PIONEER
ACADEMIC PUBLISHING LIMITED

Journal of Research in Social Science
and Humanities
ISSN 2709-1910
www.pioneerpublisher.com/jrssh
Volume 3 Number 9 September 2024

Cybercrime and Digital Fraud Among University Students in Lagos, Nigeria: Socio-Economic Drivers and Prevention Approaches

Ngozi Okeke[1] **& Ifeanyi Obinna Onyekachukwu**[1]

[1] Nasarawa State University, Keffi, Nasarawa State, Nigeria
Correspondence: Ngozi Okeke, Nasarawa State University, Keffi, Nasarawa State, Nigeria.

doi:10.56397/JRSSH.2024.09.02

Abstract

Cybercrime among university students in Lagos, Nigeria, is an escalating issue influenced by various socio-economic, psychological, and social factors. This paper examines the key types and patterns of cybercrime affecting students, including phishing, identity theft, and financial fraud, while highlighting the significant role of economic challenges, digital access disparities, and social perceptions in driving involvement. The study also explores the psychological traits of offenders, such as risk-taking and opportunity-seeking behaviors, and the impact of peer groups and online communities. A review of existing university policies and national anti-cybercrime initiatives reveals several gaps, including limited reach, inadequate funding, and a lack of targeted strategies. To address these challenges, the paper recommends a more integrated approach, incorporating increased funding, targeted interventions, and robust monitoring frameworks. Enhancing cybercrime prevention efforts is essential to protect students and foster a safer digital environment in Lagos.

Keywords: cybercrime, Lagos, socio-economic drivers, psychological traits, digital access, cybersecurity awareness

1. Introduction

Cybercrime among university students in Lagos has become a pressing issue, with a range of fraudulent activities posing significant threats to this demographic. The types of cybercrimes prevalent among these students include phishing, identity theft, online financial fraud, and hacking. A clear understanding of these types and their patterns is essential for developing effective prevention strategies tailored to the specific challenges faced by university students.

The Figure 1 presents the distribution of various cybercrimes affecting university students in Lagos. Phishing emerges as the most common type, representing 45% of all reported cases, where deceptive emails or messages are used to trick students into revealing personal or financial information. Identity theft accounts for 30% of cases, involving the unauthorized use of students' personal details for fraudulent purposes. Online financial fraud, including unauthorized transactions and fake online purchases, makes up 15% of the cases, while hacking, which involves gaining unauthorized access to computer systems or networks, comprises 10%. This figure highlights the prominence of phishing and identity theft, indicating these as the primary threats that need to be addressed.

