International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cybersecurity and Ethical Social Media Use: The Role of Guidance and Counseling in Zambia

Dr. Clement Mulenga Sinyangwe[1], Dr. Rose Chikopela[2]

[1]Head ICT/Lecturer, Department of CICT, Chalimbana University, Lusaka, Zambia
[2]Head Primary and Secondary Education, Chalimbana University, Lusaka, Zambia

Abstract

Zambia's rapid growth online has presented opportunities as well as difficulties, with the surge in cybercrime being a major concern. This study examined the causes of cybercrime on social media and how counseling and advice might encourage the moral use of online spaces. Data were gathered from 202 people in each of Zambia's ten provinces using a descriptive survey design. The results showed that cybercrime is common, especially among young people who use social media, and that it is driven by a number of factors, including ignorance of cyber laws, boredom, retaliation, and the idea of anonymity. Significant repercussions for victims were noted, including monetary loss, harm to one's reputation, and psychological suffering. Furthermore, it was shown that judicial actions by themselves were insufficient, even if the Cyber Crime and Security Act sought to dissuade offenders through severe measures. This study emphasizes the importance of combining counseling services with educational initiatives to effectively combat cybercrime. A combination of legal, educational, and rehabilitative techniques is needed to promote ethical behavior, as evidenced by the majority of respondents who supported counseling and guidelines on social media responsibility as effective ways to reduce cybercrime. The Zambia Information and Communications Technology Authority's (ZICTA) increased efforts to increase public awareness, the inclusion of digital ethics in school curricula, and the improvement of cybersecurity procedures by law enforcement are among its recommendations. Significant repercussions for victims were noted, including monetary loss, harm to one's reputation, and psychological suffering. Furthermore, it was shown that judicial actions by themselves were insufficient, even if the Cyber Crime and Security Act sought to dissuade offenders through severe measures. This study emphasizes the importance of combining counseling services with educational initiatives to effectively combat cybercrime. A combination of legal, educational, and rehabilitative techniques is needed to promote ethical behavior, as evidenced by the majority of respondents who supported counseling and guidelines on social media responsibility as effective ways to reduce cybercrime. The Zambia Information and Communications Technology Authority's (ZICTA) increased efforts to increase public awareness, the inclusion of digital ethics in school curricula, and the improvement of cybersecurity procedures by law enforcement are among its recommendations.

Keywords: Cyber Security, Ethics, Ethical, Prevention, Guidance, Counselling, Social Media, Zambia

Background

Cybercrime is a broad term used to describe various offenses and crimes committed in cyberspace, some of the offenses and crimes include and are not limited to cyberbullying, hate speech, abusive language,

extortion, fraud, phishing, and many more. (Sinyangwe, 2023).

Zambia, among other countries, has seen an increase in cyberspace activities, especially those performed on Internet-enabled electronic devices. Activities such as news publication through websites, blogs, Facebook, WhatsApp, and other social media platforms. The Internet has been seen as one of the biggest gifts humankinds has received in the recent years. This is because it has brought people closer together despite the distance and has made it easy for people to perform tasks and different activities; simply put, the Internet is an enabler meant to support all activities of the economy. It has brought ease to communication, education, research, business, and in achieving most tasks that human beings cannot achieve without its use. Online learning in the wake of Covid-19 has been used in both developed and developing countries. Most students in Zambia have been exposed to online learning, demanding that each student have a smartphone to learn (Chikopela et al, 2021). However, these electronic devices have caused some students to perpetrate cybercrimes.

Rajab and Cinkelr (2018) indicated that in the past few years, we have witnessed the emergence of the IoT, which has resulted in breakthroughs, advancements, and a wide range of applications that have been a regular topic in the media. The notion of the automatic cooperation of millions of different appliances inside a global network is around three decades old; however, its rapid development has begun relatively recently. Although some inventors take this concept to their logical conclusion by proposing connecting devices to the Internet, such as kitchenware, personal tools such as toothbrushes, trash bins, television sets, home electrical appliances, and circuits, to name a few, the network of "smart" devices (also known as IoT devices) provides numerous undeniable benefits to humanity.

