Technology Development and Cybercrime in Juja Sub-County

By

Ndirangu Ngunjiri

Abstract

Before technological advancements, the world primarily dealt with physical threats. However, with the rise of technology, cybercrime has emerged, becoming accessible to anyone possessing the required skills. Cybercrimes, such as stalking, hacking, phishing, online fraud, identity theft, and virus dissemination, have increased, employing increasingly sophisticated methods daily. These offenses inflict damage ranging from personal identity theft to financial losses, particularly affecting developing countries transitioning to cashless economies. This article explores the impact of technological growth on cybercrime within the Juja sub-county, illustrating how crime evolves alongside technology. An extensive review of existing literature highlights various types of cybercrimes and their consequences, emphasizing the challenges they pose to law enforcement globally. While the Internet offers immense development opportunities, it also serves as a breeding ground for criminal activities. This paradox underscores the need for enhanced regulation and enforcement, particularly in developing nations lacking adequate technology and infrastructure. The expansion of technology has made communication borderless and transnational, complicating cybercrime investigations that often require cooperation across multiple jurisdictions. The paper advocates for a comprehensive approach to combat cybercrime, including establishing robust legal frameworks, strengthening enforcement agencies with advanced technology, and empowering youth with entrepreneurial skills to deter involvement in cybercriminal activities. It also calls for universal criminalization of cyber offenses under international laws and treaties. To reduce the adverse effects of technology on development, the paper recommends creating products that are resilient to cybercrime and enhancing the processes for crime detection and investigation. Tracing the historical evolution of technology, underscores both its positive innovations and negative consequences, urging policymakers, businesses, and individuals to recognize cybercrime as a global issue requiring collective action.

Keywords: *Cybercrime, Cyberspace, hacking, Cyber-attacks, Computer Crime, Identity Theft, phishing, hackers, fintech*

Introduction

Over the past few years, advancements and breakthroughs in technology have completely transformed our lifestyles, professions, and methods of communication. Although these progressions have offered countless advantages and openings, they have also introduced fresh obstacles, especially concerning cybersecurity. Cybercrime, which refers to criminal activities carried out using computers and the internet, has become a growing concern in many parts of the world, including the Juja Sub-County in Kenya (Njuguna et al.,2021). This paper explores how technological developments and innovations have influenced the rise of cybercrime in Juja Sub-County, and discusses potential solutions to address this issue.

Cybercrimes range from minor intrusions to severe instances like identity theft and phishing. Illustrations of cybercrimes encompass scams and phishing, identity theft, ransomware assaults, hacking, and online fraud. Phishing happens when criminals send spam messages claiming to be legitimate sources to collect personal information. Prevention of phishing relies on detection measures (Khonji et al., 2013). Ransomware involves the installation of programs holding the computers of a person or programs ransom demanding payments. Credit card fraud is also a common form of cybercrime that goes unnoticed. Other forms of cybercrime include harassment and bullying, intellectual property theft, and child pornography.

There is an increased awareness globally regarding the importance of cybersecurity and the prevalence of cybercrimes. The cost of cybercrime has been increasing each year and it is expected to rise by 5.7 trillion US Dollars between 2023 and 2024 (Petrosyan, 2023). The cost currently stands at $13.83 trillion and it is expected to reach its maximum in 2028. The number of new ransomware used by cybercriminals has been on the rise with the peak attained in 2017, the number has been declining since then (Petrosyan, 2023). Figure 1 shows the number of new ransomware families that are discovered each year.

