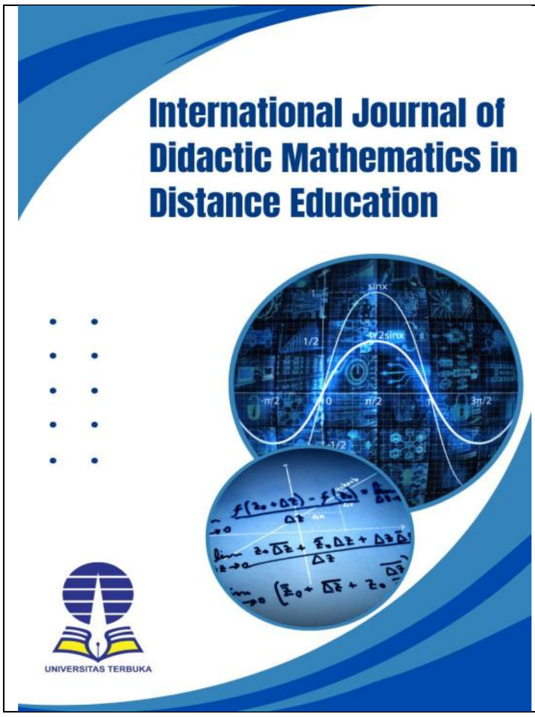
International Journal of Didactic Mathematics in Distance Education

Journal homepage: https://jurnal.ut.ac.id/index.php/ijdmde


International Journal of Didactic Mathematics in Distance Education
UNIVERSITAS TERBUKA

Students' vulnerability to cybercrime: implications for cybersecurity in the global south

Joshua Abah Abah[1*], Peter Inalegwu Agada [2]

[1]Department of Mathematics, Science and Technology Education, University of Zululand, South Africa
abahj@unizulu.ac.za

[2]Directorate of Information and Communication Technology, Joseph Sarwuan Tarka University, Makurdi, Nigeria
peter.agada@uam.edu.ng

To cite this article:
Abah, J.A & Agada, P.I. (2025). Students' vulnerability to cybercrime: implications for cybersecurity in the global south. *International Journal of Didactic Mathematics in Distance Education*, *2*(2), 141-164.

To link to this article:
https://jurnal.ut.ac.id/index.php/ijdmde

Published by:
Universitas Terbuka
Jl. Pd. Cabe Raya, Pd. Cabe Udik, Kec. Pamulang, Kota Tangerang Selatan, Banten 15437

International Journal of Didactic Mathematics in Distance Education
Volume 2, Issue 2, pp. 141 – 164, E-ISSN: 3047-9207
https://jurnal.ut.ac.id/index.php/ijdmde

Students' vulnerability to cybercrime: implications for cybersecurity in the global south

Joshua Abah Abah[1*], Peter Inalegwu Agada[2]
[1*]Department of Mathematics, Science and Technology Education, University of Zululand, South Africa, AbahJ@unizulu.ac.za
[2]Directorate of Information and Communication Technology, Joseph Sarwuan Tarka University, Makurdi, Nigeria peter.agada@uam.edu.ng

*Correspondence: AbahJ@unizulu.ac.za

Abstract
This conceptual study examines key issues around students' vulnerability to cybercrimes in the Global South. The increasing digitalization of education has exposed students in the Global South to heightened risks of cybercrime. Limited cybersecurity awareness, inadequate digital infrastructure, and socio-economic vulnerabilities make students particularly susceptible to cyber threats such as phishing, identity theft, and online fraud. This article examines the key factors contributing to students' exposure to cybercrime, including gaps in digital literacy, institutional cybersecurity policies, and the role of social and economic disparities. It also explores the broader implications for cybersecurity frameworks in the Global South, emphasizing the need for enhanced policy interventions, education reforms, and multi-stakeholder collaborations. By addressing these challenges, governments, educational institutions, and technology providers can foster a safer digital environment for students, ultimately strengthening overall cybersecurity resilience in the region. The study underscores the need for targeted cybersecurity awareness programmers and institutional policies to enhance students' online safety.

Article History
Received:
02 March 2025
Revised:
12 May 2025
Accepted:
26 May 2025
Published Online:
01 June 2025

Keywords:
Cybercrime; Cybercrime Vulnerability; Global South; Higher Education; Protection Motivation Theory.

1. Introduction

Cybercrime has emerged as a critical issue in the contemporary digital landscape, particularly across the Global South, where the rapid proliferation of internet access has facilitated a surge in cybercriminal activities. Defined as criminal acts committed through the internet or involving computer systems, cybercrime encompasses a wide range of offenses, including identity theft, online fraud, and phishing (Lusthaus, 2024; Wall, 2024). The rise of social media platforms has further complicated the cybercrime landscape, exposing users – especially young people – to various risks and vulnerabilities.

Broadly, cybercrime refers to illegal activities that involve the use of computers, digital networks, and the internet. These crimes range from financial fraud and identity theft to cyberterrorism and hacking. Cybercriminals exploit vulnerabilities in systems to steal sensitive information, disrupt services, or conduct illicit activities (Dennis, 2025; Kaspersky, 2025). With the growing dependence on digital technology, cybercrime has become a major global concern, affecting individuals, businesses, and governments (CISA, 2025).

One of the most common types of cybercrime is financial fraud, which includes phishing, credit card fraud, and ransomware attacks (Pryimenko, 2024). Phishing scams trick individuals into revealing personal information by pretending to be legitimate entities, while ransomware encrypts victims' data, demanding payment for its release. Cybercriminals also engage in corporate espionage, stealing trade secrets and intellectual property (Fox, 2024). For instance, Khan *et al.* (2023) reports that for developing countries of the Global South, research shows lax cybersecurity behavior of students both on computer and smartphone devices. Significant differences were found in the cybersecurity practices of students in terms of socioeconomic and digital divide variables. This highlights that the individuals with lower socioeconomic status and who are digitally, less connected are at a greater risk of falling victims to cyber-threats (Khan *et al.*, 2023). Also, Donalds *et al.* (2022) affirms high cybersecurity challenges, potential threats, and risks likely face by MSMEs and governments of the Global South. In the same vein, Egete *et al.* (2023) observed that all facets of international organizations and educational settings are being affected by cybersecurity concerns. Cybercrime poses a grave threat to the physical wellbeing of innocent members of the society worldwide. Individuals, governmental bodies, businesses, financial institutions, and higher education systems are all at risk from cybercriminals operating in isolation (Srivastava *et al.*, 2024). Additionally, cyberattacks on critical infrastructure, such as power grids and hospitals, can have devastating consequences, leading to financial losses and endangering lives.

To combat cybercrime, governments and organizations implement cybersecurity measures such as firewalls, encryption, and multi-factor authentication (Dennis, 2025; Fox, 2024; Kaspersky, 2025). International cooperation is also crucial, as cybercriminals often operate across borders, making prosecution difficult. Cybersecurity awareness and education play a vital role in preventing cybercrime, as individuals and businesses need to recognize threats and take proactive steps to protect their data (CISA, 2025; Pryimenko, 2024). As technology continues to evolve, so do cyber threats, making it essential for cybersecurity strategies to constantly adapt.

In Nigeria, for instance, the prevalence of cybercrime is alarming, driven by socio-economic factors, including high unemployment rates, poverty, and a cultural acceptance of illicit financial gain (Ayandele & Popoola, 2019). University students, who are among the most active internet users, often find themselves at the intersection of these risks, making them prime targets for cybercriminals. The interplay of these factors necessitates a comprehensive understanding of the vulnerabilities specific to Nigerian university undergraduates, particularly in the context of their social media behaviour.

This review explores the various dimensions of vulnerability to cybercrime among university students. It examines the theoretical, conceptual, and empirical frameworks that inform understanding of this phenomenon, discusses the prevalence and causes of cybercrime, and highlights specific vulnerabilities related to social media usage. Additionally, it presents the measures undertaken by the Nigerian government to tackle these vulnerabilities. The conceptual framework for understanding vulnerability to cybercrime among Nigerian university undergraduates involves examining the interplay between various factors influencing students' behaviours and perceptions regarding cybersecurity. This framework considers socioeconomic factors (economic challenges, such as poverty and unemployment, create an environment where students may resort to cybercrime as a quick means to financial stability); psychological factors (the desire for quick wealth, peer influence, and cultural acceptance of cybercrime can drive students toward engaging in risky online behaviours); technological factors (the rapid adoption of digital technologies and social media platforms without adequate cybersecurity measures exposes students to various cyber threats); and educational factors (lack of awareness and education regarding cybersecurity practices contributes to students' vulnerabilities, as many are not equipped with the knowledge to protect themselves effectively). The review highlights the need for targeted interventions that address these interconnected factors to mitigate the risks associated with cybercrime among university students.

2. Overview of Cybercrime in the Global South

Cybercrime is defined as criminal activities that involve the use of computers or the internet to commit illegal acts. This includes a wide range of offenses such as identity theft, phishing, online fraud, and cyberbullying (Wall, 2024). Cybercrime has emerged as a significant challenge in the Global South, affecting nations' economies, security, and societal stability. With rapid digitalization, countries in regions such as Africa, Latin America, and South Asia face growing threats from cybercriminal activities, including fraud, data breaches, and hacking. Many of these crimes exploit weak cybersecurity infrastructure, lack of regulatory enforcement, and limited public awareness (Broadhurst *et al.*, 2013). Unlike their counterparts in the Global North, these regions often struggle with limited resources to combat cyber threats, making them attractive targets for cybercriminal networks operating across borders. In Africa, cybercrime has evolved into a significant issue, particularly among the youth, who often leverage technology to perpetrate fraud and other illicit activities.

In Africa, cybercrime has become increasingly prevalent due to the rapid expansion of internet access and mobile technology. The continent has witnessed a surge in cybercriminal activities, driven by factors such as high unemployment rates, poverty, and inadequate law enforcement mechanisms. According to the African Union (2020), cybercrime costs African economies approximately $3.5 billion annually, with Nigeria being one of the most affected countries. The rise of cybercrime in Africa is often linked to the lack of digital literacy and awareness among the population, which makes individuals more susceptible to online scams and fraud.

Nigeria, for instance, is often cited as a hotspot for cybercrime in Africa, ranking first on the continent and third globally in terms of cybercrime prevalence (Ayandele & Popoola, 2019). A staggering 40% of Nigerian undergraduates and 60% of unemployed graduates are reportedly involved in various forms of cybercrime, including advance fee fraud, commonly known as "419 scams" (Ayandele & Popoola, 2019). The proliferation of internet access in the country, particularly through mobile devices, has facilitated the growth of cybercriminal activities, making it easier for individuals to engage in fraudulent schemes.

Cybercrime has become a growing concern in Africa as digital transformation accelerates across the continent. The increased use of the internet, mobile technology, and digital financial services has created opportunities for economic growth but has also exposed vulnerabilities to cyber threats (Mwangi *et al.*, 2022). Cybercriminal activities such as phishing, identity theft, financial fraud, and ransomware attacks are becoming more sophisticated. Many African countries lack the necessary cybersecurity infrastructure, policies, and awareness to effectively combat cybercrime, making them attractive targets for cybercriminals both within and outside the continent (Mphatheni & Maluleke, 2022).

