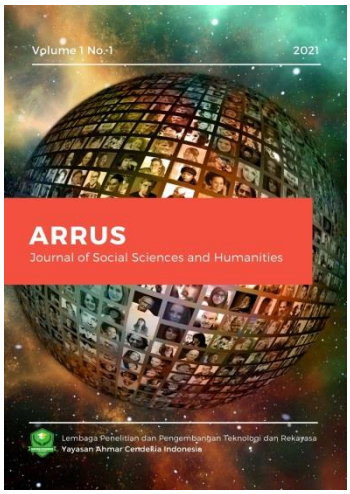
https://doi.org/10.35877/soshum490

OPEN ACCESS

ISSN: 2776-7930 (Print) / 2807-3010 (Online)



RESEARCH ARTICLE

Social Media Platforms: Exposing students to cybercrimes

Edey P. Agara[1]*, Felix E. Ojong[1], Josephat O. Emeka[1], A. M. Ogaboh Agba[1], Abayomi I. Akintola[1], Olumayowa V. Ogunsola[2]

[1]Department of Sociology, University of Calabar, Nigeria
[2]International Business School (IBS), Fontys University of Applied Sciences, Venlo, Netherlands

*Corresponding author: A. M. Ogaboh Agba, Department of Sociology, University of Calabar, Nigeria

E-mail: agbaamogaboh@gmail.com

Abstract: Today, social media becomes the order of the day in which all aspect of life is affected. The study therefore examines the phenomenon of social media use and students' exposure to cybercrimes in Nigeria. Students' exposure to Facebook, Instagram, Twitter, and WhatsApp applications were considered. A cross-sectional survey was conducted on 900 students drawn from Cross River State, Nigeria. Data were retrieved using questionnaire and Focus Group Discussion (FGD). Descriptive analysis for the study revealed that Facebook use, Instagram use, and Twitter use significantly expose students to cybercrimes. The study concluded that social media use, as beneficial as it is, has potential dangers that could impose undesirable costs on users. It was thus recommended among others that the users of social media must carefully determine the information they put on social media to avoid providing explicit personal details that can be used by hackers against them. Furthermore, government must enact appropriate legislation or enforce existing laws to checkmate the activities of cybercriminals in society.

Keywords: social media, facebook, instagram, whatsApp, cybercrime

1. Introduction

Criminal activities in society date back to time immemorial and no known society, at whatever level of development, is free from them. Societies of primitive, ancient, and medieval times as well as those of modern industrial, scientific and digital eras have their fair share of experiences of criminal activities perpetrated by their citizens or strangers, with their attendant consequences on individuals, families, communities, corporate bodies, and governments. The level of criminal activities that take place in society differ from place to place and is influenced or shaped by several factors which include the extent of technological development, the degree of compliance and adherence to religious principles and doctrines, the level of poverty of individuals, the value systems of the place, the seriousness or otherwise of sanctions and sanctioning institutions/ law enforcement agencies, etc.

In traditional societies, most crimes were planned and committed in crude and mechanical forms and involved the exertion of force by the criminals with the aid of certain physical or mechanical devices. In modern societies, crimes and the ways they are planned and executed have changed with the levels of technological advancement and sophistication, especially following the advent of ICT in general and social media in particular (Angioha, Enukoha, Agba, & Ikhizamah, 2020; Ukwayi, Akintola, & Angioha, 2019; Ukwayi, Obafaye,

https://doi.org/10.35877/soshum490

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

& Akintola, 2019). The coming of these new technologies has given birth to a new wave of criminality referred to as cybercrime-crimes committed with the aid of the internet and its associated social media networks like Facebook, Twitter, Instagram, WhatsApp, Snapchat, etc.

Illner (2016) has observed that cybercrime on interpersonal organizations can be stalled into three classifications: the customary broad-sweep scams, an attempt luring web users to click on 'ads' or sites that could trap malware to their computers; an attempt to sneak into an exposed account registered online (personal or cooperate account) for sensitive information; and utilizing web-based media as a stage to associate, trade thoughts and exchange stolen information. However, generally, crimes committed in the cyber world include reconnaissance, phishing, catfishing, fake profile, social engineering, hacking, identity theft, scamming, cyberstalking, child. pornography, cyberbullying, etc (Hernandez, 2018; Perlmutter, 2019; Emeh, Abang, Asuquo, Kalu & Agba, 2011; Emeh & Agba, 2010). These crimes take place every day and make social media a world with both good and bad sides.

