A Review of Novice Strategies against Cybercrime: How can Improved Cybersecurity Strategies be Used to Protect Mobile Devices from the Threat of Cybercrime in Zambia?

Gerry Mutibo Siampondo  
Department of Customer Experience  
Liquid Intelligent Technologies

Professor Mbuyu Sumbwanyambe  
Department of Electrical Engineering  
University of South Africa

Bwalya Chansa  
Department of Technical Sales-Cyber Security  
Liquid Intelligent Technologies

Abstract - The incidence of cybercrime in Zambia is increasingly becoming a significant concern, as evidenced by the reported cases exceeding 100,000 in 2022, with projections indicating a potential escalation in the future. The high accessibility and control of mobile devices compared to conventional computers have rendered them prime targets for cybercriminals. This review aims to evaluate the strategies employed by inexperienced individuals in combating cybercrime and suggest enhanced cybersecurity measures to bolster the safeguarding of mobile devices. The study utilized an extensive literature review methodology, examining scholarly articles, reports, and relevant online sources. The study results provide insight into the prevailing cybercrime situation in Zambia and the susceptibilities linked to mobile devices. The subsequent discourse examines diverse strategies to alleviate these susceptibilities and provides suggestions for individuals, institutions, and decision-makers to enhance cyber protection measures. The following discourse delves into the strategies employed by novices to combat cybercrime, which include the implementation of antivirus software, robust passwords, and security configurations. Nonetheless, it is contended that these tactics in isolation are inadequate in ensuring the protection of mobile devices from the perils of cybercrime. As a result, enhanced cybersecurity tactics are being investigated, including adopting dual-factor authentication, mobile device management (MDM) applications, and data encryption. The significance of education and awareness in preventing cybercrime is also deliberated. The review concludes by emphasizing the necessity of implementing advanced cybersecurity measures to protect mobile devices against cyber threats in Zambia.

Keywords: Cybercrime, mobile devices, cybersecurity strategies, novice strategies, Zambia.

INTRODUCTION  
According to Sakala (2022) cybercrime in Zambia has turned into a critical and expanding concern, as proved by the revealed cases surpassing 100,000 in 2022. This pattern is expected to continue soon. Cell phones' powerlessness and openness have made them a favoured objective for cybercriminals, outperforming the customary accentuation on PCs. The escalating apprehension about cybercrime is not confined to Zambia exclusively but is a worldwide occurrence. The increased prevalence of mobile devices and internet connectivity in Zambia has resulted in an escalated susceptibility to a range of cyber threats for both individuals and organizations. Hence, it is crucial to evaluate the efficacy of current strategies employed by novices in combating cybercrime and investigate the possibility of enhanced cybersecurity measures for safeguarding mobile devices in Zambia. Multiple underlying factors contribute to the increasing menace of cybercrime in Zambia. A significant determinant is the escalating integration of technology within the nation. Zambia's segment is portrayed by a critical extent of youthful people who logically take on innovation, habitually experiencing its complexities interestingly. People who need insight and experience with computerized stages are at a higher gamble of succumbing to cybercrime because of their restricted information and abilities to defend themselves.
A significant proportion of the Zambian population lacks awareness regarding the necessary measures and precautions that are imperative to mitigate cyber threats. The individual in question may be deficient in understanding security software implementation, formulating robust and distinctive passwords, and incorporating certain online behaviours. Insufficient cognizance exacerbates the susceptibility of both individuals and entities to cyber assaults. Cybercrime has a significant and diverse impact on Zambia. Cybercrime can hurt the standing of organizations, bringing about a decrease in client trust and unwavering ness, notwithstanding the monetary misfortunes caused (Njovu, 2020). Besides, cybercrime habitually prompts wholesale fraud, a far-reaching offence that can cause extreme repercussions for impacted people. The act of stealing personal information has the potential to result in severe financial consequences, negatively impact credit records, and even jeopardize individual safety.