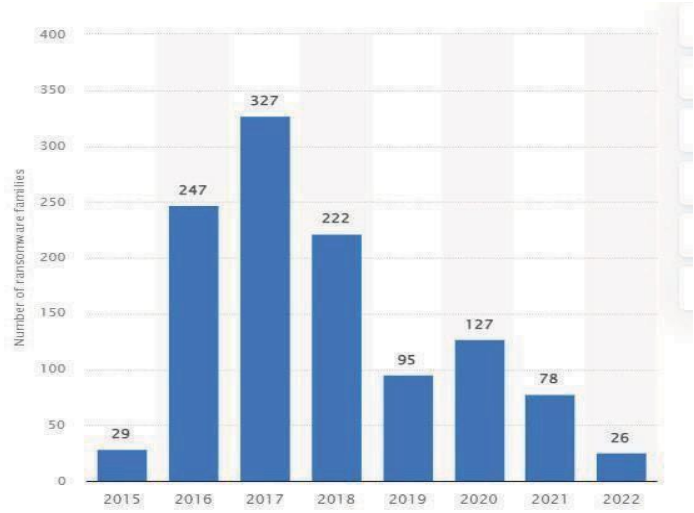

Figure 3: Number of New ransomware each year

Source: Statista,2023

Existing research shows that financial technology is the most affected sector by cybercrimes. Cybercrimes in this sector include the restriction of financial data, theft, modification of financial data, tampering with personal information stored in cards, etc. The ongoing digital transformations have led to increased risks of crimes in the financial sector, this is because of the rapid process of transformation with banks competing with the technological sector. For instance when the vulnerabilities of the SWIFT, the global financial system messaging system, were interfered with in 2016, over 100 Million dollars were lost (Maurer & Nelson, 2021) .

Deficiencies in cybersecurity law and existing loopholes are the greatest challenge to security globally in this century. Securing cyberspace is a challenge that has made it hard for even developed countries like the USA to manage their national security (Flowers et al., 2013. Countries are investing significantly in cybersecurity through the creation of institutions and security measures.

The paper addresses the issue of the recent surge in cybercrimes. There is increased development in the technology sector. As technology improves, there is also an increase in the need for people to adopt more security measures in the technology sector. More and more of human activities are being automated. Any cybersecurity dangers can affect almost all aspects of organizations. As

more and more aspects of organizations are digitized and as a large portion of everyday activities gets influenced by advancements in technology, so does cybercrime and the motivation of cybercriminals. Emily (2022) posits that technological advancement has improved the running of businesses, but that has also increased the need for cybersecurity.

Existing research shows that cybercrime is closely linked with technological advancement. However, the research also shows that technological development has led to a reduction in cybercrime (Bellasio & Silfversten, 2023). Different types of research conducted in the recent past show that an improvement in technology has encouraged more sophisticated forms of cybercrime (Oates, 2001). There is therefore a need to research to determine how technological development within Juja Sub-county in Kenya. Therefore, the main objective of this paper is to investigate how technological developments and innovations influence cybercrime in the Juja sub-county. The specific objectives are: First, to understand cybercrimes and technological developments in Kenya and specifically, the Juja sub-county. Second, to evaluate the effects of technological developments in Kenya on cybercrime in the Juja sub-county.Third, to examine the possible challenges and solutions for addressing cybercrimes in Juja Kenya

Theoretical Literature review

Diffusion of Innovation Theory

E.M. Rodgers introduced the diffusion of innovation theory in 1962, primarily employed in communication to elucidate the emergence and adoption of new concepts within a particular social group or population. The theory explains how new ideas and technology are spread (Rogers, 1962). The process by which new ideas are spread from one person to the other is heavily reliant on social capital and how cohesive a society is. The theory does not just explain the spread of ideas, technology, and information but also explains vices such as hacking, credit card fraud, and other cybercrimes.

According to the theory, people have different rates of adopting new ideas and technology. This is summarized by the chart below:

Figure 4: Diffusion of technology

Source: Leanmonitor Report,2022

Innovators and early adopters of cybersecurity benefitted from the benefits of securing their enterprises. Cybercriminals are innovators by nature and they keep coming up with new approaches when their old techniques are resolved, early adopters of cybersecurity can lock them out of their systems in time (Hasani et al., 2023). The offenders keep creating new malware and the defenders must keep innovating new methods of detecting the malware and dealing with them. One must always be ahead of the attackers to avoid being their next victim. The late majority and laggards are the ones that usually end up as victims of cyber-attacks.

