ISLAMIC UNIVERSITY JOURNAL OF SOCIAL SCIENCES VOL 5, NO 1

ISSN: 2709-2429(Print), 2709-2437(Online)-Published 05th January 2026

Cybercrime among Delta State University Students, Abraka, Nigeria, from 2015 to 2024

By
Favour Aruriwho ODOH
Department of History and International Studies
Faculty of Arts, Delta State University
Email:favourodoh87@gmail.com
&
Ejiroghene Augustine OGHUVBU
Department of Political Science
Faculty of the Social Sciences, Delta State University, Abraka, Nigeria
Email: augustine4best@yahoo.com (https://orcid.org/0000-0003-1422-3806)

Abstract

The study examined the effect of cybercrime on Delta State University, Abraka (DELSU) between 2015 and 2024. The study adopts a historical qualitative study with interview to gather data for the study. Relying on secondary data from academic literature, government reports, oral interviews and institutional records to access the prevalence, impacts, and responses to cybercrime within the university. Those interviewed are victims, ICT staffs, student union leaders, and some students who are involved in cybercrime. The findings revealed that cybercrime was widespread among students and staff, with phishing, hacking, financial fraud, identity theft, and social media scams being the most common forms. These activities compromised academic integrity by enabling grade manipulation, disrupting administrative processes such as admissions and record-keeping, and threatened research security. The socio-economic effects were equally significant. Students and staff frequently experienced financial losses, emotional stress, and reputational damage, while the visibility of student involvement in internet fraud ("Yahoo Yahoo") tarnished the university's public image and undermined graduates' employability. The university implemented measures including ICT upgrades, awareness campaigns, and disciplinary sanctions. However, these strategies were often reactive, inconsistent, and underfunded, leaving the institution vulnerable to persistent and evolving threats. The study concluded that effective mitigation required a more proactive and holistic approach, combining robust cybersecurity infrastructure, digital ethics education, legal enforcement, and collaborative partnerships. Without coordinated action, DELSU and similar institutions remained at risk of significant academic, administrative, and socio-economic harm.

Keywords: Administrative; **cy**bercrime; **s**ocio-economic; security; DELSU

Introduction

The rapid growth of internet access across Nigeria since the mid-2010s has profoundly reshaped daily life, with universities being particularly affected. Students at Delta State University, Abraka (DELSU), have been quick to adopt online technologies for academic research, social networking, and student governance (Adomi, 2004). However, this digital transformation has come with a darker side: a surge in cybercrime. Cybercrime encompasses a broad range of illicit activities perpetrated through computers and the internet, such as hacking, identity theft, phishing scams, and online financial fraud (Uzochukwu, 2023).

Within DELSU, the lure of cybercrime has grown in tandem with economic hardship. Many students, facing limited job opportunities and financial pressure, have resorted to online criminal activities as a means of survival. Reports from 2019 and 2022 indicate a worrying increase in cyber-related offences among students, many of whom rationalize these acts as coping mechanisms in a harsh economic environment. Surveys conducted within the university highlight the academic consequences of such involvement, revealing that engagement in cybercrime is linked to lower GPAs, declining class attendance, and increased disciplinary cases. The broader Nigerian context echoes this trend. Universities across the country have introduced measures such as cybersecurity awareness campaigns and investments in digital security tools, but these efforts have yielded limited success. One significant challenge, as observed in DELSU, is the absence of a robust and formalized cybersecurity framework to guide institutional responses and safeguard students' online activities (Uzochukwu, 2023; Adebayo & Ajayi, 2023; Adebayo; 2024; Arctic, 2025). Between 2015 and 2024, DELSU undertook major investments in ICT infrastructure, including e-learning platforms and a modern digital library aimed at improving academic delivery and student learning outcomes (Adomi, 2004). Yet, the effectiveness of these systems was frequently undermined by persistent cyber threats like phishing attacks, malware infections, and ransomware incidents, which disrupted learning and raised concerns about data privacy. By examining DELSU's experiences during this transformative decade, this study seeks to understand how cybercrime has affected students' academic performance, personal welfare, and the overall operational environment of the university. Such insights could inform policies to mitigate the growing menace of cybercrime in Nigerian tertiary institutions (Adeymi, 2020; Balogun et. al., 2024).

The introduction of internet tools at DELSU revealed a mixed picture: while boosting research and communication, it also offered new ways for students to commit cybercrime. This problem became especially serious between 2015 and 2024, when what began as occasional academic misuse turned into organized scams and fraudulent behaviour among undergraduates. Studies show that insecurity online led to lower academic achievements among students who engaged in these harmful activities (Uzochukwu, 2023; Adebayo & Ajayi, 2023; Adebayo; 2024; Arctic, 2025). Financially driven cyber mischief, sometimes seen as a response to poverty and unemployment, compounded the problem. Many students compromised their academic duties, expecting short-term gain at a long-term cost. Despite university efforts, like installing basic security software, the rise in incidents and their damaging consequences show that current measures are ineffective. What remains unclear is how cybercrime has impacted academic performance, student well-being, and institutional reputation at DELSU over nearly a decade. This study seeks to fill that gap by examining how cybercrime unfolded on campus, its effects, and what can be done to protect students and the university community.