Financial fraud remains one of the most prevalent forms of cybercrime in Africa, particularly in the banking and financial services sector. Cybercriminals exploit weak security measures, outdated software, and social engineering tactics to gain unauthorized access to financial accounts (Pieterse, 2021). Mobile money platforms, which are widely used in African countries such as Kenya, Nigeria, and Ghana, have also become targets for cyber fraud. Fraudsters use tactics such as SIM card swapping, fake investment schemes, and phishing attacks to defraud individuals and businesses (Tambo & Adama, 2017). The financial impact of cybercrime is significant, leading to billions of dollars in losses annually and affecting investor confidence.

Another major concern is the rise of cyberterrorism and politically motivated cyberattacks. Hacktivist groups and cyberterrorists have targeted government institutions, critical infrastructure, and media organizations to spread propaganda, disrupt services, and steal sensitive information (Bada & Nurse, 2019). Some cybercriminals engage in ransomware attacks against public and private institutions, demanding payments in cryptocurrency to restore access to critical systems. Governments across Africa have been slow in addressing these threats due to limited cybersecurity expertise, inadequate legislation, and insufficient collaboration between public and private sectors (Kshetri, 2019).

Despite the growing threat of cybercrime, efforts are being made to strengthen cybersecurity across the continent. Several African nations have established cybersecurity laws and regulatory frameworks, such as Nigeria's Cybercrimes Act (2015) and South Africa's Cybercrimes Act (2020), to address cyber-related offenses (Bada & Nurse, 2019). Regional organizations such as the African Union (AU) and the Economic Community of West African States (ECOWAS) are also promoting cybersecurity cooperation and awareness initiatives. However, enforcement remains a challenge due to weak legal systems and a lack of skilled cybersecurity professionals (Tambo & Adama, 2017).

However, challenges remain. Disparities in cybersecurity infrastructure, limited resources, and varying levels of legal frameworks across African countries hinder effective cybercrime prevention and prosecution. Additionally, the rapid pace of technological advancements requires continuous adaptation and investment in cybersecurity measures. There is also the problem of cyber criminals moving their operations to areas with less law enforcement, and weaker cyber security infrastructure (Kshetri, 2019).

To mitigate cybercrime, African governments, businesses, and individuals must adopt a proactive approach to cybersecurity. This includes investing in cybersecurity infrastructure, enhancing digital literacy, and fostering public-private partnerships to share intelligence on emerging threats (Uchendu *et al.*, 2021). International cooperation is also crucial, as cybercriminals often operate across borders, making it essential to collaborate with global law enforcement agencies and cybersecurity organizations (Broadhurst, 2006). With sustained efforts, Africa can strengthen its cybersecurity resilience and protect its digital economy from the growing menace of cybercrime.

A major contributing factor to cybercrime in the Global South is the digital divide (Abah, 2019). While internet access has expanded significantly (Iji & Abah, 2019), cybersecurity awareness and investments have not kept pace. Cybercriminals exploit outdated software, insecure networks, and low digital literacy among users to perpetrate financial fraud, identity theft, and ransomware attacks (Olayemi, 2014). Additionally, poor coordination among governments and international agencies has made it challenging to track and prosecute cybercriminals operating across multiple jurisdictions, further exacerbating the issue.

The economic impact of cybercrime on developing economies is profound. Small and medium-sized enterprises (SMEs), which form the backbone of many economies in the Global South, are particularly vulnerable to cyberattacks due to inadequate security measures. Cyber fraud, including business email compromise and financial scams, costs businesses billions of dollars annually, undermining economic growth and investment (Kshetri, 2019). Furthermore, cybercrime discourages foreign investments as concerns about data security and regulatory compliance deter multinational corporations from expanding operations in these regions.

Governments in the Global South have initiated various measures to curb cybercrime, but challenges remain. Some nations have established cybercrime laws and national cybersecurity frameworks to enhance digital resilience. However, enforcement mechanisms are often weak due to corruption, lack of technical expertise, and bureaucratic inefficiencies (Broadhurst *et al.*, 2013). International collaborations, such as partnerships with Interpol and regional cybersecurity organizations, have proven beneficial, but more cohesive efforts are needed to strengthen cybersecurity governance and law enforcement capacity.

To mitigate cybercrime in the Global South, a multi-stakeholder approach involving governments, businesses, and civil society is essential. Investing in cybersecurity infrastructure, increasing public awareness, and fostering international cooperation can help address the growing cyber threats. Additionally, enhancing digital literacy programs and adopting global best practices in cybersecurity governance will be crucial in reducing vulnerabilities and promoting a secure digital ecosystem in these regions (Kshetri, 2019). Addressing cybercrime in the Global South requires a sustained and collaborative effort to ensure digital transformation benefits all sectors without compromising security.

3. Root Causes of Cybercrime

Several factors contribute to the rise of cybercrime in the Global South, particularly among university students. Some of these factors are discussed here.

3.1. *Poverty*

High levels of poverty drive individuals to seek alternative means of income, often leading them to engage in cybercrime as a quick way to make money (Okeke & Onyekachukwu, 2024). While poverty does not justify cybercrime, addressing economic disparities can reduce the likelihood of individuals resorting to it.

Poverty has been identified as a significant driver of cybercrime, particularly among youth in developing regions. Studies conducted in Ghana and Nigeria reveal that economic hardship and social inequality compel individuals to engage in cybercriminal activities as alternative income sources. For instance, research in Agona Swedru, Ghana, indicates a strong correlation between social inequality and cybercrime, with financial constraints serving as a mediating factor (Kumah, *et al.*, 2024). Similarly, in Nigeria, poverty and unemployment are major contributors to youth involvement in cybercrime, as the lack of necessities and job opportunities pushes them toward illicit online activities (Akinyetun, 2021).

The relationship between poverty and cybercrime is further complicated by the rapid development of information technology (IT). While IT advancement offers numerous benefits, it also provides tools that can be exploited for cybercriminal purposes, especially in regions where economic disparities are pronounced. Research suggests that in areas with significant poverty, the combination of accessible technology and limited economic opportunities can lead individuals to engage in cybercrime as a means of financial survival (Kshetri, 2016).

Addressing the root causes of cybercrime necessitates comprehensive strategies that tackle both economic and technological factors. Implementing policies aimed at reducing poverty and social inequality, such as enhancing education, creating employment opportunities, and ensuring equitable access to resources, can mitigate the economic motivations for cybercrime. Additionally, promoting ethical IT practices and strengthening cybersecurity measures are essential in preventing the exploitation of technology for criminal purposes (Kshetri, 2016; Kumah *et al.*, 2024).

3.2. *Unemployment*

With limited job opportunities, many young people across the Global South resort to cybercrime as a means of survival. The high unemployment rate among graduates exacerbates this issue, as they feel pressured to find immediate financial solutions (Okeke & Onyekachukwu, 2024). Unemployment has been widely recognized as a significant root cause of cybercrime, as individuals facing financial instability may resort to illegal online activities for economic survival. According to Levi *et al.* (2017), economic hardship often pushes individuals towards cybercriminal activities such as fraud, identity theft, and hacking. The lack of employment opportunities, especially for skilled individuals in technology and computer science, increases the likelihood of engaging in cybercrime. This is particularly evident in regions with high youth unemployment, where cybercrime offers an alternative means of income, often with lower risks of detection compared to traditional crimes (Holt & Bossler, 2015).

Moreover, cybercrime presents a lucrative opportunity for unemployed individuals who possess technical expertise but lack access to legitimate employment avenues. As technology advances, cybercriminal activities become more sophisticated, attracting jobless individuals who seek financial gain through phishing, ransomware attacks, or financial fraud (Button *et al.*, 2008). In some cases, organized cybercrime networks actively recruit unemployed individuals, promising them financial stability in exchange for their skills in illegal hacking and data breaches (Holt & Bossler, 2020). This cycle of unemployment leading to cybercrime creates a dangerous environment in which economic desperation fuels digital offenses, further complicating efforts to combat cyber threats.

To address unemployment as a root cause of cybercrime, governments and organizations must invest in job creation, digital literacy programs, and cybersecurity awareness initiatives. Providing alternative pathways for employment, such as ethical hacking and cybersecurity training, can divert skilled individuals from engaging in illicit online activities (Levi *et al.*, 2017). Additionally, fostering a robust job market, particularly in the technology sectors, can mitigate the lure of cybercrime as an economic alternative (Otozi *et al.*, 2024). By addressing the economic and social factors that drive individuals toward cybercriminal activities, policymakers can create a more secure and stable digital landscape.

3.3. *Peer Influence*

The influence of peers can significantly impact students' decisions to engage in cybercrime. Many young people are drawn into cybercriminal activities by friends or social circles that normalize such behaviour (Ogunleye *et al.*, 2019). Peer influence plays a significant role in driving cybercrime in the Global South, particularly among young individuals who seek social validation and economic opportunities. Many youths in developing regions face high unemployment rates and limited access to legal income sources, making cybercrime an attractive alternative (Anyanwu, 2024). When peers engage in cybercriminal activities such as online fraud, hacking, or identity theft, they often encourage others to participate, creating a cycle of deviant behaviour. The normalization of these activities within peer groups reduces the perceived moral and legal consequences, further reinforcing involvement in cybercrime (Tade & Aliyu, 2011).

Additionally, peer influence fosters skill acquisition and knowledge transfer in cybercriminal networks. Unlike traditional crimes, cybercrime requires technical proficiency, which is often learned informally through peer interactions (Osho & Onoja, 2015). Experienced cybercriminals mentor newcomers, providing them with the necessary tools, techniques, and access to underground digital markets. In some cases, peer groups establish structured operations that mimic legitimate businesses, making it easier for new recruits to transition into cybercrime. The lack of formal cybersecurity education in many Global South countries exacerbates the problem, as young individuals rely on peer-driven learning environments that prioritize illicit digital skills (Bada & Nurse, 2019).

To address the issue of peer influence in cybercrime, governments and organizations must implement targeted interventions that provide alternative pathways for youth engagement. Educational initiatives that promote cybersecurity awareness and ethical hacking can help divert young talents away from cybercrime (Anyanwu, 2024). Additionally, fostering employment opportunities in the technology sector can reduce economic incentives for engaging in illegal online activities. Community-based programs that address social pressures and offer mentorship from positive role models may also play a crucial role in countering the influence of cybercriminal peer networks. Without such interventions, peer-driven cybercrime will likely continue to thrive in the Global South.

3.4. *Get-rich-quick Mentality*

The desire for quick wealth and material success drives many young people to engage in cybercrime. This "get-rich-quick" attitude is often fuelled by societal pressures and the portrayal of wealth on social media platforms (Meso *et al.*, 2013). The “get-rich-quick” mentality refers to the desire for fast wealth, often through risky or unethical means. This mindset can lead individuals to seek shortcuts to financial success, which sometimes includes involvement in illegal activities like cybercrime. Cybercrime offers opportunities for those seeking fast, easy money, whether through scams, hacking, or identity theft (Wall, 2024).

