TECHNOLOGICAL DEVELOPMENTS AND INNOVATIONS INFLUENCE CYBERCRIME RISE IN JUJA SUB-COUNTY

Ndirangu Ngunjiri

Abstract

Before there was technological growth, the world only had physical threats. However, the emergence of technology creates cybercrime that may be skilled via way of means of anyone. Cybercrimes have grown steadily with perpetrators growing more recent and extra state-of-the-art strategies daily. The maximum distinguished offenses are stalking, hacking, phishing, online fraud, identification theft, and dispensing viruses. These crimes purpose harm to private identification, fraud, forgery, threat, and financial losses. Cybercrimes cause severe damage in developing countries driving toward a cashless economy.

Purpose: This article aims to study the effect of the technology boom on cybercrime in the Juja sub-county as a version of crime that develops with the advancement of technology.

Methodology: The concepts of cybercrimes are introduced and different types of cybercrimes are explored as examples of some of the impacts caused by cybercrimes activities. The analysis in this paper is based on an extensive review of published research works, which provide theoretical and empirical evidence on the effects and impact of the internet on the development

Findings: There are many terrible effects the society suffers from cybercrimes and why computers or networking are geared goal for crimes. The paper commonly concludes that the net is overwhelmingly an effective device for development. Paradoxically, the net is a "double-edged sword", presenting many possibilities for people and firms to increase however an equal time, has introduced with it new possibilities to devote crime. The paper argues that the net affords new demanding situations to regulation enforcement in each evolved and growing international location. However, growing international locations go through substantially from the sports of net crime than their evolved opposite numbers as growing international locations have insufficient generation, infrastructure, and inadequate regulation enforcement expertise. Development in Technology allows cybercrimes and creates worry Information Technology widened the verbal exchange sphere making it Borderless and Transnational.

Practical implications: This paper reminds people, agencies, and coverage makers alike that cybercrime has turned out to be an international difficulty that calls for the entire participation and cooperation of each evolved and growing international location on the global level, as net crime investigations regularly require that proof be traced and accumulated in extra that one ICT

industries ought to awareness now in designing merchandise which is proof against crime and may facilitate detection and research of crime.

Value: The main novelty of this paper is that it lines the historic evolution of the technology after which sketches out a number of the improvements the net has introduced in addition to thinking about the terrible outcomes related to this generation and its effect on development.

Recommendations: Introduction of a concrete legal framework, establishment, and strengthening of cybercrime regulation enforcement agencies whole with excessive generation tracking gadgets and cutting-edge infrastructure. Empower the youths while in college with entrepreneurial skills. Cybercrime may be predicted via way of means of growing safety in the company community while speaking to the outdoor world. There is a want for the Universal Criminalization of Cyber Offences below International legal guidelines and treaties.

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

Table of Contents

Abstract i

Introduction 1

Background to the Study 1

Research Problem 2

Research Objectives 3

Theoretical Literature Review 3

Diffusion of Innovation Theory 3

Technology Acceptance Model 4

Methodology 6

Research Design 6

Data Collection 6

Data Analysis 7

Limitations 7

Findings and Discussion 8

Cybercrime in Kenya 8

Technological Developments and Innovations 10

Technological Developments and Cybercrime in Kenya 11

The Influence of Technological Developments on Cybercrime in Juja Sub-County 14

Recommendation and Conclusion 14

Potential Solutions to Address Cybercrime in Juja Sub-County 15

Conclusion 15

References 16

Introduction

Background to the Study

In recent years, technological developments and innovations have revolutionized the way we live, work, and communicate. While these advancements have brought numerous benefits and opportunities, they have also given rise to new challenges, particularly in the realm of 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. This paper will explore how technological developments and innovations have influenced the rise of cybercrime in Juja Sub-County, and discuss potential solutions to address this issue.

Cybercrimes vary from basic interference to extreme cases of identity theft and phishing. Examples of cybercrimes include phishing and scams, identity theft, ransomware attacks, hacking, and internet 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). The graph below shows the number of new ransomware families that are discovered each year.

