Academics Stand Against Poverty Vol. 1, No. 1, 56-73

A Stroke of the Keyboard and Click of the Mouse: an anatomy of cyber frauds as a growing component of illicit financial flows

Erhieyov O'Kenny[1]

Abstract:

Advances in digital technology have seen Nigerian conmen migrate their schemes to the cyber domain. With the advent of the COVID-19 pandemic these fraudsters have intensified their cyber attacks on vulnerable victims across the world. Through scams such as phony contracts, internet romance deception, and Business Email Compromise, Nigeria's cyber criminals make billions of dollars every year at the cost of individuals and corporations.

With the enactment of anti-cybercrime laws, the Nigerian government hopes to stem the tide of these practices. The Central Bank of Nigeria, for its part, has issued risk-based cyber security guidelines to financial institutions to enable them better to protect their computer systems and networks from external infiltration. At the international level, law enforcement agencies in the U.A.E have taken steps to track Nigerian cybercriminals operating from their territory, while the FBI has ramped up investigation of cases affecting the U.S..

The author recommends that individuals and corporations put locks on their SIM cards and mobile devices, activate two-tier authentication for email and social media accounts, and routinely update their computer devices and software, to enhance their cyber security.

Keywords: Nigerian Cyber Fraudsters, Advance Fee Fraud, 419, Business Email Compromise, Cybercrime Techniques.

Introduction

The COVID-19 pandemic has altered the way that we live and work. It has foisted a new normal on the entire world. To foster social/physical distancing, in an effort to curtail the spread of the virulent virus, more individuals and businesses are leveraging the virtual space for their day-to-day activities – in terms of communication, shopping, banking, commerce, learning and conferencing, as health workers strive to save lives. Amid the growing difficulties and uncertainties, cyber fraudsters have intensified their online schemes aimed at defrauding vulnerable victims of their hard-earned monies.

In the United Kingdom, the National Fraud and Cyber Security Center reported a 400% spike in cybercrimes in March 2020. Graeme Biggar, Director General of the National Economic Crime Center, warned that "fraudsters [are] using the COVID-19 pandemic to scam people…[by]

[1] Erhieyovw O'Kenny is an independent researcher working on human rights and social development issues in sub-Saharan Africa. He affirms that there is no conflict of interest in respect of the research, authorship, or publication of this paper to declare. O'Kenny received USD 5,000 for this essay, attached to its winning First Prize in the Seventh Annual Amartya Sen Essay Prize Competition.

sending emails offering fake medical support and targeting people who may be vulnerable or increasingly isolated at home."[2] In the United States Tonya Ugoretz, Deputy Assistant Director of the Federal Bureau of Investigation (FBI), noted the rise in cybersecurity complaints to the Bureau's Internet Crime Complaint Center (IC3) from an average of 1,000 to 3,000-4,000 daily.[3]

It is against this backdrop that this essay examines the cyber fraud phenomenon. The focus is on Nigerian cyber fraudsters and their mode of operation, in view of the heavy losses that individuals and businesses across the world sustain as a result of their schemes. The Nigerian cyber scammers have become a huge headache to law enforcement authorities in the U.S. and Europe. Following the arrest and subsequent extradition of the celebrated internet fraudster Ramon Olorunwa Abbas (aka Hushpuppi) from the U.A.E to the U.S. on charges of conspiracy to commit wire fraud and launder hundreds of millions of dollars obtained through cybercrime, the FBI has vowed to go after cybercriminals no matter what part of the world that they operate from.[4]

A description of the problematic activity

In the 1990s local fraudsters in Nigeria recalibrated their schemes and extended their dragnet to foreign waters. Their catches were huge: many gullible white men and women who fell like packs of card to their dubious antics. Their victims lost substantial sums of monies as a result. The phenomenon became known as 419, named after section 419 of the Nigerian criminal code. The biggest fraud, at the time, was perpetrated by a syndicate that comprised Ikechukwu Anajemba, his wife Amaka, Emmanuel Nwude-Odinigwe, Dr. Hammed Ukeh, several Asian money mules who provided bank accounts to receive the illicit funds for a cut of the proceeds, among others. Their victim was Nelson Sakaguchi, a Director at Banco Noroeste, a Brazilian bank with headquarters in Sao Paulo.

The syndicate had invited Mr. Sakaguchi to Nigeria to explore potentially high yielding business opportunities. The Brazilian was taken to a private house in Enugu state that was carefully decorated as the Central Bank of Nigeria, with the appropriate logo and other paraphernalia. With some of the fraudsters playing the role of the Governor of the Central Bank, Director of International Remittance, Director of Budget and Planning in the Ministry of Aviation, among other top portfolios, the Brazilian was assured of a major contract from the Federal Government. He left for his home country in high hopes. Not long afterwards the fraudsters sent him a fax with the news that the Nigerian government had awarded him a contract to build an airport in the Federal Capital Territory valued at $200 million. He was told he could take $13 million for himself from the deal.

---

[2] "Coronavirus-related scams increase by 400% in March, says ActionFraud.". Radio broadcast. MKFM, March 30, 2020. https://www.mkfm.com/news/local-news/coronavirus-related-scams-increase-by-400-in-march-says-actionfraud/

[3] Maggie Miller. "FBI sees spike in cyber crime reports during coronavirus pandemic." THE HILL, April 16, 2020. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic

[4] Andrew John Innocenti "Criminal Complaint by Telephone or Other Reliable Electronic Means." Affidavit. U.S. District Court for the Central District of California, June 25, 2020. https://www.justice.gov/usao-cdca/press-release/file/1292066/download

Having hoodwinked him, the fraudsters began to demand advance fees to put the contract into effect, and Mr. Sakaguchi complied. A list of payment (contained in the particulars of claim filed by the claimants' lawyer Peters & Peters of 2 Harewood Palace, Hanover Square, London which The NEWS magazine obtained) showed that between May 2, 1995 and January 20, 1998 the Brazilian remitted over $190 million via SWIFT electronic system to various accounts in several countries that the fraudsters provided.[5] Since he did not have such huge monies, Mr. Sakaguchi had to dip his hands into Banco Noroeste's coffers, for which he was later prosecuted by the authorities in Brazil. While he waited for the contract to yield the much-touted high returns, the fraudsters squandered the earnings on their extravagant lifestyle.