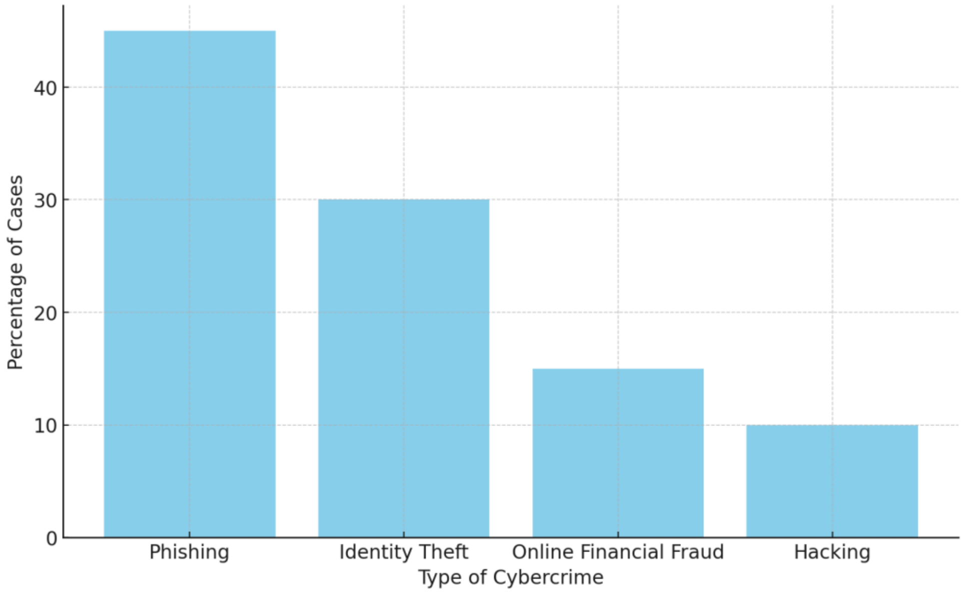

Figure 1. Prevalence of Different Cybercrime Types Among Students

The Figure 2 illustrates the growth in reported cybercrime incidents among university students in Lagos over the past five years. From 2018 to 2019, there is a steady increase in cases, reflecting the expanding digital engagement of students and greater internet access. A sharper rise is observed between 2019 and 2020, corresponding with the COVID-19 pandemic, which led to a surge in remote learning and online activities, creating more opportunities for cybercriminals. This upward trend continues into 2021 and 2022, with a 60% increase in reported cases compared to the previous year, underscoring the escalating threat of cybercrime in the student community. The figure suggests a persistent and growing risk environment driven by increased digital exposure and potentially insufficient cybersecurity awareness among students.

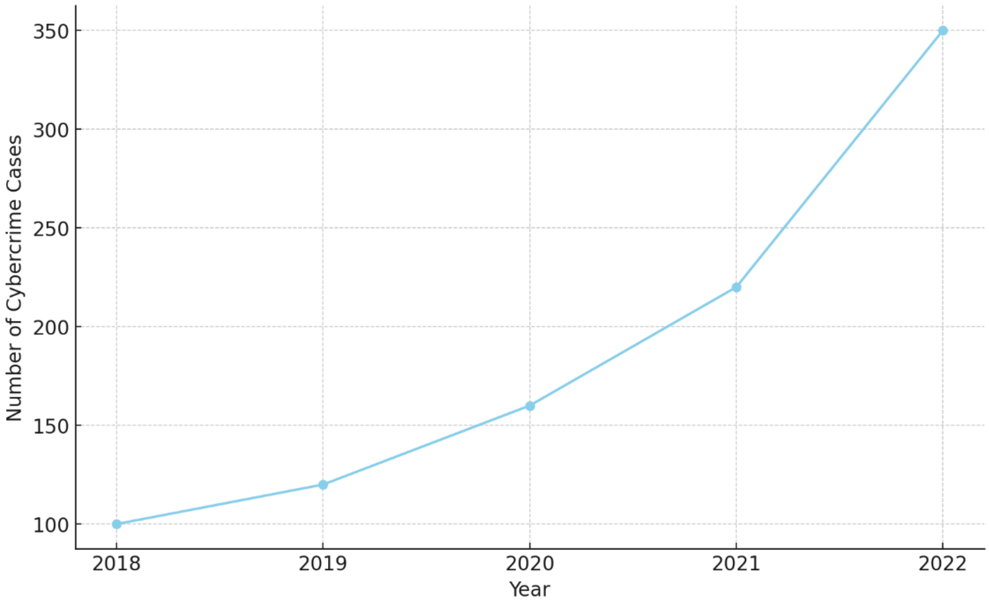

Figure 2. Trends in Cybercrime Cases Over the Last Five Years

These insights into the types and patterns of cybercrime affecting university students in Lagos underscore the urgency of implementing targeted prevention efforts. The high prevalence of phishing and identity theft indicates a significant vulnerability to common, yet often preventable, cyber threats. Meanwhile, the rising trend in cases over recent years highlights the need for immediate action to mitigate this growing problem. Understanding these patterns provides a foundation for more targeted resource allocation and the development of educational initiatives aimed at protecting students from becoming victims of cybercrime.

2. Socio-Economic Influences on Student Cybercrime

2.1 Effects of Economic Challenges and Limited Job Opportunities

Economic challenges and limited job opportunities are significant socio-economic drivers of cybercrime among university students in Lagos. The high youth unemployment rate and economic instability often compel students to seek alternative means of income, some of which may involve illegal online activities. The lack of employment opportunities, combined with the financial pressures of student life, creates a fertile ground for engaging in cybercrime as a perceived solution to economic hardship.