Technology Acceptance Model

The Technology Acceptance Model (TAM) expands upon the Theory of Reasoned Action (Ajzen & Fishbein, 1980). Initially introduced by Davis in 1989, TAM offers further insights into how individuals perceive and adopt new technologies. The model explains how the ease of use and perceived usefulness influence the acceptance of technology (Davis, 1989). The model is mainly centered on explaining the perceptions of people and how they affect their adoption of technology. Innovators and those who come up with new products are also tasked with the responsibility of influencing the beliefs of the market concerning the perceived usefulness of their products.

Rick et al., (2016) argued that when users perceive the threat of cybercrime, they are likely to reduce their usage of technology or increase their adoption of cybersecurity measures. Cybersecurity farms have the responsibility of ensuring that companies and individuals understand

the usefulness of cybersecurity for them to adopt it. At times people discover this through their experiences when they experience one or more cybercrimes while at other times, the creation of awareness and sharing of information enables people to understand the usefulness of cybersecurity.

Analyzing the interplay between technological developments, innovations, and the rise of cybercrime in the Juja Sub-county reveals a complex relationship shaped by various factors. Firstly, technological advancements have facilitated the proliferation of cybercrime by providing sophisticated tools and platforms for illicit activities. The increasing digitization of financial transactions, communication channels, and personal data storage creates lucrative opportunities for cybercriminals to exploit vulnerabilities. Moreover, innovations such as artificial intelligence and cryptocurrency present new challenges for law enforcement agencies in detecting and preventing cybercrimes. AI-powered malware can evade traditional security measures, while cryptocurrencies offer anonymity and untraceable transactions, facilitating ransomware attacks and money laundering schemes.

Additionally, the rapid expansion of internet access and mobile technologies in the Juja Sub-county has widened the pool of potential targets for cybercriminals. As more individuals and businesses embrace digital technologies, they become more susceptible to cyber threats due to inadequate cybersecurity awareness and measures. Furthermore, the lack of robust cybersecurity infrastructure and regulations exacerbates the cybercrime problem in Juja Sub-county. Insufficient investment in cybersecurity initiatives and limited enforcement of existing laws create a conducive environment for cybercriminals to operate with impunity. The nexus between technological developments, innovations, and the rise of cybercrime in Juja Sub-county and Kenya at large underscores the urgent need for comprehensive cybersecurity strategies that encompass awareness campaigns, regulatory frameworks, and technological solutions tailored to the local context. Collaboration between government agencies, private sector stakeholders, and the community is essential to mitigate the escalating cyber threats and safeguard the digital ecosystem.

Methodology

The research design provides the blueprint of a study and it guides answering the research questions and how to minimize the errors (Dulock, 1993). This study used a qualitative descriptive research design to explore how technological developments and innovations influence the rise of cybercrime in Juja Sub-County, Kenya. The descriptive research design describes the relationship that exists between two different variables, such as technological progress and cybercrimes in this case (Siedlecki, 2020). A qualitative research design explains the aspects of a phenomenon that cannot be quantitatively measured (Patton, 2005). The qualitative Secondary data sources such as newspaper articles, published reports, research articles, and Journals were analyzed to understand the relationship between technological advancements and cybercrime.

The data collection process involved gathering relevant secondary data from various sources, including online newspapers, academic journals, research reports, and other published materials. The data was collected systematically and organized for analysis. A comprehensive search was conducted to identify relevant newspaper articles related to cybercrime and technological developments in the Juja Sub-County. Both print and online newspapers were considered for gathering recent information. Government reports, organizational reports, and any other published documents concerning cybercrime, technological advancements, and their impact on Juja Sub-County were also consulted to obtain the required. This paper also used academic studies and research papers published in scholarly journals and conference proceedings, focusing on cybercrime and the influence of technology. Peer-reviewed academic journals, books, and other relevant literature discussing the relationship between technology and cybercrime were also examined to gain insights into the topic.

