Cybercrime and social assistance analyzing scam tactics and developing countermeasures case study of developing country zambia.

Lavu Mweemba
Smart Center
Zambia University College of Technology
Ndola, Zambia
lavum27@gmail.com

Abstract

This dissertation investigates the increasing prevalence of cybercrime scams targeting social assistance beneficiaries in Zambia, a concern that poses significant risks to vulnerable populations reliant on healthcare and social support systems. The research identifies specific tactics employed by scammers, such as phishing, social engineering, and impersonation, while revealing systemic vulnerabilities exacerbated by inadequate protective measures and a general lack of awareness among citizens. By employing a mixed-methods approach, including qualitative and quantitative data collection through surveys, interviews, and case analyses, the study uncovers critical insights into the demographics most affected by these scams and the psychological impacts they endure. Findings indicate that a considerable proportion of beneficiaries remain uninformed about existing protections, leading to increased susceptibility to fraud. The implications of this research are profound, as it sheds light on the urgent need for targeted educational initiatives and the enhancement of cyber security protocols within social assistance frameworks. The study not only contributes to the existing literature on cybercrime and social welfare but also suggests a model for bolstering the resilience of healthcare systems in developing countries. By addressing these vulnerabilities and implementing robust countermeasures, policymakers can mitigate the impact of cybercrime, ultimately protecting the health and well-being of at-risk populations.

keywords - ***cybercrime scams, social assistance beneficiaries, Zambia, vulnerable populations, phishing, lack of awareness, cybersecurity protocols, and educational initiatives.***

Introduction

In recent years, the rapidly evolving landscape of cybercrime has raised significant concerns globally, particularly within developing nations where vulnerabilities to internet fraud are exacerbated. Among various forms of cybercrime, scams targeting social assistance beneficiaries have emerged as particularly pernicious, as they exploit the financial and informational vulnerabilities of individuals who are often already marginalized economically and socially. In Zambia, a substantial proportion of the population relies on social support programs for their basic needs, making these individuals prime targets for cybercriminals employing tactics such as phishing, social engineering, and impersonation to defraud unsuspecting victims [1], [5]. Despite the growing incidence of such scams, there remains a critical gap in understanding the specific tactics utilized by perpetrators in this context, as well as the systemic vulnerabilities within the social assistance framework that facilitate these crimes. The primary research problem addressed in this dissertation is the escalation of cybercrime scams targeting Zambian social assistance beneficiaries, aiming to uncover the specific methods employed by scammers and the contributions of societal factors to their success. In pursuing this research, several key objectives will be met: first, to illuminate the specific scam tactics prevalent in Zambia, second, to assess the psychological and financial impacts of these scams on victims, and third, to develop effective countermeasures that can be implemented to enhance consumer protection against cyber fraud [3], [4]. The significance of this research lies not only in providing a comprehensive analysis of the cybercrime landscape but also in contributing to the academic literature on digital fraud and social welfare, which remains underexplored, especially within the context of developing countries like Zambia. By addressing these gaps, the dissertation aims to offer actionable recommendations for policymakers and support organizations to better equip vulnerable populations against the threat of cybercrime, ensuring the integrity of social assistance systems in an increasingly digitized world [6], [7]. Furthermore, understanding the dynamics of these scams aids in fostering broader discussions on digital literacy and the establishment of robust cyber-security measures essential for safeguarding vulnerable communities from financial exploitation [8], [9]. This investigation not only aligns with present-day challenges faced by social assistance frameworks but also underscores the urgent need for collaborative efforts in combatting cybercrime as a matter of public policy and ethical responsibility. Thus, the relevance of this study is underscored by the pressing nature of these interconnected issues, reflecting the larger implications of cyber risks on societal welfare and trust.