Many cybercriminals engage in scams promising quick returns, such as phishing schemes, Ponzi schemes, or fake investment opportunities. These promises prey on individuals’ desire for fast money, often leading to financial loss. Cyber-criminals who embrace the "get-rich-quick" mentality might target individuals or organizations for large sums of money, using ransomware or other hacking techniques. The idea is to make a quick profit by exploiting vulnerabilities for immediate financial gain (Campbell & Kennedy, 2012).

With the rise of cryptocurrency, cybercriminals use the allure of quick profits from digital assets to manipulate and deceive others into investing in fraudulent schemes. Some individuals, influenced by the “get rich quick” mentality, may resort to cybercrime as a way of showing off a lavish lifestyle on social media. They may engage in illicit activities to maintain an appearance of wealth. This connection underscores the dangers of an unrealistic pursuit of wealth and how it can drive people to make morally and legally questionable decisions.

3.5. *Lack of Awareness*

Many students lack awareness of the legal implications and consequences of cybercrime. This ignorance can lead to risky behaviours, as they may not fully understand the potential repercussions of their actions (Bottyán, 2023). Lack of awareness plays a crucial role in the increasing prevalence of cybercrime and the wide level of vulnerability. Many individuals and organizations fall victim to cybercriminal activities due to limited knowledge about online security threats, preventive measures, and best practices for digital safety.

3.6. *Cultural Acceptance*

In some cases, cybercrime is culturally accepted or even glamorized, particularly through social media, where individuals who engage in such activities are often portrayed as successful. Cultural acceptance plays a significant role in the prevalence of cybercrime in the Global South, where digital fraud, hacking, and cyber-enabled financial crimes are often normalized within certain communities. In many developing regions, economic hardship and limited job opportunities push individuals towards alternative means of survival, including cybercrime. The widespread acceptance of online fraud, such as “Yahoo-Yahoo” in Nigeria or “sakawa” in Ghana, reflects a societal mindset where digital crimes are perceived as legitimate ways to escape poverty (Boateng *et al.*, 2011; Oduro-Frimpong, 2014; Ojedokun & Eraye, 2012). These crimes are often glamorized in music, media, and local folklore, making them socially acceptable and even aspirational for young people seeking financial success.

The term "Yahoo-Yahoo" refers to a specific type of internet fraud that originated in Nigeria, characterized by using online platforms to deceive victims into sending money. This practice has become synonymous with cybercrime in Nigeria, particularly among young men who engage in these activities as a means of financial gain. The "Yahoo-Yahoo" culture is often romanticized in popular media, further perpetuating the cycle of cybercrime among the youth (Ayandele & Popoola, 2019). The normalization of such attitudes can lead to a broader acceptance of cybercrime as a viable career path.

Additionally, weak legal frameworks and inconsistent law enforcement contribute to this cultural acceptance. Many countries in the Global South lack stringent cybercrime laws or struggle with corruption, leading to selective enforcement where only a few perpetrators face consequences (Kshetri, 2019). This creates an environment where cybercriminals operate with minimal fear of legal repercussions, further embedding cyber fraud into the cultural fabric. In some cases, communities protect cybercriminals, viewing them as benefactors who bring economic prosperity. Without strong institutions to counteract these behaviours, cybercrime continues to flourish as a widely tolerated and even respected practice.

To combat this issue, cultural attitudes towards cybercrime must change through education, ethical digital awareness, and stronger legal enforcement. Governments, educational institutions, and community leaders must work together to shift societal perceptions by promoting legitimate digital entrepreneurship and emphasizing the long-term consequences of cybercrime (Boateng *et al.*, 2011). Public awareness campaigns, skill development programs, and stricter penalties can help reshape the narrative, discouraging cybercrime as a career path. Only by addressing the cultural roots of cybercrime can the Global South effectively curb its rise and foster a more secure digital landscape.

4. Vulnerability to Specific Types of Cybercrime in the Global South

Vulnerability to cybercrime refers to weaknesses in digital systems, networks, or human behaviours that cybercriminals can exploit to gain unauthorized access, steal data, disrupt operations, or commit fraud. These vulnerabilities can stem from outdated software, weak passwords, poor cybersecurity practices, unpatched security flaws, or social engineering tactics like phishing. Individuals, businesses, and governments can all be at risk if they fail to implement robust cybersecurity measures such as encryption, multi-factor authentication, and regular security updates. Reducing vulnerability requires a proactive approach, including user education, threat monitoring, and strong security protocols (Kidd, 2025).

The Global South, which includes developing regions in Africa, Latin America, and parts of Asia, faces distinct vulnerabilities to cybercrime due to gaps in digital infrastructure, weak regulatory frameworks, and socio-economic disparities. One of the most prevalent cyber threats in these regions is *financial fraud*, including phishing scams, credit card fraud, and mobile money fraud. Many individuals in these regions rely on mobile banking and digital wallets due to limited access to traditional banking systems, making them prime targets for cybercriminals (Donovan *et al.*, 2016). Fraudsters exploit low digital literacy and weak security measures to deceive users into revealing sensitive financial information, leading to significant financial losses and economic hardships (Kshetri, 2019).

Another pressing cyber threat is *ransomware attacks* on critical sectors, such as healthcare, education, and government institutions. Many organizations in the Global South lack the necessary cybersecurity infrastructure and expertise to prevent and mitigate such attacks, making them easy targets for cybercriminals who deploy ransomware to encrypt systems and demand payment for data recovery (Calderaro & Craig, 2020). The inability to pay ransoms or restore compromised systems results in severe disruptions to essential services, further exacerbating socio-economic inequalities and slowing development efforts in affected nations (Munoriyarwa & Mare, 2023).

Cyber-enabled human trafficking and online exploitation are also major concerns in the Global South. Weak law enforcement mechanisms, poverty, and high unemployment rates create conditions where cybercriminals exploit vulnerable populations, particularly women and children, through online recruitment for forced labour, sexual exploitation, and scams (Interpol, 2024). Social media platforms and messaging apps are frequently used to lure victims, often operating across borders, making it difficult for authorities to track and prosecute offenders effectively (Europol, 2024). This form of cybercrime not only inflicts psychological and financial harm on victims but also undermines national security and economic stability.

Another critical issue is the rise of *disinformation and cyber-political manipulation*, which has increasingly been used to influence elections, incite violence, and suppress dissent in developing nations.

State and non-state actors exploit weak cybersecurity policies, low media literacy, and unregulated digital platforms to spread misinformation, often targeting marginalized communities (Bradshaw & Howard, 2019). These campaigns can destabilize governments, undermine trust in democratic institutions, and fuel social unrest, making it a significant cybersecurity concern in the region (Freedom House, 2022). Without effective measures to counter online misinformation, the Global South remains highly vulnerable to politically motivated cyber threats.

In the same vein, *digital identity theft* is an emerging problem, particularly as governments and private institutions push for digital IDs and biometric data collection for public services. Poor cybersecurity protections in national databases and widespread corruption create opportunities for hackers to steal personal information, which can then be used for fraud, illegal immigration, or black-market transactions (OECD, 2024). Without adequate legal and technical safeguards, the digital transformation in the Global South risks exposing millions to identity-related crimes, further marginalizing vulnerable populations. Addressing these cybercrime challenges requires a multi-stakeholder approach, including stronger regulations, increased cybersecurity investments, and digital literacy programs to empower users against cyber threats (World Bank, 2025).

A major factor in vulnerability to cybercrime is lack of awareness. Lack of awareness contributes to cybercrime through many ways. In phishing scams, many users fail to recognize phishing emails or fake websites, leading to compromised personal and financial information. Cybercriminals exploit this ignorance to steal sensitive data (Aphane & Mofokeng, 2020). Similarly, weak passwords and poor security practices leads to susceptibility to cybercrime. People often use weak or reused passwords, making it easier for hackers to gain unauthorized access to accounts. A lack of awareness about two-factor authentication (2FA) further increases vulnerability.

In social engineering attacks, cybercriminals manipulate unaware individuals into revealing confidential information by pretending to be trustworthy sources (e.g., tech support scams, impersonation fraud) (Nzeakor *et al.*, 2022). Similarly, for malware and ransomware attacks, many users are deceived into unknowingly downloading malicious software through suspicious links, attachments, or websites, leading to system breaches, data theft, or financial extortion (Aphane & Mofokeng, 2020). Financial and investment scams utilize lack of knowledge about online fraud schemes, such as cryptocurrency scams or Ponzi schemes, to make individuals more susceptible to cybercriminal deception. Corporate and employee vulnerabilities is seen when businesses, employees who are not trained in cybersecurity best practices unknowingly expose company networks to cyber threats, leading to data breaches (Bougaardt & Kyobe, 2011).

University undergraduates in the Global South are particularly vulnerable to various forms of cybercrime, especially through their use of social media platforms. Many students fall victim to phishing scams, where cybercriminals impersonate legitimate entities to steal personal information. The prevalence of phishing attacks is heightened by students' tendency to click on suspicious links shared via social media (Yoro *et al.*, 2023). The oversharing of personal information on platforms like Facebook, WhatsApp and Instagram increases the risk of identity theft. Cybercriminals can easily gather information to impersonate individuals and commit fraud (Kayomb, 2024).

Social media and dating apps are often used by cybercriminals to exploit vulnerable individuals. Students seeking relationships may be targeted by scammers who manipulate them into sending money or sharing sensitive information (Tzani *et al.*, 2024). The rise of sextortion, where individuals are coerced into sharing explicit content under the threat of exposure, has become a significant concern (Henry & Umbach, 2024). Many youths are targeted through platforms like Snapchat, TikTok and Instagram, where they may feel more secure sharing personal content.

Students often download apps from unverified sources, exposing their devices to malware and ransomware attacks. This vulnerability is exacerbated by a lack of awareness regarding safe downloading practices (Onyema *et al.*, 2021). Cybercriminals frequently use social engineering tactics to manipulate students into divulging personal information (Ojugo & Eboka, 2021). This can occur through fake job offers or scholarship scams circulated on social media (Abraham & Chengalur-Smith, 2010).

It is thus obvious that students' vulnerability to specific types of cybercrime in the Global South is shaped by factors such as limited cybersecurity infrastructure, low digital literacy, weak regulatory frameworks, and high mobile internet penetration. Cybercriminals exploit these weaknesses through phishing, financial fraud, ransomware, and identity theft, often targeting individuals, businesses, and even government institutions. Socioeconomic challenges, such as poverty and inadequate cybersecurity investments, further exacerbate the risks, making it difficult for victims to recover from attacks. Additionally, the rise of digital financial services in regions with weak cybersecurity protections increases exposure to cyber fraud. Addressing these vulnerabilities requires stronger legal frameworks, capacity-building initiatives, and international cooperation.