A purposive sampling technique was used to select relevant secondary data sources for analysis. Only data that specifically pertains to technological advancements and cybercrime in the Juja Sub-County will be included in the study. The selected data sources were critically reviewed and analyzed for their relevance and reliability. The inclusion criteria required that all the data sources be recent and that the oldest source was not more than 30 years old. The data sources were also required to be reliable and relevant to technological developments and cybercrimes in Kenya.

The collected data was analyzed using thematic and content analysis. Themes related to the impact of technological developments on cybercrime trends in the Juja Sub-County will be identified and analyzed. Patterns, trends, and correlations will be examined to understand the influence of technological innovations on cybercrime. The data sources were critically evaluated to ensure their reliability and validity. Particular attention was paid to the credibility and authoritativeness of the sources. The findings from the content analysis are integrated to form a coherent understanding of how technological developments and innovations influence the rise of cybercrime in the Juja Sub- County. Existing theories or frameworks relevant to cybercrime and technology were considered in interpreting the findings to provide a theoretical perspective. The key factors influencing therise of cybercrime were identified, considering the technological landscape and its impact on cybercriminal activities in the area.

One of the limitations of this study is the availability and quality of secondary data sources. The accuracy and reliability of the data collected from newspaper articles, published reports, and other sources may vary. Efforts will be made to critically evaluate the sources and ensure the validity of the information used in the analysis.

Discussion of Findings

Cybercrime in Kenya

Cybercrime is a growing concern in Kenya, as the country continues to embrace digital technologies and the internet. As smartphone usage, social media engagement, and online activity continue to rise, cybercriminals are discovering novel methods to exploit both individuals and organizations for financial motives or nefarious purposes. This article aimed to delve into the diverse forms of cybercrimes prevalent in Kenya, elucidate their repercussions on individuals and enterprises, and examine the countermeasures being implemented to confront this escalating menace.

Phishing stands out as one of the prevalent forms of cybercrime in Kenya. This deceitful practice entails the transmission of fraudulent emails or messages to unsuspecting individuals, coaxing them into divulging sensitive information like passwords, credit card data, or personal particulars. These deceptive communications often masquerade as legitimate correspondences from trusted entities such as banks or government bodies, exhibiting a high degree of credibility. Upon

obtaining this sensitive data, cybercriminals can perpetrate various illicit activities, including monetary theft, identity fraud, or other unlawful endeavors.

Another prevalent form of cybercrime in Kenya is online fraud. This includes scams such as fake job offers, lottery scams, and online shopping scams. In these cases, individuals are tricked into sending money or personal information to cybercriminals under pretenses. These scams can have devastating consequences for victims, who may lose their life savings or fall into debt as a result.

Cyberbullying is also a significant issue in Kenya, particularly among young people. Cyberbullies use social media, messaging apps, and other online platforms to harass, intimidate, or threaten their victims. This can have serious consequences for the mental health and well-being of those targeted, leading to anxiety, depression, and even suicide in extreme cases.

The forms of cybercrimes and forms of cybercrimes reported in Kenya in 2021 are summarized in the table below:

Cybercrime	Number in thousands
Malware	181879
Botnet/DDOS	92108
Web application attacks	7037
System vulnerabilities	58046

Source: Statista,2022

Beyond the prevalent cybercrime types, Kenya grapples with the complexities of more advanced threats, including hacking, malware, and ransomware attacks. Hackers adeptly breach computer systems or networks without authorization, aiming to pilfer data, disrupt operations, or execute further malevolent deeds. Malware, encompassing viruses and spyware, surreptitiously infiltrates devices, siphoning sensitive information from users. Ransomware attacks add another layer of peril by encrypting victims' data, and extorting payment in exchange for the decryption key, often accompanied by the menacing prospect of data exposure if the ransom remains unpaid.