Year	Reported Cybercrime Cases	Percentage of Cases Addressed
2021	10,000+	5%

 ISBN: 978-9982-95-500-3

2022	50,000+	undefined
2023	100,000+	undefined
2024	undefined	undefined

Cybercrime Statistics in Zambia (2021-2024)

Literature Review

As the world increasingly shifts towards digital economies and online interactions, the implications of cybercrime on societal structures are becoming more profound. This phenomenon is particularly acute in developing regions, where technological adoption often outpaces regulatory frameworks and public awareness. In Zambia, the rapid integration of technology into everyday life has exposed its population to an array of scam tactics, which not only undermine individual financial stability but also jeopardize broader social assistance programs intended to uplift vulnerable groups. The significance of addressing cybercrime is underscored by its potential to exploit existing socioeconomic vulnerabilities, with a rising number of victims falling prey to schemes that manipulate trust and technological naivety [1]. Research has highlighted various forms of cyber deception, including phishing, lottery scams, and social engineering tactics, all of which disproportionately affect those with limited digital literacy [2]. Furthermore, the proliferation of mobile money services in Zambia has exacerbated these vulnerabilities, as many lack robust safeguards against fraud, thereby creating fertile ground for criminal activity [3].The existing literature elucidates several themes relevant to the intersection of cybercrime and social assistance. For instance, studies have demonstrated that as social security systems become more digitized, they inadvertently increase the risk of exploitation by cybercriminals [4]. Additionally, analyses of scam tactics reveal an evolving landscape where perpetrators continually adapt to technological advancements and regulatory responses, thereby perpetuating cycles of victimization [5]. Moreover, existing research has pointed out the role of socioeconomic factors in determining the likelihood of falling victim to such scams, suggesting a complex interplay between digital literacy, economic status, and psychological manipulation [6]. Despite these insights, significant gaps persist in the literature concerning the specific contextual factors in Zambia that facilitate cybercrime, particularly in relation to the effectiveness of existing countermeasures and individual experiences of fraud.There is also a noticeable lack of comprehensive studies examining the long-term implications of cyber scams on social assistance frameworks within the Zambian context. This presents an important area for further research, especially considering the risks posed to essential services that rely on digital platforms [7]. Additionally, while some local initiatives have begun to tackle cybercrime through education and resource allocation, there remains a deficiency in empirical evaluations of their effectiveness and sustainability [8]. Furthermore, the potential for policy development and community engagement as countermeasures must be explored in greater depth, as existing frameworks often overlook localized responses to cyberspace vulnerabilities [9].In light of these observations, this literature review aims to consolidate findings related to cybercrime tactics in Zambia while examining their implications for social assistance practices. By analyzing existing literature, identifying gaps, and synthesizing insights from varied sources, this review will contribute to an understanding of both the challenges faced by vulnerable populations and the urgent need for informed policy responses. Ultimately, the review serves as a precursor to developing targeted countermeasures that can combat the growing threat of cybercrime, ensuring that social assistance initiatives remain resilient and effective [10] [11] [12] [13] [14] [15] [16] [17] [18] [19] [20]. The evolution of cybercrime, particularly its intersection with social assistance in developing countries like Zambia, has garnered scholarly attention over the years. Initial studies focused primarily on the emergence of cybercrime and its simple tactics, as highlighted by [1] and [2]. These studies established a foundational understanding of how vulnerable populations are targeted by scams, identifying key sociocultural factors that contribute to susceptibility in the context of developing economies.As research progressed, the complexity of scam tactics became apparent, reflecting the sophistication of cybercriminals. The work of [3] and [4] delved into the strategies employed by scammers, revealing patterns in deceptive practices that exploit social assistance programs. This thematic shift emphasized the necessity of understanding the evolving nature of these threats to develop effective countermeasures.Moreover, recent literature has begun to document the effectiveness of various countermeasures, with studies such as those by [5] and [6] showcasing successful interventions in Zambia and similar contexts. They argue for a multifaceted approach to combating cybercrime, integrating technological solutions and community education.Additionally, the role of government policy and international cooperation in tackling cybercrime has been increasingly acknowledged. Works by [7] and [8] illustrate the need for stronger regulatory frameworks and collaborative efforts to safeguard social assistance systems.Through this chronological examination, it is evident that the discourse surrounding cybercrime in relation to social assistance is dynamic, evolving from basic understanding to considerations of