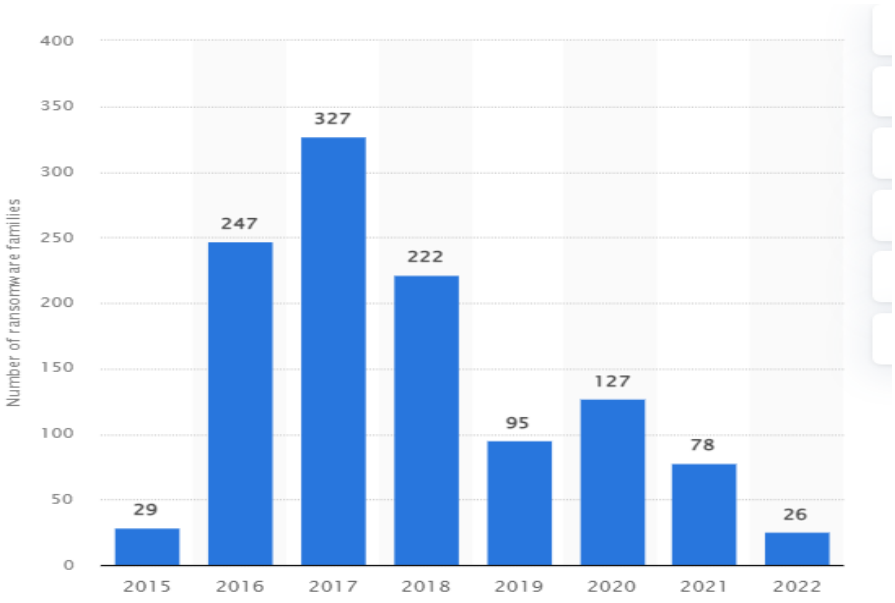


Figure 1: Number of New ransomware each year

Source: Statista

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.

Research Problem

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 et al., 2020). 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.

Research Objectives

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:

1. To understand cybercrimes and technological developments in Kenya and specifically, Juja sub-county
2. To evaluate the effects of technological developments in Kenya on cybercrime in the Juja sub-county
3. To examine the possible challenges and solutions for addressing cybercrimes in Juja Kenya

Theoretical Literature review

Diffusion of Innovation Theory

The diffusion of innovation theory was proposed by E.M. Rodgers in 1962. It was mainly used in communication to explain how a new idea rises and gains momentum through a specific social system 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:

