Research Article

Received: 8 March 2022 / Accepted: 25 April 2022 / Published: 5 May 2022

Cybercrime in Ghana and Victims Accounts

Daniel Ennin

M.Phil. Graduate,
Department of Sociology,
University of Ghana, Legon, Ghana

Ronald Osei Mensah

Centre for Languages and Liberal Studies,
Takoradi Technical University, P. O. Box 256,
Takoradi, Western Region, Ghana

DOI: https://doi.org/10.36941/mjss-2022-0019

Abstract

The main thrust of the study was to examine how cybercrime victims are being lured into virtual space by scammers and later swindled. Qualitative research method was advanced to explore the dynamics of cybercrime activities in Ghana. Secondary data were sourced from the Criminal Investigation Department of the Ghana Police Service. Purposive sampling technique was outlined to engage with the respondents. Structured interview guide was considered as a data collection instrument. In the data analysis, each of the in-depth interviews was transcribed as soon as the information was gathered and developed into codes. Six (6) internet victims took part in the study. The investigation revealed that people become internet victims as a result of unrealistic profit ventures, online romance, raffle schemes, America green card lottery and rent apartment deals. Out of the six cases, only one culprit was imprisoned and even the approach was conventional policing strategy considering the volatile nature of the cybercrime related offences. It was concluded from the discussions that the National Commission for Civic Education (NCCE) should create public awareness about the social and economic consequences of cybercrime activities in the country. The education should further emphasize on the social engineering tactics employed by the conmen to dupe their client on the internet.

Key words: *Cybercrime, Electronic media, Fraudster, Police, Social engineering, Victims accounts*

1. Introduction

Information and Communication Technology (ICT) has become important tools in today's knowledge-based society. As a result, governments and commercial establishments are increasingly relying on Internet-worked information systems to carry out services that are critical to the administrative and business successes. Technology has in many ways changed the way human beings interact with their environment to the extent that it is impossible at the moment to imagine a world without the benefits of technology and digital innovations.

Manuel Castells (2000) revealed that the world is passing from the industrial age into the

information age. This historical change is brought about by the advent of information technology and traditional social morphology is withering away. Ennin and Mensah (2019) also espoused that the network society has correspondingly created a single platform for instantaneous encounters between spatially distant actors. Social media networking sites like Facebook, WhatsApp, Youtube, Instagram, Twitter, and many others allow us to stay in touch with our friends and family to share ideas around the world while streaming media entertain individuals 24 hours a day on demand.

One thing that remains a threat to the digital society, however, is the proliferation of fraudulent activities and some schools of thought wonder whether society is benefiting from the upsurge and sophisticated technology which brings with its numerous problems related to huge financial resources to address (Daily Graphic, April 22, 2021:24). While there is no commonly established definition of the concept, it basically refers to any criminal act dealing with computers and the internet. Suman, Srivastava and Pandit (2014) defined cybercrime as "unlawful acts wherein the computer is either a tool or a target for criminal related offences". It means that on one hand, a computer may be the object of the crime when there is theft of computer hardware, or software. Computer may be the subject of a crime when it is used as an instrument to commit conventional crimes such as fraud, theft, extortion, or emerging crimes like denial-of-service attack, identity theft, child pornography, copyright infringement and email scam.

The role of ICT in an emerging economy like Ghana has been widely recognized at various levels. The recognition is reflected in actions such as the development and deployment of national ICT infrastructures, institutional and regulatory framework for smooth internet penetration. It is not surprising that Ghana was the first country in Sub-Saharan Africa that Google has mapped to set up its Artificial Intelligence headquarters. The Oracle Corporation has also joined the fray by setting up a technology-enabled start-ups in Accra for entrepreneurs and innovators worldwide to boost our digital economy (Daily Graphic, 05/04/19, Page 24). However, there has been a steady increase in cybercrime incidence in the country. The victims, in most cases, were defrauded through romance fraud, investment advanced fee payment, social media impersonation and Automated Teller Machine (ATM) card among others (Ennin & Mensah, 2018). In the 5th April, 2018 edition of the Daily Graphic published that cybercrime constituted about 82 percent of fraud related cases in the country. Figures available at the Cybercrime Unit of the Criminal Investigation Department (CID) of the Ghana Police Service revealed that Ghana lost an amount of $ 19.8 million through fraudulent activities in 2020 as against $ 11 million in the previous year, (Ghanaian Times Report, 24/11/2021). Additionally, the Unit recovered $ 101,000, six cars and three plots of land bought from the proceeds of internet fraud. These revelations stress the point that cybercrime is gaining notoriety within the borders of Ghana. What is currently lacking is the fact that there is limited information on the account of cybercrime victims in the country. The study therefore aimed at exploring the views of the victims so that their ordeals can guide our behavior in the virtual society.

2. The Purpose of the Study

The general objective of the study is to examine how cybercrime victims are being lured into virtual space by scammers and later swindled.

3. Research Questions

The following research questions guided the study:

How do the victims and the offenders come together in the virtual society?

What motivated the victim to accept fraudster's proposals on the internet without physical encounter?

What are the needed recommendations to minimize online crime?

4. Significance of the Study

The study hoped to provide the readers an understanding of cybercrime peril on the accounts of the victim's experiences and also raising awareness about the various trends' cybercriminals explore to dupe their clients online. It will serve as a reference material for government, national security architects and other stakeholders in the policy formulation and strategies to fight the menace. Given that there is a little research on internet scams, the study seeks to add to the body of knowledge.

