

## **Gender Dynamics in Facebook-related Cybercrime Victimization in Jigawa State, Nigeria**

Ukasha Ismail

### **Abstract**

*Facebook could be one of the most targeted social media platforms for cybercrime due to its large number of users. Many Facebook users experience various patterns of cybercrime victimization. However, variation in the nature, patterns and frequency of Facebook-related cybercrime victimization across genders is not given much attention. This study attempts to bridge this gap by investigating gender dynamics in Facebook-related cybercrime victimization. The study used mixed method approach. Primary data were collected using questionnaire and interview from a sample of (N=366) Facebook users in Jigawa State, Nigeria. Analysis for the study was carried out using Chi-square and T-test and thematic analysis. Findings of the study indicate significant association between gender and victimization experience. Gender and patterns of victimization revealed high variation, indicating high rate of sexually related victimization against females. The study found that females report a higher average number of victimizations than males. It revealed that both genders do not frequently report their victimization to law enforcement and other formal agencies. It recommended the need for education and awareness programmes to address the unique challenges faced by each gender to defend themselves against Facebook-related cybercrime. Interventions aimed at reducing Facebook-related cybercrime victimization in Jigawa State should focus more on females.*

**Keywords:** *Cybercrime, gender, Facebook, victimization*

### **Introduction**

The revolution in information and communications technology has influenced the proliferation of social media platforms. Facebook App was rated as the most popular social media in the world (Park & Vieraitis, 2021). Facebook is the first social media platform to reach 2.7

billion monthly active users in the second quarter of 2020 (Aliyu et al., 2020) and slightly increased to 2.98 billion as at the first quarter of 2023 (Statista Research Department, 2023). The platform's mammoth users make it one of the most targeted social media platforms for cybercriminals. Facebook-related cybercrime encompasses a range of illegal activities, including hacking, identity theft, cyberstalking, online harassment, romance scams, financial fraud, account hijacking and so on.

More so, the gender of the social network user, specifically being female, increases one's chances of experiencing online interpersonal victimization by nearly two times (Henson et al., 2011). Alam et al. (2012) found variation in offending and victimizing in terms of geographical location, age, religion, gender, and monthly income of family members. It could be that females are more attractive targets for online offenders, have social networks comprised of a greater proportion of likely offenders, or there may be a difference in online lifestyles or routine activities between male and female users. Facebook App increases the risks of cybercrime victimization among its users. Hamsa et al (2018) and Tarigan et al. (2018) argued that young populations are more likely to be the targets of crime on internet or social networking sites. In addition to age, gender, education, and financial status form significant vulnerabilities to both genders. Likewise, the gender that actively engage in online chat forums and other online communities are more likely to become victims of cybercrime (Oksanen & Keipi, 2013).

Victimization patterns have long been recognised as pivotal in understanding the dynamics of crime, particularly in relation to gender. Studies on victimization have revealed significant disparities in the way males and females experience and respond to crime. These disparities are influenced by cultural norms, societal structures, and individual behaviours. Nigeria's diverse cultural landscape influences how individuals perceive and experience crime, with factors such as

education, socioeconomic status, and cultural values playing a role in shaping vulnerabilities (Okeshola & Adeta, 2013).

While males may be exposed to crimes such as robbery, physical assault, and property theft due to their economic activities, females may be more vulnerable to domestic violence, sexual harassment, and other forms of gender-based violence (Ibrahim et al., 2019). The advent of technology and the increasing use of social media have introduced new dimensions to victimization. Cybercrime, online harassment, and identity theft have become prevalent in recent years, further complicating the traditional understanding of victimization. The victimization experiences equally vary across genders. This is especially so in Jigawa State, where the digital divide is narrow (Adewumi, 2021).

The cultural and societal norms in Jigawa State further complicate the dynamics of victimization. Gender stereotypes and traditional roles often discourage women from reporting crimes, particularly those involving sexual or domestic violence. Men, too, face societal pressures that influence their reporting behaviour, with crimes like cyber-fraud and financial victimization often going unreported due to stigma and fear of judgment (Ibrahim et al., 2019).

