ISSN: 2993-5377

Research Article

Open Access Journal of Applied Science and Technology

Navigating the Digital Landscape: Online Safety and Digital Citizenship in Nigeria

Chioma Ogechukwu Ozodo[2] and Musah Abdulmumini Yakubu[1*]

[1]*Faculty of Science and Computing, Prime University Abuja Nigeria*

[2]*Cyber security Department, Shanahan University Onitsha*

[*]Corresponding Author
Musah Abdulmumini Yakubu, Faculty of Science and Computing, Prime University Abuja Nigeria.

Submitted: 2025, Jun 09; **Accepted:** 2025, Jul 18; **Published:** 2025, Jul 23

Citation: Ozodo, C. O., Yakubu, M. A. (2025). Navigating the Digital Landscape: Online Safety and Digital Citizenship in Nigeria. *OA J Applied Sci Technol, 3*(3), 01-06.

Abstract

The proliferation of the internet and digital technologies in Nigeria has revolutionized modern life, offering unparalleled opportunities for communication, information, and connection. However, this increased reliance on digital technologies also exposes individuals to various online threats, including cyberbullying, phishing, identity theft, and other forms of cybercrime. This keynote paper examines the critical issues of online safety and digital citizenship in Nigeria, discussing the challenges and risks associated with online interactions. We investigate comprehensive strategies for promoting online safety and digital citizenship, including education, awareness, responsible online behavior, and collaborative efforts to foster a positive and secure digital environment. By addressing these challenges, we can empower Nigerians to navigate the internet safely and responsibly, unlocking the full potential of digital technologies for social, economic, and educational growth.

Keywords: Online Safety, Digital Citizenship, Nigerian Cybercrime Act, Cyberbullying, Cybercrime

1. Introduction

The internet has revolutionized modern life in Nigeria, transforming the way we communicate, access information, and connect with others [1]. This digital revolution has brought about unprecedented opportunities for social, economic, and educational growth, enabling Nigerians to bridge geographical divides, access global resources, and participate in the digital economy [2]. However, this increased reliance on digital technologies also exposes individuals to various online threats, including cyberbullying, phishing, identity theft, and other forms of cybercrime [3,14]. As the digital landscape continues to evolve, it is essential to address these challenges and ensure that Nigerians can navigate the internet safely and responsibly [4]. This keynote paper explores the critical issues of online safety and digital citizenship in Nigeria, highlighting the need for a comprehensive approach to promote a positive and secure digital environment.

The remaining part of this keynote paper is structured as follows: Section II Online Safety. Section III Digital Citizenship. Section IV Promoting Online Safety and Digital Citizenship. The conclusion to the paper is given in Section V.

2. Online Safety

2.1. Definition and Importance of Online Safety in Nigeria:

Online safety is the ability to understand and recognize threats that exist on the internet, as well as having the skills and knowledge to avoid these threats. This includes knowing how to keep personal information private and secure online, protecting devices from malware, avoiding harmful or illegal content, and managing online relationships safely [1].

Internet Safety focuses on concrete measures to protect oneself online, while Digital Citizenship is about promoting responsible and ethical behavior in the digital world. Internet Safety deals with personal protection, while Digital Citizenship encompasses how one's actions and behavior affect others online [5].

Why is Internet Safety Important for Student ?

Internet Safety is crucial for students of all ages because it teaches them how to protect themselves online. It emphasizes

the importance of being cautious about personal information, interacting with strangers, and understanding the potential risks and consequences of online activities [5].

2.2. Responsible Online Behaviour

Responsible online behaviour refers to ethical and respectful conduct exhibited by individuals when interacting with others and engaging in activities on the internet. It encompasses various principles and practices aimed at fostering positive digital citizenship and creating a safer online environment. Key aspects of responsible online behaviour include [6-7].

i. **Ethical Conduct:** Encouraging individuals to engage in ethical and respectful interactions online, including honesty, integrity, and empathy towards others.

ii. **Digital Footprint Awareness:** Understanding the implications of one's online presence, including the permanence of digital content and its potential impact on personal and professional reputation.

iii. **Online Identity:** Promoting authenticity and positive self-representation while being mindful of online personas and identity theft risks.

iv. **Honesty and Integrity:** Being truthful and transparent in online communications and interactions, avoiding deception, fraud, and manipulation.