5. Literature Review

5.1 Internet Crime Complaint Centre (IC3) Annual Report.

The wider reach of the internet has facilitated the transmission of information at a relatively cheaper rate and inadvertently exposed the entire world into a 'highly criminogenic' environment (Chu et al, 2010). Cyber space brings together offenders and victims located in different time zones to conduct businesses within a single platform and this unfolding event has become a social scourge for many countries and international communities to deal with.

To tackle this emerging crime, the United States of America in the year 2000 set up an Internet Crime Complaint Centre (IC3) aimed at receiving complaints of internet crime. These complaints address a wide array of internet scams that affect victims across the globe. Information gathered is analyzed and disseminated for investigative and intelligence purposes, and also evaluated to promote public awareness. A total of 5,679,259 complaints have been reported to the Centre since its inception. In the year 2020, the IC3 received 791,790 complaints with reported losses exceeding $4.1 billion from the victims. The figure represents a 69% increase in total complaints from the 2019 report.

The IC3 (2020) Annual Report highlighted some recurring patterns of fraud complained of by the victims. These are credit card fraud, identity theft, general merchandise and auction fraud, cyber pornography and obscenity, phishing and pharming, advance fee fraud, hacking, cyber-terrorism, and botnet. These online fraud activities are expatiate below:

5.2 Credit Card Fraud

Credit card fraud is one of the biggest challenges to business establishments in the 21st century. It occurs when the person uses another individual's credit card for personal reasons while the owner of the card is not aware that the card is being used, Schmalleger and Pittaro (2009). The authors further explained that credit card fraud is committed through an act of deception, illegal use of people's accounts for personal gain, and misrepresentation of account information to obtain goods or services. According to the Eurobarometer survey conducted in 2013 which covered more than 27000 people in all member states revealed that 76% agreed to the assertion that the risk of becoming a credit card fraud victim has increased over the years. This destructive impact hampers the digital economy and many people may not take full advantage of all the possibilities the internet brings to individuals in the postmodern world.

5.3 Identity Theft

Identity theft begins when someone takes your personally identifiable information such as your name, social security number, date of birth, and residential or office address without your knowledge for financial gain (Schmalleger & Pittaro, 2009). There are different types of schemes in which identity criminals' use. These ranged from technical and social engineering strategies. Social engineering occurs when someone either in person, over the telephone or computer, uses means to deceive someone else to divulge sensitive information. Usually, the social engineer has firsthand

information about the person and that pushes the victim to believe that he is at the right place. In the same vein, criminals who are ICT inclined can also scam the internet and redirect people's electronic mail accounts without their consent.

5.4 General Merchandise and Auctions Fraud

According to the IC3 Annual Report of 2013, auction fraud involves the misrepresentation of a product advertised for sale through the internet. In an attempt to make the deal appear legitimate, the criminal often instructs the victim to send full or partial payment to a third-party agent via wire transfer and to fax their receipt to the seller as a proof of payment. Once payment is made, the criminal pockets the money and the victim receives an item that is less valuable than what he/she was promised or in the worst-case scenario receives nothing at all.

5.5 Cyber Pornography and Obscenity

These are activities that breach the laws on obscenity and decency. Sexually explicit images and video are accessible online and it constitutes a multibillion-dollar industry (Edelman, 2009). Though these materials may not be illegal, the internet has fostered the growth of a wide range of deviant sexual behaviors and Olayemi (2014) reiterated that the internet has become a conduit for sexual predators to solicit illicit sexual services in the real world.

5.6 Phishing and Pharming

The explosive growth of online fraud has made 'phishing', and to a lesser extent 'pharming' part of nearly every Internet user's vocabulary in recent times (Olowu, 2009). Phishing and pharming are two popular forms of fraud aimed at luring victims to believe that they are at a trusted web site but in the real terms they have been enticed to a bogus web site with the intent to steal their identity and drain their financial resources (Adeniran, 2008). Every day millions of emails are sent across the globe, millions of web pages are accessed to gather information, and millions of people use online sites to transact business. We strive to trust the systems that are in place to deliver our e-mail messages and to route us to the proper web server. Unfortunately, growing cyber-thieves are using this same system to manipulate us and steal our private information.

5.7 Advance Fee Fraud

This scam is purported to have originated from Nigeria where an individual pays money to someone in anticipation of receiving something valuable in return but in the end the person will be swindled. The amount involved usually covers duty and other administrative charges to facilitate the transaction (Cukier et al, 2007). Warner (2011) explained that the scheme known in pre-internet incarnation as "419" began after the collapse of World oil prices during the 1990s which left the Nigeria oil-dependent economy shriveled. The teaming unemployed youth began to garner a culture of deception by posting pen pals to make a living. Adogame (2009) further emphasizes that the internet and email technology have changed the face, pace and fate of advanced fees fraud without geographical limitations.

5.8 Hacking

Defined broadly, hackers are individuals with a profound interest in computer technology who utilize their knowledge to access computer systems for malicious or unethical purposes (Holt & Blevins, 2007). Though hackers engage in and develop cyber security tools, individuals view hacking in its malicious context because of the economic and personal harm (Furnell, 2002). In fact, malicious

hacking is often tied to the creation and distribution of pirated softwares that can automate attacks against computer systems (Chu et al., 2010). These programs can disrupt e-mail operations, and at times damage private files in the computer.

