RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
NOVEMBER 2019

DOI:10.5281/zenodo.3550086

Contributory Factors to Internet Crimes in Nigeria – A Survey

Gbenga T. Omoniyi[1], Shahrudin Awang Nor[2], Nor Iadah Yusop[3]

[1]Awang Had Salleh Graduate School, UUM College of Arts & Sciences, Universiti Utara Malaysia, geegartea@yahoo.com
[2]Strategy Planning Division, Institute of Quality Management, Universiti Utara Malaysia, shah@uum.edu.my
[3]School of Computing, UUM College of Arts & Sciences, Universiti Utara Malaysia, noriadah@uum.edu.my

ABSTRACT: Internet crimes, also known as Cyber-crimes are act punishable by law. Nigeria government, in order to curb excessiveness of Internet crimes enacted different regulatory and prohibitory laws in support of views of some theorists who claimed that social factors increase users' vulnerability to computer and Internet attacks. Social factors such as security policy severity, security policy certainty, attitude and attachment have little or no significant relationship with the level of Internet crimes in Nigeria; involvement as a social factor has the strongest significant relationship with the level of Internet crimes in Nigeria; this is followed by commitment, belief and knowledge. Internet users can be tricked, conned and sometimes forcefully compelled to compromise and breach security metrics; security metrics are easily breached if users do not understand or employ security mechanism. Presented in this paper is the survey of the contributory factors to Internet crimes in Nigeria. Data used were gathered by questionnaire.

KEYWORDS: social factors, internet crimes, cyber-crimes, security, questionnaire, Nigeria

Introduction

Features of Internet crimes are "crimes carried out by means of the Internet and other computer networks, handling especially the infringements of copyright, Computer related extortion, child pornography, and breaching of system security." In the supplementary informative report, Internet crimes are moreover alluded to as "the Internet offenses" that are "either perpetrated against the integrity and privacy of computer systems and telecom networks." Nevertheless, despite the fact that this execution is moderately careful, there are significant gaps with respect to the determination of each element of the above definition (Tsakalidis and Vergidis 2017, 1). The pervasiveness of Internet crimes poses a peculiar risk on the economic stability of Nigeria (Waziri 2009, 1).

The upsurge of the Internet attacks and the slow action of the Nigerian government in solving it has smeared the nation globally and tarnished the credible image of the country. Consequently, foreign investors are either wary or not interested to engage in business or economic transactions with Nigeria, especially businesses that can be anchored virtually. In Ibikunle and Eweniyi (2013), the authors in their study reviewed that Nigeria is ranked among the countries where Internet crimes are rampant. The authors presented a list of challenges faced by Nigeria in fighting against Internet crimes; low enforcement of national and international laws; poverty rate, corruption and unemployment are part of the salient factors listed as impediments to curbing Internet crimes in Nigeria. Also, Ani (2011) listed human attributes such as negligence and lack of technical knowledge as parts of enabling factors to Internet crimes in Nigeria. Therefore, this implied that it is important to incorporate social factors such as users' attitude, knowledge and awareness in ensuring effective cyber security in Nigeria.

Most especially, the criminal activities that are rampant in Nigeria are financial scams, fraud, identity theft and other criminal activities that are perpetuated through the use of the Internet (Roseline and Moses-Òkè 2012). In essence, corrupt users of the Internet have continued to use the dynamism of the Internet technology to perpetuate criminal activities on other users in Nigeria. This situation has witnessed sophisticated and exceptional upsurge in recent times to the extent of becoming a global menace. As many other nationalities from around the globe are increasingly falling victims of these insidious criminalities (Ogwezzy 2012, 86). This has called for swift solution by beefing up cyber-security standards that would adequately ensure the safety of cyber

space and Internet users in Nigeria (Okonigene and Adekunle 2009, 93). Social factors usually demonstrated by people are major alleviation to every Internet security attack.

Even though security applications or other mechanism are in place, users misbehave one way or the other, either by leaking out their passwords or secret codes unknowingly or sharing it intentionally to a masquerading attacker. This again implies that Internet itself is a social-technical system that cannot function fully with technical arrangement unless it is socially employed by the users (Kainda, Flechais and Roscoe 2010, 275). Remarkably, Internet criminals in Nigeria are getting innovative, as new methods of perpetrating Internet crimes are invented on daily basis; this makes it difficult to curb the cyber criminals with existing methods (Ibikunle and Eweniyi 2013, 1). The victims of Internet crimes are increasingly growing in naiveté at the tricks impelled by these crooks. Therefore, the issue of cyber-crimes and cyber security continue to be a national concern as the current measures are deemed ineffective to ensure safety in the cyber space of Nigeria.

