EVALUATION OF TARGETED FRAUD STRATEGIES ON VULNERABLE INDIVIDUALS OF DEVELOPED NATIONS

[1]WAHAB WAJEED BOLANLE, [2]OYEDIRAN MAYOWA OYEDEPO, [3]OLUSESI AYOBAMI TAIWO

[1,2,3]Department of Elect/Elect & Computer Engineering, Bells University of Technology, Ota, Ogun State, Nigeria
E-mail: [1]bola4reel2000@yahoo.com, [2]mayor_yoppy02@yahoo.com, [3]ayobamiolusesi@yahoo.com

Abstract - The aim of this study is to analyze the different methods in which cyber criminals perpetrate their fraudulent acts on vulnerable individuals of developed nations. The set objectives of the study are to identify different strategies used to defraud vulnerable victims of developed nations, collect data from cyber criminals and victims via Google forms (questionnaires) and to analyze the data using statistical package for social sciences. Primary data were collected for the study from primary source using Google form (questionnaires). The data where then analyzed using spread sheet package. The data collected were based on the types of strategies used in targeting vulnerable individuals , benefits of the illicit acts, continents where they operate from, reactions after successful fraud, why victims fall prey to the scams and what will make fraudsters quit fraud. These parameters were used as an input in the analysis stage for the study. Recommendations and certain measures which will help individuals in avoiding being a victim of cybercrime were proposed.

Keywords - Computer, Credit Card, Cyber Crimes, Fraud, Hackers, Identity Theft, Impersonation, Romance, Scam, Vulnerability.

I. INTRODUCTION

Cybercrime is said to be a crime in which a computer system is the object/ tool used in committing an offence. The perpetrator of the crime are called cybercriminals. There are several of these types of cybercriminals. They are either the Amateurs, Hackers and organized Hackers. The amateurs are script kiddies who are equipped with little or no skills but use existing tools or instructions found on the internet for attacks on their prey.

Hackers break into computer systems to gain access either with or without permission in other to compromise the systems [1]. Cybercrimes are mostly targeted against vulnerable individuals or group of individuals of developed nation for personal gains/ financial benefits. This fraudulent acts has caused so many physical, mental and life threatening trauma to individuals whom are victims of the evil acts. These could have an adverse effect on the financial status and also pose a security threat to the nation. The most prominent of the fraud that has been perpetrated against individuals and government agencies in the developed nations in recent time includes: Credit Card Top-Up, Online/ Wire Transfer, Spamming, Phishing, Romance Scam, Buying and Selling, Lotto, Car Wrap, FBI Impersonation, Job Scam (personal assistant, nanny, mystery shoppers), Alibaba, Fraudulent Check/ Cheque, Mobile Deposit, Bid Pay e.t.c.

II. STATEMENT OF THE PROBLEM

A lot of fraud has been committed by cybercriminals in the past and recent time which are targeted at vulnerable individuals of developed nations using different strategies. However, most existing study were carried out on the impact of fraud on developing nation, third party and historic data were mostly used in their analysis. Hence, this study evaluated targeted fraud strategies on vulnerable individuals of developed nations.
selected.

III. AIM AND OBJECTIVES

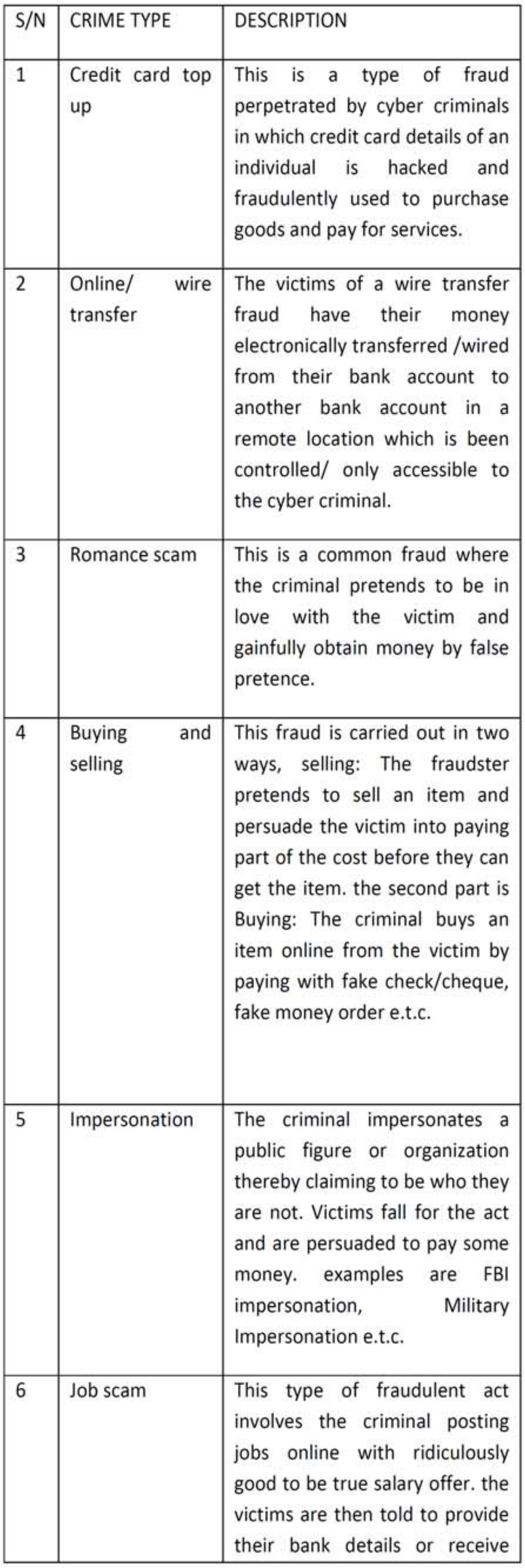
The aim of the study is to evaluate targeted fraud strategies on vulnerable individuals of a developed nation. The specific objectives are to;

