African Journal of Social Sciences and Humanities Research
ISSN: 2689-5129
Volume 7, Issue 4, 2024 (pp. 273-282)
www.abjournals.org

INFLUENCE OF WHATSAPP ONLINE PHISHING MESSAGES ON DATA SECURITY AMONG UNDERGRADUATES IN ANAMBRA STATE

Nonye Benedeth Ezeaka (Ph.D.)[1*] and Ewetuobi Esther Ifedilichukwu[1]

[1]Department of Mass Communication, Chukwuemeka Odumegwu Ojukwu University Igbariam.

[*]Corresponding Author's Email: ezeakanonye79@gmail.com; nb.ezeaka@coou.edu.ng;

Tel.: 08037711374

Cite this article:

Ezeaka, N. B., Ewetuobi, E. I. (2024), Influence of WhatsApp Online Phishing Messages on Data Security among Undergraduates in Anambra State. African Journal of Social Sciences and Humanities Research 7(4), 273-282. DOI: 10.52589/AJSSHR-LR7BIBZD

Manuscript History

Received: 11 Sep 2024

Accepted: 8 Nov 2024

Published: 15 Nov 2024

ABSTRACT: *Due to the widespread sharing of phishing emails on WhatsApp, university students face a high risk of data breaches. This study examines the impact of WhatsApp phishing messages on data security among students at Chukwuemeka Odumegwu Ojukwu University Igbariam, Anambra State. The research collected survey data from 375 students out of 17,055 based on their population and adopted Social Cognitive Theory as the theoretical framework. The findings indicate that most students are aware of these phishing messages, with scam emails and fake login pages being the most common forms. Additionally, most students believe these messages threaten their data security. The study suggests holding regular educational campaigns to address this problem. This study sheds light on the alarming risks of online phishing, revealing the vulnerabilities that university students face every day. The study aims to educate, empower, and protect students from cyber threats, fostering a safer digital campus community.*

KEYWORDS: Phishing, Data security and WhatsApp messages.

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

African Journal of Social Sciences and Humanities Research
ISSN: 2689-5129
Volume 7, Issue 4, 2024 (pp. 273-282)

www.abjournals.org

INTRODUCTION

The widespread use of digital communication apps has reshaped how people connect. WhatsApp, in particular, is a popular messaging service that allows users to communicate instantly across the globe (Smith & Johnson, 2019). However, with WhatsApp's popularity comes increased concerns about data security. Enemuo, Ezeanyi and Ezeaka (2019) suggest that the future will be driven by information, and prosperity will depend on the ability to process it effectively. This study focuses on a specific threat within the WhatsApp platform: online phishing messages. Phishing involves deceptive attempts by malicious actors to trick individuals into revealing sensitive information by disguising themselves as legitimate sources.

At Chukwuemeka Odumegwu Ojukwu University, students heavily use WhatsApp, which has led to concerns about data security due to the prevalence of phishing messages.

This study aims to understand how aware COOU undergraduates are of phishing messages on WhatsApp, determine how likely they are to fall for these phishing attempts, and investigate the strategies they use to respond to phishing attempts. Based on these objectives, the study suggests ways to improve data security for these students.

With the rise of the internet, instant messaging apps like WhatsApp have become incredibly popular worldwide (Smith & Johnson, 2019). It is crucial for university students and the public to be aware of the impact of WhatsApp phishing attacks on data security. As technology advances, it is important to address these new challenges to maintain a secure online environment, especially for younger people who are often the first to use new communication apps (Williams & Lee, 2022).

COOU students rely heavily on digital platforms, particularly WhatsApp, for both social and academic purposes. However, the increasing number of phishing scams on WhatsApp poses a serious threat to the data safety of this tech-savvy generation. Comprehension of WhatsApp phishing attacks' impact on data security among university students is crucial not only for academics but also for digital communication safety. With the rise of new communication methods, it is vital to stay ahead of these risks to ensure a secure online environment for individuals across generations (Johnson, 2021). Proactive measures are necessary to protect personal data and maintain trust in digital platforms (Williams & Lee, 2022). As WhatsApp has become the top messaging app among COOU students, there has been a rise in phishing attempts. Phishing is when people try to trick you into giving them your personal information online. This can put students' data at risk. Researchers have studied phishing in general, but there is not much research on how it specifically affects COOU students, how aware they are of it, how likely they are to fall for it, and how well they can protect themselves from it.