Pursuing this further, theorists have argued that ensuring effective Internet security stretch beyond technical measures. Hence, extending the measures of Internet security beyond technical concerns is not eccentric, as few theorists such as Mitnick and Simon (2003) claimed that social engineering serve as the most vulnerable and gullible means of launching computer and Internet attacks; this is because Internet users can be tricked, conned and sometimes forcefully compelled to compromise and breach security metrics. In fact, some researchers such as Zurko and Simon (1997) have noticed that Internet security metrics are easily breached because users do not know or understand how to employ security mechanism. Cases like this compel researchers to approach Internet attacks or crimes on both social and technical terms.

Socioeconomic Internet crimes known as 419 crimes in Nigeria might be conceptualized as purposeful extortion-based crimes that are computer or/and web-intervened, for example, Internet swindle, romance scam, and e-misappropriation. In this manner, 'Internet crime' in the Federal Republic of Nigerian is established in socioeconomics (Ibrahim, 2016). In this paper, we set the following as the objectives: 1) to carry out survey on the contributory factors to Internet crimes in Nigeria; 2) to explain the factors through statistical analysis. The rest of the paper is organized as follows. In section 2, we present the methodology used in achieving the paper objectives, the results are presented and discussed in section 3, and section 4 concludes the paper.

Methodology

The data used for this work was gathered through questionnaire. It was administered manually; however, purposely because of the large number of respondents and for the researchers to get in-depth information for the survey, the questionnaire was well packaged into sections. But it can be established that the research follows high confidentiality standard principles and with high esteem of respondents' privacy. Nevertheless, the questionnaire showcases some germane information of every participant which is key to the findings.

The Survey

The survey was based on questionnaire involving closed questions. The questions were based on respondent profile and questions on security policy severity, security policy certainty, attachment, commitment, involvement, belief, attitude, knowledge, and Internet crime.

Section One: Respondent Profile

Shown in Table 1 is the format employed in designing the questionnaire on social factors:

Table 1. Demographic Profile

Demographic Profile Please tick the appropriate answer	
1. Gender: a. Male ☐	b. Female ☐
2. Age group: a. Under 18 ☐ b. 19-24 ☐ c. 25-29 ☐	d. 30-39 ☐ e. 40-59 ☐ f. 60 or older ☐
3. Household income: a. Under N5,000 ☐ b. N6,000-50,000 ☐ c. N51,000-100,000 ☐	d. N101,000-500,000 ☐ e. N501,000-N1million ☐ f. Above N1 million ☐
4. Education level: a. High school ☐ b. College/Diploma ☐ c. Bachelor's degree ☐	d. Graduate or professional degree e. Postgraduate ☐
5. Do you have a computer? Yes ☐ No ☐	
6. Do you have Internet access? Yes ☐ No ☐	
7. Do you have a broadband or high-speed internet connection? Yes ☐ No ☐	
8. Do you use wireless Internet access? Yes ☐ No ☐	
9. Do you use Internet at all? Yes ☐ No ☐ If your answer is YES for the above question, please choose the activity you use the Internet for from the following: School/academic Work/employment Computer game Online gambling Online shopping Financial management Social network Communication	

Section Two: Social Factors

A. Security Policy Severity

Please **encircle** to indicate your opinion with the following statements

1	**2**	**3**	**4**	**5**
Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

1	If I get involved in Internet crime, I will be severely punished by the government	1	2	3	4	5
2	I think it is a problem for me if I am severely punished	1	2	3	4	5
3	I think receiving punishment would have bad influence on my life	1	2	3	4	5
4	I think being reprimanded would have bad influence on my life	1	2	3	4	5

B. Security Policy Certainty

Please **encircle** to indicate your opinion with following statements

1	**2**	**3**	**4**	**5**
Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

1	If I get involved in Internet crime, I would probably be punished	1	2	3	4	5
2	There is possibility that I would be punished, if I get involved in Internet crime	1	2	3	4	5
3	There is probability that I would be reprimanded, if I get involved in Internet crime	1	2	3	4	5
4	I think Internet security policies are effective in Nigeria	1	2	3	4	5

C. Attachment

Please **encircle** to indicate your opinion with following statements

1	**2**	**3**	**4**	**5**
Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

1	This country is important to me	1	2	3	4	5
2	I love this country	1	2	3	4	5
3	I really feel as if this country's problems are my own	1	2	3	4	5
4	I have achieved a lot of benefits through this country	1	2	3	4	5
5	I would be very happy to spend the rest of my life and career in this country	1	2	3	4	5