5. Government Initiatives to address Cybercrime Vulnerabilities in the Global South

Governments in the Global South are actively implementing initiatives to address cybercrime vulnerabilities, recognizing the critical importance of cybersecurity in safeguarding their digital landscapes. In Africa, for instance, the Economic Community of West African States (ECOWAS) adopted its Regional Cybersecurity and Cybercrime Strategy in 2021, which outlines actions for member states to strengthen cybersecurity frameworks, establish dedicated authorities, and enhance skills development to combat cybercrime effectively (DiPLO, 2021). Similarly, the Southern African Development Community (SADC) introduced a Model Law on Computer Crime and Cybercrime in 2012 to harmonize legal approaches across its member states (DiPLO, 2021). On a continental level, the African Union Convention on Cyber Security and Personal Data Protection, known as the Malabo Convention, was adopted in 2014 to establish a comprehensive legal framework for cybersecurity and data protection among African nations (African Union, 2020). International organizations are also contributing to these efforts; Interpol launched a cybercrime operations desk in 2021 to bolster the capacity of 49 African countries in combating cybercrime through intelligence-led coordinated actions (Interpol, 2021). In Latin America and the Caribbean, a regional security alliance was formed in December 2024, comprising 16 governments and international financial institutions, aiming to combat organized crime, including cybercrime, by sharing criminal records and enhancing law enforcement capabilities (Morland, 2024). These initiatives reflect a growing commitment among Global South nations to collaborate regionally and internationally to mitigate cybercrime vulnerabilities and strengthen their cybersecurity resilience.

The statistics surrounding cybercrime in Nigeria, for instance, are alarming. The Nigerian Communications Commission (NCC) reports that Nigeria loses approximately $500 million annually to cybercrime, accounting for 0.08% of the country's GDP, and over 90% of Nigerian businesses have been victims (Olomu, 2023). A report by the Economic and Financial Crimes Commission (EFCC, 2021) indicated that over 19,000 cases of cybercrime were reported in Nigeria in 2021 alone, with a significant percentage involving young adults. The FBI reported a 1,000% increase in financial sextortion incidents linked to Nigerian cybercriminals targeting minors in Western countries, highlighting the global reach of Nigerian cybercrime (Akinwotu, 2024). Different surveys also found that Nigerian university students had encountered some form of cybercrime, either as victims or witnesses (Adeniran *et al.*, 2024; Ibrahim *et al.*, 2024; Idowu & Madaki, 2021; Ogunyemi, 2024; Rufai *et al.*, 2021). This significant impact of cybercrime has driven the government into action that are beginning to yield some results.

In Nigeria, specifically, to combat the rising tide of cybercrime among university undergraduates, the Nigerian government has implemented several initiatives designed to enhance cybersecurity awareness and education. These measures include:

a) National cyber security policy and strategy: The Nigerian government has developed a comprehensive policy aimed at enhancing the country's cybersecurity framework. This policy emphasizes collaboration among various stakeholders, including educational institutions, to promote cybersecurity awareness and education among students (Federal Republic of Nigeria, 2021).

b) Cybersecurity awareness programs: Awareness campaigns targeting university students have been initiated to educate them about the risks associated with cybercrime and the importance of cybersecurity practices. These programs aim to equip students with the knowledge to protect themselves against cyber threats (Anazodo, 2025).

c) Collaboration with educational institutions: The government encourages partnerships between cybersecurity agencies and universities to integrate cybersecurity education into the academic curriculum. This includes the establishment of specialized courses and training programs focused on cybersecurity skills (Ere-Mendie, 2023).
d) Legislative framework: The Cybercrime (Prohibition, Prevention, etc.) Act of 2015 provides a legal framework for combating cybercrime in Nigeria. This legislation includes provisions that specifically address cyber offenses and promote the prosecution of offenders, thereby creating a safer online environment for students (Ibrahim, 2016).
e) Capacity building for law enforcement: The government has invested in training law enforcement agencies to better handle cybercrime cases. This includes specialized training on digital forensics and cyber investigation techniques, which are crucial for effectively addressing cybercrime incidents involving students (Bello & Griffiths, 2021).
f) Youth empowerment initiatives: Recognizing that unemployment and poverty are significant drivers of cybercrime, the government has launched various youth empowerment programs aimed at providing job opportunities and skills training. These initiatives are designed to reduce the economic incentives for young people to engage in cybercrime (Ehimen & Bola, 2010).
g) Public-private partnerships: The government has fostered collaborations with private sector organizations to enhance cybersecurity infrastructure and resources. These partnerships aim to create a more robust cybersecurity ecosystem that can better protect university students and other citizens from cyber threats (Onuora *et al.*, 2017).

By implementing these measures, the Nigerian government aims to mitigate the vulnerabilities associated with cybercrime among university undergraduates and foster a safer digital environment.

Similarly, governments in the Global South have undertaken various initiatives to address cybercrime vulnerabilities, yielding both successes and challenges. A few cases are presented here.

Success Stories

a) Bhutan: Between 2015 and 2018, Bhutan established its national Computer Security Incident Response Team (BtCIRT) with support from the World Bank. BtCIRT has significantly enhanced the country's cyber resilience by providing expert technical support, conducting over 20 workshops to build cybersecurity capacity, handling approximately 1,200 cybersecurity incidents, and issuing more than 600 alerts related to vulnerabilities and scams (World Bank, 2025).
b) Bangladesh: From 2016 to 2020, Bangladesh developed the BGD e-GOV CIRT, a dedicated response team for e-government cybersecurity incidents. This team has effectively managed cybersecurity threats, resolving 70% of reported incidents within two hours and delivering 67 technical training sessions to over 1,800 civil servants in 2021 alone (World Bank, 2025).
c) Ghana: The National Cyber Security Centre launched the "A Safer Digital Ghana" initiative in 2018, focusing on awareness raising and training across various sectors. By engaging over 275,000 participants through workshops and sensitization exercises, the program has built a network of cybersecurity professionals and provided a platform for reporting cybercrime incidents, with over 38,000 reports submitted (European Union Cyber Diplomacy Initiative, 2025).

Challenges and Failures

a) India: In 2023, India experienced a significant data breach involving the personal details of over 815 million individuals, allegedly sourced from the Indian Council of Medical Research (ICMR). The leaked information included sensitive data such as Aadhaar and passport details, raising concerns about data security and privacy (NetMission.Asia, 2024).
b) Pakistan: In June 2023, Pakistan's National Institutional Facilitation Technologies (NIFT) faced a cyberattack that compromised terabytes of data, including scans of all cheques from its database. The breach affected the banking system nationwide, leading to the shutdown of major data centres and halting certain banking services for over a week (NetMission.Asia, 2024).
c) These cases underscore the importance of continuous investment in cybersecurity infrastructure, regular audits, public awareness campaigns, and robust data protection laws to mitigate cybercrime vulnerabilities in the Global South.

6. Theoretical Framework

The theoretical framework for analyzing vulnerability to cybercrime among university undergraduates in the Global South can be grounded in several theories that explain human behaviour in the context of technology use. Below are expanded points on relevant theories.

6.1. *Protection Motivation Theory (PMT)*

Protection Motivation Theory (PMT), developed by R. W. Rogers in 1975, is a psychological framework that explains how individuals engage in protective behaviours in response to perceived threats. The core premise of PMT is that individuals are motivated to protect themselves from potential harm based on their assessments of two critical factors: perceived vulnerability and perceived severity of the threat. These factors influence their decision-making processes regarding protective actions (Floyd *et al*., 2000; Rogers, 1975).

Components of PMT

a) *Perceived Vulnerability:* This refers to an individual's belief about the likelihood of experiencing a negative outcome. In the context of cybercrime, students who believe they are at risk of cyber threats—such as phishing attacks, identity theft, or malware infections—are more likely to take proactive measures to safeguard their information.

b) *Perceived Severity:* This component involves the belief about the seriousness of the consequences if the threat materializes. For instance, if students recognize that a cyber-attack could lead to significant financial loss, academic repercussions, or personal embarrassment, they may be more motivated to adopt security measures.

c) *Response Efficacy:* This aspect assesses the effectiveness of the proposed protective behaviours. If students believe that using strong passwords, enabling two-factor authentication, or avoiding suspicious links can effectively mitigate the risk of cyber threats, they are more likely to engage in these behaviours.

d) *Self-Efficacy:* This refers to an individual's confidence in their ability to execute the protective behaviours. Students who feel capable of implementing security measures (e.g., using technology or understanding security protocols) are more likely to adopt them.

e) *Fear Appeals:* PMT also considers the role of fear in motivating protective behaviours. If students are exposed to information that highlights the dangers of cybercrime and the potential consequences of inaction, they may experience fear, which can act as a catalyst for change in behaviour.

Application of PMT to Cybercrime Vulnerability among University Undergraduates

In examining cybercrime vulnerability among university undergraduates, PMT provides a useful framework for understanding their behaviour regarding cybersecurity. Many students use social media and online platforms extensively, often without adequate awareness of the risks involved.

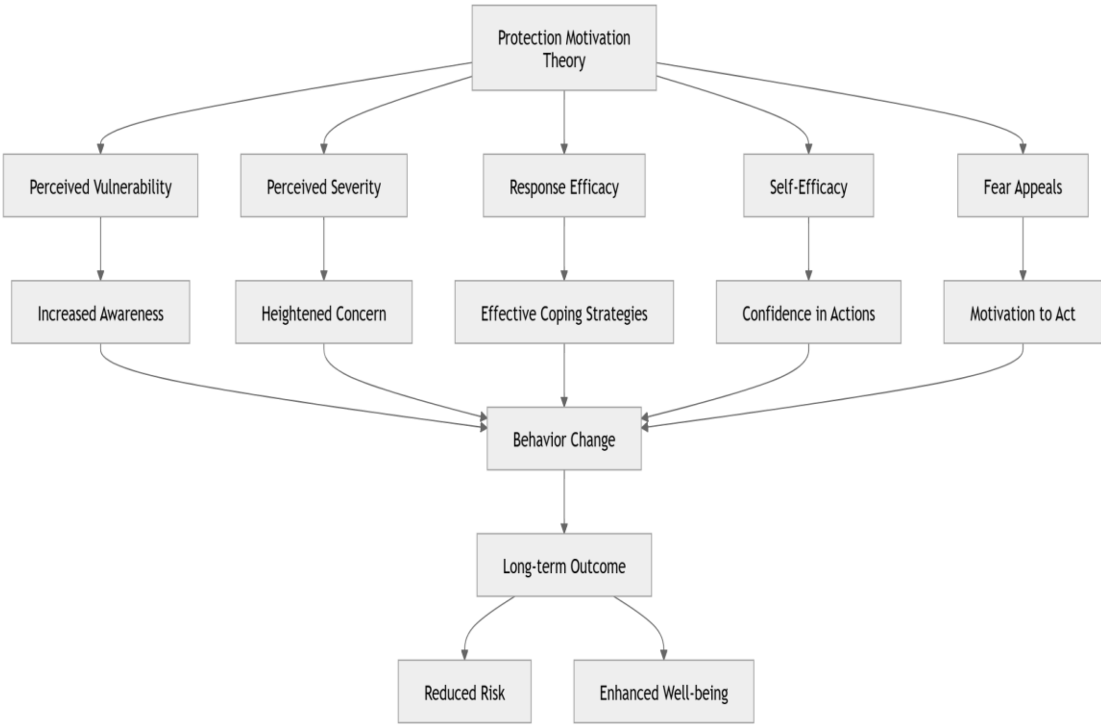
In terms of *Perceived Vulnerability and Severity*, research indicates that while students may recognize that cybercrime is a prevalent issue, they often underestimate their personal vulnerability. For example, a study by Meso *et al.* (2023) found that many students believed they were safe from cyber threats because they had not experienced cyber incidents themselves. This complacency can lead to risky behaviours, such as sharing personal information on social media or using weak passwords (Alam *et al.*, 2024). To illustrate, consider an undergraduate who frequently uses social media to connect with friends. If they come across a phishing message but do not perceive themselves as vulnerable, thinking, "that won't happen to me", they may not take the necessary precautions. This underestimation of vulnerability can lead to severe consequences, such as identity theft or financial fraud.