Methodology
A systematic exploration of the literature was carried out to conduct this review, utilizing scholarly databases, including PubMed, IEEE Xplore, and Google Scholar, as well as credible online sources and reports. The search query encompassed the keywords "cybercrime," "mobile devices," "cybersecurity strategies," and "Zambia." The literature was subjected to a screening process that considered its relevance, credibility, and recency to guarantee current and trustworthy information incorporation (Fischer & Newig, 2016). The results were systematically arranged, scrutinized, and amalgamated to furnish a thorough outline of the topic. As well as directing examination, the scientist likewise participated in a quest for news stories and blog entries relating to the topic. The scientist directed an exhaustive survey of the current writing to accumulate experiences on the different types of cybercrime predominant in Zambia, the usual methodology utilized by culprits to execute these offences, and the repercussions of cybercrime on the country. The data on cybercrime cases from the Zambian Police Service was also subjected to analysis by the researcher.

The review investigated the recurrence of cybercrime occurrences answered to policing every year, the classifications of cybercrime detailed, and the implications of these offences on the impacted gatherings. The discoveries of the information examination show a rising pattern in the detailed occurrences of cybercrime the policing in Zambia throughout recent years (Kobia, 2021). Phishing, malware, and ransomware were the most often revealed types of cybercrime in policing. The execution of these offences brought about important ramifications for the impacted gatherings, like financial hardship, encroachment upon individual personality, and impediment of social standing. The outcomes obtained from the complete survey of existing writing and meticulous examination of information show that the issue of cybercrime is on the ascent in Zambia. Further examination concerning cybercrime in Zambia is objective, and it is an officeholder upon the public authority to carry out measures to moderate this issue.

Findings

Cybercrime Landscape in Zambia
The research review gives bits of knowledge into the cybercrime situation in Zambia, explaining the different appearances of digital dangers that are boundless in the country. In Zambia, cybercrime is portrayed by pervasive events of phishing assaults, malware contaminations, fraud, and monetary misrepresentation. According to Chikumbi, (2022) the commission of these offences presents significant hazards to individuals and entities, with mobile devices being especially susceptible owing to their extensive adoption and inadequate security protocols. Phishing attacks represent a prevalent type of cybercrime within the Zambian context. Perpetrators frequently assume the guise of bona fide establishments, such as financial institutions or public authorities, through the transmission of electronic mail or text-based communications that exhibit an authentic appearance. The communications above commonly comprise hyperlinks that reroute individuals to deceptive web pages to induce them to divulge their data. Upon obtaining sensitive data from the victim, criminals utilize it for malicious intentions. The incidence of malware infections represents a significant cyber threat within the Zambian context. Malware, a type of software, is intentionally created to cause damage to computer systems or to extract sensitive information without the user's consent. Malicious software, commonly referred to as malware, has the potential to be propagated through diverse mediums such as electronic mail attachments, compromised webpages, or tangible storage devices like USB drives. Electronic devices are susceptible to data breaches, unauthorized access, or system disruption upon being infected. The emergence of ransomware attacks in Zambia has become a significant concern. Ransomware is a form of malicious software that employs encryption techniques to render the data of a targeted individual or entity inaccessible. Subsequently, the assailants request monetary compensation as a condition for decrypting the information and reinstating the authorization to access it. The perpetuation of this type of cybercrime can lead to significant ramifications for individuals and organizations, including but not limited to data loss, financial setbacks, and disruption of operations. The results additionally emphasize the main targets of cybercrime within the Zambian context. According to Zimba et al., (2022), Cybercriminals frequently target individuals, businesses, and government agencies owing to the valuable information they possess. Individuals are often singled out as potential targets due to their possession of personal information that can be exploited for malicious purposes such as identity theft or financial fraud. The financial information businesses possess renders them attractive...
targets for cybercriminals, who can exploit it for fraud or dispose of it on illicit markets. Government entities are susceptible to cyber intrusions because they manage confidential data that can be utilized for political or financial advantage.