D. Commitment

Please **encircle** to indicate your opinion with following statements

1	**2**	**3**	**4**	**5**
Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

1	I desire to succeed in Nigeria	1	2	3	4	5
2	I spend and invest much time to succeed in Nigeria	1	2	3	4	5
3	Being successful in Nigeria is important to me	1	2	3	4	5

E. Involvement

Please **encircle** to indicate your opinion with following statements

1	**2**	**3**	**4**	**5**
Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

1	I am often involved in consulting Internet for helpful information	1	2	3	4	5
2	Internet play a vital role to help with my work/studies	1	2	3	4	5
3	I often use Internet to meet new people to socialize with	1	2	3	4	5
4	I feel I spend most of my time on Internet solving work or academic related problems	1	2	3	4	5
5	Sometimes, I feel there is nothing to do on the Internet	1	2	3	4	5

F. Belief

Please **encircle** to indicate your opinion with following statements

1	**2**	**3**	**4**	**5**
Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

1	I don't think Internet crimes are harmful to anyone	1	2	3	4	5
2	I have lots of respect for a policy	1	2	3	4	5
3	It's OK to get around a policy if I can get away with it	1	2	3	4	5
4	Rules are made to be broken	1	2	3	4	5

G. Attitude

Please **encircle** to indicate your opinion with following statements

1	**2**	**3**	**4**	**5**
Strongly disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

1	I am willing to use the available antivirus to protect myself against Internet crimes and threats	1	2	3	4	5
2	I am cautious of Internet crimes threats when I'm accessing the Internet	1	2	3	4	5
3	I am willing to avoid getting involved in any Internet crime activities	1	2	3	4	5
4	I am willing to acquire more knowledge on how to protect myself from Internet crimes	1	2	3	4	5
5	I am convinced that available firewall can protect me against Internet crimes	1	2	3	4	5

H. Knowledge

Please **encircle** to indicate your opinion with following statements

1	**2**	**3**	**4**	**5**
Novice	**Beginner**	**Intermediate**	**Advanced**	**Expert**

1	I have enough computer skills to protect myself against Internet crimes	1	2	3	4	5
2	I understand the functions of all the tools used to commit Internet crimes	1	2	3	4	5
3	I know my responsibilities to protect myself against Internet crimes	1	2	3	4	5

4	I have enough knowledge of the Internet crimes	1	2	3	4	5
5	I have enough knowledge of possible Internet crimes on email systems	1	2	3	4	5
6	I have enough knowledge of possible Internet crimes on social network systems	1	2	3	4	5
7	I have the technical ability to protect myself online against Internet crimes	1	2	3	4	5

I. Internet Crimes

Please **encircle** to indicate your belief on the effectiveness of the following Internet security techniques:

1	**2**	**3**	**4**	**5**
Strongly Disagree	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

1	There are efficient security measures to protect users against Internet crimes in Nigeria	1	2	3	4	5
2	Security measures are reliable to protect Internet users from Internet crimes in Nigeria	1	2	3	4	5
3	Security measures are effective in protecting Internet users against Internet crimes in Nigeria	1	2	3	4	5
4	I think security measures cannot protect Internet users against Internet crimes	1	2	3	4	5
5	I have no awareness about Internet crimes in Nigeria	1	2	3	4	5
6	I have little technical knowledge about Internet security measures that protect users from Internet crimes	1	2	3	4	5
7	Internet crime is not a disturbing issue in Nigeria	1	2	3	4	5

Results and Discussion

Discussed in this section are the contributory results of each social factor to Internet crimes, the information got from questionnaire was used to achieve this section.

Survey Response Rate

This section highlights the respondent rate. A total number of 130 respondents were targeted and 130 questionnaires were distributed to all of them, out of which 120 questionnaires were retrieved and 8 questionnaires were considered disqualified basically on the issue of incomplete fillings, high rate of missing responses to relevant questions and similar issues, so, the overall valid retrieved questionnaires were 112 which is 93.33% usable for the purpose of the analysis. Table 2 shows the overall study survey response rate.

Table 2. Survey Response Rate

	Frequency	**Percentage (%)**
Questionnaire Distributed	130	100
Questionnaire Returned	120	92.31
Questionnaire Rejected	8	6.67
Questionnaire Retained	112	93.33

Table 3 is the descriptive statistics that shows the mean and the standard deviation of all social factors that were considered in this study.

