Journal of Education and Social Development, 2020, 4–2
December. 2020, pages 23-27
doi: 10.5281/zenodo.4362253
http://www.ibii-us.org/Journals/JESD/
ISBN 2572-9829 (Online), 2572-9810 (Print)

Impact of ICT-facilitated fraud on Sustainable Socio-economic Development in Nigeria

Faluyi, Bamidele Ibitayo[1,*], Fele, Taiwo[2] and Ayeni, Ayokunle Olusola[2]
[1,2]Department of Computer Science, Federal Polytechnic, Ado-Ekiti, Nigeria

*Email: dele.faluyi@yahoo.com

Received on 12/17/2020; revised on 12/19/2020; published on 12/19/20 20

Abstract

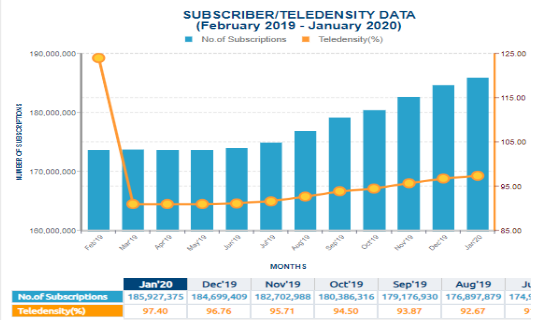
The advent of the new millennium gave way to the rapid growth of Information and Communication Technology (ICT) in Nigeria and till date all indication promises this growth will continue at a very fast pace. Unfortunately, the increase in social vices arising from the use of ICT and its infrastructure is alarming and adversely affecting the sustainable socio-economic development of Nigeria as it is a veritable tool in the hands fraudsters to easily commit crime. Government and individuals have continuously contended with these depravities as they pose a serious threat to the moral standard of societies in particular and the nation in general. This paper takes a critical look at different types of ICT-facilitated fraud often committed, examines how ICT has helped to perpetuate such fraudulent activities thereby increasing social vices and how it can be curbed to a reasonable extent using well tested knowledge. A research was conducted and questionnaires on ICT compliance and its use for online fraudulent activities analyzed using Statistical Package for Social Science (SPSS) with a reasonable conclusion drawn. We concluded by suggesting ways in which the power of ICT can be harnessed and used for more productive activities towards a sustainable socio-economic development.

Keywords: *Information and Communication Technology (ICT), Socio-Economic Development, Fraud, ICT-facilitated Fraud*

1.0 Introduction

The revolution of Information and Communication Technology has witnessed unprecedented growth over the last couple of decades and from all indications, this growth is bound to continue beyond human imagination. Fraudulent activities associated with this development has however been identified as one of the clogs in the wheels of socio-economic growth and a key factor influencing social vices. The society have to challenge these vices as they infringe on people's rights, privileges and goes against societal norms and values.

Nigeria, the largest economy in Africa also has the fastest growing telephone subscription on the continent with 185.74 million telephone users (seven per cent growth year-on-year) (O'GRADY, 2020) in January and 170 million data subscribers by the end of June 2020 (NCC, 2020).



	Jan'20	Dec'19	Nov'19	Oct'19	Sep'19	Aug'19	Ju
No.of Subscriptions	185,927,375	184,699,409	182,702,988	180,386,316	179,176,930	176,897,879	174,9
Teledensity(%)	97.40	96.76	95.71	94.50	93.87	92.67	9

Figure 1: Subscriber/Tele density Data January, 2020 (Akinpelu, 2020)

The penetration of mobile phones and data subscription into the Nigerian society has boosted ecommerce and encouraged businesses to move online rather than face to face, a new way of transacting business. ICT facilitated fraud is however a major source of concern for sustainable development of businesses in most developing countries like Nigeria.

2.0 Literature Review

There are several societal problems created by the adverse effects of ICT in the Nigeria. Unlike before, many people now choose online communication and transactions over physical interaction which makes us become more idiosyncratic and withdrawn. Under this review, we evaluated the socio-economic impact of fraud eased with the use of ICT on businesses with emphases on how it is carried out and ways of curbing it.

(Omonijo, 2012) noted that the rising cases of cheating in examinations, criminal tendencies and social vices etc. in Nigeria are caused by the early exposure of children to ICT. Many parents are too busy to train their children because of white collar jobs, economic engagements and businesses (Nwosu, 2009), leaving their wayward activities unchecked. The vacuum created by parents' absence are often filled by ICT. Time spent by women till the 20th century for home keeping and taking care of the children (Murdock,1949) is now used for money making ventures.