Despite the growing recognition of these issues, there is limited empirical research on the differences in victimization patterns between males and females in Jigawa State, Nigeria. Most existing studies on crime and victimization in Nigeria focus on urban centres, neglecting the rural and semi-rural settings that characterise much of Jigawa State (Abdullahi & Ismail, 2021). This study explores gender dynamics in Facebook-related cybercrime victimization in this unique socio-cultural context. The study attempts to examine associations between gender and victimization experience, gender and patterns of cybercrime victimization, gender and the choice of victimization reporting, gender and the choice of victimization reporting channels, gender and

frequency of victimization experiences, gender and awareness of cybercrime victimization.

### **Research Hypotheses**

The following hypotheses were formulated and tested in this study.

1.  $H_1$ : There is an association between gender and victimization experience.  
 $H_0$ : There is no association between gender and victimization experience.
2.  $H_1$ : There is an association between gender and patterns of cybercrime.  
 $H_0$ : There is no association between gender and patterns of cybercrime.  
 $H_1$ : There is an association between gender and the choice of victimization reporting channels.  
 $H_0$ : There is no association between gender and the choice of victimization reporting channels.
3.  $H_1$ : There is a significant difference in the mean number of victimizations between males and females.  
 $H_0$ : There is no significant difference in the mean number of victimizations between males and females.
4.  $H_1$ : There is an association between gender and knowledge of age as a predisposing factor of victimization.  
 $H_0$ : There is no association between gender and knowledge of age as a predisposing factor of victimization.
5.  $H_1$ : There is an association between gender and familiarity with the perpetrator.  
 $H_0$ : There is no association between gender and familiarity with the perpetrator.

### **Methods**

The study was conducted in Jigawa State. According to the National Population Commission (2006), the State has a total population of

4,384,649 citizens, and this population was projected to 7,097,407 people in 2020 based on 3.5% growth rate (Lawal, et al., 2020). The Hausas and the Fulanis are the dominant ethnic groups in the State. Islam is the predominant religion, and a Shariah legal code was introduced in the state in 2001. The State is largely characterized by informal sector activities with agriculture as the major economic activity. Majority of the population engages in subsistence farming and animal husbandry. Jigawa state records remarkable improvement in education, as several schools were established, including tertiary institutions. Currently, there are five universities – Federal University Dutse, Federal University of Technology Babura, Sule Lamido University, Kafin Hausa (state-owned), Khadija University, Majia, (Private) and As-Salam Global University (Private), Hadejia. In the year 2000, the State government established Jigawa State Institute for Information Technology in Kazaure purposefully to deploy e-governance in administering Jigawa state and to provide World-class IT training for indigenes of the state. By the year 2003, the state government also installed multi-million naira Broad-Band Access Network (Galaxy) in Dutse.

Mixed-methods approach (quantitative and qualitative) was adopted in this study. Quantitative data provide measurable patterns of victimization, while qualitative data explore personal experiences and gendered nuances. Data were collected from the respondents using structured questionnaire (printed) and in-depth interview guide. Online survey was designed using Google form to generate experiences of victims who may not speak up in one-on-one interviews. The Google form was shared in seven Facebook groups whose memberships are residents of Jigawa State. Only 48 users filled out the form and narrated the patterns of their victimization experiences. The responses were sorted and 10 were used for analysis because their completeness.

The target population comprises of Facebook users in Jigawa state, Nigeria, who are reported to be 1,098,549, by the Second Quarter of

2018, and grew to 1,768,940, by First Quarter of 2020 (National Bureau of Statistics, 2020). A sample size of 384 respondents was used in the study. This is because where the targeted population are more than 10,000 people, the recommended sample size should be 384 respondents (Mugenda and Mugenda, 1999).

The respondents were selected through multi-stage sampling method. At the beginning, Jigawa State was divided into three Senatorial zones namely South-West, North-West, and North-East zones as clusters. Judgemental sampling was used to select one urban area in each zone. These are Dutse, Kazaure and Hadejia. The selection of these areas is due to their advancement in information and communications technology (ICT). Thus, the likelihood of high Facebook users compared to other rural or semi-urban areas. The questionnaire respondents were selected through snowball techniques. The first user in each of the selected area was identified through research assistants residing in the areas. Finally, stratified random sampling was adopted to ensure that each gender was well represented.