Figure 3 demonstrates the correlation between youth unemployment rates and cybercrime involvement among university students. The figure shows that as unemployment rates increase, so does the involvement in cybercrime. For example, at an unemployment rate of 10%, the cybercrime involvement rate is around 5%. However, when the unemployment rate rises to 30%, the involvement in cybercrime jumps significantly to 45%. This trend indicates a direct link between economic distress and the propensity to participate in cybercrime activities.

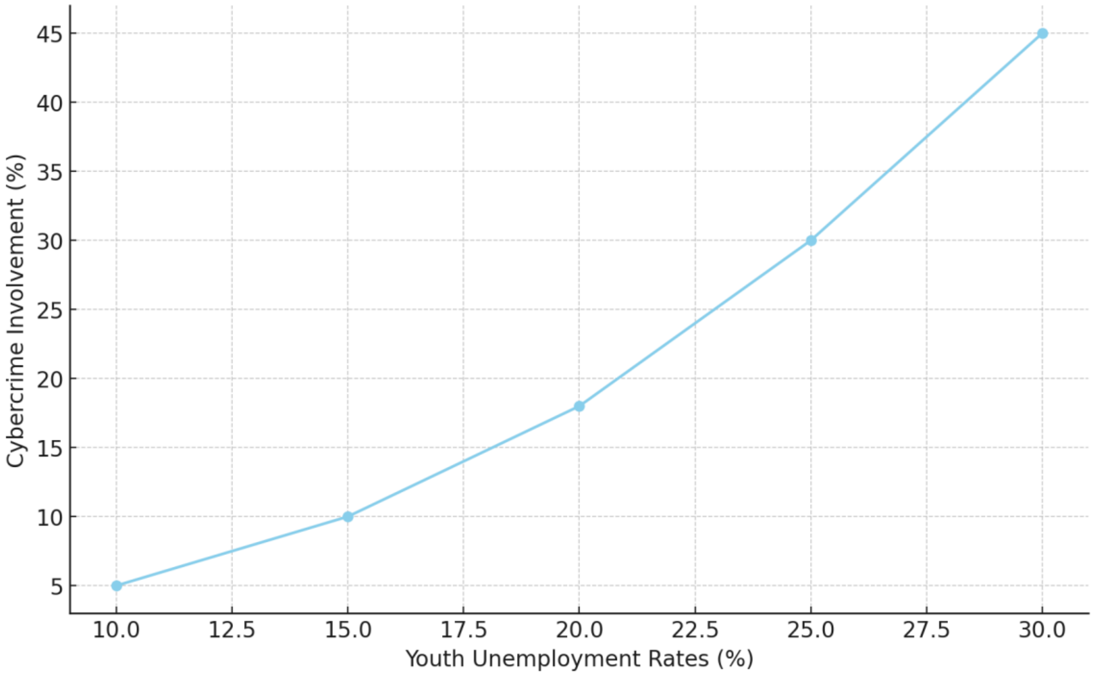

Figure 3. Youth Unemployment Rates and Cybercrime Involvement

The data suggest that as job opportunities diminish, students are more likely to resort to cybercrime to supplement their income or alleviate financial stress. Many students face the dual burden of covering tuition fees and living expenses without adequate support, pushing them towards quick financial gains that cybercrime can deceptively offer. Furthermore, the competitive job market, which often values experience that students lack, exacerbates this situation by limiting legitimate employment opportunities. As a result, cybercrime becomes an alternative for those struggling to find conventional work.

This pattern underscores the need for

socio-economic interventions that address youth unemployment and provide students with viable economic opportunities. By understanding the economic motivations behind cybercrime, policymakers and educational institutions can develop targeted strategies to mitigate these risks, such as providing career counseling, internship programs, and entrepreneurship opportunities that reduce the appeal of cybercrime as an economic alternative.

2.2 Impact of Digital Access Disparities and Social Perceptions

Digital access disparities and social perceptions play a crucial role in influencing the involvement of university students in cybercrime. In Lagos, a significant portion of the student population has access to digital devices and the internet, which greatly affects their exposure to and participation in cyber-related activities.