Without proper guidance from parents, children are negatively impacted by whatever they see on television, in videos and on the internet (Aggarwal, 2010). Others learn from domestic helps such as maids and nannies (Nwosu, 2009), this category of children tend to have early exposure to fraudulent activities.

Fraud is defined as the use of trick to get undue financial advantage over a person, while Cybercrime is any criminal act using computers and networks (UK, Police, 2020). Financial crimes committed online with the use of ICT related tools are thus referred to as online fraud, this is often categorized as a type of cybercrime and comes in different forms such as phishing/email scam, credit card reward point fraud, tax scams etc.

The use of internet in businesses have changed ways transactions are carried out and opened new, smart methods of defrauding people. Unsuspecting individuals using e-commerce platforms to perform financial transactions for payment and delivery of goods and services without physical interaction are exposed to fraud such as card testing fraud, friendly fraud, refund fraud, account take over fraud, interception fraud and triangulation fraud (Bolt, 2019).

A major challenge faced by users of the digital payment ecosystem is cybersecurity. The number of users preferring digital payments are on a daily increase, intensifying the chances of getting them exposed to cybersecurity risks such as online fraud, information theft, and malware or virus attacks. KMPG identified the dearth of awareness and poor digital payment ecosystem as the primary reasons for increase in these attacks (KMPG, 2018).

Cybercrime in general and ICT enabled frauds in particular is becoming very worrisome in developing countries like Nigeria and pose a major challenge to its overall development because many organizations and individuals are just adapting to the newness of online transactions due to the increase use and acceptance of internet technology.

Pandemics and other health challenges also contribute to the increased cases of cybercrime. For example, Interpol reports an alarming rate of cybercrime during the COVID 19 pandemic. Reports on the assessment of cybersecurity shows a substantial target shift from individuals and small businesses to major corporations, governments and critical infrastructure. Key features highlighted by the assessment includes Online Scams and Phishing, Disruptive Malware (Ransomware and DDoS), Data Harvesting Malware, Malicious Domains and Misinformation (INTERPOL, 2020).

3.0 COMMON ICT FACILITATED FRAUD

3.1 E-Mail Phishing Fraud

This is an evolving scam in which 96% of the attack arrives by email, 3% through malicious websites and 1% via mobile phones (Rosenthal, 2020). It accounts for 90% of cybersecurity breaches (Graphus, 2020) and stands out as one of the most serious threats for businesses with online facilities.

Phishing is an online attack that uses camouflaged email as a weapon. Its aim is to deceive email recipients into trusting that the message is from a trusted source, luring them to click a link or download an attachment in order to steal their information for financial fraud. Gaining recipient's trust occur in several ways including the attacker spoofing their email and setting up fake websites that looks like what the victim can trust etc. A phishing campaign generally attempts to get the victim in two ways: hand over sensitive information such as username and password to breach an account or download malware (*e.g. Ransomware*) to infect the victim's computer. (Fruhlinger, 2020). A typical example is sending out mail which looks like a message from a bank, once the link in the message is clicked, the victim is directed to a copycat website that looks like that of the bank to supply log in details which the attacker later uses to access the account.

In Nigeria, phishing emails are used extensively by fraudsters to defraud unsuspecting individuals in several ways, some examples are:

3.1.1 Advance Fee Fraud (AFF)

Also called the "The Nigerian Fraud" or "419" (named after the section in the Criminal Code in Nigeria that bans the practice) is the most attempted internet fraud among Nigeria's fraudsters and has been used for decades. With their phishing abilities, Nigeria's internet fraudsters have been dubbed 'role models' in internet scams (BBC, 2019), they dispatch millions of phishing, fraudulent mails per day to lure susceptible victims. Even with the bad grammar and unbelievable scenarios proposed by such mails, different people across the entire spectrum of human intelligence still fall for this cheap scam (Grimes, 2020).

AFF's growth in Nigeria followed a very interesting path. Before being integrated into telecommunication in the early 90's, letters sent through the Nigerian Postal Service (NIPOST) served as the primary medium of defrauding people. Committing AFF became much easier with the widespread use of computers, internet and email in the late 90's.

Victims of AFF are usually offered juicy proposals in form of quick money-making ventures, looking so real that they risk all their life savings and even borrow more in order to meet the request of the fraudsters, with great expectation of a high return on their 'investment' in the nearest future.