Quantitative data was processed and analyzed using Statistical Package for Social Sciences (SPSS) software (version 27). Chi-square tests were performed to identify patterns, correlations, and gender-based differences in victimization rates. For the qualitative data, thematic analysis was used to identify recurring themes related to gender dynamics in the interview data. The qualitative data were manually sorted and grouped based on the study objectives.

## **Results**

### **Hypotheses Tests**

Chi-square and independent test were conducted to explore gender variation in Facebook-related cybercrime victimization experience, patterns, frequency, and perception. The results are presented in the following themes: Gender and victimization experience; gender and victimization reporting channel; gender and frequency of victimization

experiences; gender and knowledge of age as a predisposing factor, and gender and familiarity with perpetrator.

**Hypothesis one**

$H_1$ : There is no association between gender and victimization experience

$H_0$ : There is an association between gender and victimization experience

**Table 1. Gender and Victimization Experience Crosstabulation**

Gender	Victimization experience		Total	Df	$\chi^2$	P-value
	Yes	No				
Male	246	4	250	1	10.616 <sup>a</sup>	.001
Female	106	10	116			
Total	352	14	366			

Table 1 indicates that males (98.4%) reported having experienced victimization. For the females, 91.4% reported having experienced victimization. The result of hypothesis test indicates statistical significance of this finding with chi-square value of 10.616 below the standard significance level (0.05). This means the null hypothesis is rejected in favour of the alternate hypothesis. This also suggests that gender is significantly associated with victimization experience.

**Hypothesis two**

$H_1$ : There is no association between gender and patterns of cybercrime

$H_0$ : There is an association between gender and patterns of cybercrime

**Table 2. Gender and patterns of victimization**

Pattern of victimization	Response		Total	Df	$\chi^2$	P-value
	Yes	No				
<b>Facebook account hijack</b>						
Male	208	42	250	1	190.731 <sup>a</sup>	.000
Female	8	108	116			
Total	216	150	366			
<b>Online advance fee fraud</b>						
Male	154	96	250	1	57.695 <sup>a</sup>	.000
Female	22	94	116			
Total	176	190	366			
<b>Sexual harassment</b>						
Male	166	84	250	1	52.348 <sup>a</sup>	.000
Female	30	86	116			
Total	196	170	366			
<b>Identity theft</b>						
Male	184	66	250	1	84.887 <sup>a</sup>	.000
Female	26	90	116			
Total	210	156	366			
<b>Romance scam</b>						
Male	166	84	250	1	56.813 <sup>a</sup>	.000
Female	28	88	116			
Total	194	172	366			

Cyberstalking						
Male	146	104	250	1	49.620 <sup>a</sup>	.000
Female	22	94	116			
Total	168	198	366			

Table 2 reveals differences in patterns of victimization among males and females. On Hijack of Facebook account, the data show that, males (83%) report experience more frequently than females (7%). Females (93%) are more likely to report not experiencing it compared to males (17%). The hypothesis test result shows Chi-square value (190.731) is high. This implies that there is a significant association between gender and experiencing Facebook account hijack. The data on online Advance Fee Fraud victimization experience suggests that 61% males are more likely to report victimization than females (19%). The Chi-square value (57.695) and P-value (.000) means that there is a significant association between gender and experiencing online advance fee fraud and it is statistically significant.

The result on Sexual Harassment victimization reveals Chi-square value (52.348) and P-value (.000). This implies that there is a significant association between gender and experiencing sexual harassment. Males report victimization more frequently (66%) than females (26%). Relating to identity theft, the result shows Chi-square value (84.887) and p-value (.000), which suggests significant association between gender and experiencing identity theft. The data indicate that males report victimization much more frequently (74%) than females (22%).