2.3. Cyber Security Best Practices

Cyber security is a multifaceted profession that protects digital assets, networks, and data from unauthorized access, modification, or destruction. To navigate the digital world safely and confidently, we can adopt the following best practices [2]:

a) **Password Security:** Emphasizing the importance of strong, unique passwords and the use of password managers to safeguard accounts from unauthorized access.

b) **Phishing Awareness:** Educating individuals about common phishing techniques and how to recognize and avoid fraudulent emails, websites, and messages.

c) **Software Updates:** Stressing the significance of keeping software, operating systems, and antivirus programs up to date to patch security vulnerabilities and prevent cyber attacks.

2.4. Digital Privacy Rights

Digital privacy is a right that endeavors to protect the personal information of users who access a service via the internet. It must ensure that they are aware of, and have control over, the treatment of their data acquired on a website, application, or social network [3, 6].

Cyber crimes against property include computer vandalism, transmission of harmful programs, and denial of service [5]. Cyber crimes against government, including cyber terrorism, threaten international governments and citizens [6]. A cyber terrorist can be described as someone who launches attacks on government or organization to distort or access stored information [2]. Key concept in digital privacy rights to note include:

1) **Data Protection:** Understanding the value of personal data and the importance of safeguarding privacy rights, including consent, transparency, and control over data collection and usage.

2) **Privacy Settings:** Empowering individuals to manage privacy settings on social media platforms, web browsers, and digital devices to control the sharing of personal information.

3) **Encryption and Secure Communication:** Promoting the use of encryption tools and secure communication channels to protect sensitive data from interception and unauthorized access.

4) **Data Minimization and Retention:** Organizations should only collect the minimum amount of personal data necessary for the intended purpose and avoid collecting unnecessary or excessive information.

5) **Protection Against Decision Making:** Individuals have the right to challenge decisions made solely based on automated processing, including profiling, that significantly affect them, and request human intervention.

6) **Transparency and Accountability:** Individuals have the right to know what personal data is being collected, how it's being used, and who it's being shared with by organizations.

3. Digital Citizenship

3.1. The Role of Nigerians

A) Definition and significance of digital citizenship in Nigeria

Nigeria does not have a specific law that defines digital citizenship. However, there are several laws and regulations that relate to digital rights and responsibilities, such as:

1) **Cybercrime (Prohibition, Prevention, etc.) Act, 2015:** This law addresses cybercrime and online offenses.
2) **National Information Technology Development Agency (NITDA) Act, 2007:** This law establishes NITDA as the regulatory body for IT development and usage in Nigeria.
3) **Nigerian Communications Commission (NCC) Act, 2003:** This law regulates the communications sector, including online activities.

While there is no single definition of digital citizenship in Nigerian law, these regulations and laws collectively promote responsible online behavior and digital literacy. A digital citizen is someone with an identity on the internet, part of a digital community, and must exercise self-awareness and awareness of others [4]. Digital citizenship comes with rights and responsibilities to protect oneself

and others [9].

3.2. Critical Media Literacy Skills

Digital literacy and online safety are vital abilities for the 21st century. They enable individuals to access, assess, produce, and communicate information through digital technology, while protecting themselves and others from online threats [4].

1) **Media Literacy:** Teaching individuals to critically evaluate digital content, including news articles, videos, and social media posts, for accuracy, bias, and credibility.
2) **Fact-Checking:** Providing fact-checking tools and techniques to verify information and combat misinformation, rumors, and fake news circulating online.
3) **Critical Thinking:** Developing critical thinking skills to analyze media messages, recognize propaganda techniques, and make informed decisions in the digital age.

