007.

Criminal Law Amendment Act 105 of 1997.

Criminal Procedure Act 51 of 1977.

Cybercrimes Act 19 of 2020.

Electronic Communications and Transactions Act 25 of 2002.

Electronic Communications and Transactions Amendment Bill (published in Government Gazette No. 35821 dated 26 October 2012).

Films and Publications Act 65 of 1996.

Financial Intelligence Centre Act 38 of 2001.

Financial Advisory and Intermediary Services Act 37 of 2002.

National Prosecuting Authority Act 32 of 1998.

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002.

South African Police Services Act 68 of 1995.

The 'National Cybersecurity Policy Framework for South Africa' (published in *GG* 39475 of 4 December 2015).

International

African Union Convention on Cybersecurity and Personal Data Protection.

Council of Europe's Convention on Cybercrime (Budapest Convention).

Secondary Sources

Books and Chapters in Books

Gottfredson, M & Hirschi, T *A General Theory of Crime* (1990) *Stanford University Press*.

Stéphane Leman-Langlois *Technocrime* (2008).

Toepoel, V 'Online survey design' in Nigel G. Fielding, Raymond M. Lee & Grant Blank (eds) *The SAGE Handbook of Research Methods* (2017) 184-202.

Valls-Prieto, J 'Fighting Cybercrime and Protecting Privacy: DDoS, Spy Software, and Online Attacks' in Maria Manuela Cruz-Cunha & Irene Maria Portela (eds) *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (2015) 146-155.

Journals

Agustina, Jose 'Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect' (2015) 9:1 *International Journal of Cyber Criminology* 35-54.

Akdemir, N & Lawless, CJ 'Exploring the human factor in cyber-enabled and cyber-dependent crime victimization: a lifestyle routine activities approach' (2020) 30:6 *Internet Research – Emerald Publishing Limited* 1665-1687.

Button, M 'The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions' (2020) 36:1 *Journal of Contemporary Criminal Justice* 39-55.

Button, M & Whittaker, J 'Exploring the voluntary response to cyber-fraud: From vigilantism to responsibilisation' (2022) 66 *International Journal of Law, Crime and Justice* (https://doi.org/10.1016/j.ijlcj.2021.100482).

Cassim, F 'Addressing the challenges posed by cybercrime: A South African perspective' (2010) 5 *Journal of International Commercial Law & Technology* 118-123.

Chigada, J & Madzinga, R 'Cyberattacks and threats during COVID-19: A systematic literature review' (2021) 23:1 *South African Journal of Information Management* 1-11 (https://doi. org/10.4102/sajim.v23i1.1277).

Cross, C, Holt, T, Powell, A & Wilson, M 'Responding to cybercrime: Results of a comparison between community members and police personnel' (2021) 635 *Trends and Issues in Crime and Criminal Justice* 1-19.

De Kimpe, L, Ponnet, K, Walrave, M Snaphaan, T & Pauwels, L 'Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims' (2020) 108 *Computers in Human Behavior* 1-11 (https://doi.org/10.1016/j.chb.2020.106310).

Dlamini, S & Mbambo, C 'Understanding policing of cyber-crime in South Africa: The phenomena, challenges and effective responses' (2019) 5 *Cogent Social Sciences* 1-13 (https://doi.org/10.1080/23311886.2019.1675404).

Du Toit, R, Hadebe, P & Mphatheni, M 'Public perceptions of cybersecurity: A South African context' (2018) 31:3 *Acta Criminologica: Southern African Journal of Criminology* 111-131.

Ezeji, C, Olutola, A & Bello, P 'Cyber-related crime in South Africa: extent and perspectives of state's roleplayers' (2018) 31:3 *Acta Criminologica: Southern African Journal of Criminology* 93-110.

Hagen, J & Lysne, O 'Protecting the digitized society – the challenge of balancing surveillance and privacy' (2016) 1:1 *The Cyber Defense Review* 75-90.

Harkin, D, Whelan, C & Chang, L 'The challenges facing specialist police cyber-crime units: an empirical analysis' (2018) 19:6 *Police Practice and Research* 519-536.

Hill, J & Marion, N 'The Use of Mythic Narratives in Presidential Rhetoric on Cybercrime' (2018) 6:2 *Journal of Qualitative Criminal Justice & Criminology* 179-203.