Romance Scam experience was reported, and the hypothesis test result presents the Chi-square value (56.813) and P-value (.000). It can be concluded that there is a significant association between gender and experiencing romance scams. The data show that males report victimization more frequently (66%) than females (24%). In other

words, females are more likely to report not experiencing romance scams compared to males. On cyberstalking, Chi-square test (49.620) shows that victimization experience is high across genders. It shows that there is a significant association between gender and experiencing cyberstalking. From the data, males report cyberstalking victimization more frequently (58%) than females (19%).

During the in-depth interview, a victim, (male, M.Sc. holder 32years) submitted that:

I have a lot of victimization experience related to Facebook-related crime. My Facebook account was hacked last year. I spent over 12 years to grow and build networks with the account. Not only hacking, I am also a victim of cyber bullying. This indicates that account hijack is commonly perpetrated against Facebook users in Jigawa state cyberbullying. I was bullied by some people especially who our opinions do not align. When I made posts on Facebook, some of them came and comment in negative manners (IDI with victim, 2024)

A victim (female. B.Ed. holder, 25 years) narrated her experience as follows:

[I received] an offensive message. There was a time when a friend that I met on Facebook started sending nude [contents] to me. I blocked him. I also had bad experiences from some people that I thought were my friends because their names looked familiar only when they started asking me to send money to them, I get to know that someone using their identity (IDI with victim, 2025).

Similarly, an interviewee (female, undergraduate, Christian, 22 years) said that “most of the people on Facebook now are bad people, and mostly sending nude pictures” (IDI with a victim, 2025).

Another victim (female, M.Sc. holder, 32 years) narrated the following:

I realized that I have fallen victim of cyber bullying when I started feeling depressed. I started isolating myself from other people. I used to think that why would people decided to make negative comments on my posts. That time I realized that I was bullied (IDI with victim, 2024).

Another victim (male, HND holder, Muslim, 35 years) who participated in in-depth interview responded differently as follows:

In respect to nudity, it normally pops up in forms of adverts or Facebook chat; I used to see nude pictures of a lady asking you to start chatting with her. Fake news and hate speeches are major reasons why I slow down my activities on Facebook. I will not take anything that tries to temper with my belief. I had a Facebook chat, like 5 years ago, which I received a message that one of my friends is stranded somewhere and needed financial assistance (IDI with Victim, 2024).

Similar to the foregoing, a participant (male, 27 years, civic society activist) added that:

Yes, I have severally fall victims of various forms of Facebook-related crime. The recent one is cyberstalking which necessitated me to even change my name from original one Facebook. I was in a situation where I got employed by one of the recognized development partners. Some people attacked my personality and all that. Secondly, some people attempted to hack my

Facebook account probably to get vital information about me. Maybe they want to get access to my contacts such as email. The attackers have also created Facebook account with my name soliciting for help (IDI with victim 2024).

When a female participant was asked about the nature of her victimization experience, she (B.Sc. holder, IT professional, 25 years) responded in the following manner:

I don't know how you call it; my negative experience on Facebook is: some people that follow me to my inbox continually asking me to have love relationship with them [cyberstalking]. And, I am not interested in it. So, I felt like I am offending them by not responding while their messages kept irritating me (IDI with a victim, 2024).

Another female victim shared her experience with cyber a scammer on Facebook. She narrated thus:

There was this Facebook friend I had ... the person is impersonating someone who's a female whereas from my observation and findings the person was a male.... After a long time of chatting, he later disclosed his identity, but I acted like I never knew. So he later asked me to send him my contact that he wants to talk to me so after giving him he later told me that , he will send me a link and I should click on the link that the link requires me to pay 5k and get 10k that ... Already I knew he was a scammer from day one even thou I pretended not to know I told him I wasn't interested after he tried and tried to convince me And I didn't fall he later blocked me after I insulted him ...

**Hypothesis three**

$H_1$ : There is no association between gender and the choice of victimization reporting channels.

$H_0$ : There is an association between gender and the choice of victimization reporting channels.

