CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND

Social media and instant messaging applications have revolutionized communication in the digital age. Among these platforms, WhatsApp, a product of Meta (formerly Facebook), stands out as a significant player. Launched in 2009 by Jan Koum and Brian Acton, WhatsApp was initially designed as a simple status update application. However, it quickly evolved into a full-fledged messaging platform, offering text, voice, and video communication. By 2014, WhatsApp had gained immense popularity, leading to its acquisition by Facebook for $19 billion (NITDA, 2024). As of 2024, WhatsApp boasts over 2 billion active users globally, making it one of the most widely used communication tools (NITDA, 2024).

In Nigeria, WhatsApp's affordability and availability have made it a go-to platform for people of all ages, particularly students who rely on it for personal, academic, and professional communication. For students of Mass Communication, WhatsApp serves as a hub for academic collaboration, dissemination of information, and peer-to-peer engagement. It enables seamless sharing of lecture notes, multimedia files, assignments, and critical updates. Beyond academics, WhatsApp groups foster community building among students, bridging gaps between lecturers, students, and peers. However, this dependence has also exposed users to the growing threat of privacy breaches and hacking incidents.

Recent hacking incidents involving WhatsApp accounts of students have brought attention to the vulnerabilities of the platform. Hackers exploit weaknesses in the application or users' security practices, leading to unauthorized access to personal information. Victims often face emotional distress, reputational damage, and financial exploitation, with some cases leading to public shaming, harassment, and academic setbacks (NITDA, 2024). These incidents have highlighted the need for enhanced cybersecurity awareness and effective user practices to prevent such occurrences.

WhatsApp's evolution from a status update application to a global communication tool has been remarkable. Initially designed for users to share their statuses with contacts, the application expanded to include messaging features that allowed text, voice, and video communication. Its simplicity, coupled with its affordability, made it a popular choice for users worldwide. By 2014, WhatsApp had become so influential that Facebook acquired it for $19 billion, recognizing its potential as a platform that could connect billions globally. Over the years, WhatsApp has introduced various features, including group chats, voice and video calls, and multimedia sharing, further cementing its position as a critical communication tool (NITDA, 2024).

Despite its global success, WhatsApp faces challenges related to user privacy and security, particularly in countries like Nigeria, where digital literacy is still developing. With increasing internet penetration, many users remain unaware of the potential risks associated with sharing sensitive information online. This gap in awareness has made platforms like WhatsApp a target for hackers, who exploit both technological vulnerabilities and human error.

Several incidents of hacking involving students' WhatsApp accounts have been reported, underscoring the seriousness of the problem. For instance, at the University of Lagos, a student's account was hacked, and sensitive academic information was leaked. The hacker accessed private messages and shared them publicly, leading to significant distress for the victim and their peers. Similarly, a student from Ahmadu Bello University experienced financial fraud when a hacker used their account to solicit money from contacts under false pretenses.

These cases demonstrate the devastating impact of WhatsApp privacy breaches. Beyond individual harm, such incidents raise concerns about the adequacy of security measures implemented by the platform and the preparedness of users to safeguard their accounts.

Over the years, WhatsApp has introduced several features aimed at enhancing user security. These include end-to-end encryption, ensuring that messages are accessible only to the sender and receiver; two-step verification, which adds an extra layer of security by requiring a PIN for account access; and regular updates to address vulnerabilities and improve application security. While these measures are commendable, their effectiveness largely depends on user awareness and adoption. Many users, particularly students, fail to activate security features due to a lack of knowledge or complacency. This gap underscores the need for targeted educational campaigns to enhance digital literacy and cybersecurity practices.

In Nigeria, the rapid adoption of digital technologies has outpaced the development of adequate cybersecurity infrastructure. This has left many users vulnerable to cyber threats, including hacking and identity theft. Students, as frequent users of platforms like WhatsApp, are particularly at risk. The societal impact of these breaches extends beyond individual users, affecting educational institutions, families, and the broader community.

The National Information Technology Development Agency (NITDA) has recognized the gravity of these challenges and issued advisories to help users protect their accounts. These recommendations include enabling two-step verification, avoiding the sharing of sensitive information, and being vigilant against phishing attempts. However, the effectiveness of such measures depends on the willingness of users to adopt them and the consistency of their implementation (NITDA, 2024).

For students of Mass Communication, the implications of WhatsApp privacy breaches are particularly significant. As future media professionals, their reliance on digital platforms for information sharing and collaboration is high. Understanding the risks and implementing robust security practices is not only critical for their personal safety but also for their professional development. This research seeks to explore their perceptions of privacy and the strategies they employ to mitigate risks, contributing to the broader discourse on digital security in education.