5.9 Cyber-Terrorism

Cyber-terrorism is the act of using internet to cause psychological harm to, or inciting physical harm against others, thereby breaking the laws pertaining to the protection of the person such as hate speech and the distribution of injurious materials (Olayemi, 2014). Perhaps the simplest description is that ideological concerns rather than economic or political considerations motivate the attack which intends to cause grave harm.

5.10 Botnet

A defining feature of today's cybercrime landscape is the extensive use of computer tools across a wide range of cyber-offences. Botnets consist of a network of interconnected, remote-controlled computers generally infected with malicious software (UNODC, 2013:32). The legitimate owner of such a system may not be aware of the fact of infection. These enable cyber criminals to send spam email or take part in the distributed denial of service attack (DDos). Such infected computers are often called "robot" or "bot" computers. When several computers are affected with a category of malware, they can be simultaneously controlled from a single command server system (CSS) to perpetuate crime.

Drawing from the literature, it is significant to note that cybercrime presents a daunting challenge to all facets of human endeavors because there is no boundary in cyberspace to limit individual's behavior. As a result, more and more criminals are exploiting the speed and conveniences to commit various crimes. The IC3 annual reports have revealed that fraudsters adopted both social engineering tactics and technical know-how to dupe the unsuspecting victims. The technical fraudsters are the IT specialists who have gone so much into IT programming and computer security professionals. They exploit the internet capabilities to hack into individuals' electronic accounts. The non-technical people are criminals in the real world who have fair ideas about IT systems and they use it to facilitate their internet fraud operations. Singh and Alshammari (2020), argued that it is difficult to punish cyber criminals due to the abstract nature of the internet and the complications involved in getting to the root of the origin of cybercrime. This creates a 'safe haven' for the perpetrators to continue their nefarious acts.

6. Methodology

The exploratory research design was advanced to examine the dynamics of cybercrime activities from the victims' perspectives. The study made use of qualitative method. The general objective of the study was to explore how victims are being lured into the virtual world and later swindled. In view of this, the researcher gathered detailed information about the cybercrime victims from the Criminal Investigation Department (CID) of the Ghana Police Service and used the report to contact some of the respondents.

Purposive sampling technique was used to engage with the participants. Six (6) respondents participated in the study. The internet fraud victims were difficult to reach. The information gathered from the CID revealed that victims are usually high-profile individuals who cannot cope with the embarrassment of people knowing that they have been duped online. Moreover, expatriates who wanted to pursue the case are being advised by their ambassadors/representatives to pull out for lack of confidence in the Ghanaian legal system which has been tainted with alleged corrupt practices and undue delay of cases. These factors might have accounted for the low response. However, Kumekpor (2002) argues that it is not always the case in research that certain characteristics are distributed

uniformly in the universe, especially hard to reach population. In such cases, it is more appropriate to identify units of the universe which satisfies the characteristics of the phenomenon under investigation. Given this, the researcher purposely selected participants who had the required knowledge that can influence the research outcomes. Bryman (2008) reiterated that sample size is not always drawn to estimate the distribution of certain traits within the population but also to gain an in-depth understanding of the social phenomenon which is unfolding.

In the data analysis, each of the in-depth interviews was transcribed as soon as the interview ended. This approach helped the investigator to identify new issues which fed into the subsequent interviews. Through the readings, codes were identified and it involved ideas and opinions shared by the respondents. All the colloquial expressions made by the participants were preserved. These words reflected the participant's understanding of internet fraud and it also enhanced the analysis. Comparison as an analytical tool was used to stimulate thinking about the responses elicited from the various categories. And thus, thematic areas emerged. The final aspect was the 'art' of the qualitative analysis in which the researcher interpreted the lived experiences of the respondents to address the research objective. Ethical considerations such as privacy, anonymity and confidentiality of the participants were adhered to by using pseudonyms to protect the respondent's identity.

7. Presentation and Discussions of Findings

The internet has become a double-edged sword of providing opportunities for the individuals and organizations and also bringing with it increased information security risks and challenges. The emergence of cybercrime activities in Ghana has occasioned financial losses to many individuals and organizations. This worrisome trend motivated the researcher to get in touch with some of the cybercrime victims to share their ordeals to serve as guide for online transactions. However, as the researcher did indicate in the earlier submission, victims were hard-to-reach population because of their status in the society and also lack of confidence in the criminal justice system accounted for the low response rate. This notwithstanding, some fascinating stories emerged from the interview conducted which showed the varying approaches being used by the scammers to outwit victims. These social engineering machinations include; abnormal profitable ventures, romance, "vehicle marked for sale", U.S Green Card lottery, and rent apartment scams. The excerpts from the interviews are expatiate below:

7.1 Abnormal Profitable ventures

By nature, everyone is seeking the best for him/herself. As a result, criminals put forward some colossal business proposals or transactions that look like manna falling from heaven. This brings about the temptation of people keeping the perceived business proposal from others in order to make maximum gain out of it. Madam Mina fell into this ploy. She shared her experience with the researcher from the following narrative.