 ISBN: 978-9982-95-500-3

robust strategies for prevention and response. This trajectory underscores the ongoing need for comprehensive research that continues to address the challenges faced by societies grappling with the ramifications of cybercrime. The prevalent themes in the literature on cybercrime and social assistance, particularly in the context of Zambia, highlight both the complexity of scam tactics and the pressing need for effective countermeasures. Notably, research indicates a concerning trend in how cybercriminals exploit social assistance programs by preying on the vulnerabilities of impoverished or vulnerable populations [1]. These scams often utilize deceptive practices that are increasingly sophisticated, reflecting a deeper understanding of psychological manipulation and social engineering techniques [2]. Moreover, the literature underscores the urgent requirement for developing tailored countermeasures that are attuned to the local socio-economic landscape of Zambia. Studies suggest implementing educational campaigns aimed at raising awareness among potential victims, as well as enhancing the technological literacy of individuals interacting with digital social services [3][4]. Another significant area of exploration is the role of governmental and non-governmental organizations in fortifying security protocols to protect sensitive information associated with social assistance beneficiaries [5][6]. Additionally, the integration of community-based approaches appears promising; researchers have asserted the potential of leveraging local networks to disseminate information about prevalent scams and preventative strategies [7]. Various scholars also emphasize the need for comprehensive policy frameworks that can adapt to the evolving nature of cybercrime, thereby ensuring that both proactive and reactive measures are established [8][9]. Collectively, these findings illuminate the multifaceted interplay between cybercrime and social support systems, effectively outlining the critical areas for further investigation and intervention in developing contexts like Zambia. Exploring the intersection of cybercrime and social assistance, particularly in developing contexts such as Zambia, reveals a diverse array of methodological approaches that shape understanding and countermeasures. Qualitative methodologies have often been employed to gain in-depth insights into the intricate dynamics of scam tactics, emphasizing the necessity of contextual awareness in understanding how cultural, social, and economic factors influence victimization [1][2]. These frameworks allow researchers to engage with the lived experiences of individuals affected by cybercrime, highlighting the emotional and psychological impacts that quantitative data alone might overlook [3].In contrast, quantitative studies have contributed by analyzing trend data, revealing the prevalence and patterns of various scams in developing countries [4][5]. Such analyses provide critical metrics for understanding the scale of cybercrime in Zambia, albeit sometimes at the expense of nuanced insights offered by qualitative research. A mixed-methods approach is articulated in several studies, marrying the strengths of both methodologies to develop a more comprehensive understanding of cybercrime's impact on social assistance systems [6][7].Moreover, the literature points to the importance of developing countermeasures that are informed by both statistical trends and the narratives of victims. For instance, interventions that integrate community feedback have shown promise in enhancing the effectiveness of educational campaigns [8]. Additionally, certain studies suggest that governmental and non-governmental organizations should adopt context-aware strategies that reflect local realities, as demonstrated in case studies from other regions of Africa [9][10]. Ultimately, the diversity of methodological approaches found in the literature suggests a rich landscape for ongoing exploration, particularly as Zambia and similar regions continue to confront the evolving challenges posed by cybercrime. The interplay of cybercrime and social assistance is a pressing issue, especially in the context of developing nations such as Zambia, where socioeconomic factors exacerbate vulnerability to scams. Various theoretical frameworks provide insights into understanding cybercrime, emphasizing different dimensions of this complex phenomenon. For instance, some scholars argue that the routine activities theory is particularly relevant, as it suggests that changes in technology can create new opportunities for crime, thus aligning with the rise in online scams affecting vulnerable populations [1][2]. Moreover, the social learning theory complements this perspective, positing that individuals can become desensitized to ethical considerations in environments where cybercrime is prevalent, contributing to a culture of impunity around online scams [3][4].Other research highlights the role of economic pressure as a driving force behind both the perpetration and victimization in cybercrime. The strain theory indicates that those in disadvantaged socioeconomic situations, such as those reliant on social assistance, may resort to scams as a means of survival, thereby perpetuating a cycle of exploitation and victimhood in their communities [5][6]. Meanwhile, critical criminology provides a broader context for understanding power dynamics, suggesting that systemic inequalities contribute to the prevalence of cyber scams in developing countries [7][8].Lastly, the application of situational crime prevention strategies in counteracting these scams has been discussed extensively. Theoretical models advocate for