Ho, H, Ko, R & Mazerolle, L 'Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review' (2022) 115 *Computers & Security* 1-24 (https://doi.org/10.1016/j.cose.2022.102611).

Huey, L, Nhan, J & Broll, R '"Uppity civilians" and "cyber-vigilantes": The role of the general public in policing cybercrime' (2012) 13:1 *Criminology & Criminal Justice* 81-97.

Jansen, J & Leukfeldt, E.R. 'Coping with Cybercrime Victimization: An Exploratory Study into Impact and Change' (2018) 6:2 *Journal of Qualitative Criminal Justice & Criminology* 205-228.

Keller, Heidi & Lee, Sandra 'Ethical issues surrounding human participants research using the internet' (2003) 13:3 *Ethics and Behaviour* 211-219.

Kshetri, N 'Cybercrime and Cybersecurity in Africa' (2019) 22:2 *Journal of Global Information Technology Management* 77-81.

Lapidot-Lefler, Noam & Barak, Azy 'The benign online disinhibition effect: Could situational factors induce self-disclosure and prosocial behaviors?' (2015) 9:2 *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*.

Leukfeldt, E.R, van de Weijer, S.G.A & Van Der Zee, S 'Reporting cybercrime victimization: determinants, motives, and previous experiences' (2020) 43:1 *Policing: An International Journal of Police Strategies & Management* 1-27.

Leukfeldt, E.R. & Yar, M 'Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis' (2016) 37:3 *Deviant Behavior* 263-280.

Lianos, H & McGrath, A 'Can the General Theory of Crime and General Strain Theory explain cyberbullying perpetration' (2018) 64:5 *Crime and Delinquency* 674-700.

Lipton, J 'Combating Cyber-Victimisation' (2011) 26 *Berkeley Technology Law Journal* 1103-1155.

McGuire, M & Dowling, S 'Cyber crime: A review of the evidence – Chapter 1: Cyber-dependent crimes' (2013) 75 *Home Office Research Report* 1-34.

Minnaar, Anthony & Herbig, Friedo 'Cyberattacks and the cybercrime threat of ransomware to hospital and healthcare services during the COVID-19 pandemic' 2021 34:3 *Acta Criminologica: African Journal of Criminology & Victimology* 155-185.

Moreno, M, Goniu, N, Moreno, P & Diekema, D 'Ethics of social media research: Common concerns and practical considerations' (2013) 16:9 *Cyberpsychology, Behaviour and Social Networking* 708-713.

Mtuze, S 'The Convergence of Legislation on Cybercrime and Data Protection in South Africa: A Practical Approach to the Cybercrimes Act 19 of 2020 and the Protection of Personal Information Act 4 of 2013' (2022) 43:3 *Obiter* 536-569.

Naidoo, Rennie 'A multi-level influence model of COVID-19 themed cybercrime' (2020) 29:3 *European Journal of Information Systems* 306-321.

Näsi, M, Oksanen, A Keipi, T & Räsänen, P 'Cybercrime victimization among young people: a multi-nation study' (2015) 16:2 *Journal of Scandinavian Studies in Criminology and Crime Prevention* 203-210.

Ngo, F & Paternoster, R 'Cybercrime victimization: An examination of individual and situational level factors' (2011) 5:1 *International Journal of Cyber Criminology* 773-793.

O'Hear, Michael & Wheelock, Darren 'Public Attitudes Toward Punishment, Rehabilitation, and Reform: Lessons from the Marquette Law School Poll' (2016) 29:1 *Federal Sentencing Reporter* 47-51.

Ojanen, T, Boonmongkon, P, Samakkeekarom, R, Samoh, N, Cholratana, M, Payakkakom, A & Guadamuz, T 'Investigating online harassment and offline violence among young people in Thailand: Methodological Approaches, Lessons Learned' (2014) 16:9 *Culture, Health & Sexuality* 1097-1112.

Sarre, R, Yiu-Chung, L & Chang, L 'Responding to cybercrime: current trends' (2018) 19:6 *Police Practice and Research* 515-518.

Siegel, Max 'Privacy, ethics, and confidentiality' (1979) 10:2 *Professional Psychology* 249-258 (http://dx.doi.org/10.1037/0735-7028.10.2.249).