> *It's unfortunate that I was a victim to this type of fraud. I checked my email and I received a message from a man called Prince. He wrote in my email portal and he said; Mina, how are you? Please forgive me, my phone got missing and I lost all my contacts that is why you have not heard from me since I returned to Germany. I discovered your email address from one of my old dairies and I decided to say hello to you and this is my German private number (I burnt those materials recently so I can't remember the number but it started like +49201…. The victim said).*

Madam Mina said she tried to figure out the person after reading the message but the name was not familiar. Upon several thoughts she considered that the man could be one of her numerous customers. She called Mr. Prince (the scammer) on his cell phone but as they were conversing the voice sounded strange and that created her doubt. So, Mina asked again; who are you? The conversation continuous;

Then Prince responded in Akan dialect "ahhhh, se won kae me a ebeye me yeea" (literally, I will be surprised if you don't recognize me). So, I accepted that he was a true friend. Since then, we communicated a lot on phone, Facebook and WhatsApp. Later on, he called me and said, Mina, business has been slow, things are not well so I have stopped my previous work, and I am now working with white men who are operating in the tourism industry. We have even decided to penetrate into the Ghana tourism industry. Then I said that could be a wonderful idea because we have so many tourism sites and places in Ghana that we have not touched on.

He said in the conversation, yeah, that is true but there is a product my people [white men] need so if you can get this product for us, you are going to make it. Initially, we ordered the product from Zimbabwe but now they have stopped supplying us. Then I said, what is the name of the product? He said the name of the product is 'Fishing Chamdize'. I was confused because I have been into the fishing industry for quite a number of years but I haven't come across such a product. I tried to find the name of the product on the internet but I didn't get it. My husband is a nautical engineer and I contacted him but he couldn't find it. I informed him that the product is not on the Ghanaian market. He replied that I should contact one Mr. Owusu at Koforidua (Regional capital), and he will show me the sample of the product. I called Mr. Owusu by cell phone and we agreed to meet on the weekend (that was Saturday) at Koforidua. When the time was approaching, Mr. Owusu called and told me that because of his busy schedules, we should rather change the venue to Aburi (near Accra), which I agreed. Finally, we met somewhere at Aburi Senior High school. He showed me a sample of the product and it was labeled 'Fishing Chamdize'. Then he said, he can supply me only 20 cartons at the moment. Each carton contained 30 bottles and the unit price was Gh¢15. So, the total cost for the first consignment would be Gh¢9000.

On her return to Accra, Madam Mina called the supposed friend (Prince) in Germany and briefed him about the transaction. Prince told her that his people need the products badly so Mina should try and export the first consignment for the meantime. The value of the first consignment would be $32000. Mina called Mr. Owusu and he delivered the goods to her in Accra. She made a part payment with the tune of Gh¢5000 and promised to settle the balance within three days. Coincidentally, Madam Mina went to the Evergreen Mall at Tema (a suburb of Accra) on the same day to purchase a few items, and she discovered a similar bottle labeled 'Vinegar', so she became suspicious. She bought one of the 'Vinegar' and compared it with the 'Fishing Chamdize' and she found out that the two products are the same. It was at this stage she realized that she had been duped. She started calling the scammers (i.e Mr. Owusu and Mr. Prince) but they sometimes switched off their phones or at times, it rang and nobody answered. What followed was the strategy she adapted to arrest the culprits.

I sat for a while and I prayed to God that he should give me wisdom to deal with these criminals and indeed the Lord showed me the way. I sent a text message to Mr. Owusu and I said, please, your balance is ready but I have been trying to reach you on your cell phone and it wasn't going true. Within a short time, he replied, telling me he is busy and that he will send his son to receive the balance on his behalf.

When I received the information from him, I drove to the Airport Police Station in Accra and lodged a complaint. I narrated the whole story to the police officers and they were shocked. Later, his son called, that I should meet him around Trasaco Villa on the Tema MotorWay. The Police Station Officer detailed three undercover officers to accompany me. So, we drove to the designated place. I got out from my car and I met the guy (son), while I was paying the remaining amount, the police officers came out from their vehicle and arrested him. In his confession statement, the culprit admitted he was part of the syndicate and through the effort of the police, Mr. Owusu was also arrested. Finally, I was able to get my money intact and the police took over the case. The investigation revealed that all the guys were living in Tema.

From the text, the fraudster used a receptive expression like, "I will be surprised if you don't recognize me" to win the trust of the victim. The narrative also revealed that the scammer knew the

victim very well and thus, when Madam Mina was doubtful about Prince credibility, he convinced Mina to believe that they share certain aspirations in common. So, she 'accepted him as a true friend'. After initiating the online friendship over days, Mr. Prince enticed Madam Mina by introducing a promising business proposal as he put it, 'there is a product my people need badly so if you can get this product for us, you are going to make it'. The prime objective of every businessman/businesswoman is profit maximization which moved Mina to pursue the $32000 deal without cross-checking the social profile of her business partner and later she was defrauded.

7.2 Romance fraud

Perpetrators use the promise of love or romance to entice and manipulate online victims. A perpetrator scouts the internet for victims and often finds them in chat rooms, dating sites and other social media handles. The conmen seduce individuals with small gifts, poetry, claims of common interest or a promise of constant companionship. Once the scammer gains the trust of the victim, he will then begin to request for money, asking the victim to receive a package or seeking other favors. This crime not only affects the victims financially but there are emotional and mental implications. Ama (victim) elucidated how she got herself into online romance and being swindled.