It often involves getting arbitrary messages via email, text or social media account about large sum of money stocked up in a bank somewhere in the world, especially war-torn country or a beautiful story of a massive inheritance that cannot be accessed because of 'the nature of the inheritance' or government restrictions and policies. The fraudsters offer a large percentage of the money as a reward if the victim agrees to help them transfer the money/inheritance out of the country. They trick people into parting away with their money, giving up their bank and credit card details. They may request for bank details to facilitate the transfer; these details are later used to steal money from their victim's account or request you to pay certain charges/taxes/fees they claim the money/inheritance has accrued over the years etc. once the first payment is made, they will still come back for more in view of the fact that you still want to be part of the deal. It will be too late before the victim realizes s/he has been duped and recouping the money 'invested' in the deal impossible because they will never be sent the money as promised. The method first found its way in Nigeria but it is now prominent in every part of the world.

3.1.2. Nigerian Prince Scam (NPS)

The NPS usually starts with an emotional, introductory email from a someone claiming to be from a royal family, member of the government or a businessman. Just like the Advanced Fee Fraud, they play on the recipient's greed by promising them a reward of a life time investment opportunity or large percentage of their inheritance if they can help move money out of their country. If an iota interest is shown, they request for bank account details appealing they want to transfer the money to the victim's account based on trust or even ask for an advanced payment to help cover the expenses for the money transfer. They either use the account details to wipe off the victim's account balance or run off with the advance payment. Over $702,000 was lost by Americans in 2018 to this type of fraud, an average of over $2,000 per victim (Leonhardt, 2019) .

3.1.3 Lottery Scam

This scam is classified as a type of advance-fee fraud. It also starts with malicious mail/text messages or call claiming the recipient just won a large amount of money or a grand prize in a lottery they may or may never have participated. They use the name of popular lottery companies so that if there isn't deep research, the message will look real. To claim the prize, the victim is required to pay an unending 'processing fee' and while urging them to respond quickly so as not to miss out, they are often told to keep the 'win' confidential for security purpose. These instructions are in a bid to discourage victims from contacting independent sources for verification before falling for the scam.

3.2 Bank Loan/Credit Card Scam

This type of fraud sounds too juicy and victims are usually businesses struggling with operational funds sourcing for 'rescue money'. Malicious messages assumed to have originated from bank saying a large sum of money has been approved as loans and sent to unsuspecting individuals. The fraudsters may request for the company/individual's account details with a minimum balance, usually a certain percentage of the supposed loan or other fees to process the fund. They may also demand for some form of collateral such as documents to landed properties before the victim can access the loan, such properties are quickly sold off without the consent of the owner while the scammers disappear into thin air.

Stolen credit cards are used to purchase and ship stolen goods. The goods are sold out at ridiculously cheap prices and the money wired back to the scammers. They either hack into a bank's database or connive with fraudulent bank officials to steal credit card information in order to defraud their customers.

Nigerians often receive unsolicited calls from scammers pretending to be customer care representatives of their banks. The calls look so real because they call out the correct customer details except the debit or credit card number. They then ask the customer to tell them their card number and Card Verification Value number so as to correct a mistake such as the date of birth on their account. These numbers are used to generate One Time Passwords (OTPs) to wipe off the victim's account.

3.3 Romance/Online Dating Scam

This entails feigning undying love towards a person with the true intention of committing fraud. They strike up love relationship with their victims, gaining their trust, confidence, love and goodwill in order to take undue financial advantage over the person. The scam often takes place via online dating or popular social media sites. The scammers create phony profiles on these sites to lure unsuspecting individuals finding love.

Nigerian men typically target elderly women. In 2019, seventeen men mostly Nigerians were arrested for defrauding vulnerable businesses and elderly women of funds to the tune of $6 million using romance scam after almost three years. In 2018 alone, over 21,000 people lost more than $143 million in this scheme (Karimi, 2019).

4.0 Curbing ICT Facilitated Fraud.

This is summarized in the following points:

1. Always have it at the back of your mind that ICT facilitated fraud indeed exists.
2. Investigate the identity of anyone you meet online, if possible have face to face interaction before any commitment.
3. Do not open suspicious emails, click on links or download attachments from suspicious sources.
4. Do not divulge personal information.
5. Check privacy and spam settings on email and social media accounts.
6. Don't be greedy, be weary of any message seeking financial aid and random payments.
7. When at crossroads, use search engines such as google to get answers on how to detect fraudulent activities in specific scenarios.