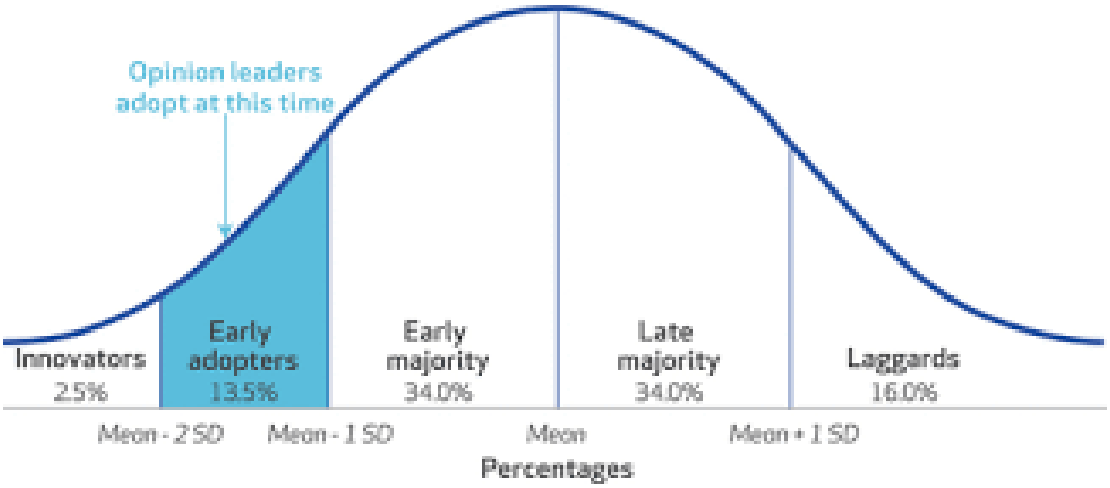


Figure 2: Diffusion of technology

Source: http://blog.leanmonitor.com/early-adopters-allies-launching-product/

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 (Williams, 2022). 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) provides an extension of the theory of reasoned behavior (Ajzen & Fishbein, 1980). The technology acceptance model was first proposed by Davis in 1989. 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.

Riek 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.

Methodology

Research Design

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 will be analyzed to understand the relationship between technological advancements and cybercrime.

Data Collection

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 will be 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.

Data Analysis

The collected data will be 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 will be 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 the rise of cybercrime were identified, considering the technological landscape and its impact on cybercriminal activities in the area.

Limitations

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.

Findings and Discussion

Cybercrime in Kenya

Cybercrime is a growing concern in Kenya, as the country continues to embrace digital technologies and the internet. With the increasing use of smartphones, social media, and online platforms, cybercriminals have found new ways to exploit individuals and organizations for financial gain or malicious intent. In this article, we will discuss the various types of cybercrimes in Kenya, the impact they have on individuals and businesses, and the measures being taken to combat this growing threat.

One of the most common types of cybercrimes in Kenya is phishing. Phishing involves sending fraudulent emails or messages to individuals to trick them into revealing sensitive information such as passwords, credit card numbers, or personal details. These emails often appear to be from legitimate sources, such as banks or government agencies and can be very convincing. Once the cybercriminal has obtained this information, they can use it to steal money, commit identity theft, or carry out other illegal activities.

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: https://www.statista.com/statistics/1278773/number-of-online-crimes-reported-in-kenya-by-type/

In addition to these common forms of cybercrime, Kenya also faces challenges from more sophisticated threats such as hacking, malware, and ransomware attacks. Hackers can gain unauthorized access to computer systems or networks to steal data, disrupt operations, or carry out other malicious activities. Malware, such as viruses and spyware, can infect devices and steal sensitive information without the user's knowledge. Ransomware attacks involve encrypting a victim's data and demanding payment in exchange for the decryption key, often with the threat of leaking the data if the ransom is not paid.

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 (*THE COMPUTER MISUSE AND CYBERCRIMES ACT, 2018* 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 addition to legislative measures, the government has also established the National Computer Incident Response Team Coordination Centre (National KE-CIRT/CC) to coordinate cybersecurity efforts and respond to cyber incidents (Communication Authority of Kenya, 2024). The center works with government agencies, private sector organizations, and international partners to monitor and mitigate cyber threats, provide training and awareness programs, and support victims of cybercrimes.

Private sector organizations in Kenya have also taken steps to enhance their cybersecurity defenses and protect themselves from cyber threats. Many businesses have invested in cybersecurity technologies such as firewalls, antivirus software, and encryption tools to safeguard their data and networks. They have also implemented security policies and procedures to educate employees about the risks of cybercrime and promote safe online practices.

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 developments and innovations have transformed the way we interact with the world around us. The advent of the internet, mobile devices, and social media platforms has made it easier for people to connect, share information, and conduct business online. Kenya is considered

the ICT hub of the East African region (International Trade Authority, 2022). However, these advancements have also created new opportunities for cybercriminals to exploit vulnerabilities in 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. In this essay, we will discuss the effects of technological developments on cybercrimes in Kenya, including the challenges they present and the strategies being employed to

address them. Ngunjiri (2022) notes 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). This includes the use of advanced malware, phishing scams, and other tactics to steal sensitive information, such as financial data and personal information. These advancements make it more difficult for law enforcement agencies to detect and prevent cybercrimes, as criminals are constantly evolving their tactics to stay ahead of authorities.