**Table 3. Gender and victimization reporting channel**

Gender	Victimization reporting channel								Total	df	$\chi^2$	P-value
	Friends	Family members	Banks	ISPs	Law enforcement agencies	IT experts	Teachers	None				
Male	116	32	14	16	8	34	4	26	250	7	276.990 <sup>a</sup>	.000
Female	0	0	0	4	2	0	92	18	116			
Total	116	32	14	20	10	34	96	44	366			

From table 3, of the 68% males, 32% preferred reporting to friends, IT experts (14%), and family members (13%). A significant number (10%) did not report victimization at all. This implies that very few reported to formal institutions like law enforcement agencies (3%) or banks (6%). Female victims predominantly reported to teachers (83%). A smaller group (16%) chose not to report victimization at all. Like males, reporting to formal institutions was minimal, with only 3% females reported to Internet Service Providers (ISPs) and 2% to law enforcement agencies.

The hypothesis test results suggest that the chi-square value (276.990) is very large, and the p-value (.000) which indicates that the result is

statistically significant ( $p<0.001$ ). Furthermore, the outcome means that the null hypothesis is rejected, concluding that gender significantly affects the choice of victimization reporting channels.

In same vein, an interviewee (male, MSc holder, 32 years) submitted that:

No, I did not report my victimization to any law enforcement agency. The reason being that even if you report they would not take any action. I have heard several things from friends who reported that nothing was being done. So, why would I attempt to report when I know they would not do something about it (IDI with victim, 2024)?

Another participant (male, HND holder, Muslim) stated that:

I have never reported my cybercrime victimization experience to any law enforcement agency. But the police are the best agency to report to because I believe the police have the technical know-how to fish out criminals if they wish to do so (IDI with victim, 2024).

In contrast, another participant (male, 27 years, civic society activist) pointed out that:

Immediately I realized that I was victimized, I rushed to the Department of State Security (DSS) office in Dutse, Jigawa state and lodged a complaint. The personnel asked me to report the incident in writing. I wrote the report and gave them my name. The personnel conducted investigation into the case (IDI with victim, 2024).

The above suggests that cyber defamation and cyber sexual harassment are more reported to law enforcement officials in Jigawa state, Nigeria. Based on the quantitative and qualitative, a substantial number of

victims of Facebook-related crime in Jigawa state, Nigeria prefer to report their experience to friends instead of law enforcement officials.

**Hypothesis four**

H<sub>1</sub>: There is no significant mean difference in victimizations between males and females

H<sub>0</sub>: There is a significant mean difference in victimizations between males and females

**Table 4. Gender and Number of victimization experiences**

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Number of victimizations	Male	250	1.4320	.67468	.04267
	Female	116	2.5517	.49947	.04638

Table 4 indicates that females report a higher average number of victimizations (2.5517) than males (1.4320). Males have a higher standard deviation (0.67468), indicating greater variability in the number of victimizations among males compared to females (SD = 0.49947).

**Table 5. Independent Samples Test: Gender and Number of victimization experiences**

	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	Df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
								Lower	Upper
Number of Equal victimization assumed	7.255	.007	-15.956	364	.000	-1.11972	.07018	-1.25772	-.98172
Equal variances not assumed			-17.768	294.621	.000	-1.11972	.06302	-1.24375	.99570

Table 5 shows that the p-value is less than 0.05. This indicates a statistically significant mean difference in victimizations between males and females. Females report on average, 1.12 more victimizations than males (MD -1.11972).

#### **Hypothesis five**

H<sub>1</sub>: There is no association between gender and knowledge of age as a predisposing factor of victimization.

H<sub>0</sub>: There is an association between gender and knowledge of age as a predisposing factor of victimization.

**Table 6. Gender and knowledge of age as a predisposing factor**

Gender	Knowledge of age as a predisposing factor of victimization			Total	Df	$\chi^2$	P-value
	Yes	No	I don't know				
Male	114	98	38	250	2	152.72	.000
Female	0	24	92	116			
Total	114	122	130	366			

Table 6 shows large chi-square value (152.728), indicating a substantial deviation from the assumption of independence. The p-value is .000, suggesting the result is statistically significant, thereby rejecting null hypothesis ( $H_0$ ). The result shows that there is a significant association between gender and knowledge of age as a predisposing factor of victimization. Specifically, males are more likely to acknowledge age as a predisposing factor of victimization compared to females.