5.0 Research Methodology

Questionnaires were designed and distributed to get valid opinions on ICT tools and its use in ICT facilitated fraud using Nigeria as a case study. Statistical Package for Social Science (SPSS) was used for analysis. The results are shown using bar chart.

Figure 2 shows the age range of people that are ICT compliant.

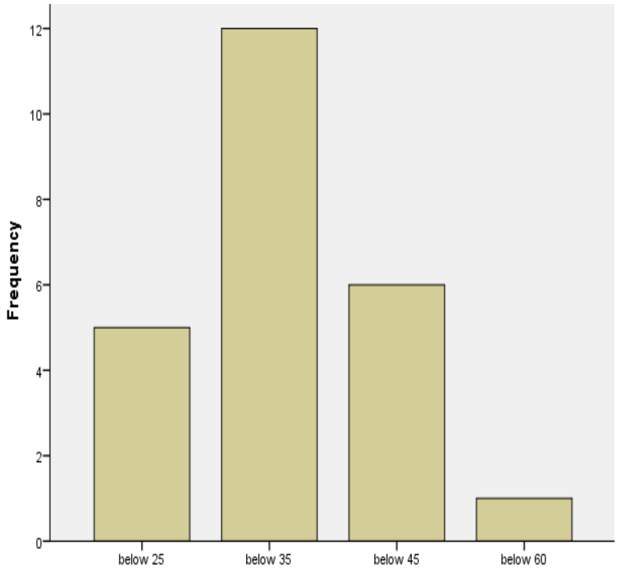


Figure 2: Chart of Age Range

The result shows that ages between 25 and 35 years are more ICT compliant, which indicates they are young, viable and prone to fraud.

Figure 3 shows the general ICT skill of the respondents.

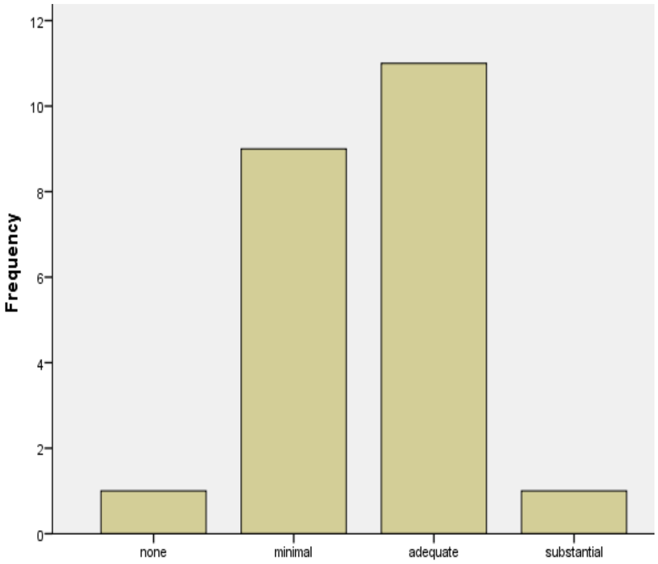


Figure 3: General ICT Skill

The result shows that general the ICT skill is adequate, which confirms that the majority of the respondents are ICT literate.

Figure 4 shows that Information Tools (IT) can be used to control e-payment.

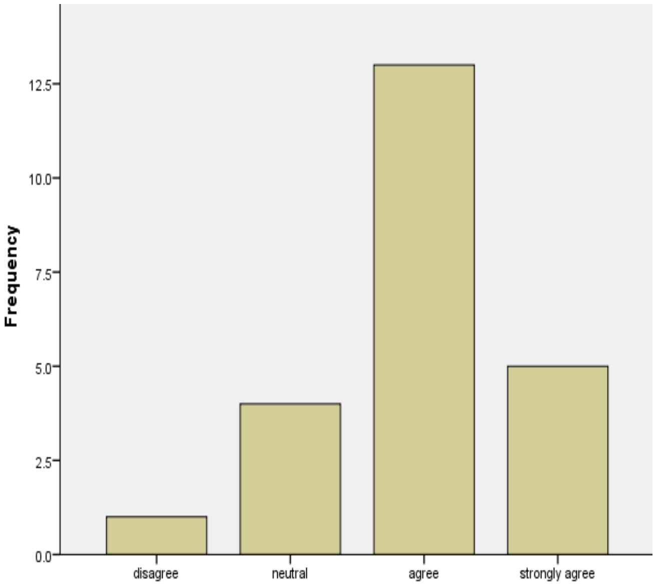


Figure 4: IT Tools to Control e-payment

The result shows that majority of the respondents agree that IT tools can be used to control e-payment.