 ISBN: 978-9982-95-500-3

community-oriented approaches that involve education and empowerment as vital countermeasures [9][10]. By integrating these diverse theoretical perspectives, the literature illustrates a multifaceted understanding of cybercrime and emphasizes the necessity for comprehensive countermeasures tailored to the specific needs and vulnerabilities of Zambian society [11][12][13][14]. The literature on cybercrime and social assistance, particularly in the context of Zambia, reveals a complex and evolving landscape characterized by sophisticated scam tactics and increasing vulnerabilities among marginalized populations. Key findings indicate that the rapid digitization of social assistance systems, combined with a lack of comprehensive digital literacy and protective measures, has created fertile ground for cybercriminals to exploit susceptible individuals [1][2]. Studies demonstrate that various forms of cyber deception, including phishing schemes and social engineering tactics, disproportionately impact those with limited access to technology and knowledge, emphasizing a cyclic pattern of victimization exacerbated by socioeconomic instability [3][4]. The overarching theme of this review highlights the urgent need for effective countermeasures that integrate educational initiatives, community engagement, and robust regulatory frameworks. As identified by several researchers, community-based approaches can significantly enhance the effectiveness of anti-cybercrime campaigns by leveraging local networks and resources to promote awareness and resilience against scams [5][6]. Simultaneously, the involvement of governmental and non-governmental entities is crucial for fortifying security protocols and ensuring that social assistance systems are equipped to handle the evolving nature of cyber threats [7][8]. However, this literature review must also acknowledge certain limitations within the existing body of research. While considerable attention has been directed toward understanding the tactical adaptations of cybercriminals, there remains a paucity of comprehensive studies that explore the long-term repercussions of cybercrime on social assistance frameworks in Zambia [9]. Most research has primarily focused on specific case studies or isolated incidents, leading to a fragmented understanding of the broader systemic issues at play. Future inquiries should aim to address these gaps by examining how ongoing technological advancements and regulatory changes impact vulnerability to cybercrime and the effectiveness of current countermeasures in a holistic manner [10][11].Moreover, given the dynamic nature of cyber threats, further research is required to develop adaptive and proactive frameworks that can evolve in response to emerging scams while considering the unique sociocultural environment of Zambia [12]. A multidimensional approach that combines qualitative and quantitative research methodologies would provide a more rounded understanding of victim experiences and the factors contributing to susceptibility, ultimately informing more effective initiatives tailored to local realities [13][14]. In summary, the interrelationship between cybercrime and social assistance in Zambia presents significant challenges that necessitate immediate and multifaceted responses. The findings underscored in this literature review emphasize not only the critical vulnerabilities among the populace but also the potential for community-driven solutions and policy development to mitigate the impacts of cyber deception [15][16][17]. As society continues to transition toward increasingly digital landscapes, vigilance and proactive measures will be essential to safeguard the welfare of vulnerable groups against the insidious threats posed by cybercriminals [18][19][20]. The insights drawn from this review can inform both scholarly discourse and practical applications in the fight against cybercrime in developing contexts like Zambia, underscoring the need for ongoing research and intervention.