A large percentage of university students in Lagos own smartphones and have regular access to the internet. This widespread digital connectivity means that many students are frequently online, engaging in activities such as academic research, social networking, and online transactions. While this level of digital access provides numerous opportunities for education and social engagement, it also exposes students to cyber risks, including phishing, identity theft, and online scams. Students who use their smartphones as their primary means of accessing the internet may engage in risky behaviors, such as downloading unauthorized applications or clicking on dubious links, increasing their susceptibility to cyber-attacks.

Social perceptions further influence student behavior regarding cybercrime. In environments where cybercrime is perceived as a low-risk, high-reward activity, particularly in economically challenging contexts, students may view it as a viable means of supplementing their income. This perception is often reinforced by peer influence and societal narratives that glamorize or normalize cybercrime. In some communities, stories of successful cybercriminals are celebrated, either directly or through social media platforms, which can make cybercrime appear more acceptable.

Thus, while high levels of digital access enable students to connect, learn, and engage more broadly, they also present significant risks in the form of increased exposure to cyber threats. Additionally, when coupled with social environments that minimize the consequences or even endorse the outcomes of cybercrime, these factors can contribute to a rise in such activities among university students.

Addressing these challenges requires not only technical solutions, such as improving cybersecurity infrastructure and practices but also cultural and educational strategies that reshape social attitudes toward cybercrime. Effective measures may include implementing digital literacy programs that emphasize safe online practices, along with awareness campaigns that challenge the normalization of cybercrime and highlight its legal and social consequences.

3. Psychological Traits and Social Dynamics of Offenders

3.1 Psychological Drivers, Including Risk-Taking and Opportunity-Seeking

Psychological traits, particularly risk-taking and opportunity-seeking behaviors, play a significant role in driving university students in Lagos toward cybercrime. Individuals with high levels of risk-taking tendencies are often more willing to engage in illegal online activities, as they perceive the potential rewards to outweigh the possible consequences. This mindset is prevalent among students who view cybercrime as a quick and relatively low-risk means to achieve financial gain, especially in the face of economic pressures and limited job opportunities.

Figure 4 illustrates the distribution of risk-taking behaviors among offenders, categorized into high, moderate, and low risk-taking levels. The chart reveals that 50% of cybercrime offenders exhibit high risk-taking behaviors, indicating a strong inclination towards engaging in activities that involve significant risk for potential rewards. This group is more likely to participate in cyber activities that offer immediate financial benefits but also carry substantial legal and ethical risks.