> *It happened when I received a message from a man called Julius living abroad on my Facebook account. I read the message and the person wrote, O' you are beautiful, responsible and you don't look like the classic girls in the U.K. So, I want to be your friend and I accepted his request. That day, we chatted for a while and I logged off. The following day he requested my phone number. Initially, I did not want to give my number to him but upon further appeal, I changed my stand, and I said let me give him a trial.*

According to Ama, they became friends for almost three months and later Julius expressed his desire to marry her. Ama accepted the proposal and she admitted that though the two did not meet physically, they were living as husband and wife. The gentleman introduced her on the phone to one of his uncles who resides in Accra. The said uncle used to call Ama and even promised to visit her at home. After Julius wooed the trust of Ama, he took the opportunity to chip in some business proposal and later he defrauded the lady. She continued with the narrative to authenticate this assertion;

> *One day, I got a call from Julius (the supposed lover) that he wants to ship some items including three accident cars and other home appliances to Ghana but the price of the freight is quite expensive, so I should help him to finance the shipment process. Fortunately for him, that month I received my two years' salary arrears and I agreed to help. He promised to pay my money and share the profit that will accrue from the transaction. Also, he has documented one of the vehicles in my name as part of his commitment toward the relationship. I was convinced that Julius was a nice man and I transferred $1800 into his foreign account. The next day, I tried to find out whether he had received the money but when I dialed the number, I got feedback that his phone was switched off. I further sent him an email and Facebook messages and yet he did not respond. I called his uncle's phone number too and it was off. I narrated the story to my friend Agnes and she told me the deal could be a '419' scam.*
>
> *I reported the matter to the Teshie Police Officers. Subsequent investigation proved that all the emails, text messages, and the phone numbers were originated from Ghana when the culprit claimed to be living in the United Kingdom. However, the police could not arrest the offenders and that ended the matter.*

Romance or 'sweetheart' scams are emotionally devastating types of fraud because dating websites allow fraudsters to cast their nets wider and disappear more easily than the traditional scams. The romance component of the online scam acts as an inducement to lure the victim before committing other criminal related offences such as financial reward. The narrative revealed that respondent succumbed to the perpetrator's request after he gradually prepared her mind that they

are married couples as she admitted; 'though we did not meet physically but we were living like husband and wife and I thought it wise to extend my financial support to him but little did I know that he is a fraudster'.

7.3 Vehicle marked "for sale" scam

Under this type of fraud, an attempt by an individual to sell his/her vehicle could make the person end up being defrauded. The question is how does a vendor of a vehicle become an online victim? For every sale invitation is accompanied by the seller's telephone number and Dolin became victim to that online marketing strategy and she explained;

> *I was selling my Toyota Camry (that is 2008 model), so I pasted my contact on the rear screen. One day I got stuck in traffic and had a call from a guy called Ayesi, and that he is interested in the vehicle I'm selling. I directed him to my house and he inspected the car. Then he told me that his brother who is outside the country will make the payment, and he is going to give out my mobile number to him. I said, alright. An hour later, I received an international call and the caller introduced himself as Mr. Asibey, a Ghanaian domiciled in the US and a senior brother to Ayesi who has expressed interest in buying my car. We negotiated the price of the vehicle and finally settled on Gh¢37,500. Though my initial target was Gh¢30,000, and I considered this as a great deal. He promised to pay the amount the next day.*
>
> *Thereafter, he called again and confirmed his desire to buy the vehicle but due to one reason or the other he does not want to pay the money to Ayesi, rather, he wants to send the money directly to me. Also, to avoid the payment of commission on money transfer, the cash would be concealed in a luggage and delivered through the courier service, registered in my name. Then I said okay. Four days later, he signaled to me that the luggage has been sent to Fedex Courier Service and the delivery charges have been added to my money so I should pay for the cost of the delivery as well. Subsequently, I received another call from Fedex agent purported to be working at 'AFGO' terminal at the Kotoka International Airport and that I have a parcel with them and I should pay a service charge of Gh¢5,600 into their MTN Mobile Money Transfer Outlet to enable them deliver the goods. After paying the said amount, all the three people in this syndicate switched off their mobile phones. I tried, tried, tried but all effort proved futile. So, in short, I went to the Criminal Investigation Department at the Police Headquarters and lodged a complaint but I got feedback that the people were scammers.*

Ghana is progressively becoming a nation of technological addicts. The addiction has manifested in the way we buy and sell our properties online. In the online business, everyone wants to sell for the best price, and invariably wants the whole process to be quick and stress free. However, Madam Dolin could not benefit from this electronic base marketing as she attempted to use mobile phone applications to sell her private vehicle. The text has revealed that scammers worked together to create a 'fraud ring' and shared data on how best to scam the woman. The first accomplice (Ayesi) interacted with the victim in the real world but the woman did not go to find out where he lives. Police could have been using the information to trace the criminal when the untoward happened. After Mr. Ayesi succeeded in convincing the victim, he handed her over to the main offender (Asibey) to reassure her that he would buy the vehicle. The third collaborator defamed the reputation of Fedex Courier Service to defraud the victim. The operation was successful because the scammers hypnotized the victim with the profit margin as she reiterated; 'though my initial target was Gh¢30,000, but I considered this Gh¢37,500 as a great deal'.

7.4 Mobile Phone scam

With regards to the Ghana telecommunication industry, customers are able to choose from multiple service providers and actively exercise their rights of switching from one mobile telecom service to another. This development has created fierce competition among the telecommunication operators

to market their services to the greater number of people and increase their subscriber base. In order to achieve this feat, these companies adopt various methods to reach out to many individuals and persuade them to join their network brand. One of the methods employed is by offering reward packages to their loyal customers. On the other hand, scammers also work behind this idea to rip-off subscribers. They circulate text messages that falsely indicate that the receiver has emerged as a winner in the promotion being run by the network provider. To redeem the prize, the victim would be asked to buy a recharge card and send the pin codes to the customized number as a prerequisite for the processing of the reward. The victim would be further promised of refunding the credit used when the process is over. It is interesting to note that the fraudsters will continue to create another condition for the potential winner until the person becomes aware that she has been defrauded.