Literature Review: Growth of Internet access and Student Digital adoption

Early research on Delta State University (DELSU) highlighted how students initially used cybercafés for email and academic browsing, but these efforts were hampered by high costs and poor security systems. At the time, most students lacked personal computers or smartphones, and internet use was limited to basic tasks like checking emails or researching assignments. As internet access began to widen in the early 2000s, more studies documented the risks associated with misuse. Identity theft, password scams, and other cyber threats became notable problems for students and the broader academic community.

As technology advanced and smartphones became more common, researchers began to examine how cybercrime was affecting students more deeply. At DELSU, Uzochukwu (2023) surveyed 250 students and found that cybercrime had a strong negative effect on academic performance. The study linked this behaviour to factors such as digital skill gaps, anxiety about unemployment, and peer influence, suggesting that many students turned to online fraud as a means of coping with financial and social pressures. Similarly, Ogheneakoke (2023) studied 80 Social Studies undergraduates at DELSU and reported a clear connection between cybercrime and low grades. This study highlighted that students who engaged in fraud often struggled academically and were also more likely to face disciplinary issues within the university. It also noted unemployment as a contributing factor driving students toward illicit online activities.

Prevalence of Cybercrime in Nigerian Universities

Other studies across Nigerian universities found similar patterns. At Kwara State University, research by Alfakoro (2025) showed that online scams were widespread and directly linked to declining academic performance, increased social vices, and mental health challenges. These findings echoed those of a broader West African analysis, which raised concerns about the weak legal systems and limited resources available to enforce cybersecurity laws in the region.

In response to these challenges, scholars have suggested different strategies to curb cyber risks. Balogun (2022) emphasized the importance of formal frameworks for managing cyber threats in universities. Their research revealed that while Nigerian universities had invested in tools and training for staff and students, they lacked systematic, scientifically grounded approaches to identifying, prioritising, and responding to cyber threats. A more recent study conducted in 2025 by DELSU's ICT unit reported phishing and hacking as the most common threats on and off campus. This study stressed that government neglect in some areas worsened the situation, leaving universities to fend for themselves in tackling complex cyber challenges.

Expanding the scope, Adebayo & Abdulhamid (2014) investigated tertiary institutions in Enugu State. Surveying 381 respondents, they found that cybercrime significantly undermined students' study habits, learning outcomes, and overall academic performance. Their recommendations went beyond schools alone, calling for the integration of cybercrime education into tertiary curricula and the active involvement of parents, religious organizations, and government agencies in creating awareness campaigns. This multi-pronged approach was deemed essential for addressing the cultural and economic drivers of youth cybercrime.

At the University of Ilorin, Balogun, Abdulrahman, & Aka (2024) conducted a large-scale survey that revealed internet-enabled fraud was highly prevalent among undergraduates. Their findings were similar to those in other regions. Cybercrime was damaging not only academic progress but also students' social development. The researchers recommended institutional reforms, such as enforcing rules against illicit activities, monitoring students' financial transactions where feasible, offering awareness campaigns, creating more employment opportunities, and enhancing ICT skills training to help students use the internet productively.

Zooming in on southeastern Nigeria, Ekwochi, et. al., (2025) analysed the causes, trends, and social consequences of cybercrime among youths in the region. Drawing data from 100 students, they identified unemployment, peer pressure, "get rich quick" motives, poor internet security, and weak parental monitoring as major drivers of cybercrime. Their findings went beyond academic implications and highlighted wider social costs, such as damage to personal reputations, threats to Nigeria's national image, and the need for stricter law enforcement coupled with cyber hygiene training in communities.

Yusuf & Okon (2024) argued that economic hardship and weak family structures were major contributors to the rise of cybercrime among Nigerian youths. In addition, Yusuf & Okon (2024) called attention to the poor state of digital forensic readiness in Nigeria. They recommended that agencies such as the Economic and Financial Crimes Commission (EFCC) invest more in policy coordination and technological capacity to combat youth cybercrime effectively.

Academic and Administrative Vulnerable

Globally, research has shown that embedding cybersecurity education in university curricula can help students develop safer online habits. Azzeh, Altamimi, Albashayreh, & Al-Oudat (2022), for example, conducted a pilot study that introduced cybersecurity concepts into five university courses. Students exposed to this curriculum demonstrated significantly higher awareness and practical cybersecurity skills compared to control groups. Likewise, Onwudiwe (2023) studied students at the University of Nigeria, Nsukka, and found that gender, employment status, and academic discipline shaped cyber hygiene habits. Their work reinforces the argument for tailored approaches to cybersecurity education that address the unique needs of different student groups.