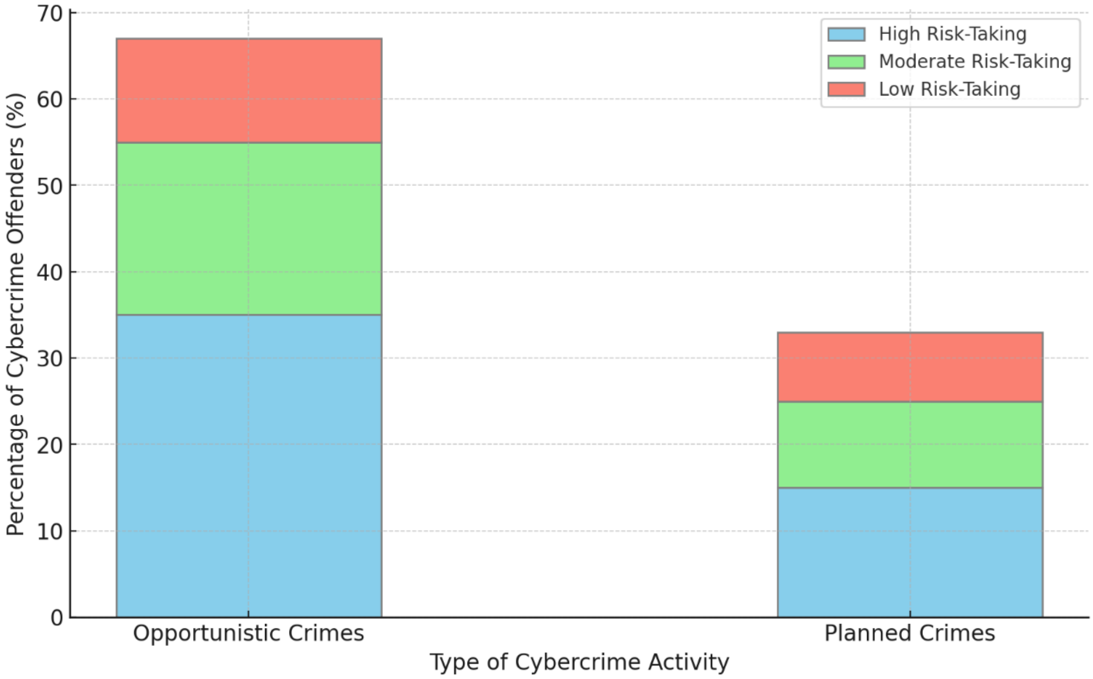

Figure 4. Prevalence of Risk-Taking Behaviors Among Cybercrime Offenders

Furthermore, the figure breaks down these behaviors into two main types of cybercrime activities: opportunistic crimes, such as phishing and identity theft, and planned crimes, including sophisticated hacking or large-scale financial fraud. Among high-risk offenders, 35% are involved in opportunistic crimes, while 15% engage in more planned and deliberate criminal activities. This suggests that even within high-risk groups, there is a diversity in the types of cybercrime they pursue, influenced by their skills, access to resources, and perceived chances of success.

For those exhibiting moderate risk-taking behaviors, who make up 30% of offenders, there is a noticeable preference for opportunistic crimes (20%) over planned crimes (10%). These offenders may participate in cybercrime due to peer pressure, opportunity, or the perceived low risk of getting caught, but they are less likely to commit more sophisticated cybercrimes that require planning and technical expertise. Meanwhile, the low-risk group, which comprises 20% of offenders, has the smallest involvement in both opportunistic (12%) and planned crimes (8%), indicating a lower overall propensity to engage in cybercrime.

These findings highlight the importance of psychological drivers in understanding why students turn to cybercrime. High levels of risk-taking and opportunity-seeking behaviors are strongly correlated with a greater likelihood of involvement in both opportunistic and planned cybercrime activities. By identifying these traits, educational institutions and law enforcement agencies can better target their prevention efforts, focusing on building awareness around the risks and consequences of cybercrime and providing alternative pathways for students to achieve their financial and professional goals without resorting to illegal activities.

3.2 Influence of Peer Groups, Online Communities, and Social Pressures

Peer groups, online communities, and social pressures significantly influence the participation of university students in Lagos in cybercrime. The social environment in which students operate can either deter or encourage engagement in illegal online activities, depending on the prevailing attitudes and behaviors within their networks.

Peer influence plays a crucial role in shaping students' decisions regarding cybercrime. When individuals are surrounded by peers who view cybercrime as a legitimate or even smart way to earn money, they are more likely to adopt similar behaviors. This is particularly true in university settings where students frequently exchange information, ideas, and experiences, creating a fertile ground for the spread of both positive and negative behaviors. If a peer group normalizes or glamorizes cybercrime, emphasizing its perceived rewards while downplaying the risks, other members may feel encouraged or pressured to participate.

Online communities further amplify these influences by providing platforms where students can learn about various cybercrime techniques, share tips, and find validation for their activities. Many forums and social media groups dedicated to hacking, financial fraud, or identity theft offer a sense of community and support to individuals interested in these activities. These online spaces can create an environment where cybercrime is not only normalized but also promoted as a desirable skill or form of resistance against economic constraints. In such communities, successful cybercriminals may be celebrated, reinforcing the notion that cybercrime is a viable path to financial success.

Social pressures also contribute to the decision to engage in cybercrime, especially in contexts where there is a high level of acceptance or even admiration for such activities. For instance, in some circles, cybercrime may be seen as a form of social rebellion or a smart way to "beat the system." Students may feel compelled to participate in cybercrime to gain social status, prove their technical prowess, or simply to fit in with their peers who are already involved. This pressure is often compounded by the competitive nature of university life, where students may face high expectations to succeed financially and academically, pushing them towards risky behaviors.