Beatrice, a 21-year-old university student was conned under this pretext of falsehood and she volunteered to express her ordeal to the researcher;

> *I received a text message on my MTN mobile phone indicating that I had won Gh¢12,000 from the MTN Mobile money promotion. When I received the message, I was happy. The text further required that I should send Gh¢1,000 worth of credit to MTN mobile number before the code could be released to me to withdraw the money.*

Madam Beatrice said she called the mobile number and she noticed that it was one Mr. Fordjor who claimed to be MTN promotion branch manager in Accra. She sent the MTN recharge cards to the supposed Manager. After receiving the recharge cards, he further proposed to have an affair with her before releasing the code. Immediately, something just trickled her mind that the man she is dealing with could be a fraudster. She reported the story to the Odokor Police Station (a suburb of Accra). She continued to explain how the event unfolded leading to the arrest of the perpetrator.

> *The police advised me, and I told him that because of my busy schedules, it would not be possible for me to travel to Kasoa (suburb of Accra) and I pleaded with him to rather visit me at Odorkor, and he agreed. So the next day he called me that he had set off and he described the attire he was wearing for easy identification.*
>
> *My father, together with some plain cloth police personnel from the Odorkor Police Station came around and monitored the fraudster. He alighted at the Odorkor Main bus stop. He called my phone and I responded. So we finally met. As we shook hands, the police officers arrested and handcuffed the fraudster and sent him to the police station for interrogation.*
>
> *At the police station, he mentioned his name as Kingsley, and denied being called Mr. Fordjor. Consequently, he was arraigned before Cocoa Affairs Circuit Court and he was sentenced to 18 months imprisonment with hard labor.*

The narrative shows among other things that police officers were proactive to contain the situation. Unraveling the wrongdoing in cyberspace requires more than being an expert in computer programming or encryption techniques. Someone must have firsthand information about the case, marshaling the needed profiling to move the investigation forward. The narrative pointed to the fact that the victim did well by providing the right information to the police. Police further acted upon the information and advised the lady to accept his 'sexual request' which led to the scammer's arrest.

7.5 America Green Card Lottery scam

Every year, the American government allocates Green Card Visas to individuals who are randomly selected from countries with low rates of immigration record to the United States. The exercise helps applicants acquire permanent residential status. There is a mad rush of Ghanaians exploring this opportunity but scammers have created dubious websites, posing as U.S officials and extorting money from the applicants. Joseph became a victim to the US Green Card visa application and what

follows is the interview granted to the researcher.

> *One day I was browsing on the internet and a message pop up at my home page. I read over and it was an advert concerning the US Green Card lottery scheme. When I clicked on the message, it was routed into another website called usafis.org. At first, I was uncertain to respond to their request but I received another message from officers claiming to be an Immigration expert from the US Homeland Security Department and that they have considered my application, so I should complete the registration and forward my personal details to them. This motivated me to log into the usafis website again and started the registration process.*

The victim paid a registration fee of $1500 through credit card transfer. This package will allow his nuclear family to join him in the US after he has won the lottery. However, Mr. Joseph could not realize this dream and expressed his sentiment. The story continued;

> *After the payment I did not hear from them. So I asked somebody who had an idea about this America Green Card and he told me that the process does not start the period I had started, rather it would be later part of the year. So, from that time I got to know that the people were scammers. Though I am a police officer, there was little I could do to retrieve my money. The mere fact that the person is holding a phone or laptop and walking on the street does not necessarily mean he has committed cybercrime offence and therefore should be arrested.*

Due to the advancement in technology, cybercrime is now easier to commit. Getting internet connectivity is very simple, so all that the criminal needs is a phone or any eligible device which can be hooked to the internet. This has made cybercrime difficult to detect because scammers may be sitting comfortably in their homes or public places of convenience where exchanging pleasantries with law enforcement officers, and yet he is duping people with huge sums of money. In view of this, the victim echoed the challenge cybercrime poses to even security personnel as he pointed out "though I am a police officer, there was little I could do to retrieve my money. The mere fact that the person is holding a phone or laptop and parading on the street does not necessarily mean he has committed cybercrime and therefore must be arrested".

7.6 Rent apartment scam

The proliferation of internet penetration has opened the country into online trading platforms which have empowered the average Ghanaian to transact various business operations. Customers are increasingly turning to these websites such as OLX.com, Tonaton,com, Jiji.com.gh, Jumia, Kiki and other free online classifieds to purchase goods thereby cutting middlemen or agents out of the transaction. Unfortunately, this has also given scammers a new avenue to find victims who are looking for good deals. 'Culture' had been a victim to this type of fraud in an attempt to hire an apartment via the internet and he spoke to the investigator;

> *I became an internet victim when I was looking for an apartment. Because of the high percentage being charged by the 'rent agents' (i.e middlemen), I decided to look for the apartment on the internet. So I registered with OLX.com; an internet trading portal. I posted on the platform that I am looking for a single room self-contained for rent. I also added my contact details. Three days later, I had a call from one Mr. Quaye, introduced himself as a landlord and he discovered my details on the OLX website, and so if I could come to Alhaji Tabora No. 3, (a suburb of Accra) to have a look at the room I am looking for. I met the man in the supposed house, negotiated the price and finally settled on Gh¢100 per month. Then he said, I need this money to pay my children's school fees that is why I have reduced the amount, so I should pay four years' advance fee. Considering the serene environment, the amount was quite cheap. The following day, my junior brother accompanied me to the house and I paid Gh¢4000 out of 4800 to the landlord. He acknowledged with the receipt to indicate that I have paid such an amount. Then he said the keys and the tenancy agreement would be ready on Sunday (that is four days after the payment). Later on, I called to find out whether the documents were ready and unfortunately his mobile phone was switched-off.*

Linking the expression to his body language, the investigator further probed to find out what happened subsequently and he continued.