Steinmetz, K 'Technocrime at the Margins: Introduction to the Special Issue on Critical or Marginal Perspectives and Issues in the Study of Technocrime' (2018) 6:2 *Journal of Qualitative Criminal Justice & Criminology* 131-135.

Tonry, M & Farrington, D. P 'Strategic Approaches to Crime Prevention' (1995) 19 *Crime & Justice* 1-20.

Tosoni, L 'Rethinking Privacy in the Council of Europe's Convention on Cybercrime (2018) 34:6 *Computer Law & Security Review* 1197-1214.

Van de Weijer, S & Leukfeldt, E.R. 'Big Five Personality Traits of Cybercrime Victims' (2017) *Cyberpsychology, Behavior, and Social Networking* 1-6 (https://doi.org/10.1089/cyber.2017.0028).

Wall, D 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' (2007) 8:2 *Police Practice and Research* 183-205.

Wright, Kevin B 'Researching internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services' (2005) 10:3 *Journal of Computer-Mediated Communication* (https://doi.org/10.1111/j.1083-6101.2005.tb00259.x).

Internet Articles

AAG 'The Latest 2023 Cyber Crime Statistics (updated March 2023)' available at https://aag-it.com/the-latest-cyber-crime-statistics/, accessed on 8 March 2023.

African Union List of Countries which have Signed, Ratified/Acceded to the African Union Convention on Cybersecurity and Personal Data Protection, available at https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf, accessed on 23 May 2021.

Aghatise, J 'Cybercrime definition' (2014) available at https://www.researchgate.net/publication/265350281_Cybercrime_definition, accessed on 8 December 2022.

Alvarez, R 'Cyber Enabled Crime vs. Cyber-Dependent Crime' 2 September 2021 *IP Probe* available at https://ipprobe.global/2021/09/02/cyber-enabled-crime-vs-cyber-dependent-crime/, accessed on 6 December 2022.

Arctic Wolf 'A Brief History of Cybercrime' 16 November 2022 available at: https://arcticwolf.com/resources/blog/decade-of-cybercrime/, accessed on 1 April 2023.

Armin, J, Thompson, B & Kijewski, P '2016 – Cybercrime Surveys Report' *Cyber Road – Development of the Cybercrime and Cyber-Terrorism Research Roadmap*, available at www.cyberroad-project.eu, accessed on 23 May 2020.

Baron, Jessica 'Social Media Platforms Increasingly Popular With Cybercriminals' 30 April 2019 available at https://www.forbes.com/sites/jessicabaron/2019/04/30/social-media-platforms-increasingly-popular-with-cybercriminals/?sh=3eccd94f7324, accessed on 2 December 2022.

Berasategui, Guillermo 'Cybercrime: Which ones are the most common threats today?' available at https://www.redpoints.com/blog/cybercrime/, accessed on 6 February 2022.

BlockSite '5 Ways to Avoid Malware While Streaming Content Online' 18 July 2022 available at https://blocksite.co/blog/5-ways-to-avoid-malware-while-streaming-content-online, accessed on: 2 December 2022.

Boitumelo Kgobotlo '"Cashflow" Ngcobo appeals jail sentence' *Sowetan Live* 12 May 2019, available at https://www.sowetanlive.co.za/sundayworld/news/2019-05-12-cashflow-ngcobo-appeals-jail-sentence/, accessed on 02 June 2021.

Bradley Prior 'These are South Africa's top scammers – according to the FBI' 7 March 2022, available at https://mybroadband.co.za/news/security/436352-these-are-south-africas-top-scammers-according-to-the-fbi.html?utm_source=dlvr.it&utm_medium=twitter, accessed on 25 March 2022.

Brown, D 'Cybercrime is Dangerous, But a New UN Treaty Could be Worse for Rights' 13 August 2021, available at https://www.justsecurity.org/77756/cybercrime-is-dangerous-but-a-new-un-treaty-could-be-worse-for-rights/, accessed on 29 December 2022.

Council of Europe Portal 'Global Action on Cybercrime' available at https://www.coe.int/en/web/cybercrime/glacy, accessed on 13 December 2022.

Council of Europe's Convention on Cybercrime (Budapest Convention), available at https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/international-and-regional-instruments.html, accessed on 23 May 2021.

Crimeweb.co.za, available at http://crimeweb.co.za, accessed on 9 July 2021.