#### **Hypothesis six**

$H_1$ : There is no association between gender and familiarity with the perpetrator.

$H_0$ : There is an association between gender and familiarity with the perpetrator.

**Table 7. Gender and familiarity with perpetrator**

Gender	Familiarity with perpetrator		Total	df	$\chi^2$	P-value
	Yes	No				
Male	126	124	250	1	89.158 <sup>a</sup>	.000
Female	0	116	116			
Total	126	240	366			

From table 7, all the respondents who were familiar with the perpetrator were males. None of the females reported familiarity with the perpetrator. This indicates a gender-based disparity in familiarity with the perpetrator, which could have important implications for understanding the context of the situation and designing interventions or policies. The result of hypothesis test indicates that the observed chi-square value (89.158) is very large, while the p-value is .000. This means the result is statistically significant. Thus, the null hypothesis ( $H_0$ ) is rejected. In view of the above, there is evidence to suggest that gender and familiarity with the perpetrator are not independent.

### **Discussion**

This study explores gender variations in Facebook-related cybercrime victimization among Facebook users in Jigawa State, Nigeria. The results show significant relationship between gender and cybercrime experience and perception of the users. The data indicates that both males and females have experienced victimization. The result of Chi-square test is statistical significance of this finding. This finding corroborates with Henson's et al. (2011) that the gender of the social

network user, specifically being female, increases one's chances of experiencing online interpersonal victimization by nearly two times.

The qualitative and quantitative findings revealed that across all patterns of cybercrime victimization experience, males consistently report higher rates of victimization than females. All the chi-square tests show statistically significant results, indicating strong evidence of gender-based differences in experiences of victimization. Males appear more vulnerable to Facebook-related crimes, having reported higher victimization experiences in Facebook account hijack, online advance fee fraud, harassment, stalking and romance scam. This is possibly due to greater online activity or different online lifestyles in Jigawa State. Females show higher frequencies of non-victimization responses. This may be partly because of cultural influence that discourage exposing females' victimization experience. However, specific crimes like sexual harassment still affect females significantly. Duggan (2017) reported that 53% of women aged 18–29 have experienced online harassment, with many cases linked to Facebook.

In addition, the present study findings confirm that of Bratton et al. (2020) that there exists relationship between Facebook use and online harassment among female adolescents between 13 and 17 years of age. This is partly because sexual abuse is often prompted by the easy exchange of photographs, text or the presence of web cams on social media platforms like Facebook. The above findings are also in line with a report by Internet Crime Complaint Centre-FBI (2019) which revealed that old adults suffer more from identity theft, cyber defamation perhaps due to their status and positions of authority.

On choices of victimization reporting channels across genders, the results suggest that males are more likely to report victimization informally (friends, family, or IT experts). Females overwhelmingly report to teachers, suggesting a preference for trusted authority figures in educational settings. Both genders report does not prefer reporting

to formal institutions like law enforcement or banks. The low usage of formal institutions like law enforcement agencies and ISPs indicates potential trust or accessibility issues. Accordingly, Ibrahim et al. (2019) observed that both males and females have tendency to avoid reporting their victimizations due to stigma and fear of societal labelling.

Furthermore, this study found that females report a higher average number of victimizations than males. This indicates that there is a statistically significant difference in the mean number of victimizations between males and females. This also suggests the inability of females to prevent revictimization after their first experience. In harmony with this finding, Wright and Wachs (2019) discovered that reliance of information and communication technologies (ICTs) make it difficult for Facebook users, especially females to defend themselves against cyberstalking and harassment. In the same vein, Peterson (2017) stated that cyberbullying and harassment, including threatening or sending unsolicited sexual messages are common among children and adolescents.

The study findings revealed significance variation in knowledge of males and females about age as a predisposing factor of Facebook-related cybercrime victimization. In line with the above findings, Anand (2014) discovered that young people post too much personal and sensitive information on Facebook that can be harvested for their victimization. Similarly, Wolak and Finkelhor (2011) found that young people mostly engage in risky behaviours on Facebook that make them suitable for sexual victimization. This reveals that young people, regardless of their genders, are more vulnerable to cybercrime victimization on Facebook compared to old adults.