This study investigates the risk of data security breaches among COOU students caused by WhatsApp phishing messages. The lack of knowledge about how common and harmful these phishing attempts are makes it hard to make specific plans to protect students.

The study made use of the following research questions:

1. To what extent are the respondents aware of online phishing messages from WhatsApp?
2. What is the nature of online phishing messages circulated through WhatsApp among the respondents?

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

3. Do WhatsApp online phishing messages affect respondents' data security?

This study mainly uses Bandura's Social Cognitive Theory (SCT) (1986). SCT says that people imitate and learn from the actions of others. In this case, SCT explains how WhatsApp phishing messages make COOU students more aware and responsive to them by seeing what their classmates do and say. Bandura (1986) explains that people can learn from the experiences and behaviors of others, which can build a collective understanding of cybersecurity.

Social Cognitive Theory (SCT) suggests that people learn by observing actions and outcomes of others. In this study, SCT can explain how college students enhance their understanding of phishing scams on WhatsApp. By witnessing how their friends handle these scams, they can gain knowledge and develop appropriate responses, thus improving their awareness and protective behaviors.

WhatsApp Phishing among Undergraduates

WhatsApp is widely used by university students to communicate with one another, making it a major messaging platform. However, students using WhatsApp are also exposed to online security risks, one of which is phishing. This study aims to understand the extent of WhatsApp phishing among university students, its effects, and the reasons why students are susceptible to it.

Cybercriminals often use phishing to trick people into giving up sensitive information by sending fake messages or setting up fake websites. Studies by Bada et al. (2016) and Kumar and Rajavel (2018) explain how phishing attacks work and how cybercriminals use tactics like text messages to do them. Alqarni, Alzahrani, and Alanazi (2020) studied how college students feel about the risks of phishing on messaging apps like WhatsApp. Their research shows that while students know about phishing, they do not always think it is a big deal, which makes them more likely to fall victim to attacks.

WhatsApp phishing is a serious threat to data security. Liang et al. (2017) highlight that potential threats can lead to identity theft, financial losses, and damage to reputation. It is especially prevalent among undergraduates, who may not be fully aware of the risks involved. Alam, Farhana, and Islam (2021) noted that educational interventions are crucial for mitigating these risks by raising awareness, promoting safe online behaviors, and addressing vulnerabilities.

WhatsApp phishing poses serious problems for undergraduates. To reduce risks and keep students' personal information safe, schools need to take steps to address these vulnerabilities and improve data security. Educational institutions should develop targeted strategies to combat WhatsApp phishing by understanding how common it is, how it affects students, and what causes it.

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

African Journal of Social Sciences and Humanities Research
ISSN: 2689-5129
Volume 7, Issue 4, 2024 (pp. 273-282)

www.abjournals.org

Data Security on WhatsApp

WhatsApp is a crucial tool for university students, allowing them to communicate both academically and socially. Security measures safeguard user information and communications from unauthorized access, use, or damage. These measures include:

1. End-to-End Encryption: Messages and calls are encrypted to ensure privacy between sender and recipient only.

2. Secure Connection: Data is protected during transmission using Transport Layer Security (TLS).

4. Two-Factor Authentication: Login and account access require an additional verification step.

5. Security Updates and Patches: Regular updates address vulnerabilities and enhance app security.

6. Data Storage and Backup: Stored data and backups are encrypted and restricted to appropriate individuals.

7. Privacy Settings: WhatsApp allows users to manage their privacy by controlling who can contact them, view their online status, and access their data. Despite its popularity, data security on WhatsApp raises concerns, especially related to the handling of sensitive information. This review examines the challenges, risks, and possible solutions for data security on WhatsApp in universities. WhatsApp is widely used by university students. Al-Rahmi, Othman and Musa (2018) and Mishra and Yadav (2019) indicate its popularity for communication such as group discussions, assignment coordination, and social networking.