Negative influence of extravagant lifestyles

With the proceeds of the advance fee fraud, the Anajembas, for instance, acquired 30 houses in Nigeria, the U.S. and Britain, a fleet of exotic cars, large shareholdings in First Homes (a subsidiary of First Bank of Nigeria) and more, as investigations by TELL magazine uncovered.[6] Emmanuel Nwude-Odinigwe, the deceptively gentle-looking member of the syndicate who reportedly played the role of Governor of the Central Bank of Nigeria, purchased 20 houses in Nigeria and abroad. He had large shareholdings in the Union Bank of Nigeria (which helped him to secure the position of Executive Director), and in G. Cappa PLC (where he was also a Director), among other prime investments, until law enforcement agents got on his trail.[7]

The fraudsters wore costly designer outfits, frolicked at exclusive parties and nightclubs, gave house-warming parties at which popular musicians were paid to entertain the crème-de-la-crème guests, had chieftaincy titles conferred on them, moved about in exotic bullet-proof cars, and undertook frequent pleasure trips abroad accompanied by concubines. They lived like high-flying princes with vast fortunes at their disposal. The allure of such an extravagant lifestyle prompted many youths to follow suit. Many of them quickly jettisoned legitimate work to embrace advance fee fraud as a way of life because of the stupendous wealth that it could generate in the shortest possible time.

Escalation of the problematic activity

In 2001 the Nigerian government deregulated the communications industry, which was monopolized by the state-owned enterprise Nigeria Telecommunications Ltd. (NITEL) for decades. Several Global System for Mobile Communications (GSM) operators were licensed to provide voice, internet and data services to the teeming populace. Huge investments in state-of-the-art digital switches, base stations, cell sites, fiber optics and broadband were made over the years. Stiff competition among the licensed GSM operators swiftly brought charges down. The Nigerian telecoms market would become one of the fastest growing in the world. Mobile subscribers hit the 172 million mark in 2017, and over 112 million Nigerians had access to the internet in 2018.

[5] Tayo Odunlami. "The Biggest 419 Affair Ever." The NEWS, September 1, 2003, pp. 20-21.
[6] Dayo Aiyetan. "The $254 Million Scam." TELL, August 19, 2002, p.26.
[7] Ibid.

Local fraudsters quickly latched onto the digital revolution to perpetrate their schemes. They migrated from the traditional mode of operation, where communication with potential victims was mostly done by way of physical contact, analog phone calls, fax and postal mail, to the virtual space. Hiding under the anonymity that the virtual space confers, they were able to orchestrate various kinds of online frauds by simply stroking the keyboard and clicking the mouse of their computer devices. It was then that they became known as the *Yahoo Boys* or *Yahoo Yahoo Boys,* apparently due to attacks on Yahoo Mail accounts that they orchestrated. (At the time the vulnerability of Yahoo Mail to external intrusions was thought to be high). In the current dispensation where computers, laptops, tablets, and smart phones with enhanced Internet capacities are readily available at affordable costs, the population of cyber criminals in Nigeria has grown exponentially, with attacks on unsuspecting victims constantly on the rise.

Tactics and techniques

In August 2001, the U.S. Consulate in Nigeria raised the alarm that millions of Americans were receiving via conventional mail and emails bogus offers with possible criminal intent.[8] Through what the cyber fraudsters term *bombing,* dubious business proposals are sent to masses of email addresses, sometimes harvested with an email extractor (a potent software tool that can extract email IDs from web pages automatically) on a day-to-day basis. The cyber fraudsters often pick their victims from the wide array of profiles in social media platforms, dating sites, web forums for professionals and similar locations. They make extravagant business offers while posing as high-profile personalities in Nigeria and abroad. In fact, there are no limits to the array of claims that they make.

Monies quoted in the business offers run into millions of dollars. Potential victims are promised a certain percentage as reward for their assistance. Assistance here implies that the potential victims accept their nomination as emergency beneficiaries of what are, unbeknown to them, bogus funds domiciled in fictitious accounts that the fraudsters seek to transfer. This is the bait. Once the targets respond affirmatively, they are asked to send their personal information including their bio data, contact addresses, bank account details, telephone numbers, and so on.

The fraudsters typically send potential victims various official-looking but forged documents in an effort to validate their false claims. They then demand advance fees to facilitate the transfer of the bogus funds to the bank accounts of the victims. Should a victim send money (often through Western Union or Money Gram for funds not exceeding $10,000 in a single transaction or via wire transfer for larger sums) the fraudsters escalate their demand for funds under various guises. This continues until the victims have exhausted every possible avenue of getting money. Some victims borrow money from family, colleagues, friends, and even from banks, to satiate the seemingly endless demands of the fraudsters in the hope of getting the bigger reward afterwards. When they finally come to realize with whom they are dealing, the fraudsters disappear, and the money is irretrievably gone.

[8] Public Affairs Section of the U.S. Consulate General, Lagos, Nigeria. "U.S. Embassy and Nigerian Police Join Forces to Fight '419' Fraud." Crossroads, vol. 8, no.. 8, August–October, 2001, p.3.

With advancement in Information and Communication Technology, cyber fraudsters are able to constantly change their tactics and formats. Business Email Compromise (BEC) has become the fastest growing component of their operations, generating the highest illicit earnings thus far. BEC, as defined in an affidavit filed at the United States District Court for the Central District of California by the FBI, typically involves "a computer hacker gaining unauthorized access to a business-email account, blocking or redirecting communications to and/or from that email account, and then using the compromised email account or a separate fraudulent email account…to communicate with personnel from a victim company and to attempt to trick them into making an unauthorized wire transfer."[9] They are mostly implemented via phishing emails.

In some cases the fraudsters create email accounts and/or websites that resemble those of real government offices, business entities, financial institutions or multilateral agencies, from which they write to officials of businesses on a subject of interest to them. The targets are often tricked into clicking the accompanying links and/or downloading the attached files that have been infected with malware, ransomware, spyware or other malicious software.

Once the unwary victims fall for the trick their email accounts and/or computer systems are automatically compromised. The cyber fraudsters then methodologically sift through the email exchanges in an effort to construct their manipulative strategies. The American cybersecurity company Secureworks, which has studied email scams emanating from the West African sub-region, notes: "The attackers get inside the email systems of companies…looking for business-to-business transactions…If two companies are about to make a deal, the scammers use their inside access to email systems to modify invoice details and direct payments into accounts they control."[10]

Other fraudulent online schemes that Nigerian scammers perpetrate include romance scams (typically these schemes target vulnerable elderly women seeking love and affection), lottery scams, inheritance scams, shopping frauds, and denial-of-service attacks. There seems to be no limit to the array of online scams, as the fraudsters are ingenious and tech savvy. They also keep track of unfolding developments in the world that they manipulate to achieve their ends. In the case of the COVID-19 pandemic, Nigerian fraudsters have created fake shops, tracking apps, websites, social media accounts, and email addresses, with which they make claims to manufacture and/or supply Personal Protective Equipment.[11] INTERPOL said the German health authorities, in their desperate bid to procure much needed face masks in the wake of the pandemic, were swindled out of €800,000. In an attempt to trace and block the movement of the funds, the international organization found out that the money was moved from the Netherlands through the U.K., with Nigeria being the final destination.[12]