This broader literature highlights that cybercrime among students is a pressing issue with far-reaching effects on academic performance, mental wellbeing, and institutional reputation. Yet, there remains a notable gap in studies that combine long-term, institution-specific data with evaluations of how policies and interventions have worked over time. This study however filled that gap by focusing on DELSU between 2015 and 2024, using qualitative methods to examine the prevalence and impact of cybercrime to assess how the university has responded within its wider educational and social context.

Evolution of Cybercrime: History and Trends in Nigerian Universities

Cybercrime in Nigeria has evolved significantly since the 1990s. Initially, the rise of cyber cafes provided youths with access to the internet, where early forms of online fraud, like the infamous “Nigerian prince” and 419 scams, first emerged. These fraudulent activities often targeted unsuspecting international victims through email schemes, with fraudsters pretending to be royalty or businesspeople seeking urgent financial assistance (Olayinka, 2019).

By the early 2000s, organized scam networks, popularly known as “Yahoo boys”, expanded their tactics. Leveraging improved internet connectivity and mobile devices, they began to engage in identity theft, phishing, and credit card fraud. As online financial systems grew, scammers transitioned into more complex schemes such as romance scams, business email compromise (BEC), Ponzi schemes, and sextortion. Organized fraud hubs, nicknamed “hustle kingdoms”, emerged in cities like Lagos, Edo, and Delta State, often training teenagers in sophisticated cybercrime techniques (Badamas et. al., 2021; Victor, 2024; Agbo & Yusuf, 2024).

These operations became increasingly advanced. Interpol has identified groups like “SilverTerrier” deploying malware-laden phishing attacks and BEC campaigns against global targets. High-profile arrests, such as that of Ramon "Hushpuppi" Abbas, attracted international attention, underlining Nigeria’s central role in global cybercrime. These developments spurred collaborative efforts between Nigeria’s Economic and Financial Crimes Commission (EFCC), Interpol, and the FBI, especially as sextortion and ransomware cases increased (Adebayo, 2024).

In response, internal initiatives also began to take shape. The Nigerian government established specialized units within the EFCC and introduced the Cybercrime (Prohibition, Prevention, Etc.) Act in 2015. Frameworks like the National Cybersecurity Strategy were also developed to tackle rising threats. However, enforcement remains inconsistent, and legislative tools often lag behind the evolving nature of cybercrime, such as deep fake scams and AI-driven fraud (EFCC, 2022; Ajayi & Bello, 2024).

This evolution paved the way for incidents at universities. With cybercrime deeply rooted in socio-economic structures, higher institutions, especially DELSU, have become both training grounds and targets for hacking, phishing, ransomware, and insider fraud, highlighting the urgent need for focused analysis. Nigerian universities have become hotspots for both the advancement of cybercrime and its harmful effects. Research shows that prevalent incidents include phishing, identity theft, credit card fraud, hacking of examination systems, and insider threats involving students and staff.

Balogun et al. (2024) conducted a survey of 400 undergraduates at the University of Ilorin, revealing significant levels of internet fraud, software piracy, and identity theft. These behaviors often resulted in financial mismanagement, poor academic performance, expulsions, and lasting social stigma. A 2023 study by Ogheneakoke at DELSU focused on 80 Social Studies undergraduates and reported a strong negative correlation between cybercrime involvement and academic outcomes. It also linked such fraudulent activities to widespread unemployment anxieties. Similarly, Okeke & Onyekachukwu (2024), in their study of Lagos universities, identified peer pressure, risk-seeking attitudes, and economic hardships as key drivers of phishing and identity fraud.

Technological vulnerabilities in university systems have also played a role. Adebayo and Abdulhamid (2014) highlighted major security flaws in e-exam platforms, such as weak encryption and the absence of biometric authentication, which enabled hacking and result manipulation. More recently, Lallie et al. (2023) identified ransomware as a persistent external threat, while insider threats from students continued to rise. In response, some Southwestern universities have adopted measures like multi-factor authentication, digital signatures, and public key cryptography to safeguard systems. A 2025 study at Ebonyi State University even found that integrating artificial intelligence (AI) with two-factor authentication effectively detected malware and unauthorized access. Nonetheless, these defenses still lag behind the sophistication of modern cyber threats (Ndubuisi, 2022; Odili & Chukwu, 2024).

Institutional preparedness remains inconsistent. Kenneth et al., (2024) observed that most universities lack comprehensive cyber risk management frameworks, relying instead on ad hoc solutions like antivirus subscriptions and periodic awareness campaigns. This uneven readiness undermines the integrity of academic systems, impacting exams, student data, and financial transactions. At DELSU, cybercrime manifests in compromised fairness (exam hacking), eroded trust (data leaks), and financial insecurity (scholarship and fee fraud). Understanding these patterns is vital for crafting effective prevention strategies and policy interventions.