> *So on weekend, I went to the house and met a fair lady. She asked me, gentleman how may l help you? I narrated the story to her and she said; this is my house and I have only one tenant. She pauses, scratched her head and said; O' the '419' people have been using my house to bait innocent victims, and this is about fourth incidence. She also tried the supposed landlord telephone number but it was unreachable. She led me to the 'Hong Kong' Police Station and I lodged a complaint but the officers failed to arrest the perpetrator.*

Ghana's prospects of becoming a cashless economy could be undermined by internet fraudsters. This is informed by the fact that when people's behavior in the superhighway cannot be protected by law enforcement agencies, it creates mistrust in the system. Consequently, the government could lose revenue mobilization from the online classified agencies because customers will be hesitant to patronize services in cyberspace.

8. The Baits Explored by the Conmen

Understanding who the criminal is likely to target can assist in taking preemptive actions to forewarn and prepare for all forms of internet fraud. Intelligent criminals always target people whose circumstances are loaded with some form of vulnerability. Internet users have to be on guard against all forms of solicitation that come from strangers with very enticing dividends. Usually, they gain some profit at the initial stage of the transaction. This success takes them deeper into the fraud-ring as they build more relationships with the scammer and become embroiled with financial entanglement out of which only the perpetrator will gain. Information gathered indicated that people become victims to the internet fraudsters because of unrealistic benefits, and Mina for instance, developed interest to stay in the business as a result of $32,000 profit margin. Culture also admitted, "Considering the serene environment, the amount was quite cheap" and Beatrice on the other hand confessed; "though my initial target was GH¢30,000, so I considered this GH¢37,500 as a great deal". Since the victims were drawn from the police sources, the researcher wanted to find out the outcome of the cases but only one offender out of the six cases was successfully put on trial and imprisoned. So, when the question was put to Mina about the police reaction and response, she responded;

> *Even though I got my money, I was quite disappointed because the police could not pursue the case further and I didn't know why they stopped the prosecution. Because I was insisting that the fraudsters should be jailed to serve as a warning to others. When I contacted the officer in charge of the case, he said, ohh, Mina, thank God you were able to retrieve your money. Pursuing this case in court would be a herculean task.*

Ama added;

> *I reported the matter to the Teshie Police Officers. Subsequent investigation proved that all the emails, text messages, and the phone numbers originated from Ghana when the culprit claimed to be living in the United Kingdom. However, the police could not arrest the offenders and that concluded the case.*

Dolin also re-echoed the same outcome and she said;

> *So, in short, I went to the CID headquarters and lodged a complaint but later I got feedback from the officers that the people were scammers and since their mobile phones were not active, it would be very difficult to track them.*

Joseph admitted, "Though I am a police officer, there was little I could do to retrieve my money".

Culture could not hide his frustration and he explained;

> *The police investigation was like go and come, go and come. I didn't see any serious outcome. Even the CID man who was handling the case told me that it would be very difficult to apprehend the fraudster since I didn't know where the man was living. And also, he is not a magician to locate the man but I should pray that one day I will meet him somewhere. However, I suggested to him to contact the telecom company and cross-check his contact details but the investigator further said it will be a very difficult task. So later I stopped going to the police station because going there every day was like, I am wasting my precious time and money.*

It was only Beatrice's case that the police were able to arrest the culprit but the approach was conventional policing tactics considering the volatile nature of the cybercrime related offences, information can be distorted within milliseconds.

9. Conclusion and Recommendation

Unlike nuclear energy, electricity, or explosives all of which pose clear physical danger, computer systems in everyday life pose no intrinsic threat to our body make-ups. They cannot make us gasp for breath or cry in pain yet they may conjure forces which can cause grave social, economic and political harm in our quest to achieve better height. Our interdependence on the internet in research findings, communications, financial transactions and other social activities push us into cyber threats.

The study has shown that abnormal profit margins enticed victims to commit themselves to the various online deals. It is further revealed Ghana Police Service is lacking the technological capabilities to deal with the tempo of cybercrime threat in the country due to the failure of the organization resistant to change in structure and practices. Therefore, it behooves on individuals and corporate entities to fashion out ways of providing alternative security measures for their online transactions. To achieve this protection, extra vigilance and due diligence should be a hall mark before people commit themselves into electronic businesses. Besides, the Government through the National Commission for Civic Education (NCCE) should create public awareness about the nature, magnitude, social and economic consequences of cybercrime activities in the country. The education should be emphasized on the social engineering machinations used by the fraudster to defraud people in cyberspace.

10. Acknowledgements

This article has its roots from the M.Phil. thesis of the corresponding author and our sincere gratitude go to Prof. Chris Abotchie of blessed memory, Prof. Dan-Bright S. Dzorgbo and the Ghana Police Service for the guidance and information shared through its completion.