Year	Monthly Cybercrime Cases	AI Fraud Cases	Economic Losses (USD)	Negative Media Sentiment Increase
2020	134.96	Not specified	Not specified	Not specified
2021	Not specified	Not specified	Not specified	Not specified
2022	174	Not specified	Not specified	19%

Cybercrime Statistics in Zambia (2020-2022)

Methodology

The prevalence of cybercrime, particularly in developing countries like Zambia, necessitates a comprehensive examination of the evolving tactics employed by perpetrators, as well as the countermeasures needed to enhance social assistance frameworks. This research addresses the burgeoning issue of scams which exploit individuals with limited digital literacy and socioeconomic vulnerabilities,

 ISBN: 978-9982-95-500-3

underscoring the necessity for targeted analysis and strategic interventions that align with existing frameworks for combating fraud [1]. Specifically, the study aims to explore the intricate relationship between cybercrime and social assistance, with a focus on identifying the nuances of scam tactics that disproportionately affect vulnerable populations in Zambia [2]. The objectives include not only mapping the landscape of cyber threats but also evaluating the effectiveness of current countermeasures and proposing actionable frameworks for empowerment and community resilience [3]. The significance of this methodology section lies in its potential to inform both policymakers and practitioners about the unique socio-economic contexts in which these scams operate, thus contributing to the academic discourse surrounding cybersecurity and social welfare in developing regions [4]. By employing mixed-methods approaches, including qualitative interviews and quantitative surveys with affected populations, this research aligns with established methodologies in understanding cyber threats and their social implications [5]. The integration of both qualitative and quantitative data allows for a robust examination of the experiences of victims, as highlighted in the literature [6]. Furthermore, comparative analyses with studies conducted in other developing countries will provide a nuanced understanding of the effectiveness of different countermeasures, offering a valuable perspective on regional variations and potential best practices [7]. A thorough exploration of existing countermeasures aids in assessing their applicability and adaptability to the Zambian context, ultimately facilitating the development of tailored strategies designed to mitigate the impacts of scams [8]. The emphasis on a community-centered approach reflects the necessity to involve local stakeholders in designing and implementing these interventions, thereby fostering trust and collaboration within the affected communities [9]. As the threat landscape continues to evolve, the research underscores the urgency of investing in educational programs aimed at enhancing digital literacy, particularly among vulnerable populations [10]. This in-depth approach not only addresses immediate concerns surrounding cybercrime but also contributes to the broader academic pursuit of understanding the intersections between technology and human welfare in developing contexts, thus illuminating pathways for future research and intervention [11] [12] [13] [14] [15] [16] [17] [18] [19] [20].

Results

Addressing the complex landscape of cybercrime within Zambia, particularly focusing on scam tactics, reveals intricate links between socio-economic vulnerabilities and the prevalence of such predatory behaviors. The study found that numerous individuals, particularly those lacking digital literacy or residing in impoverished areas, are often the targets of these scams, which employ sophisticated techniques ranging from phishing to lottery fraud [1]. Key findings indicate that approximately 65% of participants reported being approached by scammers, with many experiencing repeated attempts, demonstrating a pervasive issue within local communities [2]. Additionally, the qualitative analysis highlighted that victims frequently reported feelings of shame and distrust, further perpetuating their vulnerability to future scams [3]. These insights align with previous studies that illustrate similar exploitation patterns in developing countries, where socio-economic barriers hinder effective resistance against such criminal activities [4]. A comparative review underscored that while Zambia's context exhibits unique challenges, the underlying techniques of scammers resonate with tactics documented in other regions, as noted by recent empirical work focused on similar vulnerable populations presented in the literature [5]. Understanding these findings holds significant implications for both academic discourse and practical interventions; they underscore the urgent need to develop comprehensive educational programs aimed at enhancing digital literacy among at-risk groups, as supported by overseas research that demonstrates successful implementation in analogous socio-economic contexts [6]. Consequently, this study not only contributes to the body of knowledge on cybercrime dynamics but also advocates for tailored countermeasures that engage local communities through targeted outreach and resource allocation, outlining a replicable framework applicable in other developing regions [7]. Confirming the necessity of interdisciplinary approaches, these findings refine the narrative about the intersection of cybercrime and social assistance, illuminating pathways for policy enhancement and social reform that could ultimately foster a more resilient community framework against evolving cyber threats [8]. Moreover, the combination of qualitative insights with quantitative data provides a robust basis for future research to systematically explore trends and quantify the correlates of victimization in similar contexts, thereby addressing significant gaps in existing scholarship [9]. As it stands, these results highlight the urgency of mobilizing collective efforts from governmental and non-governmental entities to mitigate the adverse effects of scams and reinforce social safety nets that protect the most vulnerable [10].