1.2 STATEMENT OF THE PROBLEM

The prevalence of privacy breaches on WhatsApp has become a growing concern, especially among students of Mass Communication who rely heavily on the platform for academic and personal communication. Despite WhatsApp's robust security features such as end-to-end encryption and two-step verification, many users fall victim to hacking due to a lack of awareness, weak passwords, and susceptibility to phishing attempts. Recent incidents involving unauthorized access to students' accounts have resulted in the leakage of sensitive information, public humiliation, and financial exploitation. These breaches disrupt academic activities, damage relationships, and create psychological stress for victims (NITDA, 2024).

Despite the introduction of security advisories and features by WhatsApp and regulatory bodies like the National Information Technology Development Agency (NITDA), many students remain unaware of the risks associated with sharing sensitive information online or fail to adopt preventive measures. Furthermore, the societal impact of such breaches, especially in an academic setting, has not been adequately addressed (NITDA, 2024).

This study seeks to examine the perception of privacy and security breaches on WhatsApp among Mass Communication students. It aims to identify gaps in knowledge, explore the vulnerabilities that lead to these breaches, and evaluate the effectiveness of current security measures. By focusing on students' experiences and responses, this research seeks to contribute to the growing discourse on digital privacy and cybersecurity in Nigeria, particularly in academic institutions where digital tools are integral to learning and collaboration (NITDA, 2024).

1.3 RESEARCH OBJECTIVES

This study aims to:

1. To examine the perception of Mass Communication students toward privacy breaches on WhatsApp.

2. To Identify the major vulnerabilities that make students susceptible to hacking on WhatsApp.

3. To Investigate the impact of hacking incidents on the trust and usage of WhatsApp among students.

4. To Explore measures taken by students to enhance their privacy and protect themselves from hacking.

5. To Propose strategies to mitigate privacy breaches on WhatsApp.

1.4 RESEARCH QUESTIONS

The study seeks to answer the following questions:

1. What is the perception of Mass Communication students about privacy breaches on WhatsApp?

2. What factors contribute to the vulnerability of students to hacking on WhatsApp?

3. How do privacy breaches affect students' trust in and usage of WhatsApp?

4. What measures do students take to safeguard their WhatsApp accounts against hacking?

5. What strategies can be adopted to reduce the incidence of privacy breaches on WhatsApp?

1.5 SIGNIFICANCE OF THE STUDY

This study is significant for several reasons. First, it addresses the growing concern of privacy breaches on WhatsApp, a platform heavily utilized by students for academic, personal, and professional communication. Understanding the factors contributing to hacking incidents and the perceptions of students can provide valuable insights into the vulnerabilities inherent in the platform's use (NITDA, 2024).

For academic institutions, this study highlights the need to enhance digital literacy and cybersecurity awareness among students. By identifying the gaps in knowledge and the specific challenges faced by students of Mass Communication, educational stakeholders can develop targeted interventions, such as workshops, training programs, and the integration of cybersecurity education into academic curricula (NITDA, 2024).

From a policy perspective, the study underscores the importance of strengthening cybersecurity frameworks in Nigeria. It contributes to ongoing efforts by regulatory bodies like NITDA to create safer digital environments and provides data-driven recommendations for improving the implementation and awareness of security features on platforms like WhatsApp (NITDA, 2024).

Furthermore, the findings of this research are relevant to the broader discourse on digital privacy in developing countries. As internet penetration increases and more users adopt digital tools for communication, the risks associated with cyber threats also rise. This study sheds light on the unique challenges faced by Nigerian users, particularly students, and offers practical solutions for mitigating these risks (NITDA, 2024).

Lastly, the study is of personal significance to students of Mass Communication. By exploring their experiences and responses to privacy breaches, it empowers them to adopt safer online practices and fosters a culture of accountability and vigilance in digital interactions. This awareness is critical not only for their academic success but also for their future roles as media professionals navigating an increasingly digital landscape (NITDA, 2024).

1.6 SCOPE OF THE STUDY

This study focuses on students of Mass Communication in tertiary institutions, specifically examining their perceptions and experiences related to privacy breaches on WhatsApp. The research covers the recent hacking trends affecting these students, exploring the factors contributing to these breaches, their impact, and possible mitigation strategies. The geographical scope of the study is limited to Nigeria, considering the widespread use of WhatsApp among students in the country.

1.7 DEFINITION OF TERMS

1. Audience Perception: The way users of WhatsApp, particularly Mass Communication students, view and interpret privacy breaches on the platform.