The number of cybercrimes in Kenya and online crimes increased from 339.1 million in 2021 to over 700M online crimes in 2022 (Lawi, 2023). The number of cyberattacks increased to over 860

million in 2023 (Musau, 2024). About 79% of these attacks were due to system vulnerabilities. The number of cybercrimes has been increasing from 7.7 million attacks 7 years ago to now over 800 million. Malicious attacks constitute 14% of the attacks, while "Distributed Denial of Services (DDoS)" contributed to approximately 6.55 of all the attacks.

The impact of cybercrime in Kenya is significant, affecting individuals, businesses, and the economy as a whole. Victims of cybercrimes can suffer financial losses, emotional distress, and damage to their reputations. Businesses may face disruption to their operations, loss of sensitive data, and damage to their brand image. The economy as a whole can suffer from the loss of consumer trust, reduced investment, and increased costs associated with cybersecurity measures.

To combat the growing threat of cybercrime in Kenya, the government and law enforcement agencies have taken steps to strengthen cybersecurity measures and improve awareness among the public. The Computer Misuse and Cybercrimes Act passed in 2018 (Governement of Kenya, 2018), provides a legal framework for prosecuting cybercriminals and protecting individuals and organizations from online threats. The Act criminalizes offenses such as unauthorized access to computer systems, cyberbullying, and online fraud, with penalties including fines and imprisonment.

In tandem with legislative actions, the government has set up the National Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) to streamline cybersecurity endeavors and address cyber incidents (Government of Kenya, 2024). This center collaborates with government bodies, private sector entities, and international collaborators to surveil and alleviate cyber threats, administer training and awareness initiatives, and extend assistance to victims of cybercrimes.

Private sector entities in Kenya are proactively fortifying their cybersecurity fortifications to shield against cyber threats. Numerous businesses are allocating resources toward cybersecurity technologies like firewalls, antivirus software, and encryption tools to fortify their data and networks. Additionally, they're instituting robust security policies and protocols to enlighten employees about the perils of cybercrime and advocate for secure online conduct.

Despite these efforts, cybercrime remains a significant challenge in Kenya, with new threats emerging regularly and cybercriminals becoming increasingly sophisticated in their tactics. To

effectively combat cybercrime, a multi-faceted approach is needed, involving collaboration between government agencies, law enforcement, private sector organizations, and the public. This includes investing in cybersecurity infrastructure, improving awareness and education programs, and strengthening legal frameworks to prosecute cybercriminals and protect victims. These efforts led to a 55% reduction in the number of cybercrimes in Kenya by the end of 2023 (Mwangi, 2023).

In a nutshell, cybercrime is a growing threat in Kenya, with a wide range of offenses including phishing, online fraud, cyberbullying, hacking, and malware attacks. These crimes have serious consequences for individuals, businesses, and the economy, leading to financial losses, emotional distress, and damage to reputation. To address this challenge, the government, law enforcement agencies, and private sector organizations must work together to strengthen cybersecurity measures, raise awareness among the public, and prosecute cybercriminals effectively. By taking a proactive and collaborative approach, Kenya can better protect itself from the growing threat of cybercrime and ensure a safe and secure online environment for all.

Technological Developments and Innovations

Technological advancements and innovations have revolutionized our interactions with the world. With the emergence of the internet, mobile devices, and social media platforms, connecting with others, sharing information, and conducting business online has become more accessible. Kenya stands out as the ICT hub of the East African region (International Trade Authority, 2023). Nevertheless, these advancements have also introduced new avenues for cybercriminals to exploit vulnerabilities within digital systems and networks.

One of the key technological developments that have influenced the rise of cybercrime in the Juja Sub-County is the proliferation of mobile devices. According to the World Bank, Kenya's ICT sector has grown by over 10.8% since 2016 (World Bank Group , 2019). Over 10 years ago, very few Kenyans had access to Android phones, but almost 85% of the people can now access these devices and about 80% of the country has access to a 3G network (Ngila, 2020). With the increasing popularity of smartphones and tablets, more people are accessing the internet and conducting transactions online. In 2010, internet penetration in Kenya was 9.7%, this has grown to over 89.7% in less than 15 years. There has also been a rise in fintech and other technologies within the past decade. Content consumption and other uses of technology such as online taxis, as well as e-commerce development are major developments in the technology sector. This has made

it easier for cybercriminals to target individuals and organizations through phishing scams, malware attacks, and other forms of cybercrime.