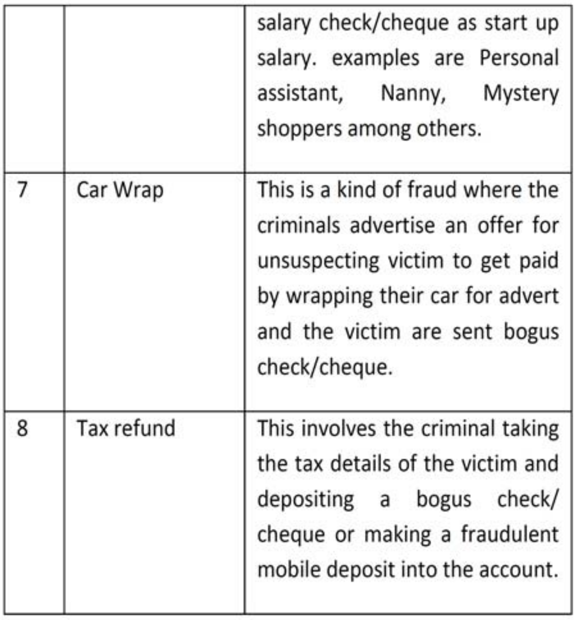
- Identify different strategies used to defraud vulnerable victims of developed nations.
- Collect first hand data directly from the victims and cybercriminals using Google form (questionnaire)
- Analyze the data using statistical package for social sciences

IV. LITERATURE REVIEW

A system can often be broken into by an unauthorized person. When describing the activities of cybercriminals, there is the need to analyze the ways in which the criminals perpetrate the acts for the purpose of financial gain. According to [1], a lot of efforts has been put in place in addressing cybercrime. Examples are defending the networks, avoiding data breach, detecting and reducing criminal activities and prosecuting the criminals[2], [3].

A recent report by daily trust, 2010 which was reported by the Internet Crime Complaint centre, partnering between the Federal Bureau of Investigation (FBI) and America's National white collar crime centre, revealed that Africa/ Nigeria was ranked third among the list of top 10 sources of cyber crime in the world[4].





S/N	CRIME TYPE	DESCRIPTION
1	Credit card top up	This is a type of fraud perpetrated by cyber criminals in which credit card details of an individual is hacked and fraudulently used to purchase goods and pay for services.
2	Online/ wire transfer	The victims of a wire transfer fraud have their money electronically transferred /wired from their bank account to another bank account in a remote location which is been controlled/ only accessible to the cyber criminal.
3	Romance scam	This is a common fraud where the criminal pretends to be in love with the victim and gainfully obtain money by false pretence.
4	Buying and selling	This fraud is carried out in two ways, selling: The fraudster pretends to sell an item and persuade the victim into paying part of the cost before they can get the item. the second part is Buying: The criminal buys an item online from the victim by paying with fake check/cheque, fake money order e.t.c.
5	Impersonation	The criminal impersonates a public figure or organization thereby claiming to be who they are not. Victims fall for the act and are persuaded to pay some money. examples are FBI impersonation, Military Impersonation e.t.c.
6	Job scam	This type of fraudulent act involves the criminal posting jobs online with ridiculously good to be true salary offer. the victims are then told to provide their bank details or receive salary check/cheque as start up salary. examples are Personal assistant, Nanny, Mystery shoppers among others.
7	Car Wrap	This is a kind of fraud where the criminals advertise an offer for unsuspecting victim to get paid by wrapping their car for advert and the victim are sent bogus check/cheque.
8	Tax refund	This involves the criminal taking the tax details of the victim and depositing a bogus check/ cheque or making a fraudulent mobile deposit into the account.