In line with *Response Efficacy* and *Self-Efficacy* components of PMT, the effectiveness of protective measures is also critical. If students believe that strong password usage or regular software updates will significantly reduce their chances of falling victim to cybercrime, they are more likely to adopt these behaviours. Educational campaigns that demonstrate successful prevention strategies can enhance response efficacy. Moreover, self-efficacy plays a crucial role. If students feel they lack the technical skills to secure their devices, they may avoid implementing necessary measures altogether. For instance, a student might refrain from installing antivirus software simply because they feel overwhelmed by the technical aspects of doing so.

With *Fear Appeals*, in the Global South, awareness campaigns highlighting the dangers of cybercrime can serve as effective fear appeals. For example, stories of fellow students who have lost money to online scams can generate fear and prompt behavioural changes. When students see tangible examples of cybercrime's impact on their peers, they are more likely to reassess their vulnerability and take protective actions.

Figure 1

PMT Components (Rogers, 1975)



Rogers (1975) Protection Motivation Theory offers valuable insights into understanding and addressing cybercrime vulnerability among university undergraduates in the Global South. By enhancing students' perceptions of vulnerability and severity, increasing their belief in the efficacy of protective measures, and bolstering their self-efficacy, educational institutions can foster a culture of cybersecurity awareness and proactive behaviour. This approach not only equips students with the necessary skills to protect themselves but also contributes to a broader effort to mitigate the rising tide of cybercrime in an increasingly digital world. Leveraging PMT can guide interventions aimed at improving cybersecurity awareness and practices among students, ultimately reducing their vulnerability to cyber threats.

6.2. *Social Learning Theory*

Social Learning Theory (SLT), developed by Albert Bandura in the 1970s, posits that individuals learn behaviours through observation and imitation of others, even without direct reinforcement (Bandura, 1977). In the context of cybercrime, students may adopt risky online behaviours by observing peers or influencers who engage in unsafe practices, such as oversharing on social media or using weak passwords. The influence of social circles and online communities can significantly impact students' perceptions and behaviours regarding cybersecurity. Understanding these dynamics is crucial for developing targeted interventions (Ogunleye *et al.*, 2019).

Key Components of Social Learning Theory

a) *Observational Learning:* This is the core concept of SLT, where individuals can learn behaviours by observing others, particularly role models. In the context of cybercrime, students may observe peers engaging in risky online behaviours, such as sharing personal information or engaging in cyberbullying.

b) *Attention:* For observational learning to occur, individuals must pay attention to the model. Factors that affect attention include the model's characteristics (e.g., attractiveness, credibility) and the perceived relevance of the behaviour being demonstrated.

c) *Retention:* After observing a behaviour, individuals must be able to remember it to reproduce it later. This involves cognitive processes that allow for the encoding and storage of the observed behaviour.

d) *Reproduction:* This refers to the ability to replicate the behaviour after it has been observed and retained. In the context of cybercrime, this could involve a student who has seen a peer successfully navigate a phishing scam and then attempts to replicate that behaviour, believing it to be harmless or beneficial.

e) *Motivation:* Motivation to engage in the learned behaviour is crucial. This can be influenced by external reinforcement (rewards or punishments) or internal factors (personal beliefs and values). If students see peers gaining social status or financial gain from cybercrime, they may feel motivated to imitate those behaviours.

Application of Social Learning Theory to Cybercrime Vulnerability among University Undergraduates

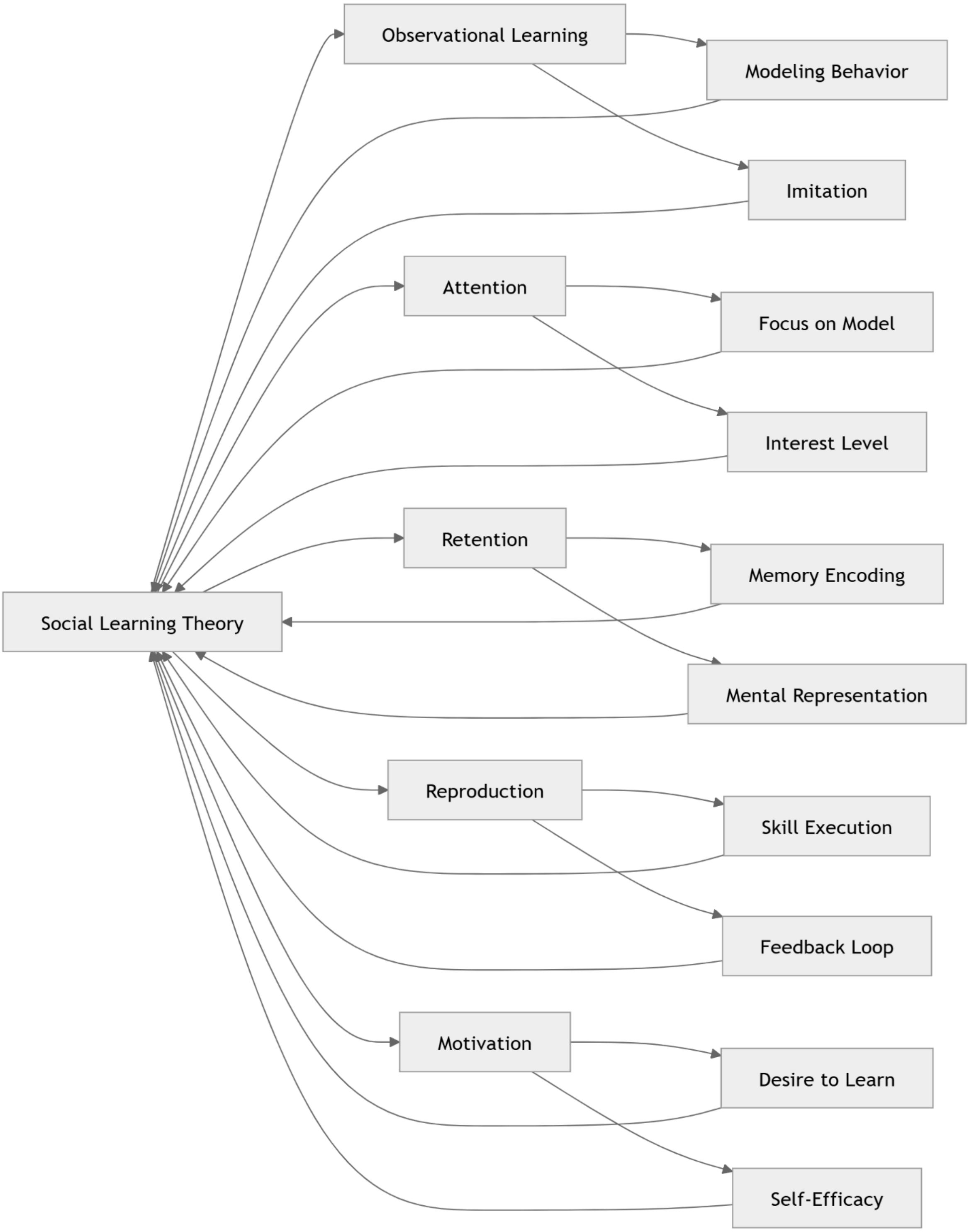
In examining the vulnerability of university undergraduates to cybercrime in the Global South, SLT provides a useful lens to understand how behaviours are learned and reinforced within social contexts. In terms *Observational Learning and Cybercrime*, many university students frequently use social media platforms, where they are exposed to various online behaviours, including both positive and negative actions. For instance, if a student observes friends engaging in activities like hacking or bypassing security protocols without facing immediate consequences, they may view such behaviours as acceptable or even desirable. This observational learning can lead to the normalization of risky online practices.

With regards to *Attention and Retention*, the characteristics of the celebrities that students observe – such as their perceived expertise or popularity – can significantly impact students' attention and retention. If a student follows a popular influencer who shares tips on "hacking" or "tricking" online systems, they may pay closer attention to those behaviours. The retention of these behaviours can manifest in their own online activities, increasing their vulnerability to engaging in cybercrime (Muraina *et al.*, 2022).

Regarding *Reproduction and Motivation*, once students have observed and retained their behaviour, the next step is reproduction. If they believe they can successfully replicate the observed behaviours – such as using social engineering techniques to deceive others – they may feel emboldened to try these methods themselves. The perceived rewards, such as gaining access to restricted content, achieving social status, or even financial gain, can further motivate them to engage in cybercriminal activities. This is particularly relevant in the Global South, where economic factors may drive some students towards cybercrime as a means of financial survival (Abdulla *et al.*, 2023).

Figure 2

SLT Components (Bandura, 1977)



Social Learning Theory offers a valuable framework for understanding the dynamics of cybercrime vulnerability among university undergraduates in the Global South. By recognizing the role of observational learning, attention, retention, reproduction, and motivation, educational institutions can develop targeted interventions to mitigate these vulnerabilities. For instance, promoting positive role models in cybersecurity can help reshape students' perceptions and behaviours regarding online safety. Additionally, awareness campaigns emphasizing the consequences of engaging in cybercrime can discourage imitation of negative behaviours seen in peers or online influencers.

6.3. *General Strain Theory*

General Strain Theory (GST), developed by Robert Agnew in the 1990s, posits that individuals experiencing stress or strain are more likely to engage in criminal behaviour as a coping mechanism (Agnew, 1992). General strain theory was developed by sociologist Robert Agnew to address the shortcomings of original strain theories developed by Merton and Durkheim. Agnew's general strain theory argues that certain strains or stressors placed on members of society may lead certain individuals to engage in criminal activity. For university students in the Global South facing academic pressure, financial difficulties, and unemployment, this strain may lead some to view cybercrime as a viable option for financial gain. GST highlights how negative emotions resulting from strain can drive deviant behaviour, providing insight into the motivations behind students' engagement in cybercriminal activities (Boateng *et al.*, 2011; Oduro-Frimpong, 2014; Ojedokun & Eraye, 2012).