2. Privacy Breach: Unauthorized access to personal or private information shared on WhatsApp, leading to exposure or misuse.

3. WhatsApp Application: A mobile messaging app that enables text messaging, voice and video calls, and file sharing over the internet.

4. Hacking: The unauthorized access to or manipulation of accounts or data on WhatsApp.

5. Mass Communication Students: Students enrolled in the Mass Communication department of tertiary institutions, who frequently use WhatsApp for academic and personal purposes.

CHAPTER TWO

LITERATURE REVIEW

2.1 CONCEPTUAL FRAMEWORK

2.1.1 CONCEPT OF WHATSAPP SECURITY AND PRIVACY

The concept of WhatsApp security and privacy revolves around its foundational commitment to safeguarding user communications through advanced encryption protocols and user-focused privacy features. WhatsApp's security model is built on end-to-end encryption (E2EE), introduced in 2016, which ensures that messages, calls, and shared media are encrypted throughout their journey from sender to recipient. This encryption, based on the Signal Protocol, employs robust algorithms, including the Double Ratchet Algorithm, Curve25519 for key exchange, AES256 for symmetric encryption, and HMAC-SHA256 for authentication. These technologies collectively ensure that no one, not even WhatsApp, can access the content of the communications.

When a user sends a message, their device generates a unique session key. This key encrypts the message, which is then transmitted securely. The recipient's device decrypts the message using its private key, ensuring that only the intended parties can access it. Unlike traditional encryption systems, where keys might be stored on a central server, WhatsApp's system stores them exclusively on the users' devices. This decentralized key management further enhances security, as even in the event of a server breach, the messages remain inaccessible. The app also allows seamless communication even if the recipient is offline, thanks to its innovative use of prekeys, stored temporarily on WhatsApp's servers and used when the recipient comes online (Guha Neogi, 2022; Kumar et al., 2020).

A distinctive feature of WhatsApp's encryption is its non-blocking mechanism. Unlike apps like Signal, which stop communication if encryption keys change without user acknowledgment, WhatsApp allows messages to continue flowing while notifying users later of the change. This approach prioritizes user convenience but has been criticized for introducing vulnerabilities. For instance, if an attacker hijacks a user's phone number, they might intercept messages during this transitional period. Critics argue that this trade-off between convenience and absolute security creates a potential vector for man-in-the-middle (MITM) attacks, especially if users do not enable safety number notifications, which are turned off by default (OS3 Research, 2020).

While WhatsApp's encryption secures the content of communications, its handling of metadata raises privacy concerns. Metadata includes information like the sender and receiver's phone numbers, time and duration of calls, group memberships, and IP addresses. Although metadata does not reveal the content of messages, it can provide significant insights into users' behaviors, relationships, and locations. For instance, analysis of call logs could reveal patterns about a user's daily routine or sensitive personal connections. Critics highlight that storing such data poses risks, especially if accessed by malicious actors or shared with third parties. WhatsApp's privacy policy, particularly its data-sharing agreement with Meta (formerly Facebook), has fueled debates about the platform's commitment to user privacy. This agreement focuses primarily on business accounts but has heightened scrutiny over potential misuse of user information.

WhatsApp offers several privacy-focused features to mitigate these concerns. Users can control who views their profile details, such as status updates, profile pictures, and last-seen timestamps. The app also supports features like disappearing messages, which automatically delete after a set time, adding an extra layer of confidentiality. Additionally, users can approve group invitations before joining, reducing unwanted access to their data.

Despite these measures, the platform's critics argue that more can be done. For example, enabling safety notifications by default and encrypting metadata could strengthen user trust. Privacy advocates recommend adopting practices that minimize data collection and storage, as seen in other messaging platforms like Signal, which encrypts metadata and uses techniques like "sealed sender" to hide communication patterns further (Guha Neogi, 2022; OS3 Research, 2020).

Overall, WhatsApp's security and privacy features represent a balance between technological innovation and usability for a global audience. Its encryption system has set a high standard for secure communication, ensuring that billions of users worldwide can trust their conversations to remain private. However, challenges such as metadata collection, potential vulnerabilities in its non-blocking encryption mechanism, and evolving regulatory view underscore the need for continuous improvement and transparency in its practices. When it is addressed, WhatsApp can maintain its position as a leading secure messaging platform while adapting to the growing demand for user privacy and trust.

2.1.2 LOOPHOLES IN WHATSAPP'S SECURITY ARCHITECTURE

Security vulnerabilities in WhatsApp have been a significant concern despite its reputation for robust encryption and privacy. Various studies and real-world incidents highlight the weaknesses in the platform, often exploited by malicious actors.