A-Types of online threats with Nigerian case studies

Various cybercrimes are committed daily in Nigeria, including fraudulent emails, pornography, identity theft, hacking, cyber harassment, spamming, ATM spoofing, piracy, and phishing [2, 7].

Being online brings enormous benefits to children, but it also poses risks, such as cyberbullying, online sexual exploitation, image-based abuse, exposure to sexual content online, and exposure to cyber-hate and violence (including self-harm) [2]. The prevalence of cyberbullying victimization varies widely across studies due to differences in definitions, time parameters, samples, and measurement tools [8], [10, 16-17].

1) **Cyberbullying :** Cyberbullying is a form of bullying or harassment that occurs online, including [14, 2]:

- Spreading rumors or images posted on someone's profile or passed around for others to see.
- Creating a group or page to make a person feel left out.
- Harassment through email, text message, or social networking sites.

2) **Phishing/Cyber Stalking:** Cyber stalking involves using the internet to repeatedly harass another person, potentially sexually or motivated by anger [2-3]. Leaving personal information online can make individuals vulnerable to cyber stalking

3) **Malware and Cyber Attacks:** Malware, including viruses, Trojans, and worms, can infect computer systems, destroying valuable information [2-3]. Techniques like the salami attack, which targets financial data, can be mitigated by avoiding unsolicited emails and using proprietary antivirus software [13].

4) **Online harassment or Cyber Terrorism:** Cyber terrorism refers to any act intended to instil fear by accessing and distorting useful information in organizations or government bodies using computers and the internet [2-3]. This includes cyber extortion, where hackers attack websites, email servers, or computer systems, demanding ransom in return [2].

4. Promoting Online Safety And Digital Citizenship

The internet has revolutionized modern life, offering unparalleled opportunities for communication, information, and connection. However, this increased reliance on digital technologies also exposes individuals, especially children, to various online threats [7, 9].

Being online offers children a rich universe of opportunities for learning, play, self-expression, leisure, and entertainment. Digital environments have reshaped children's lives, their families, and schools [7, 11, 15]. The internet has become ubiquitous in high-income countries, with approximately:

Figure 1 illustrates global and Nigerian internet access and usage. This data is crucial for understanding digital safety and citizenship activities' base. The graphic demonstrates that developed regions have near-universal internet connectivity for families. Eurostat (2019) reports that 98% of European homes with dependent children have internet. UK (89%), US (95%), and Australia (97%), have similar percentages (Australian Bureau of Statistics, 2016; US Census Bureau, 2019; Office for National Statistics, 2021). These data show that internet safety and digital citizenship are essential to daily life.

Data on Nigeria shows serious issues. Only 43.8% of Nigerian homes have internet connectivity (National Bureau of Statistics, 2020), leaving a huge fraction offline. Internet use varies by age and gender even among those with access. The National Population Commission (2019) reports that 63.2% of Nigerians aged 15-49 use the internet, peaking at 71% among 15-24-year-olds. Only 55% of 10-14-year-olds and 35% of 5-17-year-old households have internet connection (Multiple Indicator Cluster Survey, 2016-17; Global Kids Online, 2019).

This access discrepancy highlights the need for Nigeria to focus on online safety and digital citizenship. As we empower more Nigerians to navigate the digital landscape responsibly, we must address access gaps and provide instructional materials and safety measures to everybody, especially vulnerable populations like children and youth.

Also, just 61% of Nigerian internet users utilise the internet everyday, and gender differences (47% of women vs. 54% of men) emphasise the need for targeted inclusive digital engagement programs. We can close these gaps and make the internet safer and fairer for all Nigerians by promoting digital citizenship and online safety.