Perlmutter (2019) maintained that social media has become deep-rooted into many people's lives and is often referenced in news reports. For instance, a research report by Smith and Anderson (2019) on social media use in 2018 shows that 74% of Facebook users in the US say they visit the site daily with 51% visiting several times a day. This frequency in its use makes social media a very convenient environment for the criminally minded users and a potentially dangerous environment for other users with no criminal intent. Corroborating this stance also, researchers from CISCO have maintained that Facebook has become a host to a good number of busy marketplaces and interactions used by cyber-criminals to buy and sell stolen commodities.

Social media use does not only provide cyber-thieves with a fertile ground for their nefarious activities but also makes other users become exposed or vulnerable to cybercrime. This happens especially when they place vital personal or corporate information on social media sites; interact with some other social media users who may be known or unknown to them; click on certain links that are placed on social media sites by some other users who operate under various guises. In GoMedia, it is noted that social media networks like Facebook may seem harmless, but by making data about oneself public, people end up putting themselves and those around them in danger.

University students happen to be among the most predominant users of social media, and it may be reasonable to think that they may also constitute part of the biggest populations with the highest vulnerability to cybercrime. Given the widespread use of social media by people from all walks of life, and given the frequency and ease with which cybercriminals surf and situate themselves on social media, one begins to wonder how vulnerable or how exposed social media users are to cybercrimes in the world in general and Nigeria in particular. Therefore, the preoccupation of this study is to examine the extent to which social media use exposes people to cybercrimes using students from Universities in Cross River State as a case study. Consequently, the study sought to:

(1) Determine the extent to which Facebook use exposes University students to cybercrimes in Cross River State, Nigeria.
(2) Find out the extent to which Instagram use exposes University students to cybercrimes in Cross River State, Nigeria
(3) Examine the extent to which WhatsApp use exposes University students to cybercrimes in Cross River State, Nigeria.

2. Materials and Method

The study adopted the cross-sectional survey design which is known to be amenable to generalization using a sample drawn from a large population. The population of the study consists of all undergraduate and postgraduate students at the University of Calabar and the

https://doi.org/10.35877/soshum490

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Cross River University of Technology. The University of Calabar has a student population of about 44,999 students, while the Cross River State University of Technology (CRUTECH) has a student population of 14,999 students. Therefore, the population of the study consists of 59,998 students derived from both universities in Cross River State. A sample of 900 students (respondent) was used for the study comprising 461 respondents from the University of Calabar and 439 respondents from Cross River University of Technology. This sample was arrived at using Taro Yamane's formula for calculating sample size for a given population. The study used the multi-stage sampling technique comprising purposive, simple random, accidental, and snowball sampling techniques. The purposive sampling technique was used to select two out of the three universities in the state which are the University of Calabar and Cross River University of Technology. These two universities were so selected because, apart from being older than Arthur Jarvis University (which has barely started operation as a private University), they have a large number of students both undergraduate and postgraduate who use a variety of social media networks. Furthermore, the simple random sampling technique was used to select faculties in the two universities. In selecting the respondents from the faculties that were used for the study, the accidental and snowball sampling techniques were used. Data obtained from the field were properly computed and analysed hypothesis by hypothesis, and each was tested at 0.05 level of significance. The researchers employed both descriptive and inferential statistics in the course of the study. Descriptive statistics like the mean and simple percentages were used to display and analyse the demographic characteristics of respondents while inferential statistics, basically the Pearson Product Moment Correlation Coefficient (r) statistic and the Multiple linear regression statistics were used to determine the existence of any statistically significant relationship between independent variable and the dependent variable. Data were computed using the Statistical Package for Social Sciences (SPSS), and all results were tested at 0.05 level of significance.

3. Results

Out of the nine Hundred (900) copies of the questionnaire administered, only 785 (87.2%) questionnaires were returned and used to generalise the study's findings. Responses retrieved from the field were coded and descriptive results presented in frequency and percentage tables and result subjected to parametric analysis using Pearson's Product analytical tool. For easy explanation, response options designated as "often" and "sometimes" were reported as agreeing to the question, while the response options designated as "rarely" and "not at all" were reported to disagree with the statements in the sub-scales.