Cybercrime.org.za, available at https://cybercrime.org.za/reporting, accessed on 6 July 2021.

Europol 'Definition of 'economic crime'' available: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/economic-crime, accessed on 22 January 2023.

Gondwe, Moss 'South Africans must up their game against cybercrime' *Mail & Guardian* 12 October 2022 available at https://mg.co.za/opinion/2022-10-12-south-africans-must-up-their-game-against-cybercrime/, accessed on 12 December 2022.

Hove, K 'The SADC Model Law on Computer Crime and Cybercrime: A Harmonised Assault on the Right to Privacy?' 18 July 2017 available at https://www.linkedin.com/pulse/sadc-model-law-computer-crime-cybercrime-harmonised-assault-kuda-hove, accessed on 27 September 2021.

Illidge, Myles 'South African justice department clueless about hacked data' 12 January 2022, available at https://mybroadband.co.za/news/security/429804-south-african-justice-department-clueless-about-hacked-data.html, accessed on 16 February 2022.

Information Technology Laboratory Computer Security Resource Centre 'Definition of phishing' available at https://csrc.nist.gov/glossary/term/phishing, accessed on 2 December 2022.

Internet Service Providers' Association 'Reporting cybercrimes' (2022) available at https://ispa.org.za/wp-content/uploads/2022/10/ISPA-Advisory-Reporting-Cybercrimes-Updated-October-2022.pdf, accessed on 12 December 2022.

Jenik, Claire ‘Statista’ available at https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet- in-one-minute/, accessed on 12 August 2021.

Johnson, J ‘Most commonly reported types of cyber crime 2020’ 18 March 2021 available at https://www.statista.com/statistics/184083/commonly-reported-types-of-cyber-crime/, accessed on 6 April 2021.

Microsoft Digital Defense Report 2022, available at https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022, accessed on 29 December 2022.

Microsoft Security Intelligence ‘Global threat activity’ available at https://www.microsoft.com/en-us/wdsi/threats, accessed on 13 January 2023.

Moyo, A ‘Top-notch Cyber Crimes Act ultimately fails to deliver’ 2 June 2022 *ITWeb* available at https://www.itweb.co.za/content/PmxVEMKEyOovQY85, accessed on 3 December 2022.

National Prosecuting Authority of South Africa ‘Specialised Commercial Crime Unit’ available at https://www.npa.gov.za/specialised-commercial-crime-unit, accessed on 13 December 2022.

Office of the Provincial Commissioner Western Cape ‘Media Statement’ 19 February 2022, available at https://www.saps.gov.za/newsroom/msspeechdetail.php?nid=38210, accessed on 8 December 2022.

Parliamentary Monitoring Group ‘Cybercrimes Bill’ available at https://pmg.org.za/bill/684/, accessed on 26 March 2021.

Rawat, A.S. ‘An Overview of Descriptive Analysis” 31 March 2021, available at https://www.analyticssteps.com/blogs/overview-descriptive-analysis, accessed on 5 December 2022.

South African Banking Risk Information Centre ‘Who We Are’ available at https://www.sabric.co.za/who-we-are/, accessed on 21 January 2023.

Stouffer, Clare ‘Is my phone listening to me? Yes, here’s why and how to stop it’ 15 August 2022 available at https://us.norton.com/blog/how-to/is-my-phone-listening-to-me#, accessed on 2 December 2022.

United Nations Conference on Trade and Development, available at https://unctad.org/page/cybercrime-legislation-worldwide, accessed on 26 February 2022.

United Nations Office on Drugs and Crime, ‘Situational Crime Prevention’ available at https://www.unodc.org/e4j/en/cybercrime/module-9/key-issues/situational-crime-prevention.html, accessed on 18 March 2022.

United States Department of Justice, Bureau of Justice Statistics ‘National Crime Victimization Survey: Identity Theft Supplement 2012’ *Inter University Consortium for Political and Social Research* available at: https://bjs.ojp.gov/library/publications/victims-identity-theft-2012, accessed on 29 May 2020.

Vermeulen, Jan ‘TransUnion hackers leak Cell C and ANC member databases’ 23 March 2022, available at https://mybroadband.co.za/news/security/438560-transunion-hackers-leak-cell-c-and-anc-member-databases.html?utm_source=dlvr.it&utm_medium=twitter, accessed on 25 March 2022.