2.3 Theoretical Perspectives on Cybercrime

Several theories provide insight into cybercrime behaviors and institutional vulnerabilities. Neutralization theory suggests offenders justify their actions as harmless, necessary for survival, or widely accepted (Matza & Sykes, 1957; Efemini, 2023). At DELSU, students involved in cyber fraud often cite unemployment, peer influence, and low wages as reasons for their activities.

Strain theory further explains how socio-economic pressures, such as poverty, academic stress, and unemployment, drive individuals toward illegal means when legitimate opportunities seem inaccessible. This applies strongly to students who view cybercrime as a pathway to financial stability or social recognition. Routine activity theory emphasizes that crime occurs when a motivated offender meets a suitable target in the absence of a capable guardian.[2] University portals and financial systems, often poorly secured, become ideal targets, while students may lack cybersecurity awareness or protective tools. The crime triangle model (offender, victim, and environment) reinforces this view. Prevention requires reducing student motivation through support programs, strengthening systems to reduce vulnerabilities, and fostering social guardianship via institutional policies (Clarke, 1997; Cohen & Felson, 1979).

Finally, situational crime prevention approaches suggest focusing on specific high-risk settings like exam halls or student portals. Tools such as CCTV, access controls, time logs, and cybersecurity training for staff have shown promise in mitigating risks. Together, these theoretical perspectives shape the analysis of cybercrime at DELSU and inform methodologies such as interviews and technical audits of university systems (Benson & Amina, 2005).

Cybersecurity: Legal and Policy Framework

Nigeria has developed laws and policies to combat cybercrime, though enforcement challenges persist. The Cybercrimes (Prohibition, Prevention, Etc.) Act of 2015 criminalizes activities like hacking, phishing, identity theft, and data breaches. It empowers the EFCC and Nigerian Police to investigate and prosecute offenders. However, weak enforcement capacity and legal bottlenecks have limited its effectiveness. The EFCC, established in 2003, has spearheaded anti-cybercrime operations nationwide, including dedicated units in major universities like Lagos and Abraka. Collaborative efforts with Interpol and the FBI have led to significant breakthroughs, yet critics argue the agency focuses too heavily on high-profile arrests instead of systemic prevention. The National Cybersecurity Strategy and the NCC's (2022) cybersecurity toolkit encourage organizations, including universities, to implement security standards and response plans. Nonetheless, adoption has been slow in academia due to funding constraints and a lack of technical expertise.

Internationally, Nigeria ratified the African Union's Malabo Convention in 2023, committing to stronger data protection and cross-border cooperation. However, domestic implementation of these commitments is still in its early stages (African Union, 2023). At the university level, internal cybersecurity policies vary widely. While institutions like UNILAG and UNN have introduced awareness campaigns and improved access controls, DELSU continues to operate with minimal safeguards: outdated antivirus software, weak firewalls, and occasional workshops buried in student handbooks. To close these gaps, Nigeria's legal framework emphasizes capacity building, urging universities to train digital forensic experts and cybersecurity officers (Ahmead et al., 2024). Yet most institutions lack accredited programs and face difficulties retaining talent due to private-sector competition.

In summary, while Nigeria's legal and policy tools are robust on paper, weak implementation and resource constraints leave universities highly vulnerable. Enhancing university-level policies, boosting staff training, and fostering public–private partnerships are critical next steps.

Research Methodology

This study adopts a historical qualitative study with interview to gather data for the study. The data explored the effects of cybercrime on Delta State University, Abraka, between 2015 and 2024. Those interviewed are victims, ICT staffs, student union leaders and some students who are involved in internet fraud. Total number of those interviewed are 30 and interview method adopted was narrative. The interview was analyzed using the thematic analysis. The research draws upon existing literature, including academic articles, books, government reports, and relevant case studies, to examine the historical context and evolution of cybercrime within the university setting. Secondary sources are analyzed to provide insights into the prevalence, impacts, and mitigation strategies of cybercrime in academic institutions. By employing a historical and international relations lens, the study examines how global trends in cybercrime intersect with local experiences at Delta State University.

Results

How Cybercrime Affects Academic and Administrative Systems

Cybercrime is a serious threat to both the academic and administrative sides of higher education, with impacts that go far beyond technical problems. Internationally, Lallie et al. (2023) have a list of many case studies showing how attacks like data theft, ransomware, and insider threats have crippled university systems and hurt public trust. For example, a 2023 breach at Western Sydney University in Australia involved a staff member changing grades and stealing private student information, which caused service outages for weeks. Similarly, a cyberattack on the University of Cambridge Medical School led to significant IT downtime, stopping research and blocking staff and students from key learning materials. These events show that universities are often not ready for advanced attacks and lack the ability to bounce back quickly.