3.1. Presentation of Result

3.1.1. Objective one

To what extent does Facebook use expose University students to cybercrimes in Cross River State, Nigeria? Responses were presented showing frequency and percentages in Table 1 and the parametric statistics presented in Table 2. The computation of Facebook use in Table 1 reveals that about 708 (90.2%) use Facebook to connect with friends around the world, while less than half 77 (9.8%) of the respondents use it. On whether Facebook is used to like and reply to comments, 646 (82.2%) agreed to its use to a large extent, while 139 (17.8%) are seldom about it. Consequently, 476 (60.6%) use Facebook to seek public attention, while 309 (39.4%) are unconcern about public attention. Responses on the use of Facebook to post personal pictures and videos showed that 575 (73.2%) agreed to a large extent, while 210 (28.6%) are rarely perturbed about it. Responses on whether 'Facebook is used to support a social cause' reveals that 551 (70.2%) used it to a large extent, while 234 (29.8%) have rare use of it. Responses on whether 'Facebook is used to make new friends', 594 (75.7%) agreed to a large extent, while 191 (24.3%) were not concerned with making new friends on Facebook. Furthermore, 643 (81.9%) use Facebook, to read comments from other platforms, while 142 (18.1%) have little reaction to it. Based on these results, it

https://doi.org/10.35877/soshum490

OPEN ACCESS

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

was concluded that Facebook is largely used among youths in Nigeria. This result was further subjected to parametric statistics (Pearson Product Moment Correlation) to establish whether its influence in exposure to cybercrime is statistically significant and reported in Table 2.

Table 1: Showing the frequency distribution, of Facebook use.

Facebook use	Often	Some-time	Rarely	Not at All	Mean	SD
I use Facebook to connect with friends around the world	441 (56.2%)	267 (34.0%)	46 (5.6%)	31 (3.9%)	1.58	0.774
I use Facebook to like and reply to people's comment	407 (51.8%)	239 (30.4%)	65 (8.3%)	74 (9.4%)	1.75	0.958
I use Facebook to seek public attention	252 (32.1%)	224 (28.5%)	152 (19.4%)	157 (20.0%)	2.27	1.114
I use Facebook to post personal pictures and videos	285 (36.3%)	290 (36.9%)	121 (15.4%)	89 (11.3%)	2.02	0.986
I use Facebook to support a social cause.	286 (36.4%)	265 (33.8%)	126 (16.1%)	108 (13.8%)	2.07	1.035
I use Facebook to make new friends	349 (44.5%)	245 (31.2%)	134 (17.1%)	57 (7.3%)	1.87	0.944
I use Facebook to read comments from other platforms	357 (45.5%)	286 (36.4%)	64 (8.2%)	78 (9.9%)	1.83	0.951

The parametric statistics for question one as presented in Table 2, revealed that the result was statistically significant where r(783%) = 0.377; p <0.05. This owes to the fact that the calculated r-value of 0.377 was greater than the critical r-value of 0.195, at 0.5 alpha (α) level of significance. Consequently, the squared correlation coefficient (0.377%)2 indicates that the proportion of Facebook users has a significant influence on the exposure to cybercrime. Therefore, 14.2 percent of the variance in cybercrime in the State is accounted for by Facebook use. From the calculation, the degree of effect is minimal, implying that Facebook use correlates moderately and positively with exposure to cybercrime. Therefore, an increase in Facebook use would directly lead to a moderate increase in cybercrime. Therefore, we can conclude that Facebook use has a statistically significant influence on cybercrime in Cross River State.

Table 2: Pearson product-moment correlation coefficient analysis showing the relationship between Facebook use and exposure to cybercrime.

Variables	No. of responses	Mean statistics	Standard Deviation	Degree of freedom	R-value	P-value
Facebook Use	785	13.389	4.815	783	0.377**	<.005
Exposure to Cyber Crime.	785	19.541	5.498			

**. Correlation is significant at the 0.05 level, critical r-value= 0.098

3.1.2. Objective two

To what extent does Instagram use influence University students' exposure to cybercrime in Cross River State? Responses were presented showing frequency and percentages in Table 3 and the parametric statistics presented in Table 4. The computation result reveals that 497 (54.3%) uses Instagram to post messages to individuals and groups, while 288 (45.7%) rarely use it.

On whether Instagram is used to follow friends online, 535 (68.2%) strongly agreed to a large extent, while 250 (31.8%) use it rarely. More so, 518 (66.0%) use Instagram to keep up with the trend of things, while 267 (37%) are rarely perturbed to use it. Furthermore, 495 (54.1%) use Instagram to stay on top of popular posting trend, while 290 (45.9%) uses it to a little extent. On whether they used Instagram to follow celebrities, 499 (63.6%) used it to a large extent while 286 (36.4%) stated a minimal use to it. Also, 452 (57.6%) use Instagram

https://doi.org/10.35877/soshum490

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

to tag posts, photos and videos, while 333 (42.4%) are seldom about it. Furthermore, 473 (60.1%) use Instagram to post messages to individuals and groups, while 312 (39.9%) rarely use it. Based on these results, it was inferred that Instagram is used is largely used among youths in Nigeria. This result was further subjected to parametric statistics (Pearson Product Moment Correlation) to establish whether the influence is statistically significant and presented in Table 4.