However, not all cyberspace users fully apply the Internet in an ethical or acceptable manner; there have been many issues raised in society over its usage, most of which are based on moral degradation towards global citizens. Misuse of cyberspace can have many detrimental repercussions among students, including decreased academic performance, poor social skills, reduced self-worth, isolation, loneliness, depression, anxiety, truancy, and suicide. Guidance and counselling on social media usage play a critical role in helping perpetrators, as well as students who fall victim to cyberspace misuse, by taking a strength-based approach, teaching soft skills and social-emotional learning, encouraging students to become more assertive, empathic, empowered, assisting students in regaining control, focusing on setting realistic goals, and encouraging increased parental involvement and monitoring of social media usage (Paolini, 2018; Chikopela et al, 2022).

The increase in digital space in Zambia and other countries has expanded dramatically over the last few decades, with the expansion of social media space being the most notable phenomenon. According to available data, social media is used by more than half of the world's population, making it an essential component of any brand's primary marketing platform. Social media has created a space for people to communicate, express their opinions, and share content, in addition to marketing and brand-building. Content posted on social media draws criticism from various user demographics, some of which constitute hate speeches. Hateful comments on social media are a growing problem in the online world and a top priority for social media developers, marketers, and law enforcement. Hateful comments and discourse on social media can cause public tension and even violence (National Assembly of Zambia, 2022).

Many concerns have been raised in Zambia regarding hate speech, particularly on online and social media platforms. Evidence from the Zambia Information and Communications Technology Authority supports the exponential growth in the number of people engaging in cybercrime and hate speeches. In addition, in 2020, Zambia Information and Communications Technology Authority (ZICTA) revealed a number of

complaints coming as a result of social media and online platforms throughout the annual report, which highlighted a summary of the cyber offenses reported on a monthly basis to the authority, the types of applications used by perpetrators, and complaint volumes by category and province. (ZICTA, 2020).

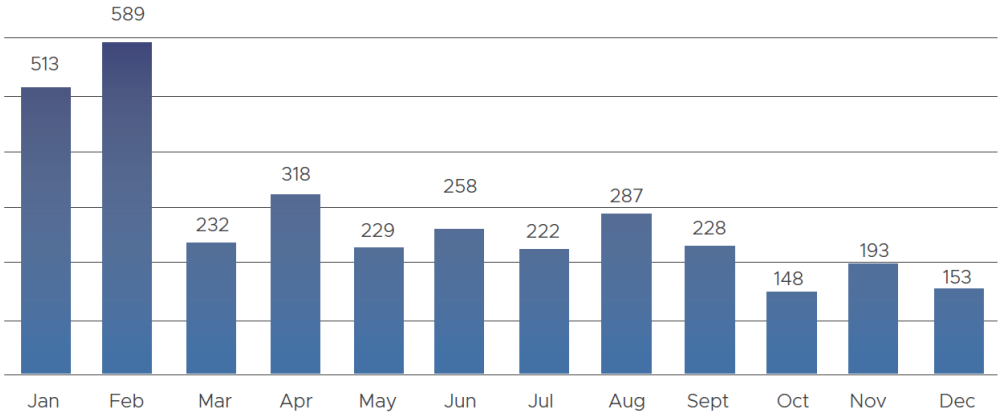

Figure 1: *Cyber Cases Received in 2020*
Source: ZICTA (2020)

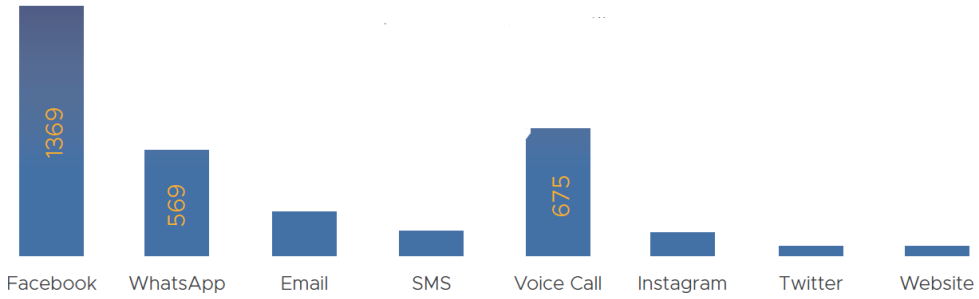

Figure 2: *Applications used by Perpetrators*
Source: ZICTA (2020)