Key Components of General Strain Theory

Agnew (1992) identifies three primary sources of strain:

a) *Failure to Achieve Goals:* This occurs when individuals are unable to achieve positively valued goals, such as educational success, financial stability, or social status. For example, students who struggle with academic performance may feel frustrated and resort to negative behaviours.

b) *Loss of Positive Stimuli:* This type of strain happens when individuals lose something valuable, such as the death of a loved one, the end of a relationship, or loss of status. Such losses can create feelings of grief and anger, which may lead to maladaptive behaviours.

c) *Presentation of Negative Stimuli:* This strain results from exposure to negative experiences or conditions, such as bullying, family conflict, or community violence. Students experiencing such negative stimuli may react by engaging in deviant behaviours as a coping mechanism.

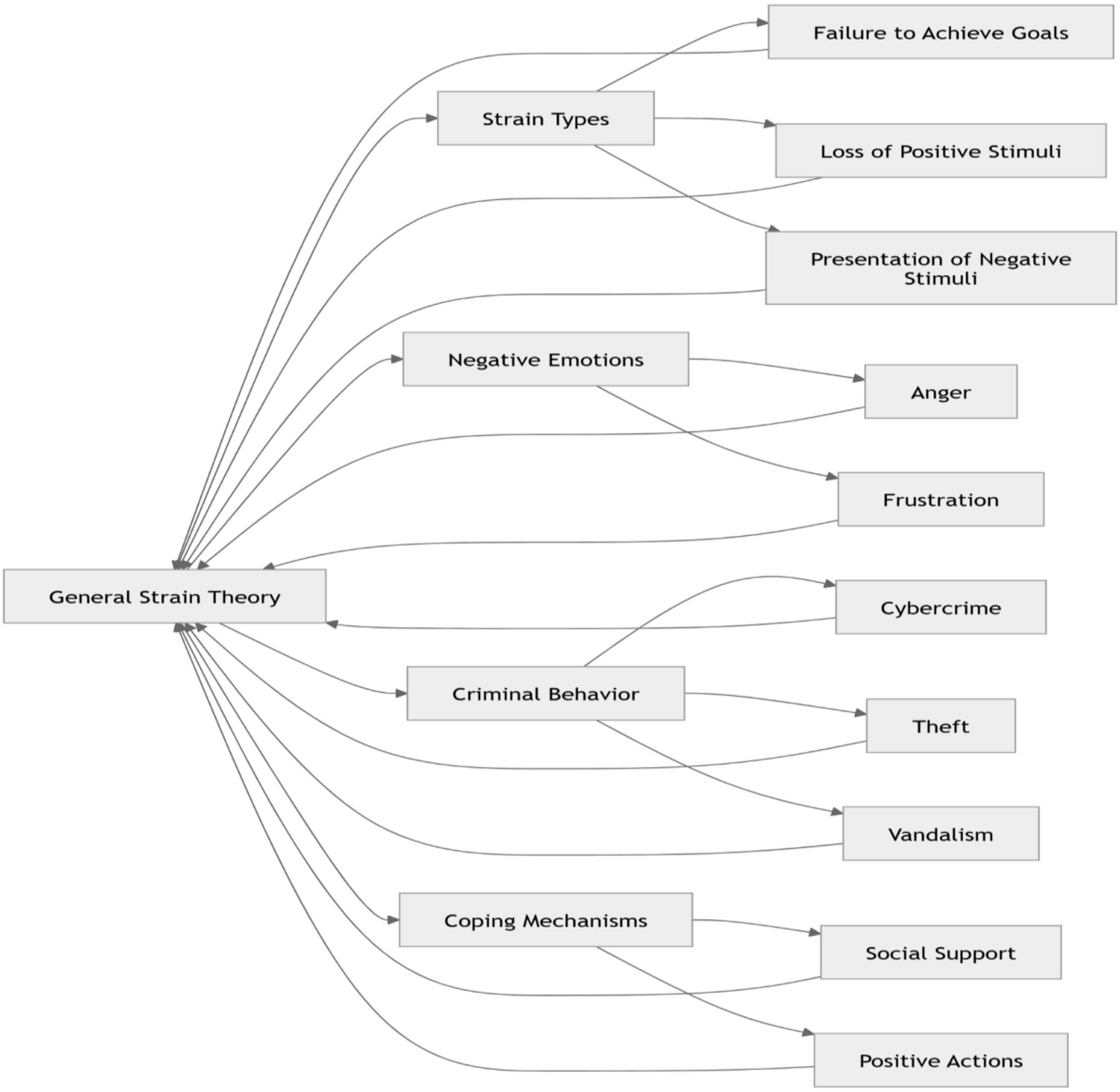
These sources of strain lead to *negative emotions*, such as anger, frustration, and disappointment. These emotions can increase the likelihood of engaging in criminal behaviour as individuals seek to cope with or escape their feelings. For *Coping Mechanisms*, GST posits that individuals may respond to strain in various ways. Some may engage in pro-social behaviours, while others may resort to criminal activities. The likelihood of choosing criminal behaviour often depends on the individual's social environment and available coping resources. GST emphasizes *Social Support and Control*. The presence of social support systems can mitigate the negative effects of strain. Strong social ties and community support can provide individuals with alternative coping mechanisms, reducing the likelihood of engaging in criminal behaviour.

Application of General Strain Theory to Cybercrime Vulnerability among University Undergraduates

In examining cybercrime vulnerability among university undergraduates in the Global South, GST provides a useful framework for understanding how different strains can lead to increased susceptibility to engaging in cybercriminal activities. Students go through different types of strain. With regards to *Failure to Achieve Goals*, many university students face immense pressure to succeed academically and secure future employment. In the Global South, where economic conditions can be challenging, students who struggle to meet these expectations may experience significant strain, increasing susceptibility to cybercrime (Kshetri, 2019). For instance, a student who fails exams or struggles to find internships may feel frustrated and hopeless, leading them to consider alternative means of achieving success, such as engaging in cybercrime (Igba *et al.*, 2018). With *Loss of Positive Stimuli* Students may also experience losing a scholarship or facing financial difficulties within the family. Such losses can lead to feelings of despair and anger. For example, a student who loses financial support may resort to hacking or online scams as a means of regaining financial stability. *Presentation of Negative Stimuli* such as cyberbullying or harassment on social media, can further exacerbate strain. Students subjected to online bullying may experience emotional distress, leading them to retaliate through cybercrime or other deviant behaviours (Anyanwu, 2024).

The *negative emotions* resulting from these strains – such as anger and frustration – can drive students toward cybercrime as a coping mechanism. For instance, a student who feels marginalized or bullied might engage in hacking or identity theft to regain power or control. The availability of *effective coping mechanisms* is crucial in determining how students respond to strains. Those with strong social support systems – such as friends, family, or mentorship – are more likely to cope positively with strain and less likely to engage in cybercrime. Conversely, students who lack such support may feel isolated and resort to criminal behaviours to alleviate their negative emotions (Agnew, 1992).

Figure 3
GST Components (Agnew, 1992)



7. Implications for Cybersecurity in the Global South

In the Global South, where digital adoption is rapidly increasing, students represent a particularly vulnerable group to cybercrime (Otozi *et al.*, 2024). Many students access the internet through personal and institutional networks with limited cybersecurity awareness. Their dependence on online platforms for education, communication, and financial transactions makes them prime targets for cybercriminals. The lack of stringent cybersecurity measures in educational institutions and limited legal frameworks in many countries further exacerbate this vulnerability, leading to significant risks for students and broader societal consequences.

One major implication of student vulnerability to cybercrime is the increased risk of identity theft and financial fraud (Parrish *et al.*, 2018). Many students in the Global South lack cybersecurity training and are unaware of phishing scams or fake websites designed to steal their personal data. Cybercriminals exploit this ignorance to access sensitive information such as banking details, academic records, and social media accounts (Cheng & Wang, 2022). In regions where digital banking is growing but security literacy remains low, such breaches can lead to severe financial losses and long-term damage to students' financial stability.

Another concern is the rising threat of online harassment and cyberbullying. Many students engage in social media without understanding the risks associated with oversharing personal information. Cybercriminals, scammers, and malicious actors often use these platforms to manipulate, threaten, or exploit young internet users. In extreme cases, this vulnerability has led to psychological distress, reputational damage, and, in some instances, self-harm or suicide. Weak cyber policies in schools and universities fail to protect students from such dangers, leaving them exposed to online abuse.

The proliferation of digital learning platforms also raises cybersecurity challenges in academic institutions. Universities and schools in the Global South often lack the budget or expertise to implement robust cybersecurity infrastructure. This makes online learning management systems and student databases attractive targets for hackers. Ransomware attacks on educational institutions have increased, with cybercriminals demanding payment to restore access to critical academic resources. Without proper defenses, schools risk losing valuable data, disrupting learning, and exposing students to further cyber threats.

Furthermore, students' reliance on public Wi-Fi and unsecured networks amplifies their exposure to cyber risks. Many students in developing regions cannot afford personal internet services and rely on free networks in shopping malls, eateries, libraries, cafes, or shared accommodations (Cojocariu *et al.*, 2020). These networks are often unsecured, making it easy for cybercriminals to intercept communications and steal login credentials. This risk is heightened when students access sensitive accounts, such as email or online banking, through these networks, inadvertently compromising their data security.

Addressing these cybersecurity risks requires a multi-stakeholder approach. Governments, educational institutions, and technology companies must collaborate to implement stronger policies, provide cybersecurity education, and enhance digital infrastructure (Kshetri, 2019). Cyber hygiene programmes in schools can equip students with knowledge about secure passwords, phishing awareness, and data protection. Additionally, governments must enforce stricter cybercrime laws and invest in cybersecurity capacity-building to safeguard students from online threats (Kundi *et al.*, 2014).

Ultimately, the vulnerability of students to cybercrime in the Global South is a growing concern with far-reaching implications (Świątkowska, 2020). As digital transformation accelerates, the gap between technological advancement and cybersecurity awareness must be bridged (Abah, 2019). Strengthening cyber defences in educational institutions, promoting digital literacy, and enacting stringent cybersecurity regulations will be essential in mitigating these risks and ensuring a safer online environment for students (Donalds *et al.*, 2022).

Evidently, cybercrime poses significant and multifaceted implications for students in the Global South, exacerbating existing inequalities. Limited access to digital literacy and cybersecurity education leaves them particularly vulnerable to online threats like phishing, identity theft, and cyberbullying. Furthermore, the potential for financial fraud and data breaches can disrupt educational pursuits and create economic hardship. The psychological impact of cybercrime, including anxiety and loss of trust, can also hinder academic performance and well-being. Additionally, the lack of robust legal frameworks and law enforcement resources in many Global South nations can impede the pursuit of justice for cybercrime victims, compounding the negative consequences.

8. Conclusion

Educational institutions must take a proactive and multifaceted approach to address the growing threat of cybercrime. Firstly, they must prioritize comprehensive cybersecurity education and awareness programs. These programmes should target students, faculty, and staff, equipping them with the knowledge and skills to identify and avoid online threats such as phishing, malware, and social engineering. This includes fostering a culture of cyber awareness, where best practices are consistently reinforced and updated to reflect evolving threats.