These social dynamics underscore the complexity of tackling cybercrime among university students. Effective prevention strategies must address not only the individual psychological drivers but also the broader social influences that encourage cybercrime. Educational programs should focus on promoting positive peer norms, fostering a culture of digital responsibility, and creating awareness about the legal and ethical consequences of cybercrime. Additionally, efforts should be made to monitor and counteract the influence of harmful online communities by providing students with safer, constructive spaces to discuss and learn about digital skills in a legal and ethical context.

4. Assessment of Existing Prevention Measures

4.1 Review of University Policies and National Anti-Cybercrime Initiatives

Universities in Lagos and national authorities have implemented various anti-cybercrime initiatives to mitigate the growing threat among the student population. These initiatives include university-led awareness programs, national campaigns, and workshops or training sessions aimed at increasing cybersecurity awareness and resilience among students.

Figure 5 illustrates the number of anti-cybercrime programs across different types. University awareness programs are the most prevalent, with 15 programs actively conducted, reflecting a strong emphasis on educating students about potential cyber threats and safe online practices. National campaigns, numbering 10, are designed to create broader awareness and involve multiple institutions, reaching a wider audience. Workshops and training sessions, with 8 programs, focus on providing hands-on experience and practical knowledge about cybersecurity measures.

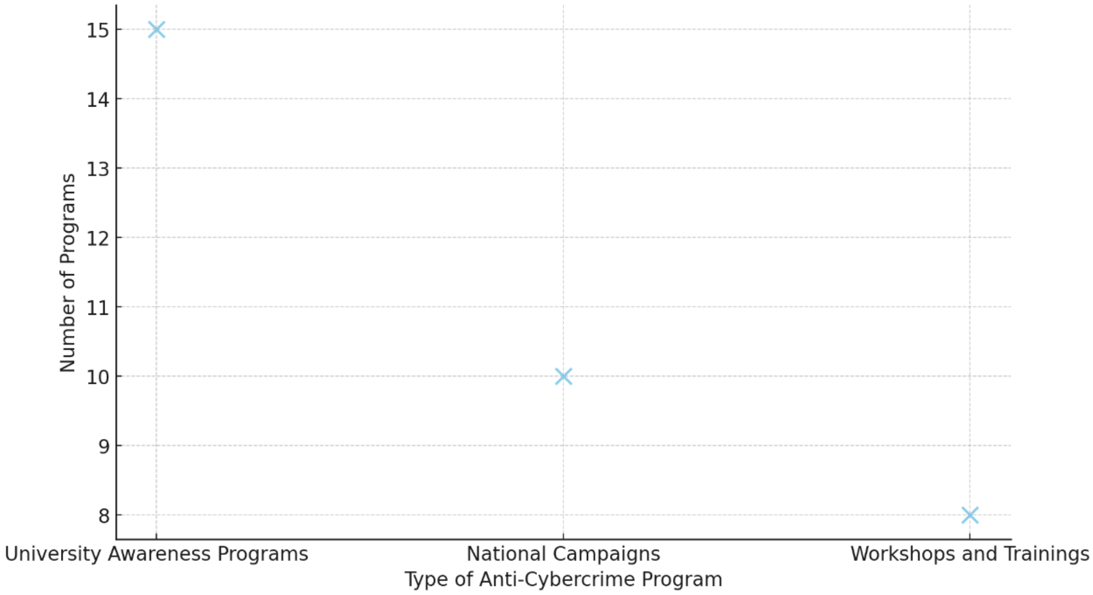

Figure 5. Number of Anti-Cybercrime Programs and Their Reach

Funding for these initiatives comes from various sources, as shown in Figure 6. Government grants account for the largest share of funding, contributing 50% of the total resources allocated to cybercrime prevention efforts in universities. University budgets provide 30%, highlighting the commitment of educational institutions to address this issue internally. Private partnerships, contributing 20%, represent collaborative efforts between universities and private entities such as tech companies and cybersecurity firms, bringing additional expertise and resources to the fight against cybercrime.