Table 3. Descriptive Statistics

Social Factors	Mean	Std. Deviation	N
A1	.48	.502	112
A2	2.66	1.018	112
A3	2.20	1.236	112
A4	2.94	1.093	112
A5	.17	.377	112
A6	.71	.458	112
A7	.76	.430	112
A8	.21	.412	112
A9	2.94	.774	112

Key: A1-Security policy severity, A2-Security policy certainty, A3-Attachment, A4-Committment, A5-Involvement, A6-Belief, A7-Attitude, A8-Knowledge, A9-Internet crime

Respondent Profile

A. Gender

The research respondents' demography data as seen in section 2 revealed that male has 51.8% and female has 48.2%. This goes to show that men have more affinity for the use of computers than the female as revealed in this study data. It also revealed that in all the location and survey site of this study, male is more than female using computer. The result in gender differences of respondent is shown graphically in Figure 1.

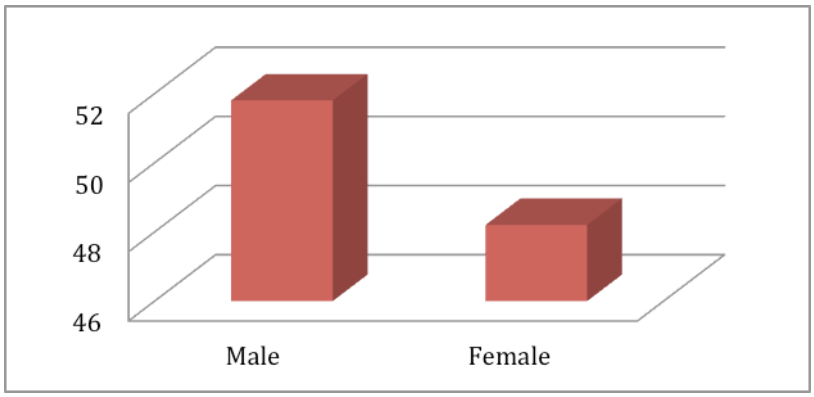

Figure 1. Graph of the gender differences of respondents

B. Age

The age bracket of all the respondents is shown in Figure 2. It shows that those in the age range of 30-39 years recorded the highest percentage of 36.6 against those in the range of 25- 29 years which recorded 26.8%. The respondents in the age range of 19-24 have 15.2%, while those in the range of 40 -45years recorded 19.6%. The respondents in the age range of 60 and older have 1.8%.

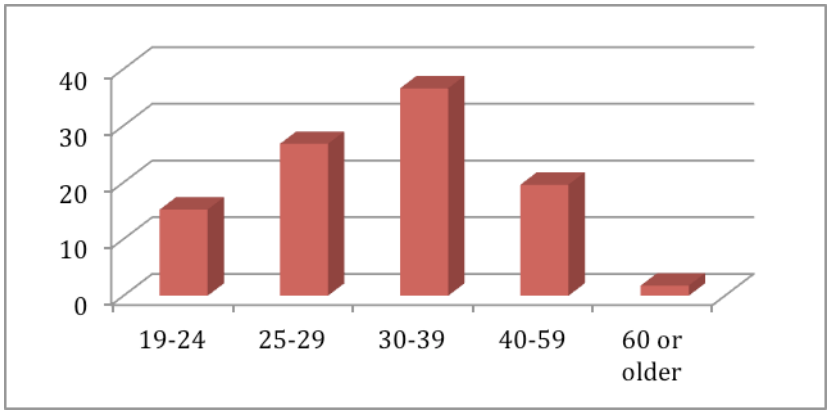

Figure 2. Graph of the age group of respondents

C. Education Level

The education level of all respondents is shown in Figure 3 and it reveals that those with postgraduate degree have the highest percentage of 45.5 while those that have bachelor degree have the closest figure of 30.4 percentage. Those with graduate or professional degree have 13.4 % while those with College/Diploma have 10.7 %.