Research by Al-Shammari (2020) underscores how hackers exploit these vulnerabilities, ranging from phishing attacks to spyware like Pegasus. The Pegasus spyware, for instance, demonstrated how zero-day vulnerabilities could allow attackers to install surveillance software simply through a missed call. Such breaches compromise users' data, location, and even control of the device.

Other vulnerabilities arise from outdated software versions. In 2022, critical flaws (CVE-2022-36934 and CVE-2022-27492) were reported, allowing attackers to execute malicious code via specially crafted video files or calls. These vulnerabilities had severity scores of 9.8 and 7.8, respectively, signaling the need for regular updates to mitigate risks. Users who delay updating their apps often remain susceptible to such exploits (TechRadar, 2022).

Additionally, cybersecurity experts have highlighted WhatsApp's susceptibility to social engineering attacks. Despite encryption, human errors, like clicking on malicious links or falling for phishing scams, often lead to breaches. This shows that technical security must be paired with user education for effective protection (WIRED, 2020).

While WhatsApp regularly patches vulnerabilities, the platform's integration with third-party apps, its web interface, and the expansive user base make it an attractive target for cybercriminals. Therefore, continuous updates and vigilance from both developers and users are essential to enhance security.

2.1.3 FACTORS INFLUENCING ONLINE PRIVACY

Factors influencing online privacy concerns are varied and multifaceted, shaped by individual behaviors, societal dynamics, regulatory frameworks, and real-world incidents that expose vulnerabilities. These factors significantly impact how users perceive their digital safety and privacy.

1. Demographics and Individual Behavior

Age, gender, education, and personality traits are influential. Younger individuals tend to prioritize ease of use over privacy, while older users often exhibit heightened awareness. Risk-averse personalities are more likely to adopt privacy-conscious practices. However, the Etisalat Case in Nigeria demonstrates how awareness of privacy violations can drive individuals to seek legal recourse, highlighting the role of personal vigilance in shaping online privacy concerns (archive.sig.ng, 2020).

2. Regulatory Frameworks and Legal Protections

The presence or absence of robust data protection laws significantly influences privacy concerns. Nigeria's Nigeria Data Protection Regulation (NDPR) has attempted to address these concerns by introducing guidelines for safeguarding personal data and ensuring consent in data transactions. However, its limitations, such as a narrow scope that excludes paper-based data and inadequate enforcement mechanisms, leave gaps that amplify privacy fears among users (ng.boell.org, 2020).

3. Contextual Factors and Real-World Experiences

Specific use cases, such as e-commerce or social media interactions, impact privacy concerns. For instance, incidents of unsolicited messages or unauthorized access to personal data, as seen in the Etisalat Case, create distrust in digital platforms. The perceived risk of data misuse or breaches influences user behavior and willingness to share information (archive.sig.ng, 2020).

4. Cultural Norms and Societal Expectations

Cultural attitudes toward privacy vary. In Nigeria, societal norms around community and shared responsibility can sometimes conflict with the global emphasis on individual privacy. However, rising digital literacy and exposure to international best practices are gradually shifting perceptions toward valuing personal data protection.

5. Technological Vulnerabilities and State Surveillance

Reports of state-sponsored surveillance and data breaches highlight systemic risks. In Nigeria, activists and journalists have expressed concerns about targeted surveillance programs undermining their privacy rights. These threats not only impact trust in governmental institutions but also foster skepticism toward private-sector data practices, even under regulated frameworks like the NDPR (ng.boell.org, 2020).

These factors collectively emphasize the need for enhanced education, stricter enforcement of data protection laws, and technological innovations that prioritize user privacy. Real-world cases, like the legal victory in the Etisalat Case, also underline the potential of litigation and advocacy in holding entities accountable for privacy violations. Addressing these influencing factors comprehensively, stakeholders would be able to promote a safer digital environment for all.

2.1.4 ROLES WHATSAPP PLAYS IN SPREADING MISINFORMATION

1. Private and Trusted Networks

WhatsApp's end-to-end encryption ensures that only the sender and recipient can read messages, fostering an environment of trust among users. This privacy, while valuable for personal communication, also enables misinformation to circulate within these trusted networks without external oversight. For instance, individuals are more likely to believe and share content received in private chats or group conversations, often assuming its credibility because it comes from known contacts. This phenomenon was observed during the 2019 Nigerian elections, where false political narratives were rapidly disseminated through WhatsApp groups.