Similarly, the finding shows a gender-based disparity in familiarity with the perpetrator. This implies that, gender is significantly associated with whether someone is familiar with the perpetrator. Accordingly, Vishwanath (2015) argued that the changing pattern of

activities on Facebook platform many users now have friends that are not known to them in person. This change makes it easy for strangers with dubious mission to harvest private information about their potential victims. That is the reason Michael et al (2014) argued that not accepting friend request from strangers is one important technique of preventing cybercrime victimization on Facebook.

### **Conclusion**

This study has established a significant relationship between gender and Facebook-related cybercrime victimization among users in Jigawa State, Nigeria. The findings reveal that while both males and females experience victimization, males report higher rates across multiple forms of cybercrime, including account hijacking, online fraud, harassment, stalking, and romance scams. This vulnerability among males may be linked to their greater online activity and risk-taking behaviours. Conversely, females tend to report fewer victimization experiences, possibly due to cultural factors that discourage them from reporting such incidents. However, crimes like sexual harassment remain a significant concern for female users.

The study also confirms gender-based differences in victimization reporting preferences. Males are more likely to report incidents informally to friends and IT experts, whereas females prefer trusted authority figures such as teachers. Both genders exhibit a reluctance to engage formal institutions like law enforcement.

Furthermore, the study identifies age as a predisposing factor in Facebook-related cybercrime, with younger users—regardless of gender—being more vulnerable due to risky online behaviours and excessive sharing of personal information. The findings also suggest that gender influences familiarity with perpetrators.

Overall, this study underscores the need for targeted interventions to enhance cybersecurity awareness, particularly among young users. Addressing cultural barriers that hinder victim reporting, improving

trust in formal reporting channels, and promoting responsible online behaviours can help mitigate the risks associated with Facebook-related cybercrime victimization.

#### **Policy recommendations**

In view of the above findings, the following are recommended for policy considerations:

1. The rate of victimization experience among both genders reveals the need for education and awareness programmes to address the unique challenges faced by each gender to defend themselves against Facebook-related cybercrime. Enhanced cyber protection measures should focus on educating males about securing their digital presence while also addressing females' concerns.
2. There is need for interventions aimed at reducing Facebook-related cybercrime victimization in Jigawa State and the focus should be more on females, given their higher reported victimization rates. The higher average number of victimizations among females highlights their increased exposure or vulnerability to certain types of cybercrime (e.g sexually related cybercrimes). Likewise, efforts to reduce victimization should focus more on understanding and addressing the specific factors that contribute to higher victimization rates among females.
3. The study exposed low victimization reporting culture across genders. Yet, a few victims reported to law enforcement. In line with this, there is need to build trust and ensure accessibility to law enforcement and other formal institutions. More so, teachers need to be equipped with the skills to handle victimization reports, as they are a primary channel for females.
4. Future Research should investigate the factors that influence higher victimization rates among males and females.

## References

- Abdullahi, A. S., & Ismail, U. (2021). Crimes and insecurity in rural Nigeria. *Dutse International Journal of Social and Economic Research*, 6(1). 15- 23
- Adewumi, A. (2021). Gender and Cybercrime in Nigeria: Exploring Vulnerabilities in the Digital Age. *Journal of African Cyber Studies*, 4(2), 56-72.
- Alam, M.A., Sarjer, A. & Alam, J. (2012). Innocent Victimization of Cyber and Social Networking Crime: An Empirical Assessment among the Graduate Students of Tangail. *Society & Change*, VI(3), 37-67.
- Aliyu, N.I., Abdulrahaman, M.D., Ajibade, F.O. & Abdurauf, T. (2020). Analysis of Cyber Bullying on Facebook Using Text Mining. *Journal of Applied Artificial Intelligence*, 1(1), 1-12.
- Anand, G. (2014). Social Networking Sites and Privacy Issues Concerning Youths. *Global Media Journal-Indian Edition*, 5(1), 1-7.
- Bratton, T.B., Lytle, R.D. & Hudson, H.K. (2020). #FollowMe: An investigation into the relationship between social media behaviors and online harassment among adolescents. *International Journal of Arts and Humanities*, 1(1), 16-27.
- Duggan, M. (2017). Online harassment. *Pew Research Center*. Retrieved from [pewresearch.org](http://pewresearch.org).
- Hamsa, S., Singh, A. & Panackal, N. (2018). Study on Effect of Social Networking Sites on the Young World of Cyber Crime. *Annual Research Journal of SCMS, Pune*, 6, 68-79.
- Henson, B., Reynolds, B.W. & Fisher, B.S. (2011). Security in the 21st Century: Examining the Link between Online Social Network Activity, Privacy, and Interpersonal Victimization. *Criminal Justice Review*, 36(3), 253-268.