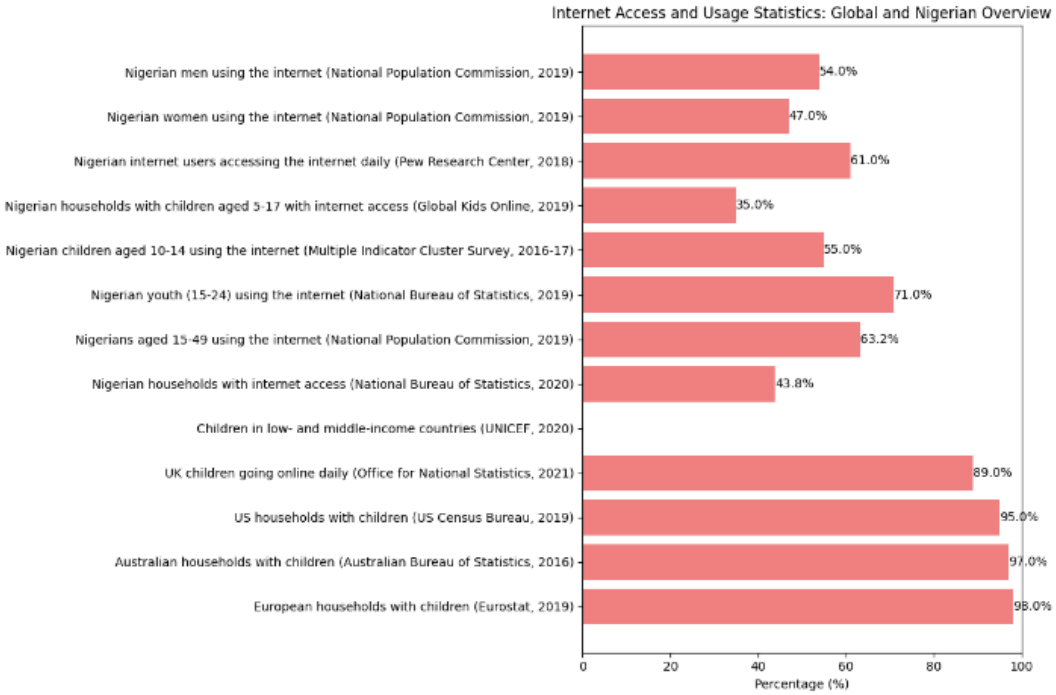

Figure 1: Internet Access and Usage Statistics [12]: Global and Nigerian Overview

4.1. Online Safety Education

Children today spend substantial time online, and being online poses new risks for their rights' violation and abuse (Committee on the Rights of the Child, 2021) [8, 10, 16]. To ensure online safety, children need education about:

- Online opportunities and risks
- Managing harms and threats online
- Using the internet in safe, respectful, and responsible ways

Schools play a vital role in promoting and teaching online safety [9]. Online safety education encompasses:

a) Digital and media literacy
b) Privacy protection
c) Intentionally enacting behaviors that support healthy, respectful, and safe online interactions [4, 8-9].

Online safety education is also referred to as e-safety education, internet safety education, cyber safety education, and 'cyberwellness' [24], with slightly different foci.

A- Strategies for Maintaining Online Safety relevant to Nigerian users.

Cyber crimes against persons include harassment, trafficking, distribution, posting, and dissemination of obscene material, including pornography and indecent exposure [3]. These crimes threaten the growth of the younger generation and can leave irreparable scars. In Nigeria, cases like the murder of Cynthia Osokogu and the experience of Uzondu, an undergraduate student who contracted HIV from a man she met on Facebook, highlight the importance of cyber security best practices [4]. Quick measures for maintaining online and digital safety include:

1) Password management
2) Privacy settings
3) Two-factor authentication.

While acknolageing Nigerian cybersecurity laws and regulations for maintaining online and digital safety are [10, 20-24]:

i. Cybercrime (Prohibition, Prevention, etc.) Act, 2015: This law criminalizes cyberbullying, online harassment, and other cybercrimes.
ii. National Information Technology Development Agency (NITDA) Act, 2007: NITDA is responsible for developing guidelines for online safety and digital literacy.
iii. Nigerian Communications Commission (NCC) Act, 2003: The NCC regulates the communications sector, including online activities, and has guidelines for online safety.
iv. Child Rights Act, 2003: This law protects children from online exploitation and abuse.
v. Violence Against Persons (Prohibition) Act, 2015: This law prohibits online harassment and violence against individuals.
vi. Freedom of Information Act, 2011: This law ensures access to information and transparency online.
vii. Data Protection Regulation, 2019: This regulation safeguards personal data and privacy online.