Another important technological development is the rise of social media platforms. Research shows that approximately 22.5 Million Kenyans had access to the internet in 2023 and the number is projected to increase to 39 million Kenyans by the year 2028 (Cowling, 2022). While these platforms have revolutionized the way we communicate and share information, they have also become breeding grounds for cybercriminals. Social media users are often targeted by scammers who use fake profiles and phishing emails to steal personal information and financial data. Moreover, the growth of e-commerce and online banking has created new opportunities for cybercriminals to carry out fraud and identity theft. With more people shopping and banking online, cybercriminals have developed sophisticated techniques to steal sensitive information and exploit vulnerabilities in digital payment systems.

Technological Developments and Cybercrime in Kenya

Technological developments have had a significant impact on cybercrimes in Kenya, as they have provided both opportunities for criminals to exploit and tools for law enforcement agencies to combat these crimes. Ngujiri(2022) noted that before technology developed the world's only threats were those from physical threats. People had to physically rob banks to steal and criminals had to engage in crimes by being at the actual scenes of crime.

One of the key effects of technological developments on cybercrimes in Kenya is the increasing sophistication of cybercriminals. The sophistication of cybercrimes has been increasing with an increase in technology. In the late 20th century, the cases of cybercrimes were low, however, as technology keeps advancing, so does the sophistication of cybercriminals (Ojedokun, 2005). As technology advances, cybercriminals can develop more complex and sophisticated methods of carrying out their illegal activities. The Business Daily newspaper in 2021 recorded that as internet usage in Kenya increased, cybercrime increased by 37% (Onyando, 2021). These advancements encompass sophisticated malware, phishing scams, and other tactics employed by cybercriminals to pilfer sensitive information, including financial data and personal details. Such advancements pose challenges for law enforcement agencies, as criminals continually adapt their tactics to outpace authorities, making it more arduous to detect and prevent cybercrimes.

Technological developments have also led to the increasing prevalence of online fraud and identity theft. With the rise of e-commerce and online banking, more and more Kenyans are conducting financial transactions online, making them vulnerable to cybercriminals who seek to steal their personal and financial information. Since the onset of the use of mobile money, over 30% of the users, approximately 5 Million accounts have been victims of theft and fraud (Sunday , 2020). Consequently, there has been a surge in cases of identity theft, wherein perpetrators utilize pilfered information to initiate fraudulent accounts or unauthorized transactions. The convenience and anonymity afforded by the internet facilitate cybercriminals in perpetrating these offenses, posinga substantial threat to individuals and enterprises in Kenya.

Furthermore, technological developments have also facilitated the spread of cybercrimes across borders. The proliferation of the internet and digital communication has empowered cybercriminals to operate from any location globally, rendering it challenging for law enforcement agencies to trace and apprehend them. Consequently, there has been a surge in transnational cybercrimes, encompassing online scams and cyberattacks, which can have profound repercussions for individuals and enterprises in Kenya. The global nature of cybercrimes presents a challenge for authorities, as they must work together with international partners to combat these crimes effectively.

In response to the growing threat of cybercrimes in Kenya, law enforcement agencies and government authorities have implemented various strategies to address the issue. One of the key strategies is the establishment of specialized cybercrime units within the police force, tasked with investigating and prosecuting cybercrimes. These units are equipped with the latest technology and training to combat cybercrimes effectively, including forensic tools to analyze digital evidence and track down cybercriminals. Additionally, the government has enacted legislation to criminalize cybercrimes and provide a legal framework for prosecuting offenders.