Table 3: Showing the frequency distribution of Instagram use

Statement	Options	Response rate	Mean	SD
I use Instagram to post messages to individuals and groups	Often	242 (30.8%)	2.27	1.113
	Sometimes	255 (23.5%)		
	Rarely	122 (15.5%)		
	Not at all	166 (21.1%)		
I use Instagram to follow friends online	Often	243 (31.0%)	2.20	1.505
	Sometimes	292 (37.2%)		
	Rarely	131 (16.7%)		
	Not at all	118 (15.0%)		
I use Instagram to keep up with the trend of things	Often	258 (32.9%)	2.17	1.061
	Sometimes	260 (33.1%)		
	Rarely	140 (17.8%)		
	Not at all	127 (16.2%)		
I use Instagram to stay on top of popular posting trend	Often	252 (23.1%)	2.24	1.102
	Sometimes	243 (31.0%)		
	Rarely	138 (17.6%)		
	Not at all	152 (19.4%)		
I use Instagram to follow celebrities	Often	255 (32.5%)	2.25	1.125
	Sometimes	244 (31.1%)		
	Rarely	119 (15.2%)		
	Not at all	167 (21.3%)		
I use Instagram to tag posts photos and videos	Often	232 (29.6%)	2.34	1.118
	Sometimes	220 (28.0%)		
	Rarely	164 (20.9%)		
	Not at all	169 (21.5%)		
I use Instagram to post messages to individuals and groups	Often	236 (30.1%)	2.32	1.118
	Sometimes	237 (30.2%)		
	Rarely	136 (17.3%)		
	Not at all	176 (22.4%)		

The parametric statistics for question two as presented in Table 4, revealed that the result was statistically significant where r(783%) = 0.332; p <0.05. This owes to the fact that the calculated r-value of 0.332 was greater than the critical r-value of 0.098, at 0.5 alpha (α) level of significance. Therefore, the squared correlation coefficient (0.332%) indicates that the proportion of Instagram users has a significant influence on the exposure to cybercrime. Therefore, 11 percent of the variance in cybercrime in the State is accounted for by Instagram use. From the calculation, the degree of effect is minimal, implying that Instagram use correlates moderately and positively with exposure to cybercrime. Therefore, an increase in Instagram use would directly lead to a moderate increase in cybercrime. Hence, we can conclude that Instagram use has a statistically significant influence on cybercrime in Nigeria.

Table 4: Pearson product-moment correlation coefficient analysis showing the relationship between Instagram use and exposure to cybercrime.

Variables	No. of responses	Mean statistics	Standard Deviation	Degree of freedom	R-value	P-value
Instagram Use	785	15.687	6.062	783	0.332**	<0.05
Exposure to Cyber Crime.	785	19.541	5.498			

**. Correlation is significant at the 0.05 level.

https://doi.org/10.35877/soshum490

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

3.1.3. Objective three

To what extent does WhatsApp use influence students' exposure to cybercrime in the state? Responses were presented showing frequency and percentages in Table 5 and the parametric statistics presented in Table 6. The computation of WhatsApp use reveals that 617 (78.6%) use WhatsApp to follow links to sites that advertise appealing contents, while 168 (21.4%) rarely use it. A similar response was observed whether WhatsApp is used to chat with friends, where 650 (86.6%) responded to a large extent and 105 (13.4%) seldom use it. Also, 647 (82.4%) of the respondents uploaded videos and pictures on WhatsApp for public viewership, while 138 (17.6%) disagreed to this claim. Responses for use WhatsApp to forward contents to individuals and groups were 652 (83.1%), while 133 (16.9%) use it to a little extent. On whether WhatsApp is used to download pictures and videos they find interesting, 643 (81.9%) of the respondents stated that they used it to a large extent while only 142(18.1%) of the respondents stated that they used it to a little extent. Furthermore, 601 (76.6%) reported that they upload and download educational materials on WhatsApp while 184 (23.4%) are not particular about its use. On the whole, WhatsApp use clearly influence the daily activities especially among youths.