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). This has led to a rise in cases of identity theft, where criminals use stolen information to open fraudulent accounts or make unauthorized purchases. The ease and anonymity of the internet make it easier for cybercriminals to carry out these crimes, posing a significant threat to individuals and businesses in Kenya.

Furthermore, technological developments have also facilitated the spread of cybercrimes across borders. With the rise of the internet and digital communication, cybercriminals can operate from anywhere in the world, making it difficult for law enforcement agencies to track and apprehend them. This has led to an increase in transnational cybercrimes, such as online scams and cyberattacks, which can have far-reaching consequences for individuals and businesses 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, 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. Many individuals and organizations in the region are not adequately informed about the risks and threats posed by cybercriminals, making them more 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.

Another factor contributing to the rise of cybercrime in Juja Sub-County is the lack of adequate cybersecurity measures and infrastructure. Many businesses and government agencies in the region do not have robust cybersecurity protocols in place, making it easier for cybercriminals to infiltrate their systems and steal sensitive information. In addition, the high cost of cybersecurity solutions and the lack of skilled cybersecurity professionals in the region have made it challenging for organizations to protect themselves against cyber threats.

Furthermore, the prevalence of social media platforms and online communication channels has made it easier for cybercriminals to target individuals and organizations in the Juja Sub-County. Scammers often use social engineering techniques to trick people into revealing their personal information or clicking on malicious links, leading to data breaches and financial losses.

Recommendation and Conclusion

Potential Solutions to Address Cybercrime in Juja Sub-County

To address the rise of cybercrime in the Juja Sub-County, it is essential to implement a multi-faceted approach that combines technological solutions, education, and collaboration between stakeholders. One of the key strategies is to raise awareness about cybersecurity risks and best practices among individuals and organizations in the region. This can be done through public awareness campaigns, workshops, and training programs that educate people about the importance of protecting their personal information and digital assets.

In addition, it is crucial to invest in cybersecurity infrastructure and resources to strengthen the region's defenses against cyber threats. This includes implementing firewalls, antivirus software, and encryption tools to protect sensitive data and prevent unauthorized access to digital systems. Organizations should also conduct regular security audits and penetration testing to identify and address vulnerabilities in their networks.

Furthermore, collaboration between government agencies, law enforcement, and cybersecurity experts is essential to combat cybercrime in the Juja Sub-County. By sharing information and resources, stakeholders can work together to investigate cyberattacks, track down cybercriminals, and prosecute offenders. Additionally, partnerships with international organizations and cybersecurity firms can help enhance the region's cybersecurity capabilities and provide access to advanced technologies and expertise.

Conclusion

Technological developments and innovations have had a profound impact on the rise of cybercrime in the Juja Sub-County. The proliferation of mobile devices, social media platforms, and online communication channels has created new opportunities for cybercriminals to exploit vulnerabilities and target individuals and organizations in the region. To address this growing threat, it is essential to raise awareness about cybersecurity risks, invest in cybersecurity infrastructure, and foster collaboration between stakeholders. By taking a proactive and multi-faceted approach, Juja Sub-County can strengthen its defenses against cybercrime and protect its residents and businesses from digital threats.

References

Ajzen, I. & Fishbein, M. (1980). *Understanding Attitudes and Predicting Social Behavior*. Prentice-Hall, Englewood Cliffs.

Bellasio, J., & Silfversten, E. (2023). *The impact of new and emerging technologies on the cyber threat ...* Kings College London. https://www.rand.org/pubs/external_publications/EP68433.html

Communication Authority of Kenya. (2024). *Home - ke-cirt*. KE. https://ke-cirt.go.ke/

Cowling, N. (2022). *Topic: Social media in Kenya*. Statista. https://www.statista.com/topics/11385/social-media-in-kenya/#topicOverview

Dulock, H. L. (1993). Research design: Descriptive research. *Journal of Pediatric Oncology Nursing*, *10*(4), 154–157. https://doi.org/10.1177/104345429301000406