---

[9] United States Attorney's Office, Central District of California. "Nigerian National Brought to U.S. to Face Charges of Conspiring to Launder Hundreds of Millions of Dollars From Cybercrime Schemes." Press Release. July 3, 2020. https://www.justice.gov/usao-cdca/pr/nigerian-national-brought-us-face-charges-conspiring-launder-hundreds-millions-dollars

[10] Jeremy Kirk. "Churchgoing Nigerians Drive Business Email Attacks." Bank Info Security, August 5, 2016. https://www.bankinfosecurity.com/church-going-nigerians-drive-business-email-attacks-a-9323

[11]"INTERPOL warns of financial fraud linked to COVID-19." INTERPOL, March 13, 2020. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19

[12] Abdur Rahman Alfa Shaban. "Account in Nigeria linked to European COVID-19 mask fraud – INTERPOL." africanews, April 15, 2020. https://www.africanews.com/2020/04/15/account-in-nigeria-linked-to-european-covid-19-mask-fraud-interpol/

Technical competencies

In terms of technical acumen James Bettke, a counter threat researcher at Secureworks, has contended that Nigerian cyber fraudsters "can't code, don't do a lot of automation, [that] their strengths are in social engineering and the ability to create agile scams."[13] Nigerian cyber fraudsters are thought to mainly leverage the abundance of personal information in social networks such as Facebook, Twitter, and Linkedin, as well as media sharing sites such as Instagram, YouTube, and Snapchat, to engineer attacks on their victims. However, this assessment is not tenable in the light of new evidence.

A recent investigation by Unit 42 of Palo Alto Networks has shown that Nigerian cyber actors currently produce an average of 840 unique samples of information stealing malware per month, as well as utilizing damaging Remote Access Trojans such as NetWire and NanoCore to cast a wider net over the virtual space (Palo Alto Networks, 2018). The revelation by FBI special agent Andrew John Innocenti that Ramon Olorunwa Abbas ('Hushpuppi') and another conspirator defrauded a law firm in New York of approximately $923,000 via a BEC scheme, as well as siphoning off millions of dollars from financial institutions in Europe and America via cyber heists, testify to the growing sophistication of Nigerian cyber criminals. They can no longer be portrayed as minor players in the fast-growing cyber fraud industry.

Assets recovered by the Dubai police, which conducted a raid on the apartment of Abbas in an operation codenamed *Fox Hunt 2*, would make even the notorious Russian hackers Maksim Yakubets and Igor Turashev of Evil Corps, who the U.S. Treasury Department sanctioned for stealing banking credentials in over 40 countries and siphoning off millions of dollars, green with envy. They included 21 computer devices, 47 smart phones, 15 memory sticks and five hard disks that contained 119,580 fraud files as well as the addresses of 1,926,400 victims.[14] Over $40 million in cash and 12 luxury cars valued at $6.8 million were recovered as well.

From the foregoing it has become clear that Nigerian online fraudsters, irrespective of what part of the world they operate from, are capable of orchestrating attacks on individuals, businesses, banks, payment solution providers, financial institutions, government departments, fin-techs, and big tech firms across the world with a high degree of precision. In order to perpetrate successful scams, the fraudsters work collaboratively for a share of the illicit proceeds. Olivia Ndubuisi, a Nigerian broadcast journalist who infiltrated one of the headquarters of internet fraudsters in Nigeria, notes that: "The Yahoo Boy rarely lives alone. He needs his comrades around him to pull off a successful scam: the document forger, the international call router, the bank account front person…the tech wizard…[and] the smooth talker."[15]

---

[13] Lily Hay Newman. "Nigerian Email Scammers Are More Effective Than Ever." WIRED, May 3, 2018. https://www.wired.com/story/nigerian-email-scammers-more-effective-than-ever/

[14] William Ukpe. "Hushpuppi extradited to the United States." Nairametrics, July 2, 2020. https://nairametrics.com/2020/07/02/hushpuppi-extradited-to-the-united-states/

[15] Olivia Ndubuisi. "Nigeria / Internet scamming. The Yahoo Boys Universe." Chronicle #37, n.d. https://www.zammagazine.com/chronicle/chronicle-37/695-nigeria-internet-scamming-the-yahoo-boys-universe

Some documented cases

In 2013, a syndicate comprising two university undergraduates, Isaiah Friday and Azzaior Samuel, and two Bureau de Change operators, Salihu Mahmoud and Dan Ibrahim, broke into the digital database of the Union Bank of Nigeria to post 2.05 billion Nigerian Naira to accounts in other branches that they control.[16]

Obinwanna Okeke, an outwardly successful Nigerian entrepreneur whom Forbes magazine has featured in its prestigious *30 under 30* list of African entrepreneurs, pleaded guilty in 2020 to charges of computer intrusion and wire fraud that caused Unatrac Holding Ltd, a British affiliate of U.S heavy equipment manufacturer Caterpillar, $11 million in losses.[17] In 2018 Okeke and his conspirators had hacked into the email account of the Chief Financial Officer of Unatrac by means of a phishing email that contained a link to a fake Microsoft Office 365 login page. Having obtained the CFO's credentials, the cyber thief studied the email flow to learn of pending financial transactions. He then created spurious money transfer requests and invoices in the CFO's name, using the company's logo.

Some years ago British retiree John Anthony Lynch suffered a financial loss of over £400,000 when Nigerian internet fraudsters trapped him with a beautiful woman and mouthwatering business deals.[18] After exhausting all of his retirement benefits, including selling his house, Mr. Lynch took out loans in order to meet the insatiable demands of the fraudsters. In 2016, a Japanese women, named as 'FK' in U.S court documents, lost $200,000 over a ten-month period to a Nigerian fraudster with the pseudo name 'Terry Garcia', a supposed American soldier on tour in Syria, and his accomplices.[19] She was said to have borrowed money from her sister, ex-husband and friends in her desperate bid to clear a bag of diamonds that the unscrupulous conman claimed he had sent to her.

In a similar fashion a Cambodian woman named Sophanmia lost $75,000 to a 19-year old Nigerian online fraudster named Chigemezu Arikibi, who just joined the game.[20] The teenager opened a fake Facebook account with the name 'Frank Williams' and another account on Instagram with the name 'Patrick Williams' with which he communicated with her. He offered to send her expensive gift items and $500,000 in cash to be used for investment in the real estate sector of the southeastern Asian country. This was the trick used in convincing her to send money to a spurious courier agent in Indonesia in her desperate bid to have the items cleared.