Table 5: Showing the frequency distribution of WhatsApp use and student exposure to cybercrime

WhatsApp Use	Often	Some-times	Rarely	Not at All	Mean	SD
I use WhatsApp to follow links to sites that advertise appealing contents	396 (50.4%)	221 (28.2%)	78 (9.9%)	90 (11.5%)	1.82	1.016
I use WhatsApp to chat with friends	478 (60.9%)	202 (25.7%)	54 (6.9%)	51 (6.5%)	1.59	0.878
I upload videos and pictures on WhatsApp for public viewership	396 (50.4%)	251 (32.0%)	89 (11.3%)	49 (6.2%)	1.73	0.893
I use WhatsApp to forward contents to individuals and groups	423 (53.9%)	229 (29.2%)	82 (10.4%)	51 (6.5%)	1.70	0.901
I use WhatsApp to download pictures and videos l find interesting	385 (49.0%)	258 (32.9%)	78 (9.9%)	64 (8.2%)	1.77	0.930
I upload and download educational materials on WhatsApp	379 (48.3%)	222 (28.3%)	99 (12.6%)	85 (10.8%)	1.86	1.012

The parametric statistics for question four as presented in Table 7, revealed that the result was statistically significant where r(783%) = 0.281; p <0.05. This owes to the fact that the calculated r-value of 0.281 was greater than the critical r-value of 0.098, at 0.5 alpha (α) level of significance. Therefore, the squared correlation coefficient (0.281%)2 indicates that the proportion of WhatsApp users has a significant influence on the exposure to cybercrime. Therefore, 7.8 percent of the variance in cybercrime in the State is accounted for by WhatsApp use. From the calculation, the degree of effect is minimal, implying that WhatsApp use correlates moderately and positively with exposure to cybercrime. Therefore, an increase in WhatsApp use would directly lead to a moderate increase in cybercrime. Hence, we can conclude that WhatsApp use has a statistically significant influence on cybercrime in Nigeria.

Table 7: Showing the Relationship between WhatsApp Use and Exposure to Cyber Crime.

Variables	No. of responses	Mean statistics	Standard Deviation	Degree of freedom	R-value	P-value
WhatsApp Use	785	10.490	4.109	783	0.281**	<0.05
Exposure to Cyber Crime.	785	19.541	5.498			

**. Correlation is significant at the 0.05 level; critical r-value (0.098).

https://doi.org/10.35877/soshum490

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

3.2. Discussion of Findings

3.2.1. Objective One

Result from research question one (to what extent does Facebook use influence University students' exposure to cybercrimes in Cross River State?) reveals that university students use Facebook to a large extent. The parametric statistics shows that Facebook use has strong statistical significance on exposure to cybercrimes among University students in Nigeria. This finding is in line with the report of Hussein (2017) that "apart from being a leading powerhouse in the social media world for obtaining and dissemination information about friends, family, and other social enterprises, it suffers a lot of misuse which tantamount to cybercrimes. These crimes are perpetrated through various means such as hacking, phishing, blackmailing, scamming, etc. which creates a lot of disturbance for its user". Hussein further added that Facebook has gradually become a seemingly safe-haven for internet fraudsters and cybercriminal.

As deduced from the report of Paganini (2012), there is no doubt that Facebook has completely transformed the way people interact but there is a dark side attached to people's love and patronage of this social media network. It was observed that on daily basis, criminals keep inventing newer ways to employ Facebook as a medium to commit new and disturbing crimes that defy regulations and authorities while making users susceptible to various degrees of losses. Paganini thus enjoined users to be knowledgeable about the common crimes committed on Facebook so that they can avoid becoming victims. Such crimes include scam, cyberbullying, stalking, robbery, defamation, harassment, and identity theft. Additionally, Robertson (2019) gave a similar report about Facebook and cybercrimes in his work entitled "Facebook still has a big problem with cybercrime group". He maintained that despite several crackdowns by cybersecurity, Facebook has been, and is still being used seriously by identity thieves, scammers, spammers, and forgers to display or hawk their services.

3.2.2. Focus Group Discussion of Objective one

Interviews from the FGDs conducted also revealed that Facebook use predisposes users on daily basis to cybercrimes of all sort while some reported that they have been victims of cybercrimes through Facebook use. The FDG participants were asked to describe how they "used Facebook in their day-to-day lives" and how they think it "exposes them to cybercrimes". Concerning how they used Facebook in their everyday lives, all respondents reported that they use it for a variety of activities which include, but not limited to: chatting with friends around the world; posting information for public consumption; accepting and sending friend request; following celebrities around the world; watching trending videos; posting personal information of events like wedding anniversaries, birthdays, childbirths, naming ceremonies; advertising or reading about business opportunities etc. Furthermore, whereas all participant reported that their daily use of Facebook increased their chances of exposure to cybercrime, through unsolicited calls, links, and messages received from fake and fraudulent users, about 51 percent reported that they have been victims of cybercrimes through Facebook use.