Hasani, T., O'Reilly, N., Dehghantanha, A., Rezania, D., & Levallet, N. (2023). Evaluating the adoption of cybersecurity and its influence on organizational performance. *SN Business & Economics*, *3*(5). https://doi.org/10.1007/s43546-023-00477-6

International Trade Authority. (2022, August 19). *Kenya - Information, Communications, and Technology (ICT)*. International Trade Administration | Trade.gov. https://www.trade.gov/country-commercial-guides/kenya-information-communications-and-technology-ict

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials*, *15*(4), 2091–2121. https://doi.org/10.1109/surv.2013.032213.00009

KNA (2023) *Government to strengthen cybersecurity measures and combat cybercrime*, *Kenya News Agency*. Available at: https://www.kenyanews.go.ke/government-to-strengthen-cybersecurity-measures-and-combat-cybercrime/ (Accessed: 29 February 2024).

Lawi, J. (2023, May 10). *Cybercrime is on the rise as Kenya faces 1 million threats every day*. The Star. https://www.the-star.co.ke/business/kenya/2023-05-10-cybercrime-on-the-rise-as-kenya-faces-1-million-threats-everyday/

Maurer, T., & Nelson, A. (2021). *The global cyber threat to financial systems – IMF F&D*. IMF. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm

Musau, D. (2024, February 29). *Kenya was hit by a record 860 million cyber-attacks in 2023*. Citizen Digital. https://www.citizen.digital/news/kenya-hit-by-record-860-million-cyber-attacks-in-2023-n328649

Mwangi, K. (2023, October 22). *Kenya cyber-attacks down 55PC on awareness drives, digital signatures*. Business Daily. https://www.businessdailyafrica.com/bd/corporate/technology/kenya-cyber-attacks-down-55pc-on-awareness-digital-signatures--4409634

Ngila, F. (2020, September 20). *How technology changed the lives of Kenyans in the past 10 years*. Business Daily. https://www.businessdailyafrica.com/bd/data-hub/how-technology-changed-lives-of-kenyans-in-the-past-10-years-2275412

Ngunjiri, N. (2022, June). *Technological Developments Influence the Cybercrime in Juja Sub-County*. University of Nairobi. https://www.researchgate.net/publication/361182962_Technological_Developments_Influence_the_Cybercrime_in_Juja_Sub-County

Ojedokun, A.A. (2005) 'The evolving sophistication of internet abuses in Africa', *The International Information & Library Review*, 37(1), pp. 11–17. doi:10.1016/j.iilr.2005.01.002.

ONYANDO, W. (2021) *Cybercrimes surge by 37PC as usage of internet increases, Business Daily*. Available at:

https://www.businessdailyafrica.com/bd/corporate/technology/cybercrimes-surge-37pc-as-usage-of-internet-increases-3582412 (Accessed: 29 February 2024).

Patton, M. Q. (2005). Qualitative research. *Encyclopedia of Statistics in Behavioral Science*. https://doi.org/10.1002/0470013192.bsa514

Petrosyan, A. (2023, October 20). *Concerns regarding cyberattacks worldwide 2023*. Statista. https://www.statista.com/statistics/1367473/concerns-of-board-directors-cybercrime-global/

Riek, 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. https://doi.org/10.1109/tdsc.2015.2410795

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. https://doi.org/10.1097/nur.0000000000000493

Sunday, F. (2020) *Phone users losing millions through identity theft, The Standard*. Available at: https://www.standardmedia.co.ke/article/2001287820/phone-users-losing-millions-through-identity-theft (Accessed: 29 February 2024).

THE COMPUTER MISUSE AND CYBERCRIMES ACT, 2018 (2018).

World Bank Group. (2019, October 31). *Kenya economic update: Accelerating Kenya's Digital Economy*. World Bank. https://www.worldbank.org/en/country/kenya/publication/kenya-economic-update-accelerating-kenyas-digital-economy