B. Roles and Responsibilities of Digital Citizens in the Nigerian Context

As digital citizens in Nigeria, individuals have essential roles and

responsibilities to uphold online etiquette, or netiquette, to ensure respectful and effective communication in online settings. These responsibilities include:

I. Building positive relationships by establishing trust, rapport, and a sense of community among online users [1].
II. Maintaining professionalism in professional or work-related online contexts to project a polished, credible image and build productive working relationships [2].
III. Enabling inclusive discussions by creating an environment where all participants feel welcome to contribute freely and have their perspectives heard and respected [3].
IV. Preventing harm by reducing the risk of unintentionally offending or harassing others, which can have serious interpersonal and even legal consequences [7].
V. Preserving online spaces by maintaining the functionality and integrity of online platforms, forums, and communities [5].

By embracing these responsibilities, digital citizens in Nigeria can facilitate more meaningful, productive, and respectful online interactions, ultimately enhancing the overall quality of the digital landscape.

C. Nigerian Regulatory Authorities Responsible for Internet Activities, Cybersecurity Laws, and Cyberspace are Listed in Table 1.

S/N	Regulatory Authority	Responsibility
1	Nigerian Communications Commission (NCC)	Regulates communications sector, including internet services and cybersecurity
2	National Information Technology Development Agency (NITDA)	Oversees IT development, usage, and cybersecurity
3	Cybercrime Advisory Council (CAC)	Advises on cybersecurity and cybercrime issues
4	National Cybersecurity Agency (NCA)	Coordinates national cybersecurity efforts
5	Nigerian Computer Emergency Response Team (ngCERT)	Responds to cybersecurity incidents
6	National Frequency Management Council (NFMC)	Manages radio frequency spectrum allocation
7	Nigerian Internet Registration Association (NIRA)	Manages Nigeria's top-level domain (.ng)
8	Nigerian Communications Satellite Limited (NIGCOMSAT)	Operates Nigeria's communication satellite
9	Office of the National Security Adviser (ONSA)	Advises on national security, including cybersecurity
10	Economic and Financial Crimes Commission (EFCC)	Investigates and prosecutes cybercrimes related to financial fraud
11	Nigeria Police Force (NPF)	Investigates and prosecutes cybercrimes
12	Ministry of Communications and Digital Economy	Oversees communications sector, including internet and cybersecurity

Table 1: Nigerian Regulatory Authorities for Internet Activities, Cybersecurity Laws, and Cyberspace [18-20].

5. Conclusion

Online safety and digital citizenship are critical components of responsible online behavior in Nigeria. By understanding the threats and challenges associated with online interactions, Nigerian science teachers and students can take steps to protect themselves and promote a positive online environment.

As we navigate the digital landscape in Nigeria, online safety and digital citizenship emerge as vital pillars of responsible online behavior. By acknowledging the threats and challenges, we can proactively safeguard ourselves and cultivate a positive digital ecosystem. Let us embrace this shared responsibility and foster a culture of digital citizenship that empowers our communities, promotes inclusivity, and ensures a secure online environment for all. The future of Nigeria's digital landscape depends on our collective actions today.

Acknowledgements

I wish to express my heartfelt gratitude to the Executive of STAN for the opportunity to serve as a Keynote Speaker at the 64th Annual Conference 2024, presenting on the topic "Navigating the Digital Landscape: Online Safety and Digital Citizenship in Nigeria". I am deeply appreciative of the support and trust of the Executive Director, President of STAN, and the dedicated members of the Computer Studies Panel, who worked collaboratively with me to deliver this presentation. I also extend my gratitude to the Panel Chair for their guidance and leadership throughout this process. Their collective efforts, confidence, and encouragement have made this achievement possible.