For instance, one female FGD participant from Unical reported that she lost her first valuable relationship through her Facebook account that was hacked. According to her, the account was hacked and hijacked by an unknown user, who went ahead to post all manner of nude pictures and pornographic videos in her timeline. The result of this was that apart from losing some of her friends in real life, she lost her cherished relationship with a man they have been on together as the man found it difficult to believe that the hacking of her account was done by a stranger who has got nothing running with her. Another (Male) FGD participant from CRUTECH recanted his ordeal through Facebook use. He reported how his quest for greener pasture landed him in the hands of evil men in the city of Lagos.

https://doi.org/10.35877/soshum490

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

According to him, a link was sent to him on Facebook about a job vacancy existing somewhere in Lagos. He clicked on the link and it opened for him to fill out his details after which he was invited for an interview. It was at the interview ground that he understood that he had been scammed as his valuables including wallet, ATM cards, ID cards etc. were taken away from him while he managed to escape for his dear life.

3.2.3. Objective Two

Result from research question two (To what extent does Instagram use influence University students' exposure to cybercrime in Cross River State, Nigeria?) reveals that University students use Instagram to a large extent. The parametric statistics shows that Instagram use has strong statistical significance on exposure to cybercrimes among University students in Nigeria. This finding corresponds with the report of Regidi (2016), to provides cogent reason Instagram is among the leading social media networks in which cybercrime is rampant and users are highly susceptible to hacking. It was maintained that some companies often use popular Instagram users with a large number of followers to promote their products. This has become a kind of motivation to people who try to seek increased followership on Instagram to make money. Consequently, cybercriminals have taken advantage of this to make people fall into their tricks. They do this by offering free Instagram followers as well as links to phoney Instagram pages. A click on such links they provide usually leads users to fake Instagram login pages, which is used to obtain their login details, access their follower accounts, and drive the users to fake online surveys.

Wilford (2017) also reported how hackers are using Instagram to target celebrities in society. Wilford noted that a group of hackers who have targeted what he called A-list celebrities' Instagram accounts may have gained access to millions of users' private data. He further cited an instance where the account of a singer named Selena Gomez was hacked. In that attack, three naked pictures of her former boyfriend were posted to her 125 million followers before her profile was shut down. This may be part of the reasons why Kothari (2016) averred that criminal offences involving misuse of popular social media sites like Facebook, Twitter, and Instagram, among others, account for more than 25 percent of the total cybercrimes being dealt with by the police in the United States.

3.2.4. Focus Group Discussion of Objective Two

Interviews from the FGDs conducted also revealed that Instagram use exposes users on daily basis to cybercrimes of all sorts while some reported that they have been victims of cybercrimes through Instagram use. Some respondents narrated certain experiences they had in the course of using Instagram. For example, one male respondent from the University of Calabar reported that on several occasions he has been embarrassed by countless pictures of both naked and semi-naked persons placed on his page by unknown persons and that has made him very careful in order not to destroy his relationship.

A 35-year female participant from CRUTECH also reported how she was scammed through Instagram. According to her account, a link that was sent to her page advertising some stuff ended up being a fake link that caused her to lose her data and her login details. She maintained that after clicking on the link and following the prompts, she got stuck at a point and only discovered afterwards that her data was used up abnormally and that, after procuring data, a further attempt to return to the initial page displayed an error in login details. This resulted in her abandoning the account and opening a new one. Also, a 29-year female respondent from CRUTECH reported that she was hurt seriously by a fraudster who has been following her seriously in a disguised form. According to her, her friends account was hacked and hijacked, and he just abandoned the account without a disclaimer. Unknown to her that the person at the other end is a fraudster, she kept chatting and interacting with him through that account to the point of making a payment for a product to a third party. When it dawned on her to confirm the payment and its authorization from him, she eventually discovered it was all scams. She ended up losing her N20,000 because several attempts to recover the money proved seriously abortive.

https://doi.org/10.35877/soshum490

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

3.2.5. Objective three

Result from research question four (To what extent does WhatsApp use influence University students' exposure to cybercrime in Cross River State, Nigeria?) reveals that University students use WhatsApp to a large extent. The parametric statistics shows that WhatsApp use has strong statistical significance on exposure to cybercrimes among University students in Nigeria. The finding is in tandem with the report of Irwin (2019), that given the steady surge in human desire to communicate/interact with each other, at whatever location, without any hitches, the mobile messaging app (WhatsApp) has carved an inch for itself in modern history. However, it is said to have certain vulnerabilities which cybercriminals are cashing on to undo users. Irwin (2019) further reported that WhatsApp has admitted that cybercriminals have exploited a major vulnerability in its voice call function to plant spyware on users' devices. This makes it possible for crooks to activate cameras and microphones of devices, assess users' emails and instant messages, and collect data relating to their locations. Irwin (2019) also reported that if you have in recent times had missed calls from unfamiliar numbers on the WhatsApp platform, then there are high chances that cybercriminals could be spying on you.