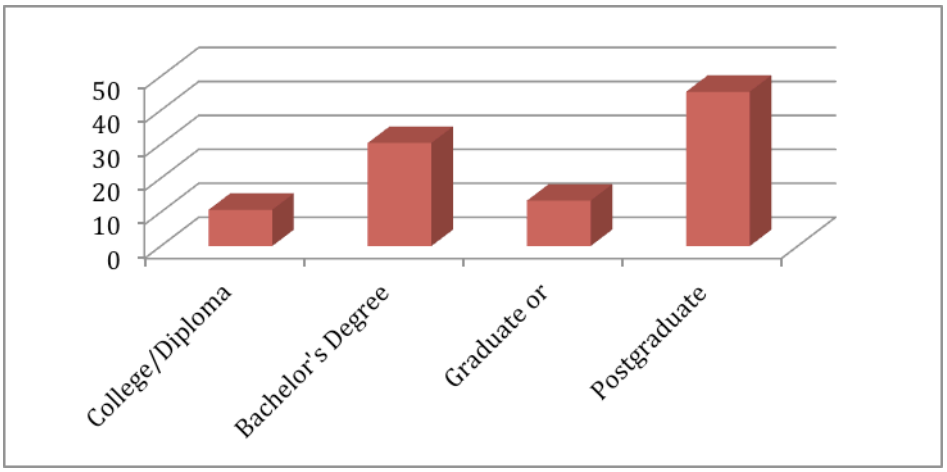

Figure 3. Graph of the education level of respondents

General Questions

The question about the possession of computer at home has 83% of the respondents declared yes while those without computer at home have 17%. Likewise, the question related to Internet accessibility at home has 70.5 % of the respondents answered no, while 29.5% of the respondents answered yes. Also, the question about broadband and high-speed Internet connection recorded 75.9% respondents answered no while 24.1 % answered yes. The question about usage of wireless Internet access recorded 78.6 % for respondents with yes as answer against 21.4% that have no as answer. The question about the use of Internet from the respondents has 99.1% that answered yes while 0.9% answered no.

Conclusion

This paper has been able to reveal the contributory factors to Internet crimes in Nigeria. This is for the purpose of understanding the criminal activities that surrounded Internet and the penalties for each offence committed. The following conclusions were reached after the study:

i. Most of social factors considered in this survey as measurement variables have low standard deviations that have values towards the mean of the set except for three of them which are security policy certainty, attachment and commitment respectively.
ii. Majority of the respondents have computer at home and have access to Internet facilities and broadband as well as fast speed Internet facilities.
iii. That male individual is more open to the use of computer than female in Nigeria and hence more prone to Internet crime than their women counterpart.
iv. Those in the age bracket of 30-39 years are more users of computer and Internet in Nigeria and they constitute the youth age of Nigeria.
v. Majority of the populace that are computer and Internet users are people with household income that is within the range of N101,000- N500,000; and they are not the highest household income earner in Nigeria.
vi. Those that have postgraduate education qualification form the majority of people that have and use computer and Internet facilities among Nigeria populace and the least users are the people with colleges and diploma certificates.

Concerning their contributory significances, Involvement as a social factor has the strongest significant contribution to the level of Internet crime in Nigeria; this is also followed by

commitment, belief and knowledge. All these social factors contributed immensely to the level of Internet crimes in Nigeria. The social factors such as security policy severity, security policy certainty, attitude and attachment have little or no significant contribution to the level of Internet crimes in Nigeria.

References

Ani, L. 2011. *Cybercrime and national security: the role of the penal and procedural law. Law and Security in Nigeria,* 197 – 232.

Ibikunle, F. and Eweniyi, O. 2013. "Approach to Cyber security issues in Nigeria: Challenges and solution." *(IJCRSEE) International Journal of Cognitive Research in science, engineering and education* 1(1): 1-11.

Ibrahim, S. 2016. "Causes of socioeconomic cybercrime in Nigeria." *2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016*, https://doi.org/10.1109/ICCCF.2016.7740439.

Kainda, R., Flechais, I. and Roscoe, A. W. 2010. "Security and usability: Analysis and evaluation." In: *ARES '10. IEEE* 275 - 282. Krakow, Poland: IEEE.

Mitnick, K. D. and Simon, W. L. 2003. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons Inc.

Ogwezzy, M. C., 2012. "Cybercrime and the proliferation of Yahoo addicts in Nigeria." *AGORA International Journal of Juridical Science* 1: 86-102.

Okonigene, R. E. and Adekunle, B. 2009. "Cybercrime in Nigeria." *Business Intelligence Journal* 93-98.

Roseline, O. and Moses-Òkè. 2012. "Cyber capacity without cyber security: A case study of Nigeria's national policy for information technology (NPFIT)." *The Journal of Philosophy, Science & Law* 12(30). Retrieved from www.Miami.Edu/Ethics/Jpsl.

Tsakalidis, G., and Vergidis, K. 2017. "A Systematic Approach toward Description and Classification of Cybercrime Incidents." *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 49(4):1–20. https://doi.org/10.1109/TSMC.2017.2700495.

Waziri, F. 2009. *Antigraft campaign: The war, the worries*. The Punch, 1st March 2009, p.1.

Zurko, M. E. and Simon, R. T. 1997. "User-Centered Security." *New Security Paradigms Workshop*. The Open Group Research Institute, Eleven Cambridge Center, Cambridge, MA 02142.