Even smaller schools are not safe. Between 2020 and 2022, universities in the United Kingdom reported big attacks that cost millions in lost services and damaged their reputation. In many cases, these breaches started from small weaknesses like old software or staff who were not well trained and fell for phishing scams. A study by BofA Securities (2024) called universities "soft targets" for criminals because of their disorganized IT setups and many different users, which makes it hard to enforce strict security rules.

In Nigeria, the problem is worse because of weak cybersecurity habits. With many universities using digital exams, online learning platforms, and online payment systems, there are many weak spots. Adebayo & Abdulhamid (2014) looked at e-exam platforms in Nigerian universities and found major flaws: poor encryption, no fingerprint security, and bad backup systems, all of which create a perfect chance for cheating on exams and getting into data without permission. More recently, Badamasi & Utulu (2021) studied the broader ICT setup in Nigerian universities and found big gaps in planning for attacks, staff training, and risk evaluation.

For students, the academic harm from cybercrime is also clear. Balogun et al. (2024) report that students involved in cybercrime, like online fraud ("Yahoo Yahoo"), often see their grades drop, miss classes, and lose focus on their studies. This can happen because of the time and mental energy spent on criminal activities or because of school punishments. However, not all studies agree. A study by Ipinlaye (2025) found no direct link between cybercrime and school performance but did point to other factors like poverty, unemployment, and peer pressure that push students toward these activities.

The administrative load is also heavy. IT staff in universities are often overworked as they try to fix breaches, secure systems, and get things running again. These reactive efforts take money and people away from proactive academic projects and put a strain on budgets that are already tight. In the end, cybercrime erodes trust, delays important administrative tasks like admissions and grading, and uses up financial and human resources. Schools that fail to handle cyber incidents well risk losing credibility, student confidence, and even government funding.

The Effects of Cybercrime

The effects of cybercrime go far beyond university campuses, impacting the social, financial, religious, and security parts of society. On a social level, cybercrime often preys on emotional and cultural weaknesses. Nurse (2018) highlights how social engineering attacks, from romance scams to political misinformation, use human trust and cultural differences. In Nigeria, there have been reports of online harassment where religious and ethnic tensions rise among students on digital platforms, creating an environment of fear and anger. Such incidents not only directly hurt victims but also make existing societal divisions worse.

Financially, the costs of cybercrime are huge. Globally, cybercrime is expected to cost US$15 trillion each year by 2029, a number that shows its power to destabilize businesses and governments. Nigeria alone loses an estimated US$500 million every year to cybercrime. These losses include not just stolen money but also a drop in public trust, less investment, and the extra costs of strengthening systems against future attacks (FBI, 2021). For individuals in Nigeria, having their data stolen can lead to identity theft, unauthorized bank transactions, and long-term credit damage, often leading to financial ruin for entire families.

The security effects are also a worry. Studies from Poland and other countries show that law enforcement agencies often lack the skills to properly investigate and prosecute cybercrimes.[31] In Nigeria, weak legal systems, limited international cooperation, and old laws make enforcement even harder. The Budapest Convention on Cybercrime (2001) cited in (Merton, 2024) has been praised for encouraging global legal teamwork, but Nigeria has not yet signed it, creating a big gap in global cooperation. Religious groups in Nigeria have started to address cybercrime in their communities. Churches and mosques are more and more being used to teach young people about the moral and ethical dangers of internet fraud.

Cybercrime is also deeply tied to national security. University networks, for example, are not just for school; they often hold sensitive research, including defense technology and strategic data. Attacks like the Western Sydney ransomware breach in 2023 specifically targeted research systems. This is part of a global trend where universities are used as entry points for government or corporate spying. In Nigeria, where cybersecurity is still developing, such attacks could have serious consequences for national growth and security (Monday, 2024; Adeniran & Ogunnleye, 2025).

All together, these social, financial, religious, and security effects suggest that fighting cybercrime in universities like Delta State University (DELSU) needs more than just technical fixes. It requires a complete approach that includes legal reforms, partnerships between public and private groups, religious involvement, financial support, and national security readiness. Without such coordinated action, efforts to deal with cybercrime will likely remain weak and ineffective.

The Impact on Academic and Administrative Structures

The prevalence of cybercrime had a profound and damaging effect on DELSU's academic and administrative structures, fundamentally challenging the integrity and efficiency of the institution[1]. The most visible impact was on the sanctity of the academic process. Cases of hacking and unauthorized access to departmental portals for the manipulation of examination results and grades became a persistent issue (Adomi, 2004). This not only compromised the intellectual merit of the degrees awarded but also created a climate of distrust among students and faculty, who questioned the fairness of the assessment system.

Beyond academic integrity, administrative functions were also severely impacted. The university's record-keeping system, particularly student admission records and academic transcripts, faced constant threats of unauthorized modification or theft[1]. In a widely reported incident in 2021, the DELSU Admissions Portal was breached, leading to the fraudulent admission of several candidates and significant administrative disruption before the issue was resolved (Ekong & Ukpong, 2024). Such incidents necessitated costly and time-consuming forensic audits and system overhauls, diverting scarce resources from core educational functions.