WhatsApp's end-to-end encryption protects messages from being intercepted. However, concerns remain about data security. Research shows vulnerabilities like phishing, data leaks, and unauthorized access. Beyond message encryption, WhatsApp raises privacy concerns due to its data-sharing practices. Studies emphasize the risk of privacy breaches and call for improved security measures. Education programs are essential to raise awareness about data security among university students, reducing potential risks. Alam, Farhana, and Islam (2021) propose educational programs aimed at enhancing students' understanding of data security risks on WhatsApp and promoting responsible usage practices.

Protecting data on WhatsApp in universities is a complicated matter that involves concerns about keeping information private, encryption, and how users behave. By using a mix of rules, technology, and teaching, universities can lower risks and keep students' personal information safe on the platform.

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

African Journal of Social Sciences and Humanities Research
ISSN: 2689-5129
Volume 7, Issue 4, 2024 (pp. 273-282)

www.abjournals.org

METHOD OF STUDY

In the study, a survey research approach was used to examine how WhatsApp phishing messages affect data security among university students in Anambra State. This method allowed the researcher to gauge the opinions of a sample group and generalize their findings to the wider population. In survey research, a representative sample was selected to represent the entire study population (Nwodu, 2006). This characteristic made the survey method the most suitable choice for this particular study.

The population of the study was the entire students of Chukwuemeka Odumegwu Ojukwu University, Igbariam Campus, which according to the Academic Planning Unit of the university was 17,055.

Table 1: List of Faculties in Igbariam Campus and Their Populations

S/N	FACULTY	POPULATION
1	Agriculture	239
2	Arts	1346
3	Education	432
4	Law	739
5	Management Sciences	3853
6	Social Sciences	7846
7	Health Sciences	1050
8	Pharmaceutical Sciences	1550
	Total	**17,055**

Source: *Academic Planning Unit, COOU Igbariam*

In determining the sample size, the Krejcie and Morgan table was used to determine the sample size. The population of the study which is 17,055 is known. Krejcie and Morgan (1970) table for sample size determination was applied to obtain the sample size of 375. Therefore, the sample size for the study comprised 375 students. A total of 375 copies of structured questionnaires were distributed to the students of Chukwuemeka Odumegwu Ojukwu University, Igbariam Campus using Proportionate Allocation Formula to assign copies of questionnaires according to population strength of their faculties.

Agriculture $\frac{239 \times 375}{17,055} = 5$

Arts $\frac{1346 \times 375}{17,055} = 30$

Education $\frac{432 \times 375}{17,055} = 9$

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

Law	739 x375 / 17,055	= 16
Management Sciences	3853 x 375 / 17,055	= 85
Social Sciences	7846 x 375 / 17,055	= 173
Health Sciences	1050 x 375 / 17,055	= 23
Pharmaceutical	1550 x 375 / 17,055	= 34
Total	**375**	

The researcher purposively selected 100 level students from one department, from each faculties and adopted simple random sampling in distributing copies of the questionnaire.

The instrument of data collection is questionnaire. A total number of 375 copies of the questionnaire were distributed to the respondents (COOU) students. Three hundred and sixty-nine copies were returned and found useful while six copies were not returned and used. The study made use of a frequency distribution table, simple percentage for data analysis and presentation.

Table 3: Demographic Characteristic of Respondents

Variables	Frequency	Percentage
Gender		
Male	148	40
Female	221	60
Total	**369**	**100**
Age		
16–20	270	73
21–26	89	24
27 and above	10	03
Total	**369**	**100**

Source: *Field Study, 2024*

Most respondents (60%) are females, and the majority (73%) are between 16 and 20 years old. In this age group, females are more common (60%) than males (40%). The 21–26 age group has a fairly even gender distribution, while the proportion of females (60%) in the 27 years and above age group is greater than the proportion of males (40%) despite the small sample size. In general, the respondents are mostly young women, with a significant majority falling into the 16–20 age range.

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

Thematic Data: Answers to Research Questions

Research Question 1: To what extent are the respondents aware of online phishing messages from WhatsApp?