Another strategy being employed to combat cybercrimes in Kenya is the promotion of cybersecurity awareness and education. The government, in collaboration with private sector partners, has launched campaigns to educate the public about the risks of cybercrimes and how to protect themselves online. This includes providing tips on how to create strong passwords, avoid phishing scams, and secure personal information online. By raising awareness about cybersecurity

issues, the government aims to empower individuals and businesses to protect themselves from cybercrimes and reduce their vulnerability to online threats.

Furthermore, the government has also partnered with international organizations and law enforcement agencies to enhance cybersecurity capabilities in Kenya (KNA, 2023) This includes sharing information and intelligence on cyber threats, conducting joint investigations, and providing training and technical assistance to strengthen cybersecurity defenses. By collaborating with international partners, Kenya can leverage their expertise and resources to combat cybercrimes more effectively and protect its citizens from online threats.

Technological developments have had a significant impact on cybercrimes in Kenya, presenting both challenges and opportunities for law enforcement agencies and government authorities. While the increasing sophistication of cybercriminals and the prevalence of online fraud pose significant threats to individuals and businesses in Kenya, the government is taking proactive steps to address these issues. By establishing specialized cybercrime units, promoting cybersecurity awareness, and collaborating with international partners, Kenya is working to strengthen its cybersecurity defenses and combat cybercrimes effectively. However, the evolving nature of technology and the global reach of cybercrimes require a coordinated and multi-faceted approach to address these challenges effectively. By continuing to invest in cybersecurity capabilities and partnerships, Kenya can better protect its citizens and businesses from the growing threat of cybercrimes in the digital age.

The Influence of Technological Developments on Cybercrime in Juja Sub-County

The influence of technological developments on cybercrime in Juja Sub-County can be seen in the increasing number of cyberattacks and data breaches reported in recent years. According to a report by the Communications Authority of Kenya (2024), cybercrime incidents in Kenya have been on the rise, with a significant number of cases reported in Juja Sub-County.

One of the main factors driving the rise of cybercrime in Juja Sub-County is the lack of awareness and education about cybersecurity (KNA, 2023). Many individuals and organizations in the region are not adequately informed about the risks and threats posed by cybercriminals, making themmore vulnerable to attacks. In addition, the rapid pace of technological advancements has made it difficult for law enforcement agencies and cybersecurity experts to keep up with the evolving tactics and techniques used by cybercriminals.

The surge of cybercrime in Juja Sub-County is exacerbated by the absence of adequate cybersecurity measures and infrastructure. Many businesses and government entities lack robust protocols, rendering them vulnerable to cyber intrusions and data theft. Moreover, the prohibitive costs of cybersecurity solutions and the scarcity of skilled professionals in the field present significant challenges for organizations seeking to bolster their defenses against cyber threats.

Additionally, the ubiquity of social media platforms and online communication channels provides cybercriminals with ample opportunities to target individuals and entities in the Juja Sub-County. Scammers often employ social engineering tactics to deceive people into disclosing personal information or clicking on malicious links, resulting in data breaches and financial harm.

Conclusion

Technological developments and innovations have had a profound impact on the rise of cybercrime in the Juja Sub-County. The surge in mobile devices, social media platforms, and online communication channels has opened up new avenues for cybercriminals to exploit vulnerabilities and target individuals and organizations in the region. To counter this escalating threat, it is imperative to heighten awareness about cybersecurity risks, allocate resources toward cybersecurity infrastructure, and cultivate collaboration among stakeholders. By adopting a proactive and comprehensive strategy, Juja Sub-County can bolster its defenses against cybercrime and safeguard its residents and businesses from digital threats.