- Ibrahim, Y., Sani, U., & Musa, A. (2019). Socio-Cultural Dynamics of Gender-Based Violence in Northern Nigeria. *Journal of Gender Studies in Africa*, 8(1), 22-35.
- Lawal, A.T., Barau, S.S. & Umoru, G.I. (2020). Resources Use Efficiency of Garden Egg (*salanum melongena*) Production in Ringim Local Government Area of Jigawa State, Nigeria. *Journal of Community & Communication Research*, 5(2), 184-189.
- Malaki, Z. (2020). E-victims: explaining online victimization for the cases of cyberbullying and cyberstalking. *Two-year Master in Criminology*. Malmö University.
- Michael, A.K, Boniface, A.K. & Olamide, A.S. (2014). Mitigating Cybercrime and Online Social Networks Threats in Nigeria: *Proceedings of the World Congress on Engineering and Computer Science*, 1, n.p.
- Mugenda, O. M., & Mugenda, A. G. (1999). *Research methods: Quantitative & qualitative approaches* (Vol. 2, No. 2). Nairobi: Acts press.
- National Bureau of Statistics. (2020). Telecoms Data: Active Voice and Internet per State, Porting and Tariff Information.  
<https://www.nigerianstat.gov.ng>.
- National Population Commission. (2006). National Population Census. *National Population Commission*, 422.
- Okeshola, F. B. & Usman, A. R. (2017). Global Positioning Systems (GPSs) and Car-Theft Control in Nigeria. In Ndubueze, P. N. (Eds). *Cyber Criminology and Technology- Assisted Crime Control: A Reader* (pp, 459-460). Zaria, Nigeria: Ahmadu Bello University Press.

- Oksanen, A. & Keipi, T. (2013). Young People as Victims of Crime on the Internet: A Population-based Study in Finland. *Vulnerable Children & Youth Studies*, 8 (4), 298–309.
- Park, Y. & Vieraitis, L.M. (2021). Level of Engagement with Social Networking Services and Fear of Online Victimization: The Role of Online Victimization Experiences. *International Journal of Cybersecurity Intelligence and Cybercrime*, 4(2), 38-52.
- Peterson, J. K. & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? *College of Liberal Arts All Faculty Scholarship*. 5. [http://digitalcommons.hamline.edu/cla\\_faculty/5](http://digitalcommons.hamline.edu/cla_faculty/5).
- Statista Research Department. (November 1, 2021). Facebook: number of monthly active users worldwide 2008-2021. [www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/](http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/).
- Tarigan, V.E., Hasibuan, L.R., Purba, P., Irawan, Sari, P.B., Rossanty, Y., Putra, M.D. & Nasution, T. (2018). Cybercrime Case on Social Media in Indonesia. *International Journal of Civil Engineering and Technology*, 9(7), 783–788.
- Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication*, 20(1), 83-98.
- Wagen, W.V & Pieters, W. (2020). The hybrid victim: Reconceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology*, 17(4), 480-497.
- Wolak, J. & Finkelhor, D. (2011). *Sexting: A typology*. Crimes against Children Research Center.

- Wright, M.F & Wachs, S. (2019). Adolescents' Psychological Consequences and Cyber Victimization: The Moderation of School-Belongingness and Ethnicity. *International Journal of Environmental Research and Public Health*, 16, 2493. 1-11.