Edwards (2020) also corroborated this in his article "Bad Chat beware of this WhatsApp Scam". Edwards called on users to beware of a dangerous hacking technique that cybercriminals have devised to access users' messages and their contacts. The technique involves a hacker posing as a friend to gain access to a victim's account. This may be the reason for which Goud (n.d) maintained that social media users who use the web version of WhatsApp and Telegram could suffer the risk of cybercrime attack. For him, the application has a vulnerability that was yet to be fixed and which enable cybercriminals to have control over subscriber's accounts also enable them to access their private data (contacts, shared files, private messages) using images that are coated with malware. In a baseline study by Halder and Jaishankar (2015), it was reported that WhatsApp has been used in India in various ways to make user become victims of various forms of ordeals by the use of abusive and threatening messages which are not only annoying but harassing as well. It has also been used to send what is referred to as emoticons including violent pictures or sexually explicit or obscene images to users. They further stated that through the WhatsApp messaging services, viral videos are made to circulate to reach those who do not ordinarily use or access search engines like Yahoo, Google, YouTube etc. to search for them.

3.2.6. Focus Group Discussion of Objective three

Interviews from the FGDs conducted also revealed that WhatsApp also exposes users on daily basis to cybercrimes of all sort while some reported that they have been victims of cybercrimes through the use of the WhatsApp application. For instance, a male respondent from Unical, aged 36, reported that before he got aware of the two-step verification setting his account was hacked and hijacked by a fraudster with who he ignorantly shared his verification code. According to the respondent, the fraudster never wasted any time. The moment he got the code, the first thing he did was to block me from accessing the account. He then started using the account to impersonate me by advertising all manner of online businesses that are acclaimed to be paying huge sums of profit to people as return on their investment within few hours of investment. He added that the hacker intended to defraud his friends who he discovered are many and seemingly well-to-do but he (the hacker) failed as I quickly made a disclaimer through other friends' accounts. This scenario was reported by several respondents from different FGD groups and became like the commonest cybercrime that happens on social media.

In like manner, a female respondent from CRUTECH, aged 32, reported how a cybercriminal invaded her privacy and flooded her space with unsolicited pornographic videos and pictures. She added that the cybercriminal then started requesting money from her with threats to make her private messages and chats public if she does not send him

https://doi.org/10.35877/soshum490

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

money. She further reported that although she did not give him any money before delisting him, she was gripped with panic as she wasn't sure of the extent of damage that would happen to her person if the fraudster had gone ahead to carry out his threat.

On a general note, it worthy to state here that all respondents agreed that all social media users are exposed or vulnerable to cybercrime on daily basis especially as the inventors or administrators have left the protection and security of individual accounts largely to their owners while the cybercriminals continue to have a seemingly unrestrained presence on social media. These criminals keep on reinventing their modes of operation and consistently lurking around every social media site to take advantage of their inherent vulnerabilities. However, whereas fifty-nine percent of respondent reported being victims of cybercrime through social media use forty-one percent reported that they had never been direct victims of cyberattacks but know, and have heard of, several persons who have been victims.

4. Conclusion and recommendations

Arising from the above, it is worthy to conclude that social media use has a very great influence on exposure to cybercrime in Cross River State. Through social media use, various people have been exposed to or become vulnerable to cybercrimes of various forms and most have become victims of cybercrimes. For example, through the use of Facebook, Twitter, Instagram, WhatsApp etc, many people have become victims of scam, hacking, phishing, bullying, harassment, while some have suffered marital or relationship problems. Through social media, scammers deploy various tricky means to get people's details and further use such details and the victims' identity to carry out criminal activities such as using the victims' credit card, opening a bank account with victims' identity, etc. Furthermore, social media use has caused great losses to consumers and businesses that do online transactions including buying and selling of goods and services. Through social media, fraudsters take advantage of people looking for romantic relationships to defraud them by playing on their emotions, obtaining money from them and eventually abandoning them. In other words, social media use has, in modern days, become one of the fastest and easiest means through which fraudsters carry out their fraudulent activities and through which users are exposed or made victims of such fraudulent activities. Hence, there is a need for social media users have to learn to minimize the risk of cyberattacks on their social media profiles by determining which information to share and which not to. This is very important as almost every social media platform gives people options and leaves them with the responsibility to decide how much information they want to share with their friends and other people on that network. It is also recommended that social media users should try as much as possible to customize the security setting of their social media profile during their first-time configuring accounts and also do regular checks of such account afterwards. Legislations against cybercrimes must be enacted and existing ones put into force to enable relevant authorities to deal effectively with offenders. Social media users must be careful when following links that are provided by unknown and uncertified persons or sources as most victims of cybercrimes are those who followed links placed by unsuspecting fraudsters.