**Novice Strategies Against Cybercrime**

In Zambia, it is a common practice for individuals and organizations to use novice strategies to safeguard themselves against cyber threats. The tactics above encompass rudimentary password safeguarding, installation of antivirus software, and constraining application authorizations. Although these measures offer a degree of safeguarding, they frequently prove inadequate in mitigating advanced cyber assaults and neglect to encompass wider security considerations. The implementation of rudimentary password safeguarding is a prevalent habit among the user population of Zambia (Mwilu, 2020). Depending on uncomplicated or readily predictable passwords can leave accounts susceptible to unauthorized entry. Individuals must comprehend the significance of generating robust, distinctive passwords and periodically modifying them to augment security. Installing antivirus software is a common approach utilized by individuals with limited experience in cybersecurity to protect their systems from potential malware attacks. Although antivirus software can identify and eliminate established threats, it may not adequately counter intricate and progressive forms of malware. To effectively reduce the risk of malware attacks, supplementary security measures, such as frequent software updates and vigilant browsing practices, must be implemented. The act of restricting application permissions on mobile devices is frequently implemented as a means of safeguarding personal information. Nonetheless, this approach could disregard other plausible susceptibilities, such as unremedied software susceptibilities or unsecured network connections. Adopting a comprehensive perspective towards mobile device security is of utmost importance for users, which entails considering various facets such as timely system updates, establishing secure network connections, and implementing application-allow listing measures.

**Improved Cybersecurity Strategies**

The study recommends implementing advanced cybersecurity measures in Zambia to safeguard mobile devices better and counter the constantly changing threat landscape. The tactics above encompass the deployment of dual-factor authentication, mobile device administration (MDM) applications, and information encryption. The execution of two-factor validation fills in as an expanded safety effort that orders clients to outfit two types of distinguishing proof before accessing their records. This approach mitigates the probability of an unpermitted section, even in the case of a secret word split difference. The execution of two-factor verification could significantly expand the security of cell phones and online records. Cell phones in the executive's (MDM) programming permit the two associations and people to oversee and get their cell phones from a distance (Oleksiewicz, 2019). Cell phone executive's (MDM) arrangements give a scope of functionalities, including gadget encryption, far-off information cleaning, and board application, which improve the degree of control and security of cell phones. Using Cell phones, the board (MDM) programming elements can successfully force security conventions and safeguard classified data, even when gadgets are lost or taken (Maurya, 2019). The execution of information encryption is a fundamental component in guaranteeing the security of cell phones. The demonstration of encoding information ensures that it will stay unintelligible to unapproved parties, even in case of gadget penetration. The demonstration of encoding secret information put away on cell phones can act as a method for people and elements to lessen the probability of information breaks and the unapproved obtaining of said data.

**Education and Awareness**

The importance of education and awareness in reducing cyber threats within Zambia cannot be overstated. The results underscore the significance of imparting knowledge to individuals, institutions, and decision-makers regarding optimal cybersecurity protocols. Through improving digital literacy and promoting cybersecurity awareness, individuals can effectively safeguard themselves against cybercrime (Herschel, 2021). The primary focus of educational initiatives should be directed towards topics that encompass safe browsing habits, identification of phishing attempts, generation of robust passwords, and evasion of suspicious links or downloads. In addition, organizations must give precedence to training their employees regarding the most effective cybersecurity practices and the possible hazards linked with cyber threats. Policymakers have the potential to enhance cybersecurity by advocating for legislation and regulations that prioritize safeguarding data, conducting cybersecurity awareness campaigns, and establishing partnerships with industry stakeholders to bolster the nation's overall cybersecurity posture.

The results of this analysis underscore the increasing menace of cybercrime in Zambia and the susceptibilities linked with mobile devices. The high occurrence rate of phishing attacks, malware infections, and ransomware incidents highlights the pressing necessity for improved cybersecurity protocols. Albeit learners ordinarily utilize fundamental secret word security and antivirus programming establishment to defend their computerized resources, these systems might demonstrate deficiencies notwithstanding progressed digital dangers. Accordingly, it is basic to execute upgraded network protection estimates like two-factor validation, Cell phone executives (MDM) programming, and information
encryption to guarantee the good defending of cell phones. Training and mindfulness crusades give people, associations, and policymakers vital information and abilities to explore the computerized climate securely (Ali et al., 2022). Zambia can gain striking headway towards upgrading its internet security and shielding its residents and organizations from cybercrime risks by stressing online protection training, upholding best practices, and empowering joint efforts among partners.