ANNEXURE "A" – SURVEY

INFORMATION SHEET AND CONSENT

I am a student at the University of Cape Town and I am conducting research towards a Master's Degree in Law. I am interested in understanding victims' experiences of cyber victimisation and their response to this crime and would like you to participate in the project.

The purpose of this study is to examine the forms of cybercrime experienced in South Africa and whether cybervictims were aware of the legal remedies available to them, and whether they knew what to do or where to go to report that they had been victims of cybercrime. This will enable us to understand what needs to be done to inform individuals of the risks that may lead to cybervictimisation and also gauge whether the response to cybercrime is adequate.

Kindly note, there is the risk that participating in this survey may be an emotional experience. Participants may have to relieve potentially traumatic experiences when recounting their cybervictimisation experience. Please bear this in mind when considering whether to participate in this survey.

Your participation in this research is voluntary and you can choose to skip any questions or stop taking the survey at any time. However, I would appreciate your participation in this project.

Please only complete the survey if you are over the age of 18 years.

We are collecting this data anonymously, which means that no-one will be able to link your answers to you, not even the researchers. The data collected in this survey may be used for potential future academic publications.

This survey should take no longer than 35 minutes to complete.

Should you have any questions regarding this research, please feel free to contact me (smtsav005@myuct.ac.za) or my supervisor A/Prof Kelley Moult (kelley.moult@uct.ac.za). If you have concerns about the research, its risks and benefits or about your rights as a research participant in this study, you may contact the Law Faculty Research Ethics Committee Administrator, Ms Lamize Viljoen, at: +27(0)21 650 3080 or lamize.viljoen@uct.ac.za. Alternatively, you may write to the Law Faculty Research Ethics Committee Administrator: Room 6.29, Kramer Law Building, Law Faculty, UCT, Private Bag, Rondebosch 7701.

If you feel overwhelmed or in need of support, please use the resources listed below:

- SA Depression and Anxiety group (SADAG) – 080 012 1314.
- SADAG Cipla WhatsApp counselling - 076 882 2775.
- Lifeline South Africa – 0861 322 322.
- Lifeline South Africa WhatsApp Counselling - 065 090 0238.
- Cybersecurity Hub (to log incidents) - cshubcsirt@cybersecurityhub.gov.za

CYBERCRIME SURVEY QUESTIONNAIRE:

GENERAL

1. Age

    a. 16 – 25
    b. 26 – 35
    c. 36 – 45
    d. 46 – 55
    e. 56 – older

2. Gender

    a. Male
    b. Female

3. In the past 12 (twelve) months, did you work for a wage, salary, commission or any remuneration?

    a. YES
    b. NO

4. If yes, are you employed:

    a. Full-time – 4 or more hours per day, at least 4 days per week
    b. Part-time – less than 3 hours per day, up to 3 days per week

5. Are you a Student?

    a. YES
    b. NO

6. [If Q5 = a] If yes, are you a:

    a. Full-time student
    b. Part-time student

7. [If Q5 = b] Which online/social media platform/s do you use the most? *[Multiple Responses Allowed – please rank in order of use]*

    a. Facebook
    b. Twitter
    c. Instagram
    d. Online Dating Sites/Applications
    e. Snapchat
    f. WhatsApp
    g. Other (please specify)

8. How often do you share information about your personal life on social media? For example, your full name, date of birth, contact details, place of work/education, relationship status, location, interests, photographs, *et cetera*.

    a. Never
    b. Almost never
    c. Occasionally/sometime
    d. Almost every time
    e. Every time

9. Do you download or make use of any of the following "free" software/apps:

    a. Online movie and/or series streaming
    b. Online document converter (word to pdf converter, etc)
    c. Online url/link creator
    d. Other (please specify)
    e. None of the above