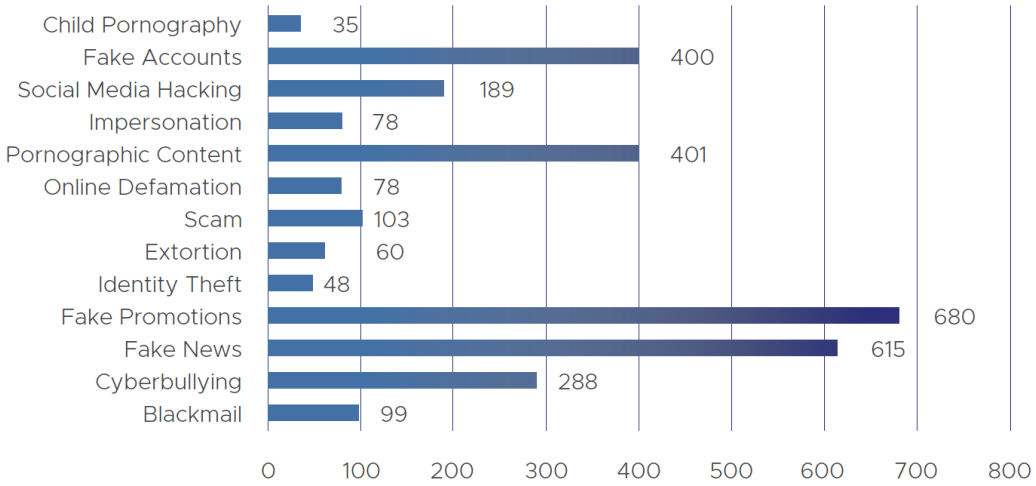

Figure 3: *Complaint Volumes by Category*
Source: ZICTA (2020)

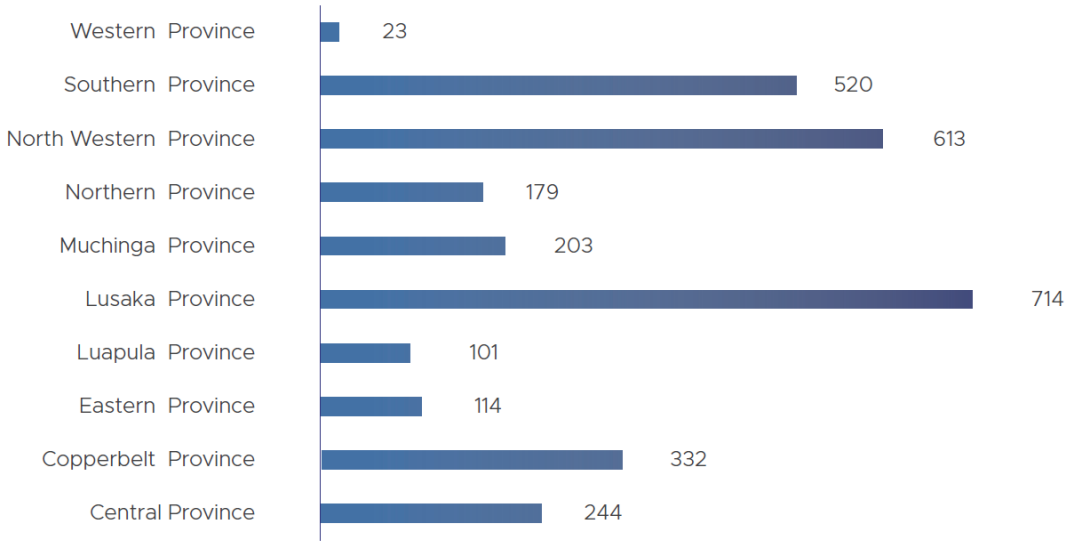

Figure 4: *Complaint by Province*
Source: ZICTA (2020)

Looking at the summary of cybercrime above, it is very likely that most perpetrators of cybercrime are those who frequently engage in cyberspace. It is, therefore, a fact that the increase has come with many controversies, disinformation, and organized social media campaigns, primarily owing to issues such as boredom, frustration, unemployment, cyber addiction, and freedom of expression among other things. In doing so, users are bound to either deliberate or undeliberately commit cybercrimes. Consequently, the Government of the Republic of Zambia decided to introduce regulations to curb the increase in cyber-related crimes.