Internet romance scams can endanger the life of victims. In 2019 a 34-year old man named Chukwuebuka Obiaku lured a 46-year old American woman retiree to Nigeria.[21] He then

---

[16] Vera Ekwebelem. "Online Burglary Escalates." Broad Street Journal, October 21, 2013.
[17] Ishita Chigilli Palli. "Nigerian Entrepreneur Pleads Guilty in $11 Million BEC Scam." Bank Info Security, June 22, 2020. https://www.bankinfosecurity.com/nigerian-entrepreneur-pleads-guilty-in-11-million-bec-scam-a-14479
[18] Ade Alade. "57-year-old Briton scammed of N1bn by a Nigerian fraud syndicate says…'I want to die'." Saturday Sun, January 12, 2013, p.14.
[19] Faith Karimi. "Men in California oversaw a romance scam that targeted women worldwide, feds say." CNN, August 24, 2019. https://edition.cnn.com/2019/08/23/us/nigeria-romance-scam-arrests/index.html
[20] Andrew Utulu. "419: Boy, 19, Nabbed For Allegedly Defrauding Cambodian Lady Of $75,000." Saturday Independent, February 29, 2020. https://www.independent.ng/419-boy-19-nabbed-for-allegedly-defrauding-cambodian-lady-of-75000
[21] "Romance scam: US woman freed after a year as hostage in Nigeria." BBC News, July 13, 2020. https://www.bbc.com/news/world-africa-53390397

held her in a local hotel for 16 months against her will, seized her credit and debit cards and forced her to part with $48,000 from her retirement benefits.

The documented cases of such practices are many and varied. New cases continue to be reported to law enforcement agencies in different parts of the world.

Magnitude and estimates

Heavy financial losses continue to be recorded in Nigeria and other countries of the world as a result of the activities of Nigerian internet fraudsters. The exposed losses to businesses worldwide are now estimated to be more than $3 billion. Unit 42 of Palo Alto Networks has estimated that, in 2017, Nigerian BEC-linked incidences shot up by 45%, representing about 17,600 attacks per month (Palo Alto Network, 2018). The U.S. Treasury Department estimates that BEC scams cost American companies more than $300 million a month, with an average of 1,100 businesses scammed every month.[22] The FBI estimates that between October 2013 and December 2016 more than 40,000 business email compromise incidences resulted in $5.3 billion in losses.[23] According to the FBI's *Internet Crime Report 2019*, its Internet Crime Complaint Center received 467,361 complaints (at an average of 1,300 daily), with recorded losses to individual and businesses put at $3.5 billion, the highest the Center has recorded so far.[24] Cyber security experts have established that 90% of all BEC schemes are perpetrated by Nigerian actors, both in and outside of Nigeria.

With respect to Nigeria an editorial in the Daily Independent notes that "Nigeria lost the staggering sum of $649 million (N250 billion) to cybercrime in 2017 … [which is] saddening and very unfortunate given that such monumental hemorrhage could have been avoided."[25] It cited the 2018 report of the Nigeria Deposit Insurance Corporation that revealed that there were 37,817 reported cases of fraud in the year under review, of which 59.2% were internet and technology related. In broad terms, cyber fraud costs Nigerian businesses billions of naira annually.

Adverse impact/damages

Cyber fraud adversely alters the lives of individual victims and can even ruin businesses. The defrauding of Mr. Sakaguchi, for instance, resulted in the liquidation of Banco Noroeste (a bank that had been in existence for about 70 years), leading to an abrupt and devastating loss of shareholders' capital. Defrauded individuals, such as those mentioned earlier in this essay, are plunged into a state of indebtedness and despair from which they may never recover. John Anthony Lynch almost committed suicide to escape the trauma caused by his devastating experience.

---

[22] Scott Ferguson. "BEC Scams Cost U.S. Companies $300 Million Per Month: Study." Bank Info Security, July 19, 2019. https://www.bankinfosecurity.com/bec-scams-cost-us-companies-300-million-per-month-study-a-12805

[23] Lily Hay Newman. "Nigerian Email Scammers Are More Effective Than Ever." WIRED, May 3, 2018. https://www.wired.com/story/nigerian-email-scammers-more-effective-than-ever/

[24] "2019 Internet Crime Report Released." FBI News, February 11, 2020. https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[25] "The Huge Losses To Cybercrime." Daily Independent, December 17, 2019. https://www.independent.ng/the-huge-losses-to-cybercrime/

Nigeria's image in the international community has been seriously dented. Howard F. Jeter, the U.S. Ambassador to Nigeria from 2001 to 2003, noted that: "Legitimate Nigerian businessmen attempting to establish trade links with the U.S. and Europe or to solicit foreign investments are greeted with negative reactions based on suspicions of '419' fraud schemes."[26] High commissions and embassies continue to issue advisories to their citizens who wish to visit Nigeria to explore potential business opportunities to be wary of Nigerian businessmen, many of whom are deemed to be 'crooked'. With reduced inflow of Foreign Direct Investment the tax generating potential of the Nigerian state is seriously hampered. Employment opportunities that should accrue from the operations of foreign businesses in Nigeria are lost. Due to the bad reputation arising from the operations of cyber fraudsters, Nigerian citizens on international travel are subjected to intense checks at airports abroad.

Businesses whose customer databases are breached and whose monies are stolen often end up losing the trust and confidence of their customers. Affected customers may sue for the damages that such breaches may cause them. Precious time is wasted as individuals and businesses strive to recover their compromised email accounts and restore the integrity of their computer systems. Larger monetary resources need to be earmarked to tighten data security. Businesses are compelled to hire formidable IT professionals to assist in the fortification of their computer systems and network servers on a regular basis, which adds to their operational costs and reduces their profitability. Some foreign entities have even blocked IP addresses in Nigeria from accessing their websites.

Enabling conditions/why cyber frauds persists

- **Growing poverty and lack of opportunities**

The latest report of the National Bureau of Statistics entitled *Poverty and Inequality in Nigeria 2019* classifies 40.1% of the population of Nigeria, or 82.9 million people, as poor (i.e. they live on N381.75 per day or N11,452.50 per month).[27] An earlier report by the Brookings Institution categorized Nigeria as the 'poverty capital of the world', with 110 million people projected to live in extreme poverty by the year 2030.[28] Unemployment currently stands at over 23%. Popular Nigerian movie actor cum musician Nkem Owoh captured the distinct correlation between poverty and advance fee fraud in the lyrics of one of his songs in Pidgin English: *"I don suffer no be small, upon say I get sense. Poverty no good at all, Neyin make I join this business. 419 no be thief, it's just a game, everybody dey play, if anyboby fall mugu, ah, my brother, I go chop am*!"[29] The English translation reads: "I have suffered so much, even though I am sensible. Poverty is not good at all, that is why I joined this [419] business. 419 is not stealing, it's just a game [that] everybody is playing. If anybody falls for my antics, ah, my brother, I will swindle him!"