10. Approximately how many hours per week do you spend engaging in the following online activities:

    a. Purchasing goods and merchandise, doing research, or gathering information, etc.
        i. 0 – 14 hours
        ii. 15 – 30 hours
        iii. 31 – 45 hours
        iv. More than 45 hours

    b. Using e-mail

        i. 0 – 14 hours
        ii. 15 – 30 hours
        iii. 31 – 45 hours
        iv. More than 45 hours

    c. Using instant messaging (such as WhatsApp, Telegram, Facebook Messenger, Skype, Microsoft Teams chat, Discord, *et cetera*)

        i. 0 – 14 hours
        ii. 15 – 30 hours
        iii. 31 – 45 hours
        iv. More than 45 hours

    d. Participating in chat rooms

        i. 0 – 14 hours

ii. 15 – 30 hours
iii. 31 – 45 hours
iv. More than 45 hours

11. Do you have any anti-virus or protective software installed on your computer?

a. YES
b. NO

CYBERVICTIMISATION

12. Which of the following have you experienced? *[You may select all that apply]*

a. Catfishing
    i. Seeing online profiles using your personal information and photographs without your consent

b. Computer virus-related
    i. Crimeware – a special type of malware designed specifically to facilitate and automate financial crime. Usually transmitted in the form of an email attachment.
    ii. Madware – helps advertising networks provide targeted advertising through the collection of location and device information from the users of free cell phone apps.
    iii. Malware – consists of programs such as viruses, worms, Trojan horses and rootkits that are designed to harm your devices.
    iv. Ransomware – a type of malware that infects a computer and demands a ransom for its removal.
    v. Trojan – a malicious programme disguised as legitimate software
    vi. Worm – a self-replicating program that is able to copy and spread itself without the help of any other program.

c. Cyberbullying
    i. Being mocked on social media because of your physical appearance, character or an experience you had
    ii. Seeing false and mean-spirited things written about you
    iii. Being invited to social media groups including gossip or inappropriate conversation
    iv. Being specifically and intentionally excluded from social media groups

d. Cyber-harassment
    i. Receiving harassing emails or messages
    ii. Receiving threatening emails or messages
    iii. Receiving obscene emails or messages
    iv. Receiving unwanted emails or messages to your personal devices without your consent

e. Identity theft
    i. Pharming – attacks that direct users from legitimate websites to fraudulent websites. These fraudulent websites look similar to the real sites but when you enter personal information, the information is captured by the attacker.

f. Financial fraud
    i. Having problems because your personal information was shared online without your consent

g. Phishing
    i. Receiving "spam" or other electronic communication to obtain your personal information
    ii. Suffering from software aiming to get your personal information

h. Other (please specify)

i. None of the above. If None of the above, proceed to question 18. If No to question 18, proceed to question 34.

13. How many of the incidents, referred to in your answer to question 13 above, have you experienced in the last 2 years?

14. What type of technology were you using at the time of your last experience referred to in questions 12 and 13 above? *[You may select all that apply]*

a. Computer
b. Laptop
c. Cell phone
d. Other (please specify)

15. In the 12 months preceding your experience of cybercrime, did you engage in any of the following activities: *[Multiple Responses Allowed]*

a. communicate with strangers online
b. provide personal information to person(s) online
c. frequently open any unfamiliar attachments to e-mails that you received, clicked on any of the web-links in the emails that you received
d. opened any file or attachment you received through your emails
e. clicked on a pop-up message that interested you
f. Other (please specify)
g. None of the above

16. Where did your experience take place?

a. E-mail
b. Facebook

c. WhatsApp
d. Instagram
e. Other (please specify)

17. Please provide a summary of your cybercrime experience. [150 words or less]

18. [If Q12 = i] Do you know anyone else who has been a victim of cybercrime?
    a. YES
    b. NO

19. [If Q18 = a] How many people do you know who have been a victim of cybercrime? [ENTER NUMBER]

REPORTING

20. Did you report your cybercrime experience?

    a. YES – If yes, proceed to question 21.
    b. NO – If no, proceed to question 24.
    c. SOMETIMES YES, SOMETIMES NO [Go to Q20 – Q23 and then Q23 onwards]

21. [If Q19 = a] Who did you report this crime to? *[Multiple Responses Allowed]*

    a. The Police
    b. Lawyer
    c. Bank
    d. National Cybersecurity Hub
    e. Internet Service Provider
    f. Friend
    g. Family member
    h. Colleague
    i. Other (please specify)

22. [If Q20 = a/b/c/d] Where did you find information on who to report the crime too?

23. [If Q20 = a/b/c/d] Did the authorities take your matter seriously and investigate the crime?

24. [If Q19 = b] What were your reasons for not reporting? Please select all that apply. *[Multiple Responses Allowed]*

    a. I did not believe it was a crime
    b. I believed it was too private or personal
    c. I dealt with it myself
    d. Someone in my household or family dealt with it
    e. I was afraid that the person who did this to me or his or her family members would harm me if I reported it to the police

f. I was afraid that other people would find out, such as neighbours or employers
g. I reported it to someone other than the police
h. I did not feel comfortable with the police or did not like the police
i. The police would not have helped
j. Reporting to the police seemed like too much trouble
k. I have had a bad experience with the police before
l. My family persuaded me not to report it to the police
m. I did not want to get the person who did this in trouble
n. There were no police in the community to talk to
o. Other reason (please specify)

25. [If Q19 = a] When you **did** report to the authorities, what were your reasons for reporting? Please select all that apply. *[Multiple Responses Allowed]*

a. I believed it was a crime and that all crime should be reported
b. I was upset by what happened
c. I felt that the person should be punished
d. I felt that the person who did it needed help, treatment, or counselling
e. I wanted it to stop
f. I wanted to protect the children
g. Other reason (please specify)

26. [If Q19 = a] How satisfied were you when you reported the crime to the authorities?

a. Completely satisfied
b. Mostly satisfied
c. Mostly unsatisfied
d. Completely unsatisfied

27. [If Q19 = a] If this were to happen to you again, would you report to the authorities in the future? Would you say…

a. Definitely yes
b. Probably yes
c. Maybe
d. Probably not
e. Definitely not

28. [If Q19 = a] Did you feel that the authorities viewed the incident as a serious crime worth investigating?
a. YES
b. NO
c. I WANT TO SAY MORE ABOUT THIS [Specify]

RECOURSE

29. Did you want the cybercriminal/offender to be punished?
a. YES
b. NO

30. How do you think the cybercriminal should have been punished?
    a. They should have been arrested
    b. I wanted my money/property back
    c. They should have been made to apologise
    d. They should have been made to take down the posts/comments

31. How much time was needed to repair the damage caused by the cybercrime?
    a. Less than 1 week?
    b. 1 to 2 weeks?
    c. 2 – 4 weeks?
    d. More than 4 weeks?

32. How much did it cost you to rectify the damage caused by the cybercrime?
    a. Less than R500?
    b. R500 – R1000?
    c. More than R1000?

POST-VICTIMISATION EXPERIENCE

33. How did you feel once you became aware you were a victim of cybercrime? *[Multiple Responses Allowed]*

    a. I felt afraid
    b. I blamed myself
    c. I felt anger
    d. I felt ashamed
    e. I felt sad
    f. I didn't want to admit it had happened to me
    g. I felt violated
    h. I felt betrayed
    i. I felt vulnerable
    j. I felt powerless
    k. Other (please specify)

34. Have you noticed any changes in your behaviour since your cybervictimisation experience? *[Multiple Responses Allowed]*

    a. I've become more protective of my belongings/information/family/friends
    b. I avoid going online
    c. I've been depressed
    d. I've become more anxious
    e. I have lost interest in technology/social media due to lack of trust and confidence
    f. Other (please specify)

35. Have you ever needed any of the following because of the cybercrime(s) that you experienced? *[You may select all that apply]*

    a. Legal assistance
    b. A protective /restraining order?
    c. Assistance from police?
    d. Counselling services, to see a psychologist or psychiatrist?
    e. Victim's advocacy services?
    f. Temporary shelter or safe housing?
    g. Transitional or permanent housing assistance?
    h. Healthcare, medical or hospital services?
    i. Other (please specify)

LEGISLATION

36. [If Q18 = b] Do you know which laws protect people from cybercrime?

    a. YES – If yes, proceed to question 37
    b. NO – If no, proceed to question 39

37. [If Q35 = a] How/where did you find out about these laws?
    a. Internet
    b. Email or newsletter
    c. Newspaper or magazine
    d. Word of mouth
    e. Other (please specify)

38. [If Q35 = a] Do you think South Africa's existing laws are sufficient to deter cyber criminals?
    a. Yes
    b. No
    c. I am not sure

39. Is there anything else you would like to tell us about cybercrime or your experience of being victimised?

40. SURVEY END

END OF SURVEY
Thank you for participating!