Problem Statement

According to information obtained from Xinhua (2021), in a statement issued through its spokesperson, the Zambian government expressed concern over the abuse of cyberspace, despite heightened campaigns against the vice. The government was concerned about the continuous increase in the abuse of cyberspace and called on all stakeholders to join forces with the government to ensure that citizens were protected from any form of cybercrime. Furthermore, the Government resolved to combat the abuse of cyberspace through various measures, including the implementation of various laws aimed at promoting the use of social media platforms (Xinhua, 2021). As a result of this pronoucement, some sections of society stated that the cyber laws being implemented by the government are a danger to the country's democracy and aimed to shrink the only existing free space, the Internet, which has been offering numerous online spaces for citizens to enjoy their freedoms and rights of association, assembly, and expression (Zambia Reports, 2019).

Furthermore, the Media Institute of Southern Africa (MISA) Zambia Chapter also cautioned the government against regulating online media spaces, saying that doing so would result in Zambians' freedoms shrinking further. (Lusaka times, 2018). The Institute mentioned that cyber laws should uphold fundamental human rights such as freedom to express, speech, online assembly, and privacy. Emanating from these controversies, the biggest question surrounding cybercrime perpetrators is why they involve themselves in these acts and whether most offenses are committed with intent. Therefore, this study sought

to establish how guidance and counselling can play a role in ensuring that users are couselled and guided on the ethical usage and application of cyberspace.

Study Ojectives

To ascertain reasons why cyberspace users commit cybercrime on various social media platforms
To establish the role of guidance and counselling in the ethical use of cyberspace in Zambia

Theoretical framework

According to (Agnew, 2018) general strain hypothesis, stress causes negative emotions, which can lead to various consequences, including delinquency. Failure to accomplish positively valued objectives (e.g., money), the removal of positively valued stimuli (e.g., loss of a valuable asset), and the presentation of adverse stimuli (e.g., physical abuse) are some of the particular strains mentioned in the theory (Hinduja & Patchin, 2012). The first examines the discrepancy between an individual's aspirations and what they achieve, which leads to disappointment and anger. When a favorably valued stimulus is withdrawn, the second type of strain is called delinquency. This unlawful activity may be construed as an attempt to reduce or eliminate the stimulation. The last form of strain occurs upon exposure to negative stimuli. This might lead to delinquency as a way of coping with or avoiding unfavorable stimuli (ibid). According to Agnew, strain does not produce crime directly but rather fosters unpleasant feelings such as anger and frustration. This is in line with Yale University psychologists' frustration-aggression theory. They felt that anger preceded frustration and that frustration might emerge as violent or non-aggressive conduct (Runions, 2013). Consequently, to release internal pressure, these unpleasant feelings require coping behaviors. Teenagers may resort to unlawful behavior and violence to cope with their limited resources and incapacity to exit difficult circumstances. Patchin and Hinduja found in their study that general strain theory may be utilized to explain criminal conduct among teenagers, such as cyberbullying.

Cyberbullying is a major and developing phenomenon in which teenagers use technology to harass or intimidate their classmates with the intent of causing direct or indirect harm. Anonymity, continual connectedness, and permanence are distinctive characteristics of the digital environment that are not present offline (Sinyangwe, 2023). This new technology allows victims to be abused at any time, and cyberbullies' anonymity makes it harder to track them. Agnew claims that stress makes individuals furious, irritated, and sad, putting pressure on the victim to take corrective actions. Victims react to this pressure by wishing to take remedial action to ease their negative sentiments. As a result, cyberbullying is a remedial step that some victims may take to alleviate their negative sentiments. Taken together, the general strain theory and frustrated aggression hypothesis provide insight into how individuals, particularly teenagers, respond to and deal with negative stress, whether by bullying others or engaging in deviant behavior to relieve stress. Cyberbullying is extraordinarily dangerous for both the perpetrator and victim in that for the perpetrator, it will leave a permanent record of their activities and postings, and they may build a negative online reputation that is accessible to future educators, admissions officers, and employers (Paolini, 2018; Cyberbullying Research Centre, 2016). The general strain theory will guide this study in establishing the causes of cybercrime and how guidance and counselling can enlighten perpetrators on the ethical use of cyberspace.

METHODOLOGY

This study used a descriptive survey design to investigate the characteristics and perceptions of Zambian

citizens from all 10 provinces. In total, 202 participants were selected using multistage sampling to ensure diverse and representative data. Data were collected using online questionnaires administered via Google Forms, which facilitated efficient and widespread access to the target population. The collected data were then analyzed using Microsoft Excel to perform descriptive statistical analyses, providing insights into the trends and patterns within the responses.