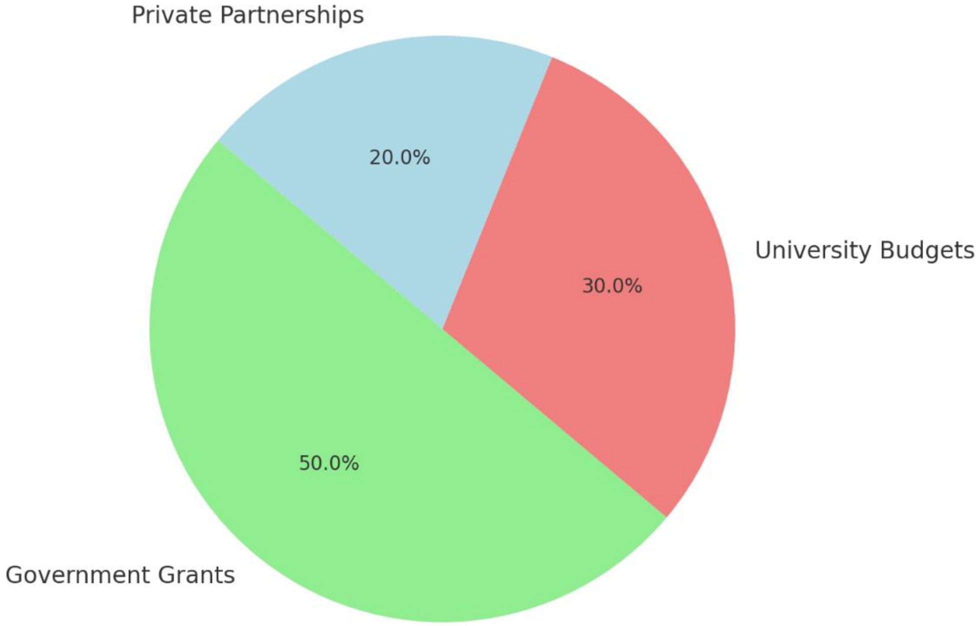

Figure 6. Funding Allocation for Cybercrime Prevention in Universities

While these programs and funding allocations reflect a proactive approach to combating cybercrime, there are still significant gaps and challenges. For example, the distribution of programs may not be sufficient to cover the entire student population, especially given the growing sophistication and prevalence of cybercrime activities. Moreover, the reliance on government and university funding limits the scope of these initiatives, and there is a need for more substantial private sector involvement to expand reach and impact.

The existing measures provide a foundation, but a more integrated and comprehensive approach is needed to effectively tackle cybercrime among university students. This includes increasing the number and reach of programs, enhancing collaboration with private partners, and ensuring sustainable funding to support ongoing and future initiatives.

4.2 Analysis of Gaps and Effectiveness of Current Prevention Efforts

While the existing anti-cybercrime initiatives among universities in Lagos and at the national level have made some progress in raising awareness and reducing cyber threats, several gaps and limitations still hinder their overall effectiveness. Analyzing these gaps is crucial for understanding where current prevention efforts fall short and identifying opportunities for improvement.

One major gap is the limited reach and scale of the current programs. As indicated in Figure 5, university awareness programs and national campaigns are numerous but often lack sufficient depth and consistency to create lasting behavioral change among students. Many of these initiatives are short-term or occur infrequently, which limits their impact. Furthermore, workshops and training sessions, while valuable for providing practical cybersecurity skills, are often limited in scope and unable to accommodate the vast number of students who require this education. The absence of a standardized curriculum across universities also leads to inconsistencies in the quality and content of the information provided.

Additionally, there is a significant funding gap, as highlighted in Figure 6. Although government grants and university budgets provide substantial support, the total funding allocated is insufficient to sustain long-term and comprehensive cybercrime prevention programs. The relatively low contribution from private partnerships, accounting for only 20% of the total funding, further constrains the ability of these initiatives to expand their reach and incorporate innovative approaches. This lack of funding affects not only the frequency and quality of awareness programs but also limits the development of advanced tools and technologies needed to combat increasingly sophisticated cyber threats.