Table 4: Provision of Information on Respondents' Level of Awareness of Online Phishing Messages from WhatsApp

Response	Frequency	Percentage
To a great extent	142	41
To some extent	102	23
To a limited extent	125	36
Total	**369**	**100**

Source: *Field Study, 2024*

Most respondents (41%) have a strong awareness of phishing scams due to previous knowledge and precautions. However, a considerable group (36%) has limited understanding, leaving them more susceptible to phishing attempts. They might benefit from educational resources to improve their comprehension of phishing and potential risks. An additional 23% of the respondents have some awareness of phishing scams. While some individuals in this group may have a basic understanding of online phishing, they may not be fully informed about the most recent methods used by scammers. Additionally, they may not be taking enough precautions to protect themselves. Despite the fact that 41% of participants showed a high level of awareness, 36% admitted to having little awareness and 23% reported having moderate awareness. This shows that there is still space for growth, especially among those with limited or medium awareness. Educational campaigns and training programs can assist in closing these knowledge gaps and enhancing participants' capacity to recognize and prevent online phishing attempts.

Research Question 2: What is the nature of online phishing messages circulated through WhatsApp among the respondents?

Table 5: Provision of Information on the Nature of Online Phishing Messages from WhatsApp

Response	Frequency	Percentage
Scam messages	182	49
Fake login pages	101	27
Investment scams	54	15
Fake updates	32	9
Total	**369**	**100**

Source: *Field Study, 2024*

The prevalence of scam messages on WhatsApp (182 or 49%), shows how easy it is for scammers to use the platform to trick people. Scammers use the app's many users and end-to-end encryption to make people give up personal information or lose money. This problem shows how important it is to teach users how to spot and stop scam messages. The existence

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

of false login pages (101 or 27%) shows that scammers are trying to steal users' account information. This tactic takes advantage of the fact that people trust familiar login pages. This makes it clear how important it is to make sure the login page is real and to use two-factor authentication.

WhatsApp is commonly used to promote investment scams (15%) that promise quick profits. These scams take advantage of people's financial hopes and emphasize the need for careful assessment of investment options and skepticism about unsolicited financial advice. WhatsApp is also used to spread fake updates (9%). These updates can lead to the installation of harmful software or malware. This underscores the importance of confirming the source of update requests and being cautious when receiving unsolicited messages.

Research Question 3: Does WhatsApp online phishing messages affect respondents' data security?

Table 6: Provision of Information on Whether WhatsApp Online Phishing Messages Affect Respondents' Data Security

Response	Frequency	Percentage
Yes	249	67
No	120	33
Total	**369**	**100**

Source: *Field Study, 2024*

Most participants (67% or 249) express concern about WhatsApp phishing messages harming their data security, indicating they are aware of the risks. However, a minority of participants (33% or 120) do not view phishing messages as a threat, possibly due to a lack of understanding or overconfidence. These results emphasize the need for continued education about online phishing and data security measures.

DISCUSSION OF FINDINGS

The study looked at COOU undergraduate students and the "Influence of WhatsApp Phishing Messages on Data Security." The results showed that many participants (142) were very aware of phishing messages on WhatsApp, suggesting that they had a good understanding of this problem. Also, 102 participants were somewhat aware, and 125 were only slightly aware. This indicates that while most students had some level of awareness, more education and outreach are needed to raise awareness about online phishing.

Alnajim and Munro (2009) emphasized the importance of user awareness and understanding in preventing phishing attacks, and our findings support this claim, indicating that users who recognize and comprehend phishing threats are less vulnerable to their success. Regarding the types of phishing messages encountered, our results revealed that scam messages (182) were the most prevalent, followed by fake login pages (101), investment scams (54), and fake updates (32). This aligns with APWG's (2020) findings that scam messages are the most common phishing attack type. This prevalence of scam messages poses a significant risk as they can lead to financial loss and identity theft. The presence of fake login pages and

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

investment scams further highlights the potential for compromised login credentials and financial fraud, emphasizing the need for vigilance against these threats.

Research findings show that most respondents (249 out of 369) believe WhatsApp phishing messages pose a threat to their data security. Many respondents also expressed concerns about fake login pages and investment scams. This indicates that people are aware of the potential risks of phishing messages to their personal information and online safety. The high number of respondents who believe phishing messages impact data security emphasizes the need for ongoing education and awareness campaigns about online phishing and data protection. This aligns with the research by Sullivan and Jakobsson (2006), who found that phishing attacks compromise users' data security.