Secondly, institutions must invest in robust cybersecurity infrastructure and systems. This involves implementing strong access controls, firewalls, and intrusion detection systems to protect sensitive data and networks. Regular security audits and vulnerability assessments are essential to identify and address potential weaknesses. Furthermore, institutions should establish clear incident response plans to minimize the impact of cyberattacks and ensure swift recovery. This also includes keeping all software and hardware up to date with the latest security patches.

Finally, educational institutions must foster a collaborative approach to cybersecurity. This includes working with law enforcement agencies, cybersecurity experts, and other institutions to share information and best practices. Establishing clear policies and procedures for data privacy and security is also crucial, along with ensuring compliance with relevant regulations. By taking these steps, educational institutions can create a safer online environment for their students and protect their valuable data.

9. Recommendations

It is important to recognize that successful cybersecurity in education is an ongoing process, and "perfect" solutions are rare. However, there are numerous examples of educational institutions and organizations implementing effective strategies. These examples demonstrate that a combination of education, technology, and collaboration is essential for effective cybersecurity in educational institutions in the Global South. Recommended strategies may include:

a) *Integrating Cybersecurity into Curriculum:* Many schools are now incorporating cybersecurity modules into their computer science and technology classes. This hands-on approach allows students to learn about threats like phishing and malware, and practice safe online behaviour. For example, some schools utilize cybersecurity simulation software that mimics real-world cyberattacks, allowing students to practice their response skills in a safe environment. Many non-governmental organizations (NGOs) provide educational resources and programmes that schools can use to teach students about online safety.

b) *Robust Network Security:* Universities and larger school districts are increasingly investing in advanced firewalls, intrusion detection systems, and data encryption. They also perform regular security audits to identify and fix vulnerabilities. Implementing "zero trust" security models, where every user and device is verified before being granted access to network resources, is gaining traction. This helps to limit the damage if a single device or account is compromised.

c) *Cybersecurity Awareness Training:* Many institutions are conducting regular cybersecurity awareness training for students, faculty, and staff. This training covers topics like password security, phishing awareness, and social engineering. Some institutions use gamified training platforms that make learning about cybersecurity more engaging. These platforms often include quizzes, simulations, and interactive exercises.

d) *Collaborative Efforts:* Universities and research institutions often collaborate with cybersecurity companies and government agencies to share threat intelligence and develop new security solutions. Information sharing and analysis centers (ISACs) exist for the education sector, allowing institutions to share information about cyber threats and best practices.

e) *Real World Simulation Programmers:* Programs that simulate phishing attacks, and other cyber-attacks have shown themselves to be very effective. By providing real world examples, and safe environments to learn in, students gain valuable experience.

Acknowledgments

The authors acknowledge the continues support of family in the course of the different study programmes accommodating this research work.

Author Contribution

Author 1: Writing - Editing and Visualization; Review & Editing, Validation and Supervision

Author 2: Conceptualization, Writing - Original Draft,

Funding Statement

This research was NOT funded.

Conflict of Interest

The authors declare no conflict of interest.

10. References

Abah, J. A. (2019). Theoretical and conceptual framework for digital inclusion among mathematics education students in Nigeria. *Global perspectives on educational issues*, *1*(1), 79-111.

Abdulla, R. M., Faraj, H. A., Abdullah, C. O., Amin, A. H., & Rashid, T. A. (2023). Analysis of social engineering awareness among students and lecturers. *IEEE Access*, *11*, 101098-101111. https://doi.org/10.1109/ACCESS.2023.3311708

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183-196. https://doi.org/10.1016/j.techsoc.2010.07.001

Adeniran, A. A., Adeniran, A. O., Familusi, O. B., & Adedayo, O. (2024). The Outlook of Cyber Security in African Businesses: Issues and Way-Out. *Management analytics and social insights*, *1*(2), 260-271. https://doi.org/10.22105/masi.v1i2.54

African Union. (2020). *African Union Convention on Cyber Security and Personal Data Protection*. Retrieved April 1, 2025, from https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

African Union. (2020). *Cybersecurity in Africa: A report on the state of cybercrime*. African Union.

Agnew, R. (1992). Foundation for a General Strain Theory of Crime and Delinquency, *Criminology*, 30, 47-87.

Akinwotu, E. (2024). FBI director urges Nigeria to do more to combat the rise of sextortion. https://www.npr.org/2024/06/14/nx-s1-5006112/the-issue-of-sextortion-was-high-on-the-agenda-when-the-fbi-director-traveled-to-nigeria

Akinyetun, T. S. (2021). Poverty, cybercrime and national security in Nigeria. *Journal of Contemporary Sociological Issues*, *1*(2), 86-109. https://doi.org/10.19184/csi.v1i2.24188

Alam, S. S., Ahsan, N., Kokash, H. A., Alam, S., & Ahmed, S. (2024). A students' behaviors in information security: Extension of Protection Motivation Theory (PMT). *Information Security Journal: A Global Perspective*, 1-23. https://doi.org/10.1080/19393555.2024.2408264

Anazodo, R. O. (2025). Cyber security administration in developing countries: a Nigerian perspective. *International Journal of Finance, Accounting and Management Studies*, *1*(4), 122-139. http://www.ijfams.com/index.php/ijfams/article/download/55/55

Anyanwu, U. S. (2024). Youth's Unemployment and Cybercrime in Nigeria. *Canadian Social Science*, *20*(5), 69-78. https://dx.doi.org/10.3968/13574

Aphane, M. P., & Mofokeng, J. T. (2020). Critical Analysis of Strategies Towards Creating an Adequate Level of Awareness on Cybercrime among the Youth in Gauteng Province. *International Journal of Criminology & Sociology*, *9*, 1385-1396.

Ayandele, O., & Popoola, O. (2022). *Yahoo Yahoo: Cyber-enabled crime and criminality in Nigeria*. SSRN. https://doi.org/10.2139/ssrn.4123456

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 393-410. https://doi.org/10.6000/1929-4409.2020.09.159

Bandura, A. (1977). *Social learning theory*. Englewood Cliffs, NJ: Prentice-Hall.

Bello, M., & Griffiths, M. (2021). Routine activity theory and cybercrime investigation in Nigeria: how capable are law enforcement agencies? *Rethinking Cybercrime: Critical Debates*, 213-235.

Boateng, R., Olumide, L., Isabalija, R. S., & Budu, J. (2011). Sakawa-cybercrime and criminality in Ghana. *Journal of Information Technology Impact*, *11*(2), 85-100.

Bottyán, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences*, *13*(3), 363-363. https://doi.org/10.24368/jates363

Bougaardt, G., & Kyobe, M. (2011). Investigating the factors inhibiting SMEs from recognizing and measuring losses from cybercrime in South Africa. In *ICIME 2011-Proceedings of the 2nd International Conference on Information Management and Evaluation: ICIME 2011 Ryerson University* (p. 62).

Bradshaw, S., & Howard, P. N. (2019). The global disinformation order: 2019 global inventory of organised social media manipulation. (Working Paper 2019.2). https://digitalcommons.unl.edu/scholcom/207/

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*, *29*(3), 408-433. https://doi.org/10.1108/13639510610684674

Broadhurst, R., Grabosky, P., Alazab, M., & Bouhours, B. (2013). Organizations and cybercrime. *Available at SSRN 2345525*.

Button, M., Johnston, L., & Frimpong, K. (2008). The fraud review and the policing of fraud: laying the foundations for a centralized fraud police or counter fraud executive?.*Policing: A Journal of Policy and Practice*, *2*(2), 241-250.

Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third world quarterly*, *41*(6), 917-938. https://cybilportal.org/wp-content/uploads/2020/10/CalderaroCraigTWQ_Transnational-governance-of-cybersecurity-policy-challenges-and-global-inequalities-in-cyber-capacity-building.pdf

Campbell, Q., & Kennedy, D. M. (2012). The psychology of computer criminals. *Computer security handbook*, 12-1.

Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192. https://doi.org/10.3390/info13040192

Chukwuma, E., & Olaniyi, O. (2022). Social media usage and cyber vulnerabilities among undergraduates in Nigeria. *African Journal of Information Systems*, 14(3), 220-234.

CISA. (2025). *Cybersecurity Best Practices*. Cybersecurity and Infrastructure Security Agency. Retrieved March 26, 2025, from https://www.cisa.gov/topics/cybersecurity-best-practices

Cojocariu, A. C., Verzea, I., & Chaib, R. (2020). Aspects of cyber-security in higher education institutions. In *Innovation in Sustainable Management and Entrepreneurship: 2019 International Symposium in Management (SIM2019)* (pp. 3-11). Springer International Publishing.

Dennis, M. A. (2025). *Cybercrime: Definition, Statistics, & Examples*. Britannica. Retrieved March 26, 2025, from https://www.britannica.com/topic/cybercrime

DiPLO. (2021). *ECOWAS Regional Cybersecurity and Cybercrime Strategy*. Retrieved April 1, 2025, from https://www.diplomacy.edu/resource/report-stronger-digital-voices-from-africa/cybersecurity-cybercrime-africa-continental-regional-policies/

Donalds, C., Barclay, C., & Osei-Bryson, K. M. (2022). *Cybercrime and Cybersecurity in the Global South: Concepts, Strategies and Frameworks for Greater Resilience*. Routledge.

Donovan, K. P., Frowd, P. M., & Martin, A. K. (2016). ASR Forum on surveillance in Africa: Politics, histories, techniques. *African Studies Review*, 31-37.

Egete, D. O., Ele, B. I., & Eko, M. C. E. (2023). Synopsis of Cybersecurity and Risks Associated with Cybercrime to Susceptible and Blameless Global Citizenries. *Applied Sciences*, *1*(5), 475-487. https://doi.org/10.59324/ejtas.2023.1(5).37

Ehimen, O. R., & Bola, A. (2010). Cybercrime in Nigeria. *Business Intelligence Journal*, *3*(1), 93-98.

Ere-Mendie, A. J. (2023). Nigerian Data Policies. *The Mediation of Sustainability: Development Goals, Social Movements, and Public Dissent*, 161.

European Union Cyber Diplomacy Initiative. (2025). *A safer digital Ghana*. EU Cyber Direct. Retrieved April 1, 2025, from https://eucyberdirect.eu/good-cyber-story/a-safer-digital-ghana

Europol. (2024). Internet Organised Crime Threat Assessment (IOCTA): Strategic, policy and tactical updates on the fight against cybercrime. https://www.europol.europa.eu/publications-events/main-reports/iocta-report

Federal Republic of Nigeria, (2021). National cybersecurity policy and strategy. https://cert.gov.ng/ngcert/resources/NATIONAL_CYBERSECURITY_POLICY_AND_STRATEGY_2021.pdf

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), 407-429.

Fox, J. (2024). *Top Cybersecurity Statistics for 2024*. Cobalt. Retrieved March 26, 2025, from https://www.cobalt.io/blog/cybersecurity-statistics-2024

Freedom House. (2022). *Freedom on the net 2022:* https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

Henry, N., & Umbach, R. (2024). Sextortion: Prevalence and correlates in 10 countries. *Computers in Human Behavior*, *158*, 108298. https://doi.org/10.1016/j.chb.2024.108298

Holt, T., & Bossler, A. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offenses.* Routledge.