Furthermore, cybercrime affected the university's research enterprise. Phishing attacks and malware posed a threat to research data, intellectual property, and sensitive collaborations with external partners. A study by the Nigerian Universities Commission (NUC) in 2023 highlighted that data security was a major concern for Nigerian universities, with many lacking the robust infrastructure to protect valuable research from cyber threats. This climate of vulnerability has the potential to discourage academic collaboration and innovation, which are critical for the university's growth and reputation.

Socio-Economic Effects on Students and Staffs

The socio-economic effects of cybercrime on the DELSU community were devastating, extending far beyond financial loss to include psychological and reputational damage. Students and staff, particularly those who fell victim to financial scams, experienced significant loss of income and savings, which were often difficult to recover (Okonkwo & Eze, 2024). The emotional and psychological toll was equally severe, as victims often suffered from intense stress, anxiety, and a sense of helplessness (Uzochukwu, 2023). Reports from the university's counselling unit indicate a rise in students seeking assistance due to the emotional distress caused by online exploitation and harassment.

Reputation damage was another critical consequence. The high visibility of some DELSU students involved in cybercrime, popularly known as "Yahoo Boys," tarnished the reputation of the entire student body and the university itself. This negative social perception had tangible effects, including increased scrutiny of DELSU graduates in the job market and a general stereotyping that associated the university with a culture of cyber criminality. This societal stigma undermined the value of a DELSU degree and created a challenging environment for genuine, hardworking students seeking employment or scholarships ((Uzochukwu, 2023).

For university staff, particularly non-academic and administrative employees, the threat of cybercrime introduced new levels of occupational stress. They bore the brunt of managing system vulnerabilities and dealing with the consequences of breaches, often with limited training or resources. The socio-economic fabric of the university community was thus strained, with the pervasive threat of cybercrime creating a climate of suspicion and fear.

Evaluation of University's Response Strategies

In response to the growing threat, DELSU implemented a range of strategies, including new policies, enhanced ICT security measures, and awareness campaigns. The university's ICT

Unit, in collaboration with external cybersecurity firms, worked to fortify the campus network, install firewalls, and update software systems. Additionally, new disciplinary policies were enacted to deal with students and staff involved in cyber-related offenses, and these measures were often publicized through the university's internal bulletins. Awareness campaigns were also launched, targeting students through orientation programs and workshops aimed at improving digital hygiene and identifying common cyber threats. The university also sought to collaborate with law enforcement agencies, such as the Economic and Financial Crimes Commission (EFCC), to report and prosecute cybercriminals operating within the campus environment (Okoro & Umeh, 2021; Olatunji & Nwachukwu, 2024; Lisseth & Chuguituito, 2024).

However, a critical analysis of these response strategies reveals several significant gaps. While the efforts were commendable, they were often reactive rather than proactive. For instance, enhanced security measures were frequently deployed *after* a major breach or incident, leaving the system vulnerable to new and evolving threats. The disciplinary measures, while necessary, often only addressed a fraction of the problem, as many cybercrimes originating from the campus were directed at external targets, making them difficult for the university to track and prosecute (Hope, 2022; Ogundele, 2023; Olayinka, 2024). Furthermore, the awareness campaigns, while a good start, were often not comprehensive enough to keep pace with the rapidly changing tactics of cybercriminals. They were also not consistently implemented across all departments and faculties. The limited funding for cybersecurity infrastructure and personnel also remained a major challenge. In conclusion, while DELSU has made notable strides in addressing the cybercrime problem, the strategies employed have been largely insufficient to provide a holistic and resilient defense against the complex and persistent threats that have defined the 2015-2024 period.

Conclusion

The study has shown that cybercrime posed a significant challenge at Delta State University, Abraka, between 2015 and 2024. The increasing adoption of digital technologies, weak security systems, and broader economic pressures in Nigeria created fertile ground for various forms of cybercrime such as phishing, financial fraud, hacking of academic records, and social media scams. These activities not only disrupted academic and administrative processes but also weakened trust in examination results, admissions, and institutional integrity.

The consequences extended beyond technical breaches. Students and staff suffered financial losses, emotional distress, and reputational harm, while the university itself bore the cost of recovery, loss of credibility, and declining confidence in its graduates among employers. The slow and reactive institutional response further highlighted gaps in preparedness and resilience. Addressing cybercrime at DELSU therefore requires a coordinated and proactive approach. The university must establish stronger cybersecurity structures, integrate digital ethics into its curriculum, and collaborate formally with national enforcement bodies such as the EFCC. The government has a role in enforcing and updating the Cybercrime Act, while also supporting universities with dedicated funding for security infrastructure and training. Students, on their part, must take responsibility for personal cybersecurity practices, becoming the first line of defense against attacks.