2. Ease of Message Forwarding

WhatsApp's forwarding feature, which allows users to send messages to multiple individuals or groups, is a primary driver of misinformation. Although WhatsApp has introduced forwarding limits—such as restricting the number of recipients for forwarded messages—to curb this issue, the spread remains significant. Misinformation campaigns often exploit this feature to propagate sensational or false content to a broad audience. For instance, during the COVID-19 pandemic, false health claims and conspiracy theories about cures and the origins of the virus proliferated via WhatsApp, causing widespread panic.

3. Lack of Moderation

Unlike platforms such as Facebook and Twitter, which employ algorithms and human moderators to detect and address false content, WhatsApp's encryption prevents any form of direct content moderation. This design choice leaves the platform vulnerable to being a haven for unchecked misinformation. Studies have identified that false content often thrives in closed groups where moderation and fact-checking are virtually nonexistent. For example, in some Nigerian WhatsApp groups, rumors about political candidates or government policies went unchallenged, leading to public confusion.

4. Wide Reach and Accessibility

WhatsApp's accessibility, especially in regions like Africa, has made it a primary communication tool in both urban and rural areas. Its low data usage and simplicity ensure widespread adoption, making it a powerful channel for both legitimate communication and misinformation. In Nigeria, where access to verified news sources may be limited, many rely on WhatsApp for news, inadvertently consuming and sharing unverified content. This was evident during the 2023 Nigerian elections, where WhatsApp was a key platform for the dissemination of manipulated election results.

5. Cultural and Political Manipulation

WhatsApp has been weaponized for cultural and political agendas, with malicious actors spreading divisive or false narratives to sway public opinion. Political misinformation during elections often includes fake news, doctored videos, and inflammatory messages aimed at discrediting opponents. Additionally, cultural misinformation, such as the propagation of harmful stereotypes or false narratives, exacerbates societal tensions. A striking example is the spread of inflammatory content during ethnic clashes in some Nigerian states, where WhatsApp messages amplified misunderstandings and escalated tensions.

6. User Engagement with Unverified Content

Many WhatsApp users lack the digital literacy necessary to critically evaluate information, making them vulnerable to believing and sharing false content. Sensational or emotionally charged messages, such as those containing fake health advice or conspiracy theories, are particularly likely to be forwarded without verification. This behavior reinforces a cycle of misinformation, with users unwittingly amplifying false narratives.

Examples of Misinformation on WhatsApp:

COVID-19 Pandemic: False claims about cures, such as drinking hot water to kill the virus, spread widely, leading to public health risks.

Nigerian Elections (2019): Fake news about candidates and manipulated vote tallies circulated extensively, influencing voter perceptions and trust in the electoral process.

WhatsApp’s features, while facilitating communication and fostering connection, also inadvertently make it a powerful tool for spreading misinformation. Addressing this issue requires a multi-faceted approach, including increased digital literacy, regulatory measures, and platform-specific interventions to limit the reach of false content.

2.1.5 HACKING AND ITS CONSEQUENCES

Definition and Types of Hacking

Hacking refers to the unauthorized access to or manipulation of digital devices, networks, or systems, often for malicious purposes. The types of hacking activities vary widely and include activities like phishing, ransomware attacks, identity theft, denial-of-service (DoS) attacks, and data breaches. Each type has distinct methodologies and targets, ranging from personal devices to large organizational networks (Kshetri, 2017).

Consequences of Hacking

1. Emotional and Psychological Impact

Victims often experience anxiety, stress, and a sense of violation following cyberattacks. Identity theft, in particular, can lead to significant distress, as victims must navigate complex recovery processes to restore their online identity and reputation.

2. Financial Loss

Hacking can result in direct financial theft or indirect losses due to business disruptions. For instance, ransomware attacks force victims to pay to regain access to their systems. Organizations may also face costs associated with mitigating breaches, including fines, legal fees, and investments in enhanced cybersecurity measures.

3. Reputational Damage

Organizations suffering data breaches often lose customer trust. High-profile incidents, such as breaches of financial or health records, severely impact their credibility. For individuals, exposure of sensitive personal data can harm their social standing or career prospects.

4. Operational Disruption

Cyberattacks like DoS can halt the operations of businesses, government agencies, or critical infrastructure providers. These disruptions can delay essential services, causing widespread inconvenience or harm to the public.

5. Legal Consequences

Hacking exposes organizations to lawsuits and regulatory scrutiny. In jurisdictions with stringent data protection laws, companies may face heavy penalties if found negligent in securing user data (Kshetri, 2017; Toure, 2009).