Table I: Types of Cyber Crimes mostly perpetrated on Developed Nations

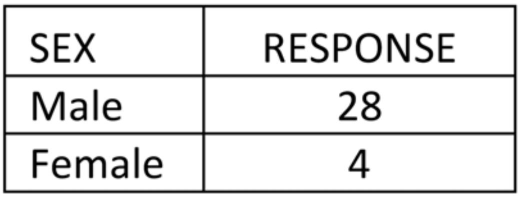
V. METHODOLOGY

The method employed the use of questionnaire which was created online using Google form. This method was adopted because it was possible to reach the target audience like the victims of cybercrime and also cyber criminals where first hand information and responses were gotten from both parties. Different strategies used by the cyber criminals to defraud vulnerable individuals were been gotten and evaluated.

Also, the data collected from the administered questionnaire was analyzed using statistical package for social sciences. A substantial amount of responses were gotten from the questionnaire for analysis.

VI. RESULTS AND DISCUSSION

From the analysis, it could be seen in table 2 that 87% of males were involved in fraudulent activities while only about 13% of females actually indulged in the act.



SEX	RESPONSE
Male	28
Female	4

Table II: Shows the Gender of the Cyber Criminals

It was observed from fig. 2 that 47% of the cybercriminals had age ranging between 21 years and 30 years old. Also, 47% had age range between 31 years and 40 years. While 10 years & 20 years, 41 years & above had 3% each.

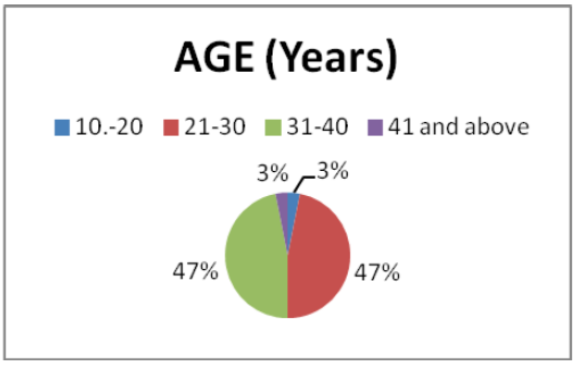


Fig. 2: The chat of the Age of the Cyber Criminals

The region/ continent where cybercrime are mostly perpetrated which is targeted at developed nations has Africa dominating, with a total of 63%, while Europe has a total of 19%, south America having 9%, north America has 6%, Oceania having a total of 3% and Antarctica had 0%. Results obtained shows that the cybercriminals have some level of education where about 63% had first degree (university graduates), 28% had college degree while 3%, 6%, had high school and masters degree, respectively.

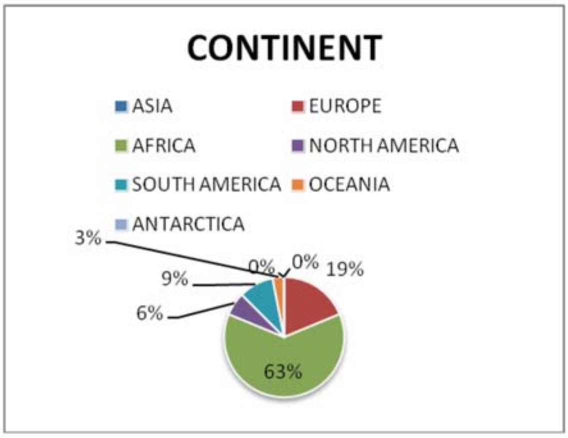


Fig. 3: Region/ Continent where most Cyber Attacks are being lunched

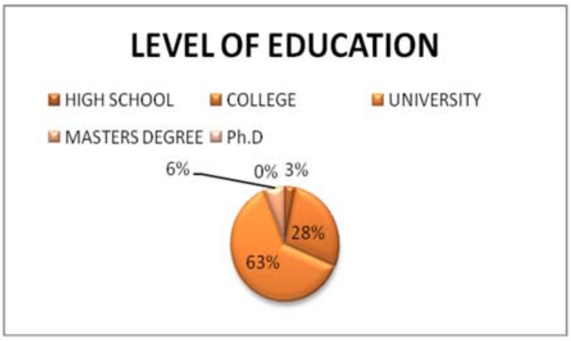


Fig. 4: Level of Education of Cyber Criminals

84% of the cybercriminals got involved in the illicit act for the sole purpose of financial gain. 16 most commonly used strategies were analyzed, Credit card fraud which is the highest strategy with 14% while online wire/ transfer fraud, Buying and selling and job scam has 13% frequency of use. online romance scam is another type which is commonly used by cybercriminals having 11%. Lotto fraud, car-wrap fraud, hacking fraud having 4% of occurrence. Also, the use of fraudulent checks/ cheque and mobile deposits had 3% occurrence, while crypto currency, spamming and phishing attacks had 2%, 1%, 1%, respectively.