PRESENTATION OF FINDINGS AND DISCUSSIONS

This study investigated the role of guidance and counselling in addressing the high prevalence of cybercrime in online spaces. To achieve this, this study developed specific objectives to understand the motivations behind cybercrime on social media platforms. The study collected data from 202 respondents aged between 15 and 55 years from all ten provinces in Zambia.

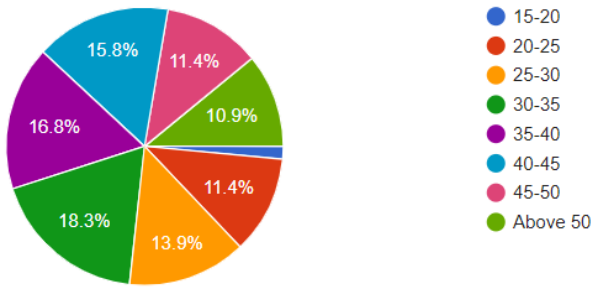

Figure 5: Age group ranges of users

This study was very extensive as it covered all the provinces in Zambia, although the largest number according to the findings of the study indicated those from Lusaka Province with 64.9%, followed by Copperbelt province with 10.9%, with the other eight provinces getting between 5 to 8%. This type of usage can be attributed to the high prevalence of economic activities being conducted online in the Lusaka and Copperbelt provinces compared with other provinces. Other factors could include the population levels in the capital and mining provinces. These were compared with the level of activities found in Lusaka and the unemployment levels that correlated with some of the responses obtained from the respondents when asked why they commit cyber offenses, indicating that boredom could be one of the reasons.

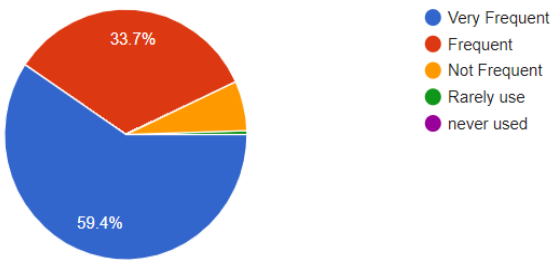

Figure 6: Representation by Province

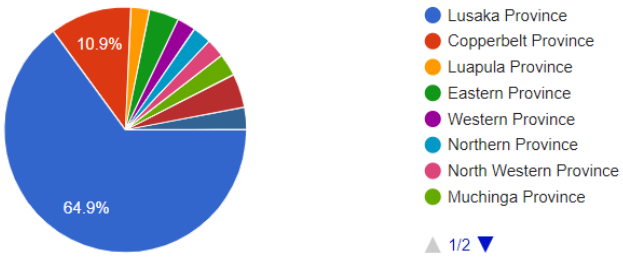

Figure 7: Frequency of use

Other reasons, such as committing cybercrimes simply for fun, can be attributed to the frequency of use, as most people who frequently use online platforms tend to commit these kinds of crimes for fun. The findings revealed that social media users in Zambia are primarily between 20 and 50 years old and are based in the Lusaka Province. Additionally, the study findings revealed that cybercrime is a prevalent issue affecting a wide range of people in Zambia, particularly those who use social media. Further findings have revealed that cybercrime can have significant consequences for victims, including financial loss, reputational damage, and emotional distress. Therefore, it is crucial to explore strategies to help prevent cybercrime and support victims. One is guidance and counselling, as alluded to by respondents on the solution to curbing cybercrime. Similarly, Paolini (2018) emphasized the use of a strength-based approach, teaching soft skills, and social-emotional learning, encouraging students to become more assertive, empathic, empowered, and assisting students in regaining control as a way to reduce cybercrime.

The study also established reasons why users commit cybercrime on various social media platforms. They include;

- Lack of respect for others
- Ignorance of existence of the cyber laws
- For Self-gain
- Revenge
- Jealousy
- They do not have anything to keep them busy
- Simply for fun
- They feel like they can't be caught
- For self-pleasure and satisfaction

Ways to prevent cybercrime

Figure 9 shows that 63.9 % respondents indicated knowledge of the effects of cybercrime. Figure 10 showed 64.4% alluded to guidance regarding the ethical or proper use of social media. 70.3% respondents also indicated knowledge of the existence of Cyber Law, as shown in figure 11 and figure 12 indicates the majority, 78.7% indicated use of counselling on the effects of cybercrime as the most effective way to curb it.