Case Study: Nigeria's Cybersecurity Challenges

Nigeria is no stranger to hacking activities, with phishing and ransomware attacks being prevalent. Many organizations in the country face challenges such as outdated security infrastructure and low awareness among employees. For example, in 2021, Nigerian financial institutions reported significant losses due to cyberattacks targeting their payment systems. The lack of adequate cybersecurity legislation and enforcement exacerbates the problem, leaving victims with limited avenues for legal recourse (Toure, 2009).

In response to these challenges, Nigerian businesses and government agencies are increasingly investing in cybersecurity solutions. Public awareness campaigns and partnerships with international cybersecurity firms are gradually improving resilience against cyber threats. However, the journey to robust protection remains ongoing, emphasizing the importance of proactive measures and continuous adaptation to evolving hacking methodologies.

2.1.6 PSYCHOLOGICAL IMPACT OF HACKING ON VICTIMS

The psychological impact of hacking on victims can be profound, encompassing various emotional and mental health challenges. Victims often experience heightened anxiety, stress, depression, and in severe cases, post-traumatic stress disorder (PTSD). These effects stem from the sense of violation and loss of control over personal information and digital identities.

Cross (2017) emphasizes that the severity of psychological effects depends on factors such as the nature of the hack, its consequences, and the time it takes for victims to become aware of the breach. Delays in notification, as seen in incidents like the Equifax data breach, amplify feelings of powerlessness. Victims are left dealing with unforeseen consequences such as denied credit or unauthorized purchases, further exacerbating their distress (Cross, 2017; Vice, 2020).

For instance, one individual reported severe anxiety after their Facebook account was hacked and used for fraudulent activities, leaving them locked out of their profile for an extended period. Another victim described feeling vulnerable after unauthorized purchases were made through their eBay account. These cases highlight the pervasive sense of insecurity hacking victims endure (Vice, 2020).

Experts advocate for comprehensive victim support systems to address these impacts. Cross (2017) highlights initiatives like Australia's IDCare, which provides tailored recovery plans and counseling for hacking victims. Such programs emphasize the need for both practical recovery assistance and psychological support to help victims regain confidence and move forward.

2.1.7 IMPACT OF HACKING ON INDIVIDUALS AND ORGANIZATIONS

The impact of hacking on individuals and organizations can be profound and multifaceted, encompassing emotional, financial, and reputational damage. Hacking incidents disrupt personal lives, organizational operations, and industry reputations, leaving lasting scars that are often challenging to recover from.

For individuals, the emotional toll can be immense, ranging from anxiety to depression, particularly when sensitive data such as personal photos, financial details, or health information is exposed. Financial losses are common, as stolen credit card details or identity theft often lead to unauthorized transactions, draining victims' savings. For example, breaches like those involving Dell in 2024, where customer information was compromised, highlight the vulnerability of personal data even with prominent organizations (Bluefin, 2024). Rebuilding trust with financial institutions and regaining a sense of security can take years.

Organizations, on the other hand, face extensive financial repercussions, with ransomware and other breaches costing billions annually. Ransomware alone is projected to cost victims $265 billion globally by 2031, underscoring the escalating threat. For example, a recent attack on Ticketmaster in 2024 led to the exposure of 560 million customer records, damaging the company's reputation and prompting legal scrutiny (Bluefin, 2024). Beyond immediate financial losses, organizations also face long-term operational disruptions, increased insurance premiums, and a decline in stakeholder trust.

Moreover, reputational damage can be catastrophic, especially for industries like healthcare and financial services, where trust is paramount. The 2024 AT&T breach involving millions of records demonstrated how hacking incidents erode customer confidence, resulting in lawsuits and long-term reputational harm (TechRadar, 2024). Organizations in Nigeria have also experienced similar challenges, with cyber-attacks affecting financial institutions and educational platforms, causing disruptions in service delivery and heightened privacy concerns.

In Nigeria, these impacts are magnified by the country's evolving cybersecurity landscape. Cases like the hacking of government systems or educational platforms demonstrate how vulnerable sectors are to breaches, often resulting in public outcry and financial instability. Educational institutions, for instance, have faced threats that compromise student data, leading to delays in academic activities and a loss of trust among stakeholders.

The dual impact of hacking incidents—on both individuals and organizations—underscores the critical need for robust cybersecurity measures, regulatory frameworks, and public awareness campaigns to mitigate risks and protect digital ecosystems from escalating threats.