Discussion
The empirical evidence indicates that the magnitude of cybercrime in Zambia is noteworthy and is projected to escalate in the forthcoming period persistently. The prevalent forms of cybercrime in the country include phishing, malware, and ransomware. Committing such offences presents a significant hazard to private citizens, commercial enterprises, and public institutions. The implementation of advanced cybersecurity measures is imperative for the adequate safeguarding of mobile devices in Zambia. Multifactor authentication is a security strategy that enhances the security of user authentication by mandating the provision of supplementary credentials, such as a verification code dispatched to the user’s mobile device, in addition to their password (Richards & Eboibi, 2021). This approach substantially mitigates the likelihood of unapproved entry, notwithstanding the eventuality of password compromise. Frequent software updates are imperative for ensuring the security of mobile devices. Frequent updates are typically comprised of security patches to mitigate vulnerabilities malicious actors exploit in the digital realm. The act of regularly updating one’s devices can reduce the likelihood of encountering malware infections and other forms of cyber threats.

According to Ndawanà et al. (2021), the implementation of data encryption is a fundamental component of ensuring the security of mobile devices. Through the implementation of encryption protocols, sensitive data stored on mobile devices can remain unintelligible and inaccessible to unauthorized individuals, even in the event of loss or theft of the device (Maluleke, 2023). The incorporation of data encryption protocols provides an additional level of security to portable electronic devices and assists in preserving confidential data. Adopting secure browsing practices is imperative to reduce the likelihood of succumbing to phishing attacks and malware infections. It is advisable for individuals to exercise prudence when accessing links or downloading files from unfamiliar sources and to authenticate the authenticity of websites prior to divulging personal data. Implementing Mobile Device Management (MDM) solutions holds considerable importance in augmenting cybersecurity measures for individuals and organizations. Mobile Device Management (MDM) software facilitates the centralized administration and safeguarding of mobile devices. Functionalities such as erasing data remotely, tracking devices, and managing applications offer enhanced control and safeguarding against possible hazards. Implementing Mobile Device Management (MDM), solutions guarantee to enforce security policies, even when a device is lost or stolen. Supplementary to technical measures, the implementation of user education programs is imperative in enhancing cybersecurity. Through promoting cybersecurity awareness and providing training on optimal practices, individuals can enhance their ability to safeguard themselves and their devices against cyber threats. It is recommended that these programs prioritize subject matters such as identifying phishing attempts, formulating robust passwords, and comprehending the hazards linked to cybercrime.

Effective management of the cyber threat landscape necessitates collaboration among stakeholders, owing to the transnational nature of cybercrime. Public-private partnerships have the potential to enable the transfer of knowledge, assets, and specialized knowledge. Information-sharing platforms facilitate the distribution of threat intelligence, allowing entities and persons to remain abreast of nascent cyber threats (Kariuki et al., 2023). The significance of international collaboration in the fight against cybercrime cannot be overstated, given that cybercriminals conduct their activities beyond national boundaries. Through cultivating collaborative relationships and strategic partnerships, Zambia can enhance its capacity to address cyber threats more efficiently and coordinatedly. In addition, cultivating a cybersecurity culture via public awareness campaigns is imperative. The campaigns above have the potential to impart knowledge to individuals regarding the perils associated with cybercrime and foster the adoption of secure practices. Establishing a cybersecurity-aware community enables individuals to adopt preemptive measures towards safeguarding their personal information and digital resources.