Recommendations

Potential Solutions to Address Cybercrime in Juja Sub-County

- To effectively address the rise of cybercrime in the Juja Sub-County, a tailored and comprehensive approach is essential, integrating technological solutions, educational initiatives, and collaborative efforts among stakeholders. One key strategy is to heighten awareness about cybersecurity risks and best practices specifically tailored to the local community. This can be achieved through targeted public awareness campaigns, specialized workshops, and training programs aimed at educating individuals and organizations in the region about the importance of safeguarding their personal information and digital assets.
- Moreover, it is critical to allocate resources towards strengthening cybersecurity infrastructure within the Juja Sub-County. This involves investing in localized solutions

such as firewalls, antivirus software, and encryption tools to fortify defenses against cyber threats tailored to the unique needs of the community. Additionally, conducting regular security audits and penetration testing exercises within local organizations can help identify and address vulnerabilities in their networks, enhancing overall cybersecurity posture.

- Furthermore, fostering collaboration among local government agencies, law enforcement authorities, and cybersecurity experts is paramount in combating cybercrime effectively. By facilitating information-sharing and resource pooling, stakeholders such as the county commissioner and the Ministry of Interior can work together to investigate cyberattacks, track down cybercriminals operating within the region, and prosecute offenders. Additionally, forging partnerships with international organizations and cybersecurity firms can provide access to advanced technologies and expertise, further enhancing the Juja Sub-County's cybersecurity capabilities in line with its specific challenges and requirements.

References

Bellasio, J., & Silfversten, E. (2023). The impact of new and emerging technologies on the cyber threat. *Kings College London*.

Cowling, N. (2022). Social Media in Kenya. *Statista*.

Dulock, H. L. (1993). Research Design: Descriptive research . *Journal of Pediatric Oncology Nursing*, 10(4),154-157.

Government of Kenya. (2018). The Computer Misuse and Cybercrimes Act. *Government of Kenya Printers*.

Government of Kenya. (2024). Communication Authority of Kenya. *Government Printers.*

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, A., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business&Economics,3(5)*.

International Trade Authority. (2023). Kenya-Information, Communications, and Technology(ICT). *International Trade Administration*.

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. *IEEE Communications Surveys & Tutorials, 15(4), 2091-2121*.

KNA. (2023). Government to strengthen cybersecurity measures and combat cybercrime. *Kenya News Agency*.

Lawi, J. (2023). Cybercrime is on the rise as Kenya faces 1 million threats every day. *The Star newspaper*.

Maurer, T., & Nelson, A. (2021). The global cyber threat to financial systems. *IMF Finance and Development*.

Musau, D. (2024). Kenya was hit by a record 860 million cyber-attacks in 2023. *Citizen Digital.*

Mwangi, K. (2023). Kenya cyber-attacks down 55pc on awareness drives, digital signatures. *Business Daily Africa.*

Ngila, F. (2020). How technology changed the lives of Kenyans in the past 10 years. *Business Daily Africa Newspaper*.

Ngujiri, N. (2022). Technological Developments Influence the Cybercrime in Juja Sub-County. *University of Nairobi.Research week presentation.*

Njuguna, D., Kamau, J., & Kaburu, D. (2021). Model for mitigating smishing attacks on mobile platforms. *In 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE*.

Ojedokun, A. A. (2005). The evolving sophistication of internet abuses in Africa. *The International Information & Library Review*, 37(1), pp.11-17.

Onyando, W. (2021). Cybercrimes Surge by 37pc as usage of the internet increases. *Business Daily Africa Newspaper*.

Patton, M. Q. (2005). Qualitative research. *Encyclopedia of Statistics in Behavioral Science*.

Petrosyan, A. (2023). Concerns regarding cyberattacks worldwide. *Statista*.

Rick, M., Bohme, R., & Moore, T. (2016). Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing*, 13(2),261-273.

Rogers, E. M. (1962). Diffusion of innovations. *New York.*

Siedlecki, S. L. (2020). Understanding descriptive research designs and methods. *Clinical Nurse Specialist*, 34(1),8-12.

Sunday, F. (2020). Phone Users losing millions through identity theft. *The Standard Newspaper*.

World Bank Group. (2019). Kenyan economic update: Accelerating Kenya's Digital Economy. *World Bank*.