Figure 5 shows that IT tools and techniques can be used to control the individual identity.

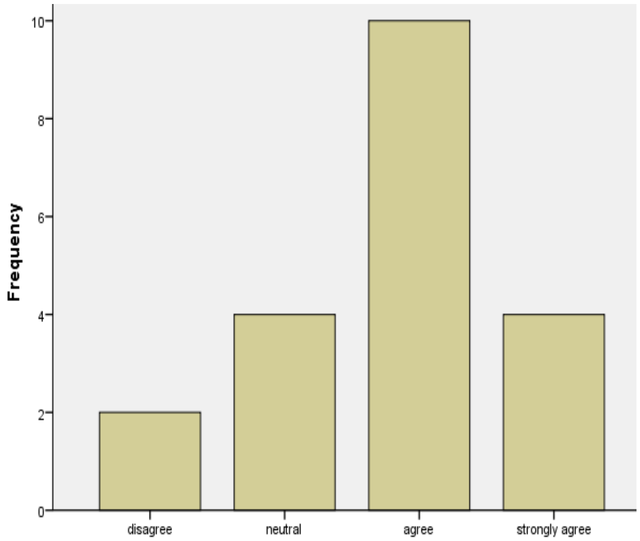


Figure 5: IT Tools to Control Individual Identity

The result shows that majority of the respondents agree that IT tools can be used to control individual identification.

Figure 6 shows that IT tools can be used for fraud detection.

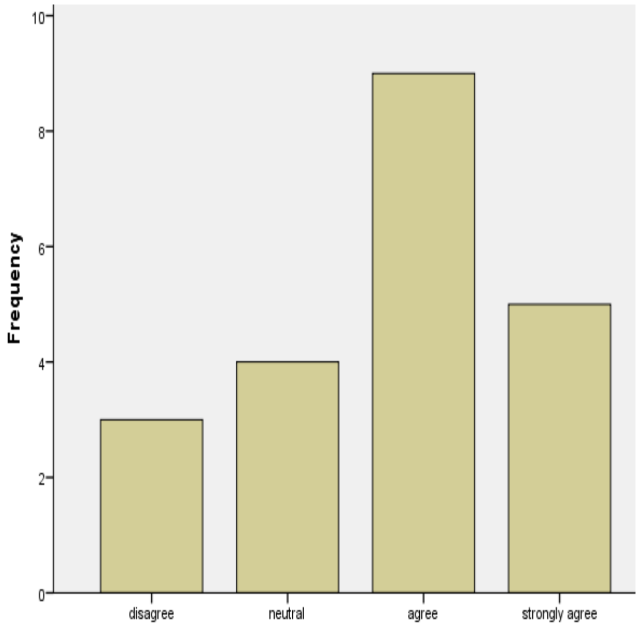


Figure 6: IT Tools for Fraud Detection

The result shows that majority of the respondents agree that IT tools can be used for fraud detection.

Figure 7 shows that continuous online auditing is effective in detecting e-fraud

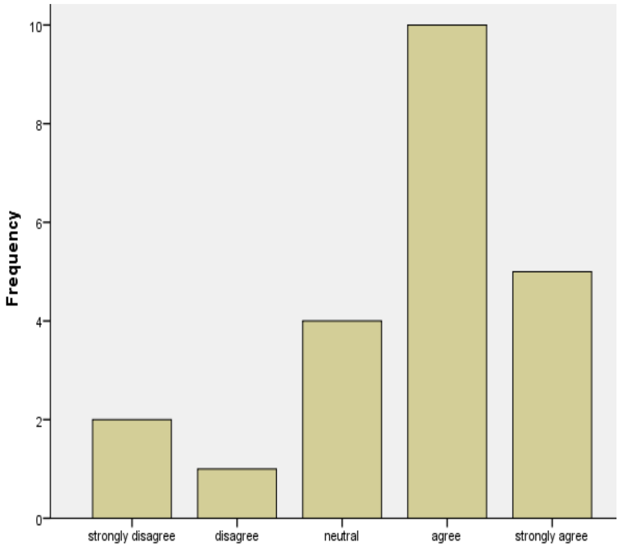


Figure 7: Continuous Online Auditing for Detecting e-fraud

The result shows that majority of the respondents agree that constant online checking is good for fraud detection.