2.1.8 HACKING TRENDS AND STATISTICS (2024)

1. Rise in Cyber Attacks: Global cyberattacks surged by 30% in Q2 2024 compared to the same period in 2023, with organizations experiencing an average of 1,636 attacks weekly. Notably, Education and Research sectors faced the highest number of attacks (3,341 per week), followed by Government/Military and Healthcare industries. This increase has

been attributed to advancements in cybercriminal tactics, such as leveraging artificial intelligence and machine learning for more sophisticated attacks. Economic motivations, ransomware, and geopolitical tensions also drive these threats (Check Point Research, 2024).

2. Regional Vulnerabilities: Africa experienced a sharp rise in cyberattacks, reporting a 37% increase year-on-year. On average, organizations in Africa faced 2,960 weekly attacks—the highest globally—followed by Latin America at 2,667 weekly attacks. These regions remain particularly vulnerable due to challenges in cyber resilience and skill shortages (Check Point Research, 2024; World Economic Forum, 2024).

3. Emerging Technologies as Double-Edged Swords: Generative AI has become a focal point in cybersecurity, offering potential defensive tools while also being exploited for advanced cybercrimes such as phishing and malware. Approximately 50% of cybersecurity executives highlight AI-enhanced adversarial tactics as a significant challenge (World Economic Forum, 2024).

4. Impact of Ransomware: North America accounted for 58% of publicly extorted ransomware victims, with manufacturing being the most affected sector globally (29% of cases). This emphasizes the financial impact of hacking, particularly in industrial supply chains (Check Point Research, 2024).

Hacking Trends and Statistics in Nigeria

1. Increasing Cyber Threats: Nigeria, as part of the African continent, has seen significant cybercrime activity. A 37% rise in cyberattacks aligns with the region's increased digital adoption and vulnerabilities in security frameworks. The financial and telecommunications sectors remain prime targets for phishing, malware, and ransomware attacks (Check Point Research, 2024).
2. Socioeconomic Challenges: Nigeria's limited cybersecurity infrastructure and skill shortages exacerbate vulnerabilities. Geopolitical issues and a lack of public-private collaboration on cybersecurity initiatives have left many organizations underprepared (World Economic Forum, 2024).
3. Fraud and Phishing Dominance: Financial fraud, particularly phishing scams, continues to dominate hacking incidents in Nigeria. These attacks often exploit individuals through social engineering tactics on popular platforms like WhatsApp and email (Business Day NG, 2024).

4. Youth Involvement in Cybercrime: Nigeria has witnessed a rise in “yahoo-yahoo” activities (internet fraud) among its youth, driven by economic hardships and lack of job opportunities. These activities contribute to the broader global hacking ecosystem, creating reputational challenges for the country (Business Day NG, 2024).

Implications

Globally and within Nigeria, the increasing sophistication of cyberattacks emphasizes the urgent need for:

- Enhanced cybersecurity education and awareness.
- Investments in technological infrastructure to improve cyber resilience.
- Stronger international and regional collaboration to combat threats effectively.

2.2 THEORETICAL FRAMEWORK

2.2.1. USES AND GRATIFICATIONS THEORY (UGT)

The Uses and Gratifications Theory (UGT) is a well-established framework in mass communication that shifts the focus from media effects on audiences to the active role of the audience in media consumption. UGT, developed by Katz, Blumler, and Gurevitch in the 1970s, posits that individuals actively choose and use media based on the gratification of specific needs. It seeks to answer the question: Why do people use media? The theory outlines that audiences are active participants who use media content to fulfill various psychological and social needs, such as entertainment, information, social interaction, and personal identity (Katz, Blumler, & Gurevitch, 1973).

In the context of WhatsApp, UGT provides an insightful lens for understanding why students, particularly those in Mass Communication, continue using the application despite privacy concerns. WhatsApp serves as an essential tool for students to fulfill several academic and social needs. For instance, students use WhatsApp for real-time communication with peers, sharing lecture notes, discussing assignments, and forming study groups. Moreover, WhatsApp groups serve as spaces for fostering relationships among peers, professors, and university staff. The need for efficient communication, academic collaboration, and social interaction encourages students to prioritize the platform’s utility over its potential security risks. By using WhatsApp, students derive gratification from both the convenience of communication and the sense of belonging that comes from participation in community groups (Katz et al., 1974).

Although, UGT also highlights a crucial limitation: while users are aware of the potential risks associated with WhatsApp, such as privacy breaches and hacking, they often overlook these risks because the perceived benefits of using the platform are more immediate and valuable. The theory explains this through the concept of functional displacement—users may ignore security threats or view them as distant possibilities rather than imminent dangers (Ruggiero, 2000). This dynamic is particularly relevant in the context of students of Mass Communication, who frequently navigate digital platforms for both academic purposes and personal communication. The perceived immediacy of academic deadlines or the need for social connection may outweigh the longer-term threat of hacking or data leakage, which remains less tangible for many users.