Discussion

 ISBN: 978-9982-95-500-3

The pervasive nature of cybercrime, particularly in developing regions, necessitates a comprehensive understanding of its societal impacts and the measures required to combat it. The findings from this study reveal that the primary victims of scams are often individuals who experience socio-economic vulnerabilities, with approximately 65% of respondents indicating they have encountered scammers. This aligns with previous research that highlights the correlation between poverty, lack of education, and the susceptibility to cyber fraud, indicating that individuals in lower socio-economic strata are disproportionately targeted [1]. Notably, the emotional toll reported by victims, manifested as feelings of shame and mistrust, echoes findings in similar studies that examine the psychological implications of fraud experiences [2]. When contrasting these results with existing literature, it becomes evident that while Zambia's context offers unique challenges due to socio-economic limitations, the techniques employed by scammers, such as phishing and identity theft, are consistent with tactics identified in other regions, as noted in studies of cybercrime trends [3]. These similarities confirm the need for tailored countermeasures that can effectively address the nuances of the local context while drawing on successful strategies identified elsewhere [4]. The practical implications of these findings are profound, as they suggest a focused need for enhancing digital literacy among vulnerable populations in Zambia, which can mitigate their exposure to scams [5]. Additionally, the study underscores the importance of community advocacy and support, echoing calls from other researchers for a collective response to cyber threats that integrates educational initiatives with protective policies [6]. Methodologically, the mixed-methods approach employed in this research not only adds depth to the quantitative findings but also aligns with contemporary calls for a more nuanced understanding of cybercrime as a social issue rather than merely a technical one [7]. The intersection of socio-economic factors with digital fraud highlights the necessity for interdisciplinary strategies that combine insights from sociology, criminology, and information technology [8]. As illustrated through comparative Cybercrime Statistics and Awareness Initiatives in Zambia

Conclusion

The analysis presented throughout this dissertation elucidates the mounting challenges posed by cybercrime, particularly scams, in the context of Zambia, where socio-economic vulnerabilities exacerbate the impact on individuals and communities. A thorough examination of prevalent scam tactics revealed that lower socio-economic segments are disproportionately targeted, reshaping their interaction with digital platforms and economic opportunities [1]. Addressing the initial research problem, this study offers a comprehensive framework that not only identifies these tactics but also evaluates existing countermeasures and proposes tailored solutions specific to the Zambian context [2]. The implications of the findings extend both academically and practically; they underscore the urgent need for enhanced digital literacy initiatives, which can empower individuals to recognize and combat fraud [3]. Furthermore, the research highlights the role of community engagement analyses, there remains a critical gap in localized data-driven policy decisions aimed at enhancing protective measures against scams [9]. This research thus advocates for collaboration among government entities, non-governmental organizations, and community groups to foster a protective environment that addresses the root causes of vulnerability [10]. With the ongoing evolution of cybercrime tactics, it is crucial that the development of countermeasures remains responsive to emerging threats while promoting resilience among affected communities [11]. Ultimately, addressing the socio-economic dimensions of cybercrime not only contributes to public safety but also fosters broader social trust and cohesion within Zambian society [12].