References

1. Isma'il, H., & Kari, A. G. U. (2023). Digital governance: A pathway for combating emerging public safety and security challenges in 21st century Nigeria.
2. Agbawe, M. (2018). Challenges and prospects of social media on digital natives: The case of Nigeria. *Information Impact: Journal of Information and Knowledge Management, 9*(3), 18-32.
3. Awoyemi, B. O., Omotayo, O. A., & Mpapalika, J. J. (2021). Globalization and cybercrimes: A review of forms and effects

of cybercrime in Nigeria. *Internal Journal of Interdisciplinary Research and Modern Education, 7*(1), 18-25.
4. Igwe, K. N., & Ibegwam, A. (2014). Imperative of cyber ethics education to cyber crimes prevention and cyber security in Nigeria. *International Journal of ICT and Management, 2*(2), 102-113.
5. Kperogi, F. A. (2019). Nigeria's digital diaspora: Citizen media, democracy, and participation (Vol. 87). *Rochester Studies in African H*.
6. Micheli, M., Lutz, C., & Büchi, M. (2018). Digital footprints: an emerging dimension of digital inequality. *Journal of Information, Communication and Ethics in Society, 16*(3), 242-251.
7. Oxley, C. (2011). Digital citizenship: Developing an ethical and responsible online culture. *Access, 25*(3), 5-9.
8. CRC Committee. (2021). General Comment No. 25 on children's rights in relation to the digital environment. *CRC/C/GC/25*.
9. Cortesi, S., Hasse, A., Lombana-Bermudez, A., Kim, S., & Gasser, U. (2020). Youth and digital citizenship+ (plus): Understanding skills for a digital world. *Berkman Klein Center Research Publication*, (2020-2).
10. Lievens, E. (2021). Children's rights in the digital environment. *Highlight Lecture Series: Digital Rights in Context*, (16/11/2021).
11. Unicef. (2021). The state of the global education crisis: a path to recovery: a joint UNESCO, UNICEF and WORLD BANK report. *Paris: UNESCO, cop. 2021*.
12. US Census Bureau. (2019). *Computer and internet use in the United States*.
13. Andreou, P. C., & Anyfantaki, S. (2019). Financial literacy and its influence on consumers' internet banking behaviour.
14. Chakraborty, S., Bhattacherjee, A., & Onuchowska, A. (2021). Cyberbullying: A review of the literature. *Available at SSRN 3799920*.
15. González-Betancor, S. M., López-Puig, A. J., & Cardenal, M. E. (2021). Digital inequality at home. The school as compensatory agent. *Computers & Education, 168*, 104195.
16. Ang, R. P. (2022). Bullying among children and youth in the digital age. *In Child Safety, Welfare and Well-being: Issues and Challenges* (pp. 31-45). Singapore: Springer Singapore.
17. Office for National Statistics. (2021). Children's online behaviour in England and Wales.
18. Eboibi, F. E. (2017). A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. *Computer law & security review, 33*(5), 700-717.
19. Uzoka, N. C. MORPHOLOGY OF PEOPLE/CLIENT'S LITIGATION: PROSPECTS AND CHALLENGES IN CONTEMPORARY NIGERIA. *MANAGAMANET, 295*.
20. Olusola, M., Samson, O., Semiu, A., & Yinka, A. (2013). Cyber crimes and cyber laws in Nigeria. *The International Journal of Engineering and Science, 2*(4), 19-25.
21. Nigerian Communications Commission. (2020). National Digital Economy Policy and Strategy (2020-2030).
22. Mbanaso, U. M., Kulugh, V. E., & Makinde, J. A. (2020). A framework for determination of critical national information infrastructure in Nigeria. Journal *of Information Science, Systems and Technology, 4*(3), 1-18.
23. Statistics, V. A. (2004). National Bureau of Statistics.
24. Salaam, T. (2017). National Bureau of Statistics. *NBS (National Bureau of Statistics) and MOFP, 4*, 29-118.

Copyright: *©2025 Musah Abdulmumini Yakubu, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.*