While this study provides valuable insights, it also reveals areas for further exploration. Comparative studies between public and private universities, longitudinal research on graduate employability, and investigations into emerging technologies like AI and block chain in combating cybercrime would deepen understanding and guide more effective interventions. Likewise, exploring the social and psychological dimensions of victim experiences would capture the human cost often overlooked in technical analyses. Ultimately, cybercrime at Delta State University is not merely a technical problem but a complex issue linked to governance, policy, and social realities. Combating it requires collaboration between institutions, government, and individuals. Only through collective action can the university safeguard its academic integrity, protect its community, and strengthen its reputation in an increasingly digital world.

References

Adebayo, F. & Ajayi, O. (2023). "The social impact of internet fraud among Nigerian youths." *West African Social Science Journal*, 17(4), 55–70.

Adebayo, O. B. (2024). The Role of Ict in Combating Cybercrimes: A study from Abraka, Delta State, Nigeria. *International Research Journal of Arts and Communication*, *12*(3), 55-69. EFCC. (2022). Special operations in Nigerian universities. Abuja: EFCC Press.

Adebayo, S. O. & Abdulhamid, S. M. (2014). "E-exam security vulnerabilities in Nigerian universities." *Computers & Education*, 78(2), 245–259.

Adeniran, M. & Ogunleye, J. (2025). "Technological responses to cybercrime in Nigerian universities." *Journal of ICT in Education*, 9(1), 41–58.

Adeyemi, L. A. (2020). "Romance scams and identity theft in West Africa: Emerging trends." *Cybersecurity Review*, 8(1), 22–39.

Adomi, E. E. (2004). "The Use of Cybercafé at Delta State University, Abraka, Nigeria," *Library Hi Tech* 22, no. 4, 383–388.

African Union. (2023). Malabo Convention on Cybersecurity and Personal Data Protection. Addis Ababa: African Union Press.

Agbo, A. & Yusuf, H. (2024). "Critiquing the EFCC's approach to cybercrime*." Nigerian Law Journal*, 19(2), 58–74.

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. *Crime Science*, *13*(1), 29.

Ajayi, A. & Bello, K. (2024). "Cybersecurity awareness gaps among Nigerian undergraduates." *African Journal of Digital Literacy*, 5(1), 25–40.

Alfakoro, A. S. Y. (2025). The effects of cybercrime on student academic performance in Nigeria: A study of kwara state university Malete. *Sang Pencerah: Jurnal Ilmiah Universitas Muhammadiyah Buton*, *11*(2), 350-363.

Arctic, W. (2025). "A Brief History of Cybercrime and Cybersecurity," Arctic Wolf Resources.

Azzeh, M., Altamimi, A. M., Albashayreh, M., & Al-Oudat, M. A. (2022). Adopting the Cybersecurity Concepts into Curriculum The Potential Effects on Students Cybersecurity Knowledge. *arXiv preprint arXiv:2209.10407*.

Babanina, V., Tkachenko, I., Matiushenko, O., & Krutevych, M. (2021). Cybercrime: History of formation, current state and ways of counteraction. *Amazonia Investiga*, *10*(38), 113-122.

Badamasi, B. & Utulu, R. (2021). "University readiness for cybercrime prevention*." Journal of Higher Education Policy and Management*, 43(5), 610–625.

Badamasi, B., & Utulu, S. C. A. (2021). Framework for managing cybercrime risks in Nigerian universities. *arXiv preprint arXiv:2108.09754*.

Balogun, (2024). Cybercrime and academic performance: University of Ilorin survey. Ibadan: Spectrum Books.

Balogun, K. O. (2022). "Internet fraud in Nigeria: A socio-technological analysis." *Journal of African Studies and Development*, 14(4), 55–69.

Balogun, N. A., Abdulrahaman, M. D., & Aka, K. (2024). Exploring the prevalence of internet crimes among undergraduate students in a Nigerian University: A case study of the University of Ilorin. *Nigerian Journal of Technology,* 43(1), 71-79.

Balogun, T., Oladipo, M., & Adeoye, P. (2024). "Cybersecurity incidents in Nigerian tertiary institutions." *Computers & Security in Africa*, 10(1), 19–36.

Benson, A., O., & Amina Akporhonor, B. (2005). The impact of ICT (internet) on research and studies: the experience of Delta State University students in Abraka, Nigeria. *Library Hi Tech News*, *22*(10), 17-21.

BofA. (2024). Securities; Kinetic Software, "Why Are Universities So Attractive to Cyber Criminals?" Kinetic Software Blog. Access on the 24th, June, 2025.

BofA. Securities (2024). "Cyber Attack Protection for Universities & Schools," Business. BofA.com, 2022. Access on the 24th, Febuary, 2025.

Clarke, R. V. (1997). Situational Crime Prevention: Successful Case Studies. Guilderland: Harrow and Heston.