6.0 Conclusion

Although ICT play major role in online facilitated fraud, its power can be harnessed, especially in developing country such as Nigeria for massive socio-economic development in terms of growth in Gross Domestic Product, Education (eLearning), healthcare, businesses, employment, productivity, wealth creation and general well-being. It is a very important tool for national development but can as well bring untold hardship to citizens if not well managed. Dealing with the menace of fraud powered by ICT starts from the home, right from young age parents must instill the positive use of ICT in their children and take stand against its adoption for fraud. Governments both at the local and federal levels should put regulations in place and enact stiff penalties on those found culpable.

Funding

This work has been supported by The Tertiary Education Trust Fund (TETFUND)

Conflict of Interest: none declared.

References

Aggarwal, R. (2010). Patterns of Domestic Injusries in Rural india. *Internet Jornal on Health*, Vol. 11(2), pp 4.

Akinpelu, O. (2020, April). *NCC Stats: MTN is Still King and Glo Continues to Lose Internet Users Despite Improvement in GSM Subscribers*. Retrieved from Technext: https://technext.ng/2020/03/11/ncc-stats-nigeria-now-has-186-million-active-phone-users-and-mtn-is-still-king/

BBC. (2019, September 19). *Letter from Africa: Why Nigeria's internet scammers are 'role models'*. Retrieved from BBC: https://www.bbc.com/news/world-africa-49759392

Bolt. (2019, November 26). *6 Common Types of Ecommerce Fraud and How to Fight Them*. Retrieved from The good: https://thegood.com/insights/ecommerce-fraud/

Fruhlinger, J. (2020, September 4). *What is phishing? How this cyber attack works and how to prevent it*. Retrieved from csoonline: https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

Graphus. (2020, January 21). *Verizon Says Phishing Still Drives 90% of Cybersecurity Breaches*. Retrieved from Graphus: https://www.graphus.ai/verizon-says-phishing-still-drives-90-of-cybersecurity-breaches/

Grimes, R. A. (2020, April 9). *14 real-world phishing examples — and how to recognize them*. Retrieved from CSO: https://www.csoonline.com/article/3235520/15-real-world-phishing-examples-and-how-to-recognize-them.html#slide6

INTERPOL. (2020, August 4). *INTERPOL report shows alarming rate of cyberattacks during COVID-19*. Retrieved from INTERPOL: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Karimi, F. (2019, August 24). *Men in California oversaw a romance scam that targeted women worldwide, feds say*. Retrieved from CNN: https://edition.cnn.com/2019/08/23/us/nigeria-romance-scam-arrests/index.html

KMPG. (2018). *Digital payments-Analysing the cyber landscape.* India: Risk Consulting - KPMG in India.

Leonhardt, M. (2019, April 18). *'Nigerian prince' email scams still rake in over $700,000 a year—here's how to protect yourself*. Retrieved from cnbc: https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html

Murdock. (1949). *Social Structure.* New York: Macmillan.

NCC. (2020, June). *Quarterly Subscriber Operator Data*. Retrieved from Nigerian Communications Commission: https://www.ncc.gov.ng/statistics-reports/subscriber-data#quarterly-subscriber-operator-data

Nwosu, N. (2009). The Family, Society and the Menace of Examination Malpractices: A Critical Overview. State and Society. *Interdisciplinary J. Nig. Sociol. Soc.*, Vo1. 1(1), pp. 87-102.

O'GRADY, V. (2020, March 12). *Nigeria still top of African mobile stats*. Retrieved from Developing Telecoms: https://www.developingtelecoms.com/telecom-technology/wireless-networks/9323-nigeria-still-top-of-african-mobile-stats.html

Omonijo, N. (2012). A Study of E-Cheating Habits of Students in three selected Universities in Nigeria. *Wufenia J. Vol. 8(4)*, pp.37-60.

Rosenthal, M. (2020, August 25). *Must-Know Phishing Statistics: Updated 2020*. Retrieved from Tessian: https://www.tessian.com/blog/phishing-statistics-2020/

UK, Police. (2020, December 5). *What is fraud and cyber crime?* Retrieved from Action Fraud: https://www.actionfraud.police.uk/what-is-fraud#:~:text=Fraud%20is%20when%20trickery%20is,dealing%20with%20computers%20and%20networks.