S/N	Fraud Strategy	Percentage %
1	Credit Card Fraud	14
2	Buying & Selling	13
3	Online Romance Scam	11
4	Mobile Deposit	3
5	Impersonation (FBI ,Police, Facebook, Instagram, Twitter)	13
6	Job Scam(Personal Assistant, Nanny, Mystery Shopper)	13
7	Online/Wire Transfer	13
8	Check/ Cheque Scam	3
9	Lotto	4
10	Car Wrap	4
11	Alibaba	0
12	Crypto Currency	1
13	Tax Refund	2
14	Hacking	4
15	Phishing	1
16	Spamming	1

Table III: Fraudulent Strategies used by Cyber Criminals

Higher percentage of the victims fall prey because they were not aware of the trap set by the criminals and they constitute about 31%. While 29% had too much trust without further verification, 29% were not smart enough to detect their vulnerability. 8% where desperate to either get rich or get items sold/ bought as shown in fig. 5. From the result in fig. 6, 52% believed that job opportunity will make them leave the criminal act, while 44% believed that a stricter penalty and arrests will make them back off and 4% believe education will make them abandon the fraudulent act.

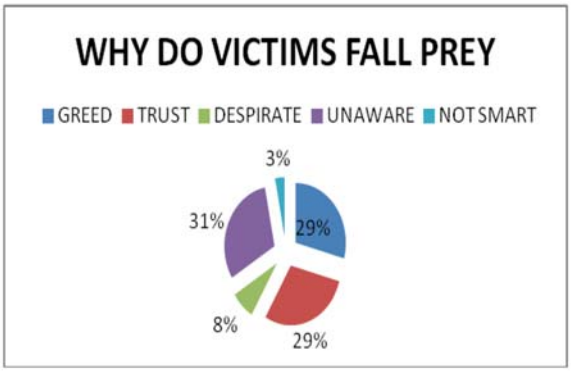


Fig. 5: why Victims fall prey to Cyber fraud

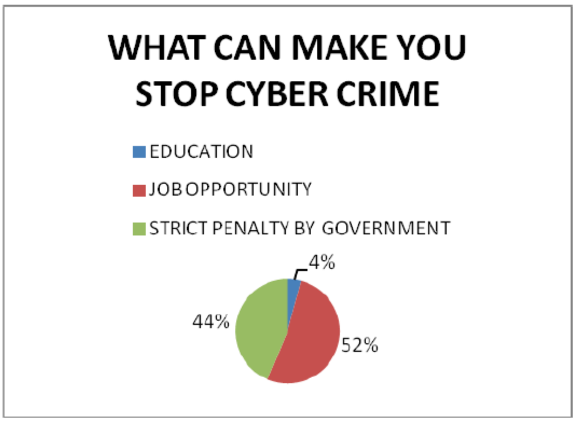


Fig. 6: Measures that can make Cyber Criminal quit fraud

VII. CONCLUSION AND RECOMMENDATION

This research has been able to Evaluate Targeted fraud strategies on vulnerable citizens of developed nations. Based on the findings, the following conclusions were drawn: From the results of the analysis, it shows that cybercrime is mostly perpetrated by male gender, with age range between 21 years and 40 years mostly from African continent. Most of the cyber criminals are educated up to university level whom indulge in cybercrime/fraud/scam majorly for financial gain. Credit card frauds, Online/ Wire transfer, Buying and Selling, FBI impersonation, Job scam are some of the most widely perpetrated fraudulent strategies used on vulnerable victims. Also, it can be concluded that majority of the vulnerable victims are either unaware, greedy or have too much trust. Having a job opportunity and a stricter penalty by the government/ law enforcement agents could deter the criminals from the fraudulent acts. It is recommended that individuals should have a proper verification before indulging in any transaction especially involving monetary transactions. Also, Government should create more jobs and lay down a stricter penalty to any Cybercriminal/Fraudster/Scammer.

REFERENCES

[1] S. R. Yerra, S. Hemraj and T. C. Panda "Effect of Cyber crime on Indian Economy" IJRTS, vol. 1,issue 10, pp. 4 -7, Sept 2014.

[2] S. Hemraj, S. R. Yerra and T. C. Panda "Cyber crime and their Impact A Review" IJERA, vol. 2, pp. 201-206, Mar 2012.

[3] K. R. Sakthidevi "Cyber Risk Management–A Conceptual Framework" IJSRR, vol. 8, issue 2, pp. 500-507, 2019.

[4] O. Maitanmi, S. Ogunlere, S. Ayinde, Y. Adekunle Impact of Cyber Crimes on Nigerian Economy IJES vol. 2, issue 4, pp. 45-51, April 2013.

★★★