References

Agba, A. M. O., Ikoh, M., Ushie, E. M. & Bassey, A. O. (2010). Telecommunication Revolution: Implication on criminality and family crises in the South-south states of Nigeria. International Journal of Computer and Information Science, 3 (1) 42 – 51.

Angioha, P. U., Enukoha, C. U., Agba, R. U., & Ikhizamah, G. U. (2020). Information Technology Predictor Variables and Employee Productivity in Commercial Banks. JINAV: Journal of Information and Visualization, 1 (1), 44 -52.

ISSN: 2776-7930 (Print) / 2807-3010 (Online)

Edwards, C. (2020). Bad chat beware this WhatsApp scam – it steals your messages and even hacks your family too. Retrieved 26th January 2021 on https://www.the-sun.com/lifestyle/tech/1883354/WhatsApp-scam-steals-your-account/#

Emeh, J. U. & Agba, A.M.O (2010). Professionalizing Teaching in Nigeria for Effective Service Delivery and National Development. European Journal of Social Sciences, 17)3), 352-359.

Emeh, J. U., Abang, J. I. Asuquo, P., Kalu, I. & Agba, A. M. O. (2011). Curriculum review: Reactions from education stakeholders in South South States of Nigeria. *Global Journal of Human Social Science,* Vol. XI, Issue II, , pp. 33 – 42

Goud, N. (n.d). Millions of WhatsApp and telegram users are vulnerable to cyberattacks. Retrieved 29th January 2021 on https://www.cybersecurity-insiders.com/millions-of-WhatsApp-and-telegram-users-are-vulnerable-to-cyber-attacks/

Halder, D., & Jaishankar, K. (2015). *Harassment via WhatsApp in urban and rural India: a baseline survey report*. Tirunelveli, India: Centre for Cyber Victim Counselling

Hernandez, E. (2018). The 16 most common types of cybercrime acts. Retrieved on 28th October 2019 from https://www.voipshied.com

Irwin, L. (2019). WhatsApp urges users to update app after massive security failure. Retrieved 23rd April 2020 on https://www.itgovernance.co.uk/blog/WhatsApp-urges-users-to-update-app-after-massive-security-failure

Kothari, V. (2016). Misuse of social media accounts for 25% cybercrimes in Pune. Retrieved on July 25, 2018, from https://timesofindia.indiatimes.com/city/pune/Misuse-of-social-media-accounts-for-25-cyber-crimes-in-Pune/articleshow/54268495.cms

Paganini, P. (2012). 7 Most Common Facebook Crimes. Retrieved on July 16, 2018, from https://securityaffairs.co/wordpress/4891/cyber-crime/7-most-common-Facebook-crimes.html

Perlmutter, D. (2019). Social media: a haven for cybercriminals. Retrieved on 23rd October 2019 from https://blog.cyberint.com/social-media-a-heaven-for-cyber-criminals

Regidi, A (2016). New-age social media cybercrimes and how to tackle them. Retrieved on July 16, 2018, from https://www.firstpost.com/tech/news-analysis/new-age-social-media-cybercrimes-and-how-to-tackle-them-3680759.html

Robertson, A. (2019). Facebook still has a big problem with cybercrime groups. Retrieved on January 6th 2021 from https://www.theverge.com/2019/4/5/18296687/Facebook-cisco-talos-cybercrime-spam-scam-identity-theft-groups-takedown

Smith, A. & Anderson, M. (2018). Social Media Use in 2018 retrieved on 25th October 2019 from https://www.pewinternet.org/2018/03/01/social-media-use-in-2018/

Ukwayi, J. K., Akintola, A. & Angioha, P. U. (2019); Biometric Security In Business Organisation: An Assessment Of Its' Impact On Checking Corporate Crime In Business Organizations In Cross River State Nigeria ; International Journal of Scientific and Research Publications (IJSRP) 9(5) (ISSN: 2250-3153), DOI: http://dx.doi.org/10.29322/IJSRP.9.05.2019.p8966

Ukwayi, J. K., Obafaye, I. S. & Akintola, A. (2019). Information and Communication Technology and Crime Control in Calabar Metropolis, Cross River State, Nigeria. European Journal of Social Sciences Studies. 4(1).

UniRank (n.d). University Ranking. Retrieved on July 29, 2018, from https://www.4icu.org/reviews/7668.htm

Wilford, G. (2017). Millions of Instagram users may have been affected by latest hack attack, social media giant warns. Retrieved on 5th November 2019 from https://www.independent.co.uk/life-style/gadgets-and-tech/instagram-cyber-attack-hack-celebrities-selena-gomez-justine-bieber-millions-ordinary-social-media-a7926211.html com.