References

Abbey, E, E. (2018). "Victims Lose $95m to cybercrime". *Daily Graphic, December 10, pp.81*

Adeniran, A., I. (2008). The Internet and Emergence of Yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology, 2(2), 368-381*

Adogame, A. (2009). 'The 419 code as Business Unusual: Youth and the Unfolding of the Advanced Fee Fraud Online Discourse'. *Asian Journal of Social Sciences, Vol. 37. Pp. 551-573.*

Bokpe, S. (2019). "Refrain from using flash drives at work: Civil, public servants cautioned". *Daily Graphic, August 4, pp.75.*

Bryman, A. (2008). *Social Research Methods (3rd. ed.).* New York: Oxford University Press.

Buami, K. (2019). "Deliberate policies needed to grow Ghana's internet space". *Daily Graphic, July 15, pp.7.*

Castells, M. (2000). *The Rise of the Network Society, The Information Age: Economy, Society and Culture, Vol. I.* Oxford: Blackwell Publishing Ltd.

Chu, B., Holt, T., & Ahn, G. (2010). *Examining the Creation, Distribution, and Function of Malware On-line.* Washington D.C, Technical Report for National Institute of Justice. NIJ Grant No. 2007IJCX0018. Available at: www.ncjrs.gov./pdffiles1/nijgrants/230112.pdf

Cukier, W., Nesselrorth, E., & Cody, S. (2007). Genre, Narrative and the "Nigeria Letter" in Electronic Mail. *In Proceedings of the 40th Annual Hawaii International Conference on System Sciences, January 03-06, HICSS.* IEEE Computer Society, Washington, DC 70

Edelman, B. (2009). Red Light States: Who Buys Online Adult Entertainment? *Journal of Economic perspectives,* 23, 209-220

Ennin, D, & Mensah, R.O. (2019). "Cybercrime in Ghana and the Reaction of the Law" *International Journal of Institute for science, Technology, and Education (IISTE),Vol.84*

Ennin, D, & Mensah, R.O. (2018). "Assessing the Various Opportunities Explored by Cybercriminals in Accra" International *Journal of Institute for science, Technology, and Education (IISTE), Vol.8, No.12.*

Frimpong, D, E. (2019). "Why Israel is spearheading global cyber security campaign". *Daily Graphic, July 7, pp.44.*

Furnell, S. (2002). Cybercrime: *Vandalizing the Information Society.* London: Addison-Wesley

Holt, T., & Blevins, K. (2007). Examining sex work from the client's perspectives: Assessing johns using online data. *Deviant Behavior,* 28, 178-198

Internet Crime Complaint Centre (IC3) 2020 Annual Report. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Internet Crime Complaint Centre (IC3) 2013 Annual Report. Available at: http://www.ic3.gov/media/annualreports.aspx).

Kumekpor, B. K. (2002). *Research Methods and Techniques of Social Research.* Accra: SonLife Press & Service

Kwofi M. (2021). "Cyber Security Authority Launched in Accra". *Daily Graphic, October 4, pp.26.*

Marcus, C. D. (2008). Identifying potential factors of adolescent online victimization for high school seniors. *International Journal of Cyber Criminology 2(2), 346-348*

News Desk Report (2021). "President welcomes Twitter Office in Ghana". *Daily Graphic, April 14, pp.38.*

News Desk Report (2019). "Strive to make technology part of Ghanaian society: Veep challenges youth". *Daily Graphic, April 5, pp.24.*

Ngnenbe, T. (2018). "Electronic Transaction Act to be reviewed next year". *Daily Graphic, December 5, pp.45.*

Ngnenbe, T. (2017). "Judiciary staff train in cyber security". *Daily Graphic, December 7, pp.69.*

Nyarko, N., & Addae-Madzi, J. (2015). "6 busted over Sim box fraud". *The Ghanaian Times, January 27, pp. 3*

Nunoo, C. (2021). "Vice-President launches platform to heck MoMo fraud". *Daily Graphic, April 22, pp.24*

Olayemi, J. O. (2014). "A socio-technological analysis of cybercrime and cyber security in Nigeria". *International Journal of Sociology and Anthropology, Vol. 6(3), pp. 116-125.*

Olayemi, J. (2014). "Combating the Menace of Cybercrime". *International Journal of Computer Science and Mobile Computing, Vol.3, Issues 6, pp.980-991*

Olowu, D. (2009). "On the Origins of Advanced Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers. *The African Journal of Information System, Volume 3/ Issue 1*

Schmalleger, F., & Pittaro, M. (2009). *Crimes of the Internet.* Saddle River, NJ: Pearson Prentice Hall

Singh, H. & Alshammari, T. (2020). "An Institutional Theory Perspective on Developing a Cyber Security Legal Framework: A Case of Saudi Arabia". *Beijing Law Review, 11, 637-650. doi:10.4236/blr.2020.113039.* Accessed on 30th March, 2022.

Suman, S., Srivastava, N., & Pandit, R. (2014). Cyber Crimes and Phishing Attacks. *International Journal on Recent Innovation Trends in Computing and Communication, 2 (2), 334-337*

The Ghanaian Times (2021). "Ghana loses $ 19.8m through fraudulent activities". https://www.ghanaiantimes.com.gh/ghana-loses-19-8m-through-fraudulent-activities/. Accessed on 30th March, 2022.

Toure, Abbel. (2019). "Data security and the role we can play". *Daily Graphic, July 8, pp.7*

Warner, J. (2011). Understanding Cybercrime: A View from Below. *International Journal of Cyber Criminology,* 5(1),736-749

UNODC (2013). *Comprehensive Study on Cybercrime.* New York: UN