Ibrahim, A. (2016). Cybercrime (Prohibition, Prevention Etc) Act, 2015: Issues and Challenges in Nigeria. In Draft Paper Presented at the 49th Annual Nigerian Law Teachers' Conference at Nasarawa State University, Keffi on behalf of Usman Danfodio University Sokoto, 22nd-27th May (pp. 15-16).

Ibrahim, Y. A., Ishaya, A. O., Yusuf, M., Nancy, I., Bijik, H. A., & Aiyedogbon, S. F. (2024). Cybersecurity and cybercrimes in Nigeria: An overview of challenges and prospects. In *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)* (pp. 1-7). IEEE.

Idowu, O. A., & Madaki, M. (2021). Cybercrimes and challenges of cyber-security in Nigeria. *International Journal of Sociology and Development*, *3*(1), 45-67.

Igba, I. D., Igba, E. C., Nwambam, A. S., Nnamani, S. C., Egbe, E. U., & Ogodo, J. V. (2018). Cybercrime among university undergraduates: Implications on their academic achievement. *International Journal of Applied Engineering Research*, *13*(2), 1144-1154. https://www.ripublication.com/ijaer18/ijaerv13n2_43.pdf

Iji, C. O., & Abah, J. A. (2019). Internet skills as a measure of digital inclusion among mathematics education students: Implications for sustainable human capital development in Nigeria. *International Journal of Education and Knowledge Management (IJEKM)*, *2*(1), 1-16.

Interpol. (2024). Inside INTERPOL's probe into cyber-enabled human trafficking. https://www.interpol.int/en/News-and-Events/News/2024/Inside-INTERPOL-s-probe-into-cyber-enabled-human-trafficking

Interpol. (2021). *INTERPOL launches initiative to fight cybercrime in Africa*. Retrieved April 1, 2025, from https://www.interpol.int/en/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa

Kaspersky. (2025). *What is cybercrime? How to protect yourself.* Kaspersky. Retrieved March 26, 2025, from https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Kayomb, M. J. (2024). *Phishing attack awareness amongst users at a university of technology in the Western Cape* (Doctoral dissertation, Cape Peninsula University of Technology).

Khan, N. F., Ikram, N., & Saleem, S. (2023). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Security Journal*, 1, 1-31. https://doi.org/10.1057/s41284-023-00375-4

Kidd, C (2025). *Vulnerabilities, Threats & Risk Explained.* Retrieved April 1, 2025, from https://www.splunk.com/en_us/blog/learn/vulnerability-vs-threat-vs-risk.html

Kshetri, N. (2016). Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future. *Crime, Law and Social Change*, 66(3), 313–338. https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cybercrime_2016.pdf

Kshetri, N. (2019) Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77-81. https://doi.org/10.1080/1097198X.2019.1603527

Kumah, P. K., Asiedu, H. B., Obeng, C., & Senior, F. A. O. (2024). Poverty as a catalyst for cybercrime: evidence from Agona Swedru, Ghana. *E-Journal of Humanities, Arts and Social Sciences*, 5(14), 2582-2596. https://doi.org/10.38159/ehass.202451410

Kundi, G. M., Nawaz, A., & Akhtar, R. (2014). Digital revolution, cyber-crimes and cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications*, *4*(4), 61-71. https://core.ac.uk/download/pdf/234677092.pdf

Levi, M., Doig, A., Gundur, R., Wall, D., & Williams, M. (2017). Cyberfraud and the implications for effective risk-based responses: themes from UK research. *Crime, Law and Social Change*, *67*, 77-96. https://doi.org/10.1007/s10611-016-9648-0

Lusthaus, J. (2024). Reconsidering crime and technology: what is this thing we call cybercrime? *Annual Review of Law and Social Science*, *20*(1), 369-385. https://doi.org/10.1146/annurev-lawsocsci-041822-044042

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*(1), 47-67. https://doi.org/10.1080/15536548.2013.10845672

Morland, S. (2024). *Latin America and Caribbean launch regional alliance against organized crime*. Retrieved April 1, 2025, from https://www.reuters.com/world/americas/latin-america-caribbean-launch-regional-alliance-against-organized-crime-2024-12-12/

Mphatheni, M. R., & Maluleke, W. (2022). Cybersecurity as a response to combating cybercrime: Demystifying the prevailing threats and offering recommendations to the African regions. *International journal of research in business and social science*, *11*(4), 384-396. https://doi.org/10.20525/ijrbs.v11i4.1714

Munoriyarwa, A., & Mare, A. (2023). *Digital Surveillance in Southern Africa*. Springer International Publishing AG.

Muraina, I. O., Agoi, M. A., Adedokun, A. A., & Oyeniran, B. A. (2022). Social engineering pressures in Nigeria institutions: Why students are the main targets? *Al-hikmah Journal of Education*, 9(2), 313-325.

Mwangi, T., Asava, T., & Akerele, I. (2022). Cybersecurity threats in africa. In *The Palgrave handbook of sustainable peace and security in Africa* (pp. 159-180). Cham: Springer International Publishing.

NetMission.Asia. (2024). *Cybersecurity challenges in South Asia: India's largest data breaches and cyberattack on Pakistan's National Institutional Facilitation Technologies (NIFT)*. Retrieved April 1, 2025, from https://netmission.asia/2024/04/08/netmission-case-study-series-2024-cybersecurity-challenges-in-south-asia-indias-largest-data-breaches-and-cyberattack-on-pakistans-national-institutional-facilitation-technologie

Nzeakor, O. F., Nwokeoma, B. N., Hassan, I., Ajah, B. O., & Okpa, J. T. (2022). Emerging trends in cybercrime awareness in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*, *5*(3), 41-67.

Oduro-Frimpong, J. (2014). Sakawa rituals and cyberfraud in Ghanaian popular video movies. *African Studies Review*, *57*(2), 131-147. https://doi.org/10.1017/asr.2014.51

OECD. (2024). *New perspectives on measuring cybersecurity*. https://one.oecd.org/document/DSTI/CDEP/MADE(2023)14/FINAL/en/pdf

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and Motivations for Cyber Fraud Involvement among Female Undergraduates of Selected Universities in South-West Nigeria. *International Journal of Cyber Criminology*, *13*(2), 309-325. https://doi.org/10.5281/zenodo.3702333

Ogunyemi, A. A. (2024). Cyber Risks and the Nigerian Business Sector: A Critical Analysis of the Emerging Cyber Insurance Market in Nigeria. *ACU Journal of Social Sciences*, *3*(1), 1-21. https://ajss.acu.edu.ng/index.php/ajss/article/download/145/87

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology*, *6*(2), 1001. https://www.cybercrimejournal.com/pdf/Ojedokun&Eraye2012julyijcc.pdf

Ojugo, A. A., & Eboka, A. O. (2021). Empirical evidence of socially-engineered attack menace among undergraduate smartphone users in selected Universities in Nigeria. *International Journal*, *10*(3), 34-54. https://doi.org/10.11591/ijeecs.v28.i3.pp1756-1765

Okeke, N., & Onyekachukwu, I. O. (2024). Cybercrime and digital fraud among university students in Lagos, Nigeria: Socio-Economic Drivers and Prevention Approaches. *Journal of Research in Social Science and Humanities*, *3*(9), 13-21. https://doi.org/10.56397/jrssh.2024.09.02

Olayemi, O. J. (2014). A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, *6*(3), 116. https://academicjournals.org/article/article1392996162_Olayemi.pdf

Olomu, S. (2023, November, 23). Nigeria tightens laws to tackle yearly cyber-crime losses of $500m. *iTWeb Africa*. https://itweb.africa/content/mYZRXM9gxVNvOgA8

Onuora, A. C., Uche, D. C., Ogbunude, F. O., & Uwazuruike, F. O. (2017). The challenges of cybercrime in Nigeria: an overview. *AIPFU Journal of School of Sciences*, *1*(2), 6-11.

Onyema, E. M., Edeh, C. D., Gregory, U. S., Edmond, V. U., Charles, A. C., & Richard-Nnabu, N. E. (2021). Cybersecurity awareness among undergraduate students in Enugu Nigeria. *International Journal of Information Security, Privacy and Digital Forensics*, *5*(1), 34-42.

Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of Nigeria: a qualitative analysis. *International Journal of Cyber Criminology*, *9*(1), 120-143. https://doi.org/10.5281/zenodo.22390

Otozi, U. J., Ephraim, B., Yinka, A. I., & Hyginus, M. C. (2024). Cybercrime and its negative effects in developing countries. *Journal of Mobile Computing and Application*, *11*(4), 10-16. https://doi.org/10.9790/0050-11041016

Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., ... & Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. In *Proceedings companion of the 23rd annual ACM conference on innovation and technology in computer science education* (pp. 36-54).

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication*, *28*, 1-21. https://doi.org/10.23962/10539/32213

Pryimenko, L. (2024). *12 Cybersecurity Best Practices & Measures to Prevent Cyber Attacks*. Syteca. Retrieved March 26, 2025, from https://www.syteca.com/en/blog/best-cyber-security-practices

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

Rufai, A., Modi, S., & Wadata, B. (2021). A survey of cyber-security practices in Nigeria. *International Research Journal of Advanced Engineering and Science*, 222-226. http://irjaes.com/wp-content/uploads/2020/10/IRJAES-V5N3P350Y20.pdf

Srivastava, A. K., Singh, A. V., & Som, S. (2024). Critical Analysis of Cybersecurity Awareness Programs in School Education. *Library of Progress-Library Science, Information Technology & Computer*, *44*(3), 18282-182303. https://doi.org/10.48165/bapas.2024.44.2.

Świątkowska, J. (2020). Tackling cybercrime to unleash developing countries' digital potential. *Pathways for Prosperity Commission Background Paper Series*, *33*, 2020-01. https://pathwayscommission.bsg.ox.ac.uk/sites/default/files/2020-01/tackling_cybercrime_to_unleash_developing_countries_digital_potential.pdf

Tade, O., & Aliyu, I. (2011). Social organization of Internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology*, *5*(2), 860-875. https://www.cybercrimejournal.com/pdf/tadealiyui2011julyijcc.pdf

Tambo, E., & Adama, K. (2017). Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa. *International Journal of Cyber-Security and Digital Forensics*, *6*(3), 126-138. https://doi.org/10.17781/P002278

Tzani, C., Ioannou, M., Fletcher, R., & Williams, T. J. V. (2024). Psychological factors leading to sextortion: The role of personality, emotional factors and sexual needs in victimisation. *Computers in Human Behavior*, *159*, 108323. https://doi.org/10.1016/j.chb.2024.108323

Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387. https://doi.org/10.1016/j.cose.2021.102387

Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.

World Bank. (2025). *Enhancing cyber resilience in developing countries: Case studies from Bhutan and Bangladesh*. Retrieved April 1, 2025, from https://www.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *International Journal of Electrical and Computer Engineering*, *13*(2), 1943. http://doi.org/10.11591/ijece.v13i2.pp1943-1953