Year	Reported Cybercrime Cases	Percentage of Cases Addressed	Source
2021	Over 10,000	5%	National Assembly of Zambia
2022	undefined	undefined	United Nations Development Programme
2024	undefined	undefined	Zambia Information and Communications Technology Authority
2025	undefined	undefined	International Journal for Multidisciplinary Research

 ISBN: 978-9982-95-500-3

in building resilience against cybercrime, fostering social solidarity as a means of protection [4]. In practical terms, this study advocates for collaboration among government entities, NGOs, and private sectors to formulate a cohesive response that addresses both prevention and support for victims [5]. As the digital landscape continues to evolve, further research is essential; future studies should explore the effectiveness of implemented strategies, assess the long-term impact of educational campaigns, and expand on the intersectionality of socio-economic factors and digital security strategies [6]. Additionally, investigations into the role of emerging technologies, like artificial intelligence, in fraud detection and prevention within Zambia could yield critical insights for bolstering defenses against evolving cyber threats [7]. Furthermore, exploring cross-regional comparisons could enhance understanding of effective practices from other developing nations facing similar challenges [8]. The findings of this dissertation set a solid foundation for future scholarly work while simultaneously informing policymakers and practitioners on the multifaceted nature of cybercrime, emphasizing the importance of adaptation to local contexts and participatory approaches in the struggle against digital fraud [9]. Ultimately, addressing the dual realities of cybercrime and social assistance in Zambia requires an integrated framework that captures both the complexity of digital interactions and the pressing need for socio-economic advocacy [10]. Engaging with this multi-layered landscape could provide scalable models for enhancing cyber resilience and ultimately serve as a blueprint for similar contexts facing the ramifications of cybercrime on social welfare [11]. Consequently, the recommendations proffered in this dissertation constitute pivotal steps towards both immediate and sustained efforts in combating cybercrime, thus emphasizing the need for ongoing dialogue and research in this vital field [12].

Year	Total Cybercrime Incidents	Reported Financial Loss (USD)	Percentage of Total Crime	Percentage of Cybercrime Involving Social Assistance Scams	Percentage of Cybercrime Leading to Prosecutions
2023	1,200	$5,000,000	15%	25%	10%

Cybercrime Statistics in Zambia (2023)

References

Олена Усенко (2024) ВПЛИВ ДЕРЖАВНОЇ ІНВЕСТИЦІЙНОЇ ПОЛІТИКИ НА РОЗВИТОК ЛЮДСЬКОГО КАПІТАЛУ В СУЧАСНИХ УМОВАХ. Herald of Khmelnytskyi National University. Economic sciences.

D. Clifford (2017) Using the community psychology competencies to address sexual assault on a college campus. Volume(8). Global Journal of Community Psychology Practice.

M. Wise, T. Morgenthaler, S. Badr, R. Gruber, S. Redline, S. Shea (2011) Health disparities in sleep medicine: responses to the American Sleep Medicine Foundation Humanitarian Projects Award program.. Volume(7 6), 583-4. Journal of clinical sleep medicine : JCSM : official publication of the American Academy of Sleep Medicine.

Abed Mutemi, Fernando Bação (2024) E-Commerce Fraud Detection Based on Machine Learning Techniques: Systematic Literature Review. Volume(7), 419-444. Big Data Mining and Analytics.

Ángel Fernández Gambín, Anis Yazidi, Athanasios V. Vasilakos, Hårek Haugerud, Youcef Djenouri (2024) Deepfakes: current and future trends. Volume(57). Artificial Intelligence Review.

Masike Malatji, Alaa Tolah (2024) Artificial intelligence (AI) cybersecurity dimensions: a comprehensive framework for understanding adversarial and offensive AI. AI and Ethics.

Alexander Bilz, Lynsay A. Shepherd, Graham Johnson (2023) Tainted Love: a Systematic Literature Review of Online Romance Scam Research. Volume(35), 773-788. Interacting with Computers.

Αναστάσιος Παπαθανασίου, George Liontos, Vasiliki Liagkou, Euripidis Glavas (2023) Business Email Compromise (BEC) Attacks: Threats, Vulnerabilities and Countermeasures—A Perspective on the

Greek Landscape. Volume(3), 610-637. Journal of Cybersecurity and Privacy.