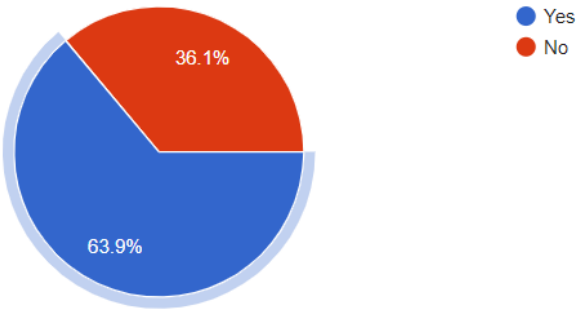

Figure 8: Knowledge on the existence of Cyber Law

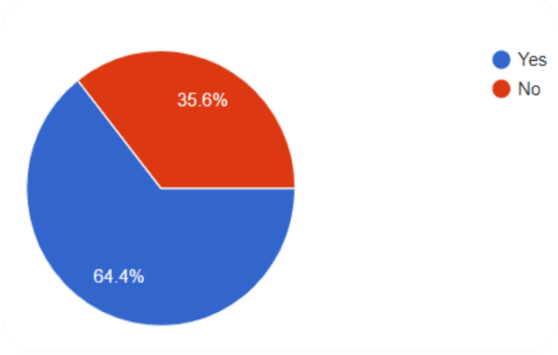

Figure 9: Knowledge on the effects of cyber crime

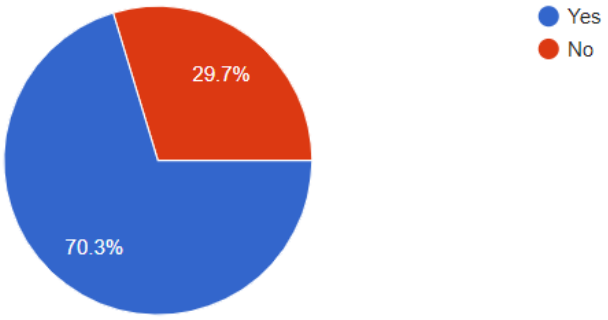

Figure 10: Guidance on the ethical/Proper use of social media

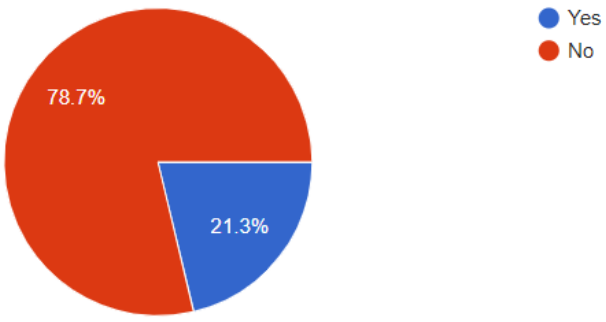

Figure 11: Counselling done on the effects

The results of this study clearly indicate the need for guidance and counselling in promoting ethical behavior and responsible use of cyberspace in Zambia. The study also found that while the Cyber Crime and Security Act was introduced to impose penalties on perpetrators, punitive actions alone may not be

sufficient to deter individuals from committing offenses. This study suggests that promoting ethical behavior in cyberspace requires not only legal measures but also education and counselling to raise awareness about the impact of cybercrimes on individuals and society. By providing guidance and counselling to individuals, especially young people, they can learn about the consequences of cybercrime and how to use technology in a responsible and ethical manner. This, in turn, can help create safer and more secure cyberspace in Zambia.

Conclusion

The widespread abuse of cyberspace, particularly on social media platforms, has become a significant concern, with many users lacking adequate knowledge of the legal implications and criminal activities associated with such behavior. The prevalence of cyberbullying, misinformation, privacy violations, and other forms of online misconduct highlight the urgent need for interventions to address the root causes of this issue. Counselling and educational programs targeting abusers can play a critical role in mitigating these problems by promoting responsible digital behavior and raising awareness of ethical and legal boundaries in online environments. Such rehabilitative approaches could help individuals understand the consequences of their actions, reducing the misuse of cyberspace and fostering a safer and more respectful digital community.