Undergraduates at COOU frequently encounter online phishing messages on WhatsApp, especially scam messages. Most students are aware of phishing, but there is a need to educate them further about it and data security. Most respondents recognize that phishing messages impact their data security, emphasizing the importance of addressing this issue. The study's results suggest the need for tailored awareness campaigns and educational programs to improve undergraduates' data security.

The major findings are as follows:

1. Many respondents are aware of WhatsApp online phishing messages, but there is still a significant lack of awareness.
2. Scam messages are the most common type of phishing message, followed by fake login pages, investment scams, and fake updates.
3. The majority of respondents believe that WhatsApp online phishing messages compromise their data security.

CONCLUSION

A study explored the impact of phishing messages on WhatsApp on the data security of undergraduate students at COOU. The results indicate that there is a crucial need for increased awareness and education about phishing and data protection. Students were exposed to various phishing tactics, including scam messages, fraudulent login pages, investment scams, and fake updates, making them susceptible to attacks. Additionally, the majority of the respondents acknowledged that WhatsApp phishing messages posed a threat to the security of their personal information.

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD

RECOMMENDATIONS

1. To enhance awareness and knowledge, the study suggests holding regular workshops and awareness campaigns to teach COOU students about phishing scams on WhatsApp.

2. Offer instruction on spotting and reporting suspicious messages and fabricated updates. Students will learn to spot suspicious messages, including those with urgent or threatening language, unknown senders or numbers, and requests for personal information or passwords.

3. Provide resources and support to victims of phishing attacks. Establish individual support or counseling services for students who have been victims of WhatsApp phishing scams.

REFERENCES

Alam, M. S., Farhana, R., & Islam, M. R. (2021). Educational Interventions to Enhance Awareness of WhatsApp Phishing Threats among Nigerian Undergraduate Students. International Journal of Computer Science and Network Security, 21(1), 55-60.

Al-Rahmi, W. M., Othman, M. S., & Musa, M. (2018). The Impact of WhatsApp Use on Student Performance in Secondary School. Journal of Information Technology Education: Research, 17, 419-432.

Alqarni, A., Alzahrani, A., & Alanazi, O. (2020). Nigerian Undergraduate Students' Perceptions of WhatsApp Phishing Threats: A Study on Security Awareness. International Journal of Computer Applications, 177(14), 30-34.

Bada, M., Idowu, P. A., & Owonikoko, D. (2016). A Study of Phishing Attacks on WhatsApp. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 5(2), 550-553.

Bandura, A. (1986). Social foundations of thought and action: A social cognitive theory. Prentice-Hall.

Bandura, A. (2018). Toward a psychology of human agency: Pathways and reflections. Perspectives on Psychological Science, 13(2), 130-136. doi:10.1177/1745691617719679

Brown, A., & Williams, M. (2018). Digital literacies: Concepts, policies and practices. Routledge.

Enemuo, C.J., Ezeanyi, B.C. & Ezeaka, N.B. (2019). Extent of information Communication Technology (ICT) Integration among students in Tertiary Institutions in Anambra State. *International Journal of Education and Research 7 (7)*

Johnson, A. (2021). Data security in the age of digital communication. Journal of Cybersecurity Studies, 8(2), 45-62.

Jones, C., Smith, D., & Johnson, A. (2020). Cybersecurity: Safeguarding the modern digital world. Wiley.

Liang, H., Xue, Y., & Lai, K. (2017). Impact of Phishing on Data Security: A Case Study of WhatsApp Users in Nigeria. Journal of Cybersecurity Research, 2(1), 23-36.

Mishra, P., & Yadav, A. (2019). Role of WhatsApp in Academic and Social Communication among College Students. International Journal of Information Management, 49, 17-26.

Smith, D., & Johnson, A. (2019). The impact of instant messaging on global connectivity. International Journal of Communication, 13, 1245-1263.

Williams, M., & Lee, S. (2022). Emerging challenges in digital communication security. Journal of Information Security, 14(1), 78-92.

Article DOI: 10.52589/AJSSHR-LR7BIBZD
DOI URL: https://doi.org/10.52589/AJSSHR-LR7BIBZD