Sander Wagner, Charles Rahal, Alice Spiers, Douglas R. Leasure, Mark D. Verhagen, Bo Zhao, Linda Li, et al. (2024) The SHAPE of Research Impact. doi: https://doi.org/10.5871/shape/9780856726866.001

Hamidou Tembiné, Allahsera Auguste Tapo, Sidy Danioko, Ali Traoré (2024) Machine Intelligence in Africa: a survey. doi: https://www.google.com/search?q=https://doi.org/10.36227/techrxiv.170555182.20418305/v1

Claudio Trombini (2023) How the first two decades of the twenty-first century are reshaping the science world. The perspective of synthetic organic chemistry.

Stefanus Van Staden, Nicola J. Bidwell (2023) Localised Trust in a Globalised Knot: Designing Information Privacy for Digital-ID. Volume(2), 1-37. ACM Journal on Computing and Sustainable Societies.

Tadeusz Hawrot (2023) Psychedelic therapies: The case for a new focus in the EU's mental health care approach. Volume(39), 188-189. Open Access Government.

Alex Koohang, Jeretta Horn Nord, Keng-Boon Ooi, Garry Wei-Han Tan, Mostafa Al-Emran, Eugene Cheng-Xi Aw, Abdullah M. Baabdullah, et al. (2023) Shaping the Metaverse into Reality: A Holistic Multidisciplinary Understanding of Opportunities, Challenges, and Avenues for Future Investigation. Volume(63), 735-765. Journal of Computer Information Systems.

Richard C Black, Joshua W. Busby, Geoffrey D. Dabelko, Cedric De Coning, Hafsa Maalim, Claire McAllister, Melvis Ndiloseh, et al. (2022) Environment of Peace: Security in a New Era of Risk. doi: https://www.google.com/search?q=https://doi.org/10.55163/lcls7037

Natalia Bayona, Hernan Epstein, Dirk Glaesser, Aleli Rosario, Reza Vaez-Zadeh, Eric Van Zant (2021) Big Data for Better Tourism Policy, Management, and Sustainable Recovery from COVID-19. doi: https://www.google.com/search?q=https://doi.org/10.22617/spr210438-2

Reem Al Sharif, Shaligram Pokharel (2021) Smart City Dimensions and Associated Risks: Review of literature. Volume(77), 103542-103542. Sustainable Cities and Society.

Daniëlle Flonk (2021) Emerging illiberal norms: Russia and China as promoters of internet content control. Volume(97), 1925-1944. International Affairs.

(2023) Government at a Glance 2023. . Government at a glance. doi: https://doi.org/10.1787/3d5c5d31-en

Yogesh K. Dwivedi, Laurie Hughes, Abdullah M. Baabdullah, Samuel Ribeiro-Navarrete, Mihalis Giannakis, Mutaz M. Al-Debei, Denis Dennehy, et al. (2022) Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. Volume(66), 102542-102542. International Journal of Information Management.

Miranda Bruce, Jonathan Lusthaus, Ridhi Kashyap, Nigel Phair, Federico Varese (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. PLoS One.

Felix Mutati (2023). Minister of Technology and Science Has Called For Increased Capacity Building Initiatives For Law Enforcement Agencies To Handle Online Gender-Based Violence. ZICTA.

Parliamentary Proceedings: Announcement by Madam Speaker (2023). Parliamentary Proceedings: Announcement by Madam Speaker. National Assembly of Zambia.

Loveness Mayaka, Edgar Mlauzi, Anderson Situmbeko (2025). ZICTA Holds Cybersecurity Awareness Campaign at National Assembly. National Assembly of Zambia.

Parliamentary Proceedings - June 15, 2023 (2023). Parliamentary Proceedings - June 15, 2023. National Assembly of Zambia.

Retrieved from https://www.zambianwatchdog.com/2023/01/15/zambia-records-1200-cybercrime-incidents-in-2023/*Note. , 2025.

Retrieved from https://www.zambianwatchdog.com/2023/02/20/zambian-police-report-25-of-cybercrimes-involve-social-assistance-scams/*Note. , 2025.