---

[26] Public Affairs Section of the U.S. Consulate General Lagos, Nigeria. "U.S. Embassy and Nigerian Police Join Forces to Fight '419' Fraud." Crossroads, vol. 8, no. 8, August –October, 2001, p.3

[27] "82.9m Nigerians Are Poor –NBS." The Pointer, May 5, 2020, p.5.

[28] Homi Kharas, Kristofer Hamel and Martin Hofer. "Rethinking global poverty reduction in 2019." Brookings Institution, December 13, 2018. https://www.brookings.edu/blog/future-development/2018/12/13/rethinking-global-poverty-reduction-in-2019/

[29] Nkem Owoh. "I go chop your dollar." Kas-Video Entertainment, 2005. VCD.

Contributing to the endemic poverty in Nigeria is massive official corruption. The oil wealth of the nation is being siphoned off by politicians in collusion with bureaucrats. Gabriel Ogunjobi, a journalist and intern with the internet platform African Liberty, captured this as follows: "The desperation for survival of many of Nigerian youths is tough. Most are unemployed and can barely afford to feed themselves. The misappropriation of public funds that could have created jobs and other economic opportunities by corrupt politicians is the real problem here."[30]

- **Negative influence of extravagant wealth**

The extravagant lifestyle of cyber fraudsters continues to draw many poor people into the morally corrupt profession. Celebrated internet fraudsters such as Hushpuppi lived in the exclusive Palazzo Versace Apartments in Dubai, had $40.9 million in cash at home, 12 luxury cars parked in his garage valued at $6.8 million, among other luxurious things of life. Always clad in customized designer outfits and sporting expensive wrist watches, he exhibited his super expensive lifestyle via regular social media posts. His followers on Instagram numbered well above two million. Many upcoming youths crave to be like him, not minding how he made his wealth. Rev. Christopher Omotunde, Bishop of the Ekiti Diocese of the Anglican Communion, has posited that the mindless pursuit of wealth by most Nigerians is the cause of the increasing rate of criminalization in the nation.[31]

Nigeria generally lacks good societal role models. Political leaders and public sector officials continue to demonstrate unbridled passion for monumental corruption. Here is a country that posthumously honored the late Gen. Sani Abacha, the despotic military head of state who stole billions of dollars from the national treasury.[32] Amaka Anajemba, a member of the syndicate that defrauded a Brazilian banker of millions of dollars which resulted in the collapse of Banco Noreste, was appointed Managing Director of the Enugu State Waste Management Board by Governor Ifeanyi Ugwuanyi in 2016.[33]

- **Easy to learn and low risk**

Many Nigerian cyber fraudsters are inducted into the clandestine profession by their streetwise peers. Cybercrime techniques are easy to learn and execute as they do not require much education or technical acumen. The entry costs are low. The requirements are a simple computer device (up-and-coming fraudsters often start with second-hand laptops), internet access, and hacking toolkits, readily available in the black market of the dark web, for those who want to venture into hacking schemes.

---

[30] Gabriel Ogunjobi. "Internet Fraud is Destroying Nigeria – thanks to the Government." African Liberty, September 23, 2019. https://www.africanliberty.org/2019/09/23/internet-fraud-is-a-problem-in-nigeria-but-the-government-is-worse/

[31] Rotimi Ajomoyela. "Fake lifestyle, bane of crime in Nigeria – Anglican Bishop." Vanguard, November 11, 2019. p. 11.

[32] Olu Fasan. "Nigeria shames itself by posthumously honouring Abacha." Vanguard, May 14, 2020. https://www.vanguardngr.com/2020/05/nigeria-shames-itself-by-posthumously-honouring-abacha/

[33] "Ugwuanyi's Curious Love for Amaka Anajemba." This Day, August 28, 2016. https://www.thisdaylive.com/index.php/2016/08/28/ugwuanyis-curious-love-for-amaka-anajemba/

Chigemezu Arikibi, the 19-year old Nigerian internet fraudster who defrauded a Cambodian woman of $75,000 while posing as an American pilot working for a British airline, confessed: "It was Ugochukwu my friend who taught me how to do internet fraud. Ugochukwu used to communicate with white (oyibo) people on the internet and when he is chatting, I will be looking. I learned job from him for one week and I started my own."[34] Investigations by the Nigerian Economic and Financial Crimes Commission (EFCC) have shown that there are informal training centers where upcoming cyber con artists are coached in the art of online fraud by older fraudsters. Training centers in Lagos[35].and Akwa Ibom[36] were exposed by operatives of the EFCC, acting on intelligence. Unlike perpetrators of such crimes as armed robbery, kidnapping, militancy and piracy, which are risky to execute, many cyber fraudsters work remotely from their homes and other hidden locations, almost unrestrained. Nowadays they hardly use public cybercafés, to avoid being apprehended by prowling plain clothes law enforcement officials. Even when they are caught Nigerian fraudsters are confident that they can avert prosecution by using their vast illicit wealth to bribe law enforcement and judicial officials.

- **Cinematic influence**

It has been said that the foreign movies of the 1970s, 80s and 90s that depicted carefully orchestrated heists, armed robberies, bank frauds, among other cleverly executed crimes, have corrupted the traditional values of Nigerian society. The early Nigerian fraudsters began to put the tricks that they saw in these movies into practice. They soon turned the art against whites, mostly in Europe and America, using the justification that they were taking back the huge resources that the white imperialists stole from Africa during the period of the transatlantic slave trade and colonialism.

- **Greed**

While some individuals can easily spot emails with bogus offers, which are often full of grammatical errors and implausible scenarios, others continue to fall for the tricks of the cyber fraudsters. Greed, the unbridled desire to reap bountifully where one has not sown or to immensely benefit from illicit activities, is what makes most of the victims succumb to the wiles of cyber fraudsters. For instance, individuals who receive emails that announce that they have won lotteries they did not enter or that nominate them as emergency beneficiaries of inheritances that they are not entitled to should be wary. Nigerian cyber fraudsters are very smart. They know that greed is a part of human nature, that human beings naturally desire fortunes without having to work for them. So they make enticing offers that play on the psyche of their victims.

---

[34] Andrew Utulu."419: Boy, 19, Nabbed For Allegedly Defrauding Cambodian Lady Of $75,000." Saturday Independent, February 29, 2020. https://www.independent.ng/419-boy-19-nabbed-for-allegedly-defrauding-cambodian-lady-of-75000

[35] Xavier Ndah and Raji Adebayo, "EFCC Smokes Out Yahoo Boys' Kingpin in Lagos Hotel, Arrest 26 others." Independent, December 5, 2019, p.7. https://www.independent.ng/efcc-smokes-out-yahoo-boys-kingpin-in-lagos-hotel-arrests-26-others/

[36] Nsikak Nseyen. "EFCC arrests operators of 'yahoo academy' in Akwa Ibom," December 1, 2019. https://dailypost.ng/2019/12/01/efcc-arrests-operators-of-yahoo-academy-in-akwa-ibom-photos/

Greed is also something that rears its ugly head in the camp of the fraudsters themselves, especially when it comes to sharing their ill-gotten gains. In the Sakaguchi swindle hsaga, the originator of the scam, Dr. Hammed Ukeh, felt his fellow conspirators had sidelined him in the sharing of the booty, so he wrote a petition to the police informing on his fellow criminals. Fraudsters who feel their accomplices have sidelined or cheated them often use secret cult groups or hired assassins to exact revenge.

- **Bag eggs in the law enforcement agencies**

Typical Nigerian fraudsters offer bribes to law enforcement officials who are closing in on them. For instance Amaka Anajemba, after she took over the reins of her husband's vast illicit business empire upon his sudden death, attempted to bribe Mallam Nuhu Ribadu, the chairman of EFCC at the time, with N30 million when he brought charges of fraud and money laundering against her.[37] But the czar of the anti-graft agency, who was awarded the prestigious Sheikh Tamin Bin Hamad Al Thani International Anti-Corruption Excellence Award in Doha Qatar in 2018, was said to have declined the bribe. Many corrupt law enforcement officers would readily accept such bribes and let the culprits go free. Some would even tamper with evidence. In one incident, Hussani Abubakar, a staff member of the EFCC, stole vital exhibits from the forensic section of the anti-graft agency that could have been used as evidence in the prosecution of a local cyber fraudster.[38]

Hope Olusegun Aroke, a convicted internet fraudster serving time in the Maximum-Security Prison in Kirikiri, Lagos, has been under investigation in relation to a $1 million mega scam.[39] It appears that compromised elements in the prison system had allowed him access to the internet and a mobile phone, with which he plotted the scheme with the aid of external collaborators.

Some policemen hide under the cloak of fighting cybercrimes to enrich themselves. There have been reported cases of unauthorized stop-and-search operations on the roads, streets, and markets of cities and towns across Nigeria. Private residences, restaurants, bars, hotels, guest houses, and nightclubs, among other public places have also been raided, almost indiscriminately. Phones, laptops and other personal effects have been searched and confiscated on flimsy reasons. Individuals have been arrested on unfounded allegations only to be asked to part with some money before they are let go. A case in point is 21-year-old Isaac Ogbechie who, in one of the police checkpoints along the Benin-Asaba expressway, was accused of being a yahoo boy.[40] He said the police seized his mobile handset because it contained photos of some white people, as well as impounding his laptop because he did not have the purchase receipt. To gain public support, law enforcement agents must be seen to be sincere in the fight against cybercrimes.

---

[37] Geoffrey Ekenna. "Ready to Spill the Beans." Newswatch, February 23, 2004, p. 20.
[38] "Ex- EFCC Staff Jailed for Stealing Exhibits." EFCC, February 20, 2020. https://efccnigeria.org/efcc/news/5488-ex-efcc-staff-jailed-for-stealing-exhibits
[39] "Internet fraud: Nigerian scammer 'pulls off $1m heist' from prison." BBC News, November 19, 2019. https://www.bbc.com/news/world-africa-50480495
[40] Awele Ogboru and Omo Oyibode. "Police Checkpoints: Security Tools or Extortion Joints?" The Pointer, February 1, 2020, p.8.

- **Lapses in documentation**

To register a SIM card in Nigeria, a prospective subscriber is required to provide a government-issued ID card (e.g. an international passport, a driver's license, a voter's card, a national identity card) in addition to providing their bio data and contact details. Due to the proliferation of forgery in the country cyber fraudsters can register their SIM cards with fake documents, which the telecoms operators spend little time checking. In the same manner, in collusion with compromised staff of banks, cyber fraudsters can open bank accounts using fake names and documents. Because Nigerian banks lag behind in conducting KYC (Know Your Customer), these accounts often bypass the laid-down processes of due diligence. With payment options such as Western Union and Money Gram, which are irreversible, cyber fraudsters are able to receive $10,000 or below from their victims in a single transaction, once they can answer the relevant test questions, provide the Money Transfer Control number, the sender's name, expected amount, as well as the country from where the money is sent, while using fake documents and accounts to identify themselves. It has baffled EFCC investigators how the convicted internet fraudster Hope Olusegun Aroke was able to open two bank accounts, as well as buy a luxury house and car, under the fictitious name 'Akinwunmi Sorinmade' while doing time in prison.[41]

- **Spiritual powers**

Many cyber fraudsters are deeply involved in fetishes. Armed with the personal information of potential victims (e.g. name, date of birth, home address, place of residence, nationality, photographs) they often consult witch doctors and juju priests.[42] They offer sacrifices at fetish shrines where the spirits of their potential victims are supposedly hypnotized and their minds captured. This may explain why some of the victims of the online fraudsters would readily empty their bank accounts as well as borrow money from family and friends to meet the demands for money that the fraudsters make. Some of the fraudsters even go to the extent of making human sacrifices. A case in point is 29-year-old internet fraudster Taiwo Akinola, who attempted to murder his mother Alice Iyabo Akinola as part of a ritual that was supposed to make his online scam business prosper.[43]

- **Hard-to-get justice and minimal sentences**

Nigerian courts are currently overwhelmed with cases. The Federal High Court, for instance, which has 36 divisions, has over 200,000 cases to hear while it has only 82 judges.[44] This has caused long delays in the dispensation of justice.

---

[41] "Internet fraud: Nigerian scammer 'pulls off $1m heist' from prison." BBC News, November 19, 2109. https://www.bbc.com/news/world-africa-50480495

[42] Juju priests, the equivalent of voodoo priests in Caribbean countries such as Haiti, ostensibly serve as mediums between the physical and spiritual worlds.

[43] "How 'yahoo-boy' try to kill im mam for money rituals." BBC Pidgin News, August 20, 2015. https://www.bbc.com/pidgin/tori-45248779

[44] Ade Adesomoju, Tunde Ajaja and Alexander Okere. "Justice suffers as 82 justices handle over 200,000 cases in federal high courts." Punch, July 21, 2019. https://punchng.com/justice-suffers-as-82-judges-handle-over-200000-cases-in-federal-high-courts/

Even when fraudsters are successfully prosecuted in a court of law, the penalties for the crimes are typically low. For instance, the Lagos High Court had, in July 2005, convicted and sentenced Amaka Anajemba to a paltry two and half years jail term in addition to ordering her to return $25.5 million. An unemployed Nigerian man named Lawal Sholaru, who defrauded U.S. citizen David Geobel through Business Email Compromise, was sentenced to six months imprisonment with the option of paying a fine of N100,000 in lieu of serving the jail term.[45] The low sentences are never sufficient to deter cyber criminals from continuing with their activities.

- **Silence**

Many cases of cyber fraud go unreported as the victims choose to be silent. They are either afraid that the lost monies are too small to warrant being reported or that the chances of recovering them are slim. Some are afraid that they themselves could become complicit, or could be accused of being complicit, in the illicit schemes of the fraudsters.

- **Alternative storage medium**

Cryptocurrencies such as Bitcoin are serving as means to conceal illicit monies. The BBC reported that money mules who assisted the Nigerian internet fraudster Olalekan Jacob Ponle ('mrwoodberry' to his Instagram followers) in laundering the millions of dollars that he siphoned off from firms in Chicago, Iowa, Kansas, Michigan, New York and California, had converted the cash to Bitcoin in order to conceal the trail.[46]

Efforts at stemming the menace

- **Cooperation/collaboration**

The U.S. has been in the forefront of efforts to stem cybercrimes and advance fee frauds. As far back as 2001 the U.S. Embassy in Nigeria provided the Interpol Office and Special Fraud Unit of the Nigeria Police Force packages worth $150,000 which consisted of vehicles, computers, large generators, fireproof safes, VHF radios, and computer training for investigators, to enhance their operations.[47] The sharing of intelligence among agencies is yielding results. In May 2019 U.S. law enforcement kick-started Operation reWired, in conjunction with the law enforcement agencies of some other countries, including Nigeria. The cooperation was instrumental in the apprehension of over 80 persons, most of them Nigerians, for varying cybercrimes. It also disrupted the flow of $118 million and led to the recovery of about $3.7 million.[48] A previous collaboration codenamed Operation Wire Wire resulted in the arrest of 74 online fraudsters in 2018.

---

[45] Eniola Ayoola. "Unemployed man bags six months imprisonment for $1,200 internet fraud." NNN, May 20, 2020. https://nnn.ng/unemployed-man-bags-6-months-imprisonment-for-1200-internet-fraud/

[46] Larry Madowo. "How the US caught flashy Nigerian Instagrammers 'with $40m'." BBC News, July 8, 2020. https://www.bbc.com/news/world-africa-53309873

[47] Public Affairs Section of the U.S. Consulate General, Lagos, Nigeria. "U.S. Embassy and Nigerian Police Join Forces to Fight '419' Fraud." Crossroads, vol.8, no.8, August – October 2001, p.2-3.

[48] Abubakar Idris "FBI announces arrest of 167 alleged fraudsters in Nigeria in anti-fraud operation." techcabal, 11 September 2019. https://techcabal.com/2019/09/11/fbi-announces-arrest-of-167-alleged-fraudsters-in-nigeria-in-anti-fraud-operation/

Although the U.S has no formal extradition treaty with the U.A.E, due to the gravity of the cyber frauds allegedly perpetrated by 'Hushpuppi' and 'Woodberry' Abu Dhabi heeded Washington's request to extradite the suspected fraudsters to the U.S for immediate prosecution. The evidence gathered by the FBI is overwhelming. If convicted the Nigerians could spend 20 years in prison in the United States.

- **Arrest and prosecution**

Surveillance, intelligence sharing, and inter-agency cooperation has led to an increase in the arrest and prosecution of culprits. In 2019 law enforcement authorities in the U.S. unsealed a 252-count grand jury indictment, citing conspiracy to defraud and launder money, against 80 people (most of them Nigerians) in a $46 million internet scam.[49] Damilola Otuyalo, who is wanted by the London Metropolitan Police in connection with a £500,000 scam, was arrested by the EFCC following actionable intelligence.[50] A suspected billionaire internet kingpin Onwuzuruke Kingsley Ikenna, aka Nwanta Anayoeze Yonaracha, believed to be a specialist in BEC schemes, was arrested by the EFCC in Umuahia Abia state on January 26, 2020.[51] Damilola Ahmed Adeyeri, who allegedly hacked the official email address of the American Cranes Manufacturing Company and stole $82,570, and his mother Kareem Adeyeri, following a petition by the FBI, are now in EFCC custody.[52]

- **Legislative/judicial/financial reforms**

Through acts of the Nigerian parliament the Economic and Financial Crimes Commission was established in 2003 and the Independent Corrupt Practices Commission in 2009 to investigate and prosecute cases of corruption, including cases of advance fee fraud and cybercrimes. The National Information Technology Development Agency (NITDA) came into being via the NITDA Act 2007. As an arm of the Federal Ministry of Communications it is charged with formulating and driving the national policy on information and communications technology.

To facilitate the prosecution of culprits, the Cybercrime (Prohibition, Prevention, etc) Act of 2015 was enacted. In the past computer-generated evidence was not admissible in Nigerian courts, but with the new Evidence Act 2011, in obvious recognition of advancements in digital communication, computer evidence is now admissible, provided it has not been tampered with.[53] The Central Bank of Nigeria released a Risk-based Cybersecurity Framework and Guidelines

[49] "US charges 80 people, mostly Nigerians, in $46 m internet scam." Aljazeera, August 23, 2019. https://www.aljazeera.com/economy/2019/8/23/us-charges-80-people-mostly-nigerians-in-46m-internet-scam
[50] Dimeji Kayode-Adedeji. "EFCC Foils Man's Attempt To Smuggle In Hard Drug For Detained Son." Premium Times, February 18, 2020. https://www.premiumtimesng.com/regional/ssouth-west/377935-efcc-foils-mans-attempt-to-smuggle-in-hard-drugs-for-detained-son.html
[51] Xavier Ndah. "Suspected Billionaire Internet Fraud Kingpin Arrested in Umuahia." Daily Independent, 5 February 2020. https://www.independent.ng/suspected-billionaire-internet-fraud-kingpin-arrested-in-umuahia/
[52] Odita Sunday and Matthew Ogune. "Mother, son jailed three years for $82,570 internet fraud." The Guardian, 29 January 2020. https://guardian.ng/news/mother-son-jailed-three-years-for-82570-internet-fraud/
[53] Stanley Nnabuo. "Admissibility of Electronic/Computer-Generated Evidence in Nigeria: Concerns and Disputations." Zeeblen Chambers, March 20, 2019. https://zeeblenchambers.com/admissibility-of-electronic-computer-generated-evidence-in-nigeria-concerns-and-disputations/

(effective January 1, 2019) to enable deposit money banks and payment service providers to counter the growing threats that cyber fraudsters pose (Central Bank of Nigeria, 2018).

- **Demolition of the notorious Oluwole market**

This infamous market place in the Balogun area of Lagos state was, for many years, a location where expert forgers of the criminal underworld operated. Anyone could procure all kinds of documents, including national identity cards, driver licenses, international passports of Nigeria and other countries, bank account statements, letter-heads of government offices, and certificates of different kinds, no matter what they wanted to use them for. The market was demolished by the Lagos State Government some years ago.

- **Reformation**

To mould the character of future generation of Nigerians, the EFCC has decided to catch them young. It has inaugurated Integrity Clubs in some schools, one of which is the Excellent Kiddies Montessori Academy in Bwari Abuja.

Further recommendations

The activities of cyber fraudsters are threatening the realization of inclusive sustainable development goals. Justice for victims is often hard to get, as it can take law enforcement officials years to get to the root of the matter. Even in cases where the cyber fraudsters are apprehended it is hard to recover the stolen monies, because they have been used to finance their extravagant lifestyles. We must therefore do everything possible to stem the growing tide of cyber fraud. The following recommendations will further help in addressing the problem.

- Law enforcement officials in Nigeria require relevant ICT training to better perform their tasks. In particular, officials require the latest training in cybercrime investigation and digital forensics. They require well-equipped computer forensic laboratories to be able to correctly analyze cybercrimes involving among other activities electronic intrusions, identity theft and digital impersonation. Training in network investigation, social media investigation, evidence recovery, unbreakable procedures for defending networks, Random Access Memory analysis, is also relevant. Big tech companies such as Microsoft, HP, Cisco, Google, and Facebook can play big roles in this regard.

- To deter cybercrimes the names of convicted perpetrators should be published in major Nigerian newspapers periodically. Before they begin to serve their jail sentences the culprits should be taken to their family houses in their home states to publicly shame them. As Gabriel Ogunjobi has noted: "There should be no sympathy whatsoever for anyone found guilty of perpetuating such selfish crimes."[54]

[54] Gabriel Ogunjobi. "Internet Fraud is Destroying Nigeria – thanks to the Government." African Liberty, September 23, 2019. https://www.africanliberty.org/2019/09/23/internet-fraud-is-a-problem-in-nigeria-but-the-government-is-worse/

- The prevailing situation in Nigeria, where convicted cyber fraudsters get only one, two or three-year jail terms for serious financial crimes, whereas persons convicted of stealing a mobile phone can get jail terms of five or more years, is lamentable. This is a travesty of justice. After serving these minor prison terms the convicts are likely to go back to the illegal activities. Stronger jail sentences will help to deter such crimes.

- Again, while serving their jail sentences, convicted cyber fraudsters should be trained in vocations such as fashion design/tailoring, welding, generator set repair and similar trades, so they can be gainfully employed when they complete their sentences. They should also be given civics lessons so as to disorientate their minds from their past way of life.

- Specialized courts should be established to deal with the rising cases of financial crimes so that justice can be dispensed in a timely manner. Justice delayed, as a popular maxim puts it, is justice denied.

- The moral decadence in Nigeria ought to be addressed. The relevant government agencies (e.g. Ministries of Information and Culture, Youths and Sports, the National Orientation Agency) and the clergies of religious institutions should intensify their effort at inculcating the right values in Nigerians through enlightenment campaigns and sermons. That 'legitimate hard work pays' is the mantra that should be adopted and institutionalized in Nigeria to reawaken the youth and gear their minds towards positive endeavors. The efforts of the many Nigerians who have attained great success at home and abroad through legitimate means could be highlighted to inspire the country's youth.

- Financial institutions and payment service providers should endeavor to carry out credibility checks on their in-house ICT staff, as well as on the staff of contractor firms entrusted with the responsibility of maintaining their critical computer/network infrastructure. In the case of the cyber attack orchestrated on the Union Bank of Nigeria cited earlier in this essay, it was one of the computer technicians doing maintenance work in one of the branches on a part-time basis who enabled the fraudsters to gain access to the database of the bank.

Conclusion

It is the duty of individuals and businesses to take responsibility for their data security. They should put locks on their SIM cards in addition to putting passwords on their mobile handsets and other computer devices. Measures such as the following will help: (i) not using public cybercafés for online financial transactions; (ii) being wary of unsolicited emails and/or opening links and files attached to them; (iii) ensuring that a two-tier authentication step is activated for all of their email and social media accounts; (iv) not logging into public Wi-Fi, which is known to be susceptible to intrusive attacks; (v) not downloading apps or files from untrusted sources; (vi) having very strong antivirus scanners fitted to computer devices to detect and remove malicious malware; and (vii) carrying out regular updates of Android devices to install the latest Google security patches, which will optimize system stability. Furthermore, individuals and businesses should endeavor to use very strong passwords (combinations of letters, figures and symbols) for their email and social media accounts. They should not use the same password for all their accounts.

It has come to light that Yahoo Mail is still susceptible to intrusive attacks. In 2014, for instance, Yahoo suffered monumental data breaches in which the vital information of 500 million users, including names, email addresses, telephone numbers, birth dates, and encrypted passwords, were stolen in what was thought to be the biggest single computer intrusion on a corporate entity of all time.[55] Therefore Yahoo Mail (now owned by Verizon Communications) and other email service providers should take adequate steps to fortify their servers against external attackers.

Indeed, not only email service providers but all tech companies and IT firms need to improve the security of their systems on a regular basis, in view of the growing sophistication of cyber criminals. One way to do this would be to hold regular carefully controlled hacking competitions, in order to identify system weaknesses that cyber criminals could potentially exploit.

References

Central Bank of Nigeria. (2018). Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers. https://www.cbn.gov.ng/Out/2018/BSD/RISK%20BASED%20CYBERSECURITY%20FRAMEWORK%20FINAL.pdf

Palo Alto Networks. (2018). Silverterrier: The Rise of Nigerian Business Email Compromise. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/whitepapers/unit42-silverterrier-rise-of-nigerian-business-email-compromise

[55] Nicole Perlroth. "Yahoo Says Hackers Stole Data on 500 Million Users in 2014." The New York Times, September 22, 2016. https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html