The research results underscore the noteworthy danger posed by cybercrime in Zambia, with a particular focus on targeting mobile devices. Response in similar issue in Nigeria Chioma et al., nd) recommended that advanced cybersecurity tactics be employed. The tactics above encompass multifactor authentication, frequent software updates, encryption of data, secure browsing practices, Mobile Device Management (MDM) solutions, and educational initiatives for users. Effective cybersecurity measures require collaboration, partnerships among stakeholders, and public awareness campaigns. Through implementing these tactics and cultivating a cybersecurity-aware culture, Zambia has the potential to enhance its capacity to safeguard individuals, enterprises, and governmental entities against the constantly evolving menace of cybercrime.
Conclusion
The results of this analysis underscore the pressing need for improved cybersecurity measures aimed at safeguarding mobile devices against the growing menace of cybercrime in Zambia. Although novice strategies may provide a foundation, they are inadequate in addressing the dynamic and ever-changing landscape of cyber threats. Implementing comprehensive measures that effectively tackle the constantly evolving nature of cybercrime is of utmost importance. Adopting advanced cybersecurity measures, such as multifactor authentication, periodic software upgrades, data encryption, and user training initiatives, can substantially mitigate the likelihood of succumbing to cyber attacks for individuals, institutions, and policymakers. The strategies above offer a strong safeguard against cyber threats such as phishing attacks, malware infections, and other potential hazards that present a considerable peril to mobile devices. The potential danger posed by cybercrime in Zambia should not be underestimated. The proliferation of technology and the expansion of connectivity have led to an escalation in cyber threats. Thus, individuals, corporations, and government organizations must acknowledge the gravity of the circumstance and adopt preemptive measures to safeguard their digital resources. The significance of stakeholder collaboration and cooperation cannot be overstated in tackling the cross-border dimensions of cybercrime. The exchange of knowledge, resources, and best practices in combating cyber threats can be facilitated through public-private partnerships, information-sharing platforms, and international collaboration. In addition, cultivating a cybersecurity culture via public awareness campaigns is crucial in enabling individuals to embrace certain practices and contribute to a more secure digital milieu.

Recommendations
The review's results suggest that several crucial suggestions can be put forth to safeguard individuals, organizations, and the broader digital environment of Zambia against cybercrime. Initially, it is recommended that individuals prioritize implementing robust authentication techniques, such as multifactor authentication, to augment the security of their mobile devices (Maharaj & Munyoka, 2019). Incorporating extra security measures notably diminishes the likelihood of unapproved entry to confidential and personal data. In addition, individuals must regularly update their software, encompassing operating systems and applications. Frequent updates are typically comprised of security patches that aim to mitigate vulnerabilities and safeguard against newly emerging threats. Moreover, individuals must exercise prudence when perusing the internet and disseminating personal information on digital platforms. Maintaining awareness of current scams and phishing attacks is of utmost importance, and exercising caution when encountering dubious links or divulging personal information to unverified sources is strongly advised. Through vigilance and adherence to secure online practices, individuals can substantially diminish the probability of succumbing to cybercriminal activities.

Implementing comprehensive mobile device management (MDM), solutions is imperative for organizations. Mobile Device Management (MDM) solutions facilitate the centralized management and security of mobile devices, implementation of security policies, and remote data wiping for organizations in the event of loss or theft. It is recommended that routine security evaluations be carried out to detect and rectify weaknesses in the infrastructure and applications of mobile devices (Cornelius & Simon, nd). Furthermore, organizations must provide their employees with extensive cybersecurity education, enabling them to possess the expertise and proficiency to recognize and address potential cyber hazards proficiently.

The role of policymakers in shaping the cybersecurity landscape of Zambia is of utmost importance. The prioritization of cybersecurity legislation delineating specific guidelines and regulations for individuals and organizations is imperative for policymakers. Moreover, establishing platforms for sharing information among pertinent stakeholders, including government agencies, private sector entities, and cybersecurity specialists, facilitates the dissemination of threat intelligence and fosters cooperative endeavours in the fight against cybercrime. The allocation of resources towards public awareness campaigns holds equal significance in educating the populace on the perils of cybercrime and cultivating a society mindful of cybersecurity in Zambia. By adopting these suggested measures, stakeholders such as individuals, institutions, and policymakers can collaborate to enhance cybersecurity protocols, alleviate the vulnerabilities associated with cybercrime, and guarantee a more secure digital landscape for Zambia. Implementing proactive measures and a shared dedication to cybersecurity is essential in preserving mobile device security and upholding digital data's confidentiality and authenticity.

REFERENCES:
2. Cornelius, C., & Simon, T. Investigate And Evaluate The Security Measures Commonly Used In Electronic Banking Transactions In Zambia And Possible Solutions.