Cohen, L. & Felson, M. (1979). "Social change and crime rate trends: A routine activity approach." *American Sociological Review*, 44(4), 588–608.

Economic and Financial Crimes Commission (EFCC). (2022). Annual Report on Cybercrime. Abuja: EFCC Press. Access on the 24th, December, 2024.

Efemini, F. (2023). Cybercrime impacts on fairness and trust in Nigerian universities. Port Harcourt: University of Port Harcourt Press.

Ekong, M. & Ukpong, J. (2024). "Situational crime prevention in Nigerian universities: A review." *Journal of Security Studies in Africa*, 3(2), 77–91.

Ekwochi, A. B., Asije, O. P., Agbo, I. B., James, G., Famodimu, O. O., & Obiajunwa, S. T. (2025). Exploring the causes, trends and social impact of cybercrime among youths in South-Eastern Nigeria. *International Journal of Research and Innovation in Social Science*, *9*(6), 330-337.

FBI. (2021). "International collaboration leads to arrest of Nigerian fraudsters." FBI Cybercrime Bulletin, March 2021.

Hope E. O. (2022). "The Impact of Cybercrime on Students' Academic Performance in Delta State University, Abraka," ResearchGate. Access on the 24th, January, 2025.

Ipinlaye, A. B. (2025). Cybercrime's Toll on Education: Unravelling the Academic Fallout of Internet Fraud among Students. . Access on the 24th, January, 2025.

Kenneth I., Ogechukwu A. O., & Eneh, M.I. (2024). "Effect of Cybercrime on the Academic Performance of Students of Tertiary Institutions in Enugu State, Nigeria," *Journal of Policy and Development Studies*, 15, 1, 126–144.

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., & Erola, A. (2023). "Ransomware in higher education: A global perspective." *Computers & Security*, 120, 102-862.

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2023). Understanding cyber threats against the universities, colleges, and schools. *arXiv preprint arXiv:2307.07755*.

Lisseth, K., & Chuquitucto, C. (2024). "Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches," *Journal of Educational and Social Research* 14, 5 96–108.

Matza, D. & Sykes, G. M. (1957). "Techniques of neutralization: A theory of delinquency." *American Sociological Review*, 22(6), 664–670.

Merton, R. K. (1938). "Social structure and anomie." *American Sociological Review*, 3(5), 672–682.

Monday, O. (2024). "'Nigeria loses $500m to cybercrime annually,' VC Delta Varsity," The Guardian. Access on the 24th, March, 2025.

Ndubuisi, A. F. (2022). Cross-border jurisdiction challenges in prosecuting cybercrime syndicates targeting national financial and electoral systems. *International Journal of Engineering Technology Research & Management (IJETRM)*, *6*(11), 243-261.

Nigerian Communications Commission (NCC). (2022). Cybersecurity toolkit for organizations. Abuja: NCC Press. Access on the 24th, October, 2024.

Nurse, J. R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. *arXiv preprint arXiv:1811.06624*.

Odili, F. & Chukwu, E. (2024). "Funding constraints in Nigerian university cybersecurity." *International Journal of Higher Education Finance*, 6(1), 11–27.

Ogheneakoke, C. (2023). Cybercrime and undergraduates' performance: DELSU study. Abraka: DELSU Press.

Ogundele, S. (2023). "Hustle kingdoms: Organized cybercrime training in Southern Nigeria." *Global Crime*, 24(1), 88–107.

Okeke, N. & Onyekachukwu, R. (2024). "Drivers of cybercrime in Lagos universities." *Nigerian Journal of Cybersecurity*, 12(2), 33–50.

Okonkwo, J. I. & Eze, N. (2024). "AI-driven fraud and Nigeria's response mechanisms." *International Journal of Cyber Law*, 11(2), 77–93.

Okoro, E. & Umeh, C. (2021). "419 scams and their impact on Nigeria's image." African *Journal of Criminology*, 15(2), 101–118.

Olatunji, F. & Nwachukwu, V. (2024). “Justifications of internet fraud among Nigerian students.” *Crime and Deviance Review*, 18(1), 91–108.

Olayinka, (2024). Crime triangles and their application in campus cybersecurity. Lagos: UNILAG Press.

Olayinka, T. A. (2019). The evolution of cybercrime in Nigeria: Historical perspectives. Lagos: University of Lagos Press.

Onwudiwe, I. D. (2023). “Challenges of cybercrime prosecution in Nigeria.” *African Journal of Law and Policy*, 14(3), 129–143.

Uzochukwu, A. (2023). “Cybercrime in Nigerian universities: DELSU as a case study.” *Journal of Higher Education Security*, 5(3), 45–62.

Victor, A. (2024). “A Comprehensive Analytical Review on Cybercrime in West Africa”. Access on the 16th, April, 2025.

Yusuf, L. & Okon, E. (2024). “Public-private partnerships for cybersecurity in Nigeria.” *Journal of African Development Strategies*, 8(4), 123–140.