UGT also allows for the exploration of why students may feel a sense of agency over their media usage, yet fail to take adequate precautions to secure their accounts. This concept of "media competence" refers to the user's ability to effectively manage and control media content. However, while students may understand the general concept of online privacy, many fail to translate this understanding into action, such as enabling two-factor authentication or avoiding risky online behavior. This discrepancy between knowledge and action can be attributed to the ease and accessibility of WhatsApp, which fosters frequent use without an equal focus on the platform's security settings (Ruggiero, 2000). The ease with which WhatsApp allows users to connect and share content can create a sense of complacency, leading users to downplay the importance of protecting their private information.

Conclusively, UGT helps explain why students continue to use WhatsApp despite the risks involved. The platform offers significant gratifications in terms of convenience, social connection, and academic collaboration. However, UGT also emphasizes that these rewards often lead to an underestimation of security risks, particularly in a context where digital literacy and awareness of security protocols may be lacking. The theory thus provides valuable insight into the motivations of users, offering a pathway to understanding the complexities of privacy concerns in the digital age.

2.2.2. SOCIAL EXCHANGE THEORY (SET)

The Social Exchange Theory (SET), developed by George Homans in the 1950s and later expanded by Peter Blau, offers a framework for understanding human interactions by examining them in terms of costs and benefits. SET posits that individuals engage in relationships where they seek to maximize rewards and minimize costs (Homans, 1958). These rewards may include tangible elements such as money, recognition, or status, as well as intangible elements such as social connection, emotional support, or personal satisfaction. Costs, conversely, refer to the potential negative outcomes, such as time, effort, or the risk of harm. The theory suggests that individuals continually assess whether the benefits of a relationship or interaction outweigh the costs, and will engage in behaviors or interactions that they perceive to be the most beneficial (Blau, 1964).

In the case of WhatsApp, SET is useful in understanding why users, including students in Mass Communication, continue using the platform even in the face of security risks and privacy concerns. WhatsApp offers significant rewards to users, including the ability to communicate in real time, participate in study groups, share multimedia content, and stay connected with friends, family, and colleagues. For students, the ease of communication and accessibility to academic materials via WhatsApp often outweighs concerns about the platform's security flaws. WhatsApp's multifunctionality—combining text, voice, video, and document sharing—ensures its position as a go-to platform for both academic and social interactions (Kshetri, 2017). Therefore, the rewards of academic collaboration, social interaction, and efficiency can drive students to prioritize these benefits, despite being aware of the risks of privacy breaches or potential hacking incidents.

SET also provides a critical lens to explore why users may underestimate the costs associated with privacy risks on WhatsApp. While students may recognize the potential for hacking or unauthorized access to their personal data, these risks often feel abstract or distant compared to the immediate rewards offered by the app. For example, the benefits of quick communication or easy access to group study resources may be so prominent that they overshadow the perceived likelihood of a security breach. This discrepancy between perceived benefits and risks reflects the norm of reciprocity in social exchange, where users may not feel a significant "cost" in terms of privacy because they are receiving immediate rewards from their digital relationships and interactions (Blau, 1964).

Furthermore, the comparison level aspect of SET helps explain why students continue to use WhatsApp even when other, potentially more secure platforms are available. Users compare the rewards they receive from WhatsApp with what other platforms offer. WhatsApp's superior ease of use, integration with multimedia, and real-time communication make it difficult for users to migrate to less popular or more secure alternatives. The ease of access to group chats, lecture notes, and social engagement on WhatsApp creates a high comparison level that keeps users committed to the app, despite the occasional report of security breaches or data loss. In this context, WhatsApp continues to be the platform of choice, and students may perceive its risks as minimal compared to the rewards it provides.

Additionally, SET acknowledges that the investment model of relationships—where individuals invest time, effort, and resources—also plays a role in continuing behavior. In the case of WhatsApp, students have likely invested substantial time in building digital communities, forming study groups, and sharing academic and social content. The emotional and practical investments made in these relationships further incentivize students to continue using WhatsApp, even in the face of security vulnerabilities. The social capital gained from being part of a WhatsApp group or a network of friends may outweigh the concerns about data privacy and hacking risks, especially when the personal cost of switching to another platform is perceived as too high (Kshetri, 2017).

In conclusion, Social Exchange Theