

Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA

Proceedings of the Cyber Secure Nigeria Conference – 2023

Cybercrime On Social Media In Nigeria: Trends, Scams, Vulnerabilities and Prevention

Oni Damilola, Arshad Emmanuel & Pham Bich Ngoc
Department of Informatics & Computer Engineering
International School Vietnam
National University - Hanoi, Vietnam

E-mails: 21070917@vnu.edu.vn; 22070002@vnu.edu.vn; 21070100@vnu.edu.vn
Phone: +84335892092; +84374421683; +84847336153

ABSTRACT

Cybercrime on social media in Nigeria allow for an in-depth analysis of the role of social media in facilitating cybercrime activities in Nigeria, focusing on the prevalent scams, tactics used by cybercriminals, and the vulnerabilities that individuals and organizations face. It would also provide an opportunity to delve into the specific case studies, such as advance fee fraud, romance scams, and phishing, as well as exploring additional examples and their implications. By examining the impact of social media on cybercrime in Nigeria, this research contributes to a better understanding of the evolving nature of cyber threats in the digital landscape. It would also shed light on the specific challenges faced by Nigerian society, particularly with the high number of social media users in the country. Furthermore, the research proposes recommendations and strategies to enhance cybersecurity awareness, digital ethics, and protective measures for individuals, businesses, and policymakers to mitigate the risks associated with cybercrime.

Keywords: Cybercrime, Social Media, Nigeria, Trends, Scams, Vulnerabilities, Prevention

Proceedings Citation Format

Oni Damilola, Arshad Emmanuel & Pham Bich Ngoc (2023): Cybercrime On Social Media In Nigeria: Trends, Scams, Vulnerabilities and Prevention. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12th July, 2023. Pp 143-150. <https://www.csean.org.ng/>. dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P17

1. INTRODUCTION

Cybercrime is a growing threat to businesses and individuals of all sizes. Cybercriminals are increasingly using social media to target victims. Social media platforms are a rich source of information for cybercriminals.

They can use social media to gather personal information about victims, such as their names, addresses, and phone numbers. They can also use social media to exploit victims' emotions, such as their fears and desires.¹

Nigeria, a country with a population of over 200 million had over 31.6 million active social media users. With most popular social media platforms with WhatsApp having over (95%) users, Facebook having over (88.8%), Facebook Messenger having over (69.9%), Instagram having over (69.4%) and Twitter having over (61.2%). With a high number of users this social media platform is the most popular social media platform used by cybercriminals in Nigeria.² These platforms are popular because they allow cybercriminals to reach a large number of people and to build trust with their victims.

Cybercriminals in Nigeria use social media to carry out a variety of scams, with the most common scam been:

- Advance fee fraud (AFF): This is the most common type of scam in Nigeria. In an AFF scam, the cybercriminal will contact the victim and offer them a large sum of money in exchange for their personal information or bank account details.³
- Romance scams: In a romance scam, the cybercriminal will create a fake profile on a dating site or social media platform and pose as someone they are not. Scammers prey on those looking for love connections, generally by posing as potential partners. They use emotional manipulation to persuade them to provide money, gifts, or personal information. They will then build a relationship with the victim and eventually ask for money.⁴ Nigeria is one of the most common countries where romance scams originate. In 2022, the Federal Trade Commission (FTC) received over 50,000 reports of romance scams in the United States, and about 10% of those reports involved scammers from Nigeria⁵
- Phishing: In a phishing scam, the cybercriminal will send emails or text messages that appear to be from a legitimate source. These emails or text messages will often contain a link that, when clicked, will take the victim to a fake website that looks like the real website. Once the victim enters their personal information on the fake website, the cybercriminal will steal it.

The average victim of a cybercrime attack in Nigeria loses N1.2 million. This is a significant amount of money, and it can have a devastating impact on the victim's financial well-being. Most cybercriminals pick most of their victims on social media.⁶

1.1 How cybercriminals act

The findings of this research provide insights into the ways in which cybercriminals use social media to target victims. With a great increase in the numbers of social media users in Nigeria also there has been a great increase in the numbers of cybercriminals in the country. These cybercriminals have created their own techniques for stealing this information, although their preferred strategy continues to be social engineering-based attacks. A phishing attack is one of the social engineering offenses that enables the perpetrator to commit identity theft.

The biggest worry has been phishing because so many internet users fall for it. It is a form of social engineering in which a phisher tries to persuade users to give up their sensitive information by fraudulently using a reputable or well-known organization in an automated manner so that the internet user believes the message and gives the attacker the victim's sensitive information. Using Facebook as a case study these cybercriminals clone a Facebook and send the links to innocent people mostly with the promise of winning huge amount of money from network provider, once the user clicked, they are prompted to login and they input their login details with the hope of winning freebies but in the process, cybercriminals steal these login details and easily takes over the victim real Facebook account. Alternatively, cybercriminals could exploit other mediums to execute their attacks such as Voice over IP (VoIP), Short Message Service (SMS) and Instant Messaging (IM) ⁷.

Phishers have also turned from sending broadcast messages on WhatsApp, which target unspecified victims, into more selective phishing by sending their links to targeted individuals, a technique called “spear-phishing.” In order to accomplish their objectives, cybercriminals typically prey on individuals who lack digital/cyber ethics or who have received inadequate training. Individuals' susceptibility to phishing varies depending on their characteristics and level of awareness; as a result, in the majority of attacks, phishers use hacking techniques that take advantage of human nature rather than advanced technologies. More recently, these cybercriminals take advantage of the recently concluded general election to fool their prey. Many Political-themed scam messages sent by cybercriminals to their victim with the promise of huge amounts of money from a presidential or governorship candidate of a political party, they exploit this recently.

During the covid-19 pandemic, there was a huge increase in the number of cybercrimes in Nigeria as most of these criminals developed a scheme that is similar with the palliatives that the government announced.⁸ Cybercriminals also developed schemes using the identities of donors that were listed by the Nigerian government on the website of the Presidential Task Force on COVID-19 example the original covid-19 fund was set up to give beneficiaries N20,000 but cybercriminals created a fraudulent scheme to model this by creating a website with the promise of N20,000 to people who visited the website or who share the links. The scam message had a fake government seal on the upper left corner, to deceive people into thinking it was a genuine message from the federal government. A prospective victim is congratulated to be eligible for the funds after answering a series of questions. The person is required to click a green button beneath the page which has the inscription “SHARE NOW”.

The person is advised to only share with seven WhatsApp groups. Then, the person would be asked to send bank details with sensitive information i.e. BVN. They subsequently hacked their accounts and cleared the funds after this. Also, during the covid cybercriminals created another means promising people zero interest loan according to the speech given by the president to help the people with conditional cash transfer and loan. During the pandemic most people realized that the interconnectivity of social media means it is a perfect hunting ground for illegal activity, and increasingly people realized that their "friend" may not actually be their friend as various means were used by the people to achieve their malicious aim.⁹

2. STRATEGIES TO AVOID ATTACKS FROM CYBER CRIMINALS.

2.1 What can the common man do to avoid being a victim of cyber-criminals in Nigeria?

1. **Using strong and unique password on social media-** Creating strong and unique passwords for your social media accounts, including Facebook, is essential to protect your personal information from cyber criminals.¹⁰ Here are some important steps to follow when it comes to password security:
 - a. **Complexity:** Create passwords that are complex and not easily guessable. Include a combination of uppercase and lowercase letters, numbers, and special characters. Avoid using common phrases, dictionary words, or personal information that can be easily associated with you.
 - b. **Length:** Make sure your password is at least eight characters long. However, the longer the password, the more secure it will be. Aim for a password length of 12 characters or more to enhance its strength.
 - c. **Avoid Personal Information:** Refrain from using personal information such as your name, birthdate, or the names of your family members or pets in your password. This information can be easily obtained by cyber criminals through social engineering or online searches.
 - d. **Unique Passwords:** Avoid using the same password across multiple platforms or accounts. If one account gets compromised, having unique passwords will prevent unauthorized access to your other accounts.
 - e. **Password Manager:** Consider using a password manager tool to generate and securely store your passwords. Password managers can create strong passwords for you and remember them, so you don't have to rely on memory or writing them down.
 - f. **Regularly Change Passwords:** It's good practice to change your passwords periodically, even if there's no indication of a security breach. Aim to change your Facebook password at least every three to six months. Regularly updating your passwords reduces the risk of unauthorized access to your account.
2. **Think before you click:** generally, cyberattacks come through the use of social engineering by promising the victim huge amounts of money or reward after doing little tasks e.g., sharing links. It should be noted by individuals that nothing comes free, therefore any links online that promise huge amounts of money after minimal work should be regarded as a scam. The common man should know that no man will give him a huge amount of money or reward by just randomly sharing links or answering a few

questions online.¹¹ Therefore it is essential to think very well before clicking a link or forwarding a link so as not be susceptible to cyber-attacks from anyone. If you receive messages or offers that seem too good to be true, exercise caution. Cyber criminals may attempt to lure you into scams, phishing attempts, or other fraudulent activities. Verify the authenticity of such messages before taking any action.

3. **Using Multi factor authentication-** The obvious truth is Traditional user ID and password logins have a number of serious flaws, one of which is how easily credentials may be stolen. Cybercriminals can use brute force attacks to take control of a social media account without the multi factor authentication.¹² Almost all social media have Multi factor authentication but only few users are exploring this means, what is multi-factor authentication? Multi Factor Authentication (MFA) is a security mechanism that confirms a user's identity for a login or other transaction by requiring multiple ways of authentication from separate categories of credentials. Multifactor authentication combines two or more separate forms of identification: what the person is (through biometric verification methods) and what they have (such as a security token or password). Making it more difficult for an unauthorized person to access a target, such as a physical place, computing device, network, or database, is the aim of MFA. The attacker must still overcome at least one or more barriers even if one is compromised or broken in order to get access to the target. There are 3 types of multi-factor authentication,
 - a. **First type – Something You Know** – includes secret handshakes, code words, PINs, combinations, and passwords. This includes whatever you can remember and then type, say, do, perform, or otherwise remember when necessary.
 - b. **Second type – Something You Have** – encompasses all tangible objects, including USB drives, token devices, smart phones, smart cards, and keys. (A token device generates a PIN that is time-based or can calculate a response using a challenge number that the server has supplied.
 - c. **Third type – Something You Are** – incorporates any aspect of the human body that can be used for authentication, including voice, palm, retina, and iris scans in addition to fingerprints and facial recognition.
4. **Be mindful of what you share:** Avoid sharing sensitive personal information, such as your full address, phone number, or financial details, on social media platforms. Cyber criminals can exploit this information for malicious purposes, using WhatsApp as a case study WhatsApp is a popular messaging app in Nigeria. When using WhatsApp or any other social media platform, it's crucial to be mindful of the information you share, especially sensitive personal information. Here are some important considerations:
 - a. **Personal Identifiable Information (PII):** Avoid sharing sensitive PII on WhatsApp, such as your full address, phone number, social security number, financial details, or any other personally identifiable information.¹³ Cyber criminals can exploit this information for various malicious purposes, including identity theft, financial fraud, or targeted scams.

- b. **Group Chats:** Be cautious when sharing personal information within WhatsApp group chats. Ensure that the group members are trusted individuals who have a legitimate need to access the information. Avoid sharing sensitive details that are unnecessary or could potentially be misused.
- c. **Forwarded Messages:** Exercise caution when forwarding messages that contain personal or sensitive information. Verify the authenticity and relevance of the information before forwarding it to others. Think twice before sharing messages that request personal or financial information from you or others.
- d. **Encryption and Security:** Understand the security features and encryption protocols of the messaging platform you're using, such as WhatsApp's end-to-end encryption. While encryption helps protect the content of your messages, it doesn't guarantee complete security if other privacy practices are not followed. Be cautious of sharing sensitive information regardless of encryption.

By being mindful of what you share on WhatsApp and following these guidelines, you can protect your personal information from falling into the wrong hands and minimize the risk of cybercriminals exploiting your data for malicious purposes. Always prioritize your privacy and practice responsible sharing habits on social media platforms

3. CONCLUSION

In conclusion, the implications of cybercriminals in Nigeria pose significant threats to individuals and the society as a whole. As technology advances and more people engage in online activities, cybercriminals have taken advantage of this digital landscape to carry out various malicious activities. The consequences of cybercrime include financial losses, identity theft, data breaches, and emotional distress.

Nigeria, like many other countries, faces specific challenges when it comes to cybercrime. Factors such as limited cybersecurity awareness, weak legislation and law enforcement, and socio-economic conditions contribute to the prevalence of cybercriminal activities.¹⁴ It is imperative for individuals in Nigeria to be vigilant and take proactive measures to protect themselves from cyber threats, particularly on social media platforms.

It is important to recognize that combating cybercrime requires a collective effort involving government agencies, law enforcement, businesses, and individuals working together to create a safer digital environment. It is crucial for the Nigerian government to strengthen cybersecurity legislation, establish specialized cybercrime units, and enhance international cooperation to combat cybercriminal activities effectively. Additionally, fostering partnerships between educational institutions, businesses, and government agencies can help promote cybersecurity awareness and skill development¹⁵.

Ultimately, by adopting a proactive and informed approach, individuals in Nigeria can navigate social media platforms safely and protect themselves from the growing threat of cybercrime.

REFERENCES

1. Ali, Mazurina Mohd, and Nur Farhana Mohd Zaharon. 'Phishing—A Cyber Fraud: The Types, Implications and Governance'. *International Journal of Educational Reform*, 11 March 2022, 10567879221082966. <https://doi.org/10.1177/10567879221082966>.
2. BeyondTrust. 'Privilege Escalation Attack and Defense Explained'. Accessed 22 June 2023. <https://www.beyondtrust.com/blog/entry/privilege-escalation-attack-defense-explained>.
3. "'COVID-419": How Cybercriminals in Nigeria Exploited Schemes to Help People in Need | ENCA'. Accessed 22 June 2023. <https://www.enca.com/news/covid-419-how-cybercriminals-nigeria-exploited-schemes-help-people-need>.
4. cycles, This text provides general information Statista assumes no liability for the information given being complete or correct Due to varying update, and Statistics Can Display More up-to-Date Data Than Referenced in the Text. 'Topic: Social Media in Nigeria'. Statista. Accessed 22 June 2023. <https://www.statista.com/topics/10117/social-media-in-nigeria/>.
5. GCFGlobal.org. 'Internet Safety: Creating Strong Passwords'. Accessed 22 June 2023. <https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/>.
6. 'How To Avoid Online Dating Scams & Romance Swindlers'. Accessed 22 June 2023. <https://www.identityguard.com/news/online-dating-scams>.
7. Investopedia. 'What Is Personally Identifiable Information (PII)? Types and Examples'. Accessed 22 June 2023. <https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp>.
8. ISSAfrica.org. 'Cybercrime in Nigeria Demands Public-Private Action'. ISS Africa, 19 October 2020. <https://issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action>.
9. Kolade, Elizabeth. 'Cybersecurity in Nigeria's Financial Industry: Enhancing Consumer Trust and Security'. Carnegie Endowment for International Peace. Accessed 22 June 2023. <https://carnegieendowment.org/2022/05/13/cybersecurity-in-nigeria-s-financial-industry-enhancing-consumer-trust-and-security-pub-87123>.
10. Nabiebu, Miebaka, and Shishitileugiang Aniashe Akpanke. 'Covid- 19 Pandemic and Anti-Cybercrimes Crusade in Nigeria: Changing the Narratives for a Better Enforcement Regime'. *Journal of Legal, Ethical and Regulatory Issues* 24, no. 3S (16 August 2021): 1–803.
11. 'Nigerian Advance Fee Fraud | Office of Justice Programs'. Accessed 22 June 2023. <https://www.ojp.gov/ncjrs/virtual-library/abstracts/nigerian-advance-fee-fraud-0>.
12. Onuora, Augustine C. 'The Challenges of Cybercrime in Nigeria: An Overview'. *AIPFU Journal of School of Sciences (AJSS)*, 1 January 2017. https://www.academia.edu/41472768/The_Challenges_of_Cybercrime_in_Nigeria_An_Overview.
13. 'Romance Scammers' Favorite Lies Exposed | Federal Trade Commission'. Accessed 22 June 2023. <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/02/romance-scammers-favorite-lies-exposed>.

14. Security. 'What Is Cybercrime? Definition from SearchSecurity'. Accessed 22 June 2023.
<https://www.techtarget.com/searchsecurity/definition/cybercrime>.
15. 'What Are Social Engineering Attacks? (Types & Definition)'. Accessed 22 June 2023.
<https://www.digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack>.