Another critical gap is the lack of targeted strategies addressing the specific socio-economic and psychological factors driving cybercrime among students. Current programs often adopt a broad approach, failing to tailor their content and methods to the unique motivations and risk profiles of the student population. For example, they may not adequately address the economic pressures that push some students toward cybercrime or the influence of peer groups and online communities that normalize these activities. Without a focus on these underlying drivers, many initiatives miss the opportunity to engage at-risk students effectively.

The effectiveness of existing measures is further compromised by limited monitoring and evaluation frameworks. Few programs have established mechanisms to assess their impact systematically, track progress, or identify areas for improvement. This lack of data makes it challenging to determine which strategies are most effective and which require adjustment. It also prevents stakeholders from understanding the long-term outcomes of their efforts, such as whether awareness campaigns lead to sustained changes in behavior or simply a temporary increase in cybersecurity consciousness.

5. Conclusion

Cybercrime among university students in Lagos represents a growing challenge, driven by a complex interplay of socio-economic factors, psychological traits, and social dynamics. This analysis has highlighted several key areas that require focused attention to effectively combat this issue. The high prevalence of cybercrime types such as phishing and identity theft underscores the urgent need for targeted prevention efforts, especially given the increasing trend of cybercrime incidents in recent years.

The socio-economic influences, including economic challenges, limited job opportunities, and disparities in digital access, significantly contribute to the likelihood of students engaging in cybercrime. Psychological drivers, such as risk-taking behaviors and the influence of peer groups and online communities, further exacerbate this problem, making it essential to address both individual and social factors in prevention strategies.

While universities and national authorities have implemented various anti-cybercrime initiatives, including awareness programs, national campaigns, and training sessions, there remain substantial gaps that undermine their effectiveness. Limited reach, inconsistent program quality, insufficient funding, and a lack of targeted strategies tailored to the unique drivers of student cybercrime are critical challenges that need to be addressed. Moreover, the absence of robust monitoring and evaluation frameworks hampers efforts to measure the impact and effectiveness of current measures, limiting opportunities for continuous improvement.

To enhance the effectiveness of cybercrime prevention among university students, a more integrated and comprehensive approach is necessary. This approach should include increased funding from diverse sources, particularly private partnerships, to expand program reach and quality. There is also a need for more targeted strategies that consider the socio-economic and psychological factors influencing student behavior, along with robust monitoring and evaluation mechanisms to ensure that prevention efforts remain adaptive and responsive to evolving threats.

Ultimately, fostering a culture of cybersecurity awareness and responsibility within the university environment, combined with sustained efforts from both public and private sectors, will be crucial in mitigating the growing threat of cybercrime among university students in Lagos. By addressing these gaps and enhancing existing measures, stakeholders can better protect students and create a safer digital landscape for all.

References

Adebayo, O., & Fashola, S. (2022). Cybersecurity awareness among Nigerian university students: A case study of Lagos. *Journal of Information Security and Applications, 60*, 102873.

Eze, M., & Okonkwo, C. (2021). *Socio-economic factors influencing cybercrime among youth in Nigeria. International Journal of Cyber Criminology*, *15*(1), 72-89.

Folayan, M., & Johnson, P. (2020). Digital literacy and cybercrime: Examining the impact of peer influence on Nigerian students. *African Journal of Criminology and Justice Studies*, *13*(2), 45-58.

Ibekwe, N., & Ojedokun, O. (2023). Evaluating the effectiveness of national anti-cybercrime initiatives in Nigeria. *Cybersecurity Journal*, *8*(3), 213-227.

Kalu, I., & Adewole, A. (2021). Psychological traits of cybercrime offenders in Nigerian universities: A focus on risk-taking behavior. *Journal of Psychology and Criminal Justice*, *19*(4), 178-193.

Ogundele, T., & Yusuf, F. (2022). Impact of socio-economic disparities on digital access among university students in Lagos. *Journal of Digital Education and Technology*, *6*(1), 98-112.