Recommendations

This study recommends ZICTA to provide more education and awareness regarding the consequences of cybercrime.

The study also recommends that law enforcement agencies provide counseling and guidance programs that help individuals, especially young people, understand the effects of cybercrime and the responsible use of social media. Such programs can be integrated into the school curricula, community outreach programs, and social media platforms.

It is also recommended that law enforcement agencies develop better software-based security protocols to help in the investigation and prosecution of cybercrime, and the establishment of reporting mechanisms that make it easier for individuals to report cybercrime.

References

1. Agnew, R. (2018). Building on the Foundation of General Strain Theory. *Recent Developments in Criminological Theory, 38(4), 311–354. https://doi.org/10.4324/9781315089089-22*
2. Chikopela R., Ndhlovu D., Mandyata J. M. & Mpolomoka D. L. Enhancing Teaching and Learning of Open and Distance Learning (ODL) Students with Disabilities using Digital Technologies in Universities, Zambia. *European Journal of Open Education and E-Learning Studies. Volume 7 | Issue 1 | 2022. DOI: 10.46827/ejoe.v7i1.4119*
3. Chikopela R, Mpolomoka D. L., Sikanyika S. F., Sondashi S., Kalizinje N. C., & Zimba J. Student's perspectives on enhancing research in ODL in selected higher learning institutions in Zambia. *International Journal of Research and Scientific Innovation (IJRSI) | Volume VIII, Issue I, January 2021 | ISSN 2321–2705*
4. Hinduja, S., & Patchin, J. W. (2012). Cyberbullying: Neither an epidemic nor a rarity. *European Journal of Developmental Psychology, 9(5), 539–543. https://doi.org/10.1080/17405629.2012.706448*

5. National Assembly of Zambia. (2022). *Information Brief on Cyber Security and Cybercrime Trends in Zambia*. 2022.
6. Paolini, A. (2018). Cyberbullying: role of the school counselor in mitigating the silent killer epidemic. *International Journal of Educational Technology, 5(1), 1-8*
7. Rajab, H., & Cinkelr, T. (2018). IoT based Smart Cities. *2018 International Symposium on Networks, Computers and Communications, ISNCC 2018, 1–4. https://doi.org/10.1109/ISNCC.2018.8530997*
8. Sinyangwe Clement Mulenga, Phiri. william A. (2023). *Adaptation and Application of Ethics in ICT: A Zambian and Regional Ethics Handbook for ICT Proffessionals and Users*. 1–90.
9. Xinhua. (2021). *Zambian gov't expresses concern over abuse of cyberspace*. XINHUANEW. http://www.xinhuanet.com
10. ZICTA. (2020). *2020, Annual Report Annual Report: Advancing the Nation to a digital Society*. ZICTA Annual Report, December, 2–2.
11. ZICTA. (2021). *Annual Report Annual Report: A Regulator Advancing the Nation to a Digital Society*. ZICTA Annual Report, December, 2–2.
12. Kabwama, S., & Moonga, L. (2019). Cybercrime in Zambia: nature, extent and impact. *Journal of Crime and Society, 31(3), 325-345.*
13. Mwamwenda, T. S. (2017). Cybercrime in Africa: trends, challenges and solutions. *In Proceedings of the 2017 International Conference on Information and Communication Technology for Development for Africa (pp. 25-33). ACM.*
14. Banda, J. (2020). Cybersecurity and cybercrime in Zambia: challenges and opportunities. *International Journal of Cybersecurity Intelligence & Cybercrime, 9(1), 1-20.*
15. Masiye, F., & Sampa, L. (2017). Cybercrime and cyber security in Zambia. *Journal of Cybersecurity and Information Management, 4(2), 36-45.*
16. Mulenga, E. M., & Yilma, H. T. (2019). Cybersecurity threats and challenges in Zambia. *International Journal of Innovative Research in Science, Engineering and Technology, 8(10), 4889-4895.*
17. Sinyangwe, C. M., Kunda D., and Phiri, W (2023). *Development and evaluation of a framework for detecting hate speech and abusive language in Zambia using machine learning* publisher?
18. Ghiță, C. M., & Stanciu, G. D. (2020). Cybercrime in Europe: the impact on individuals and organizations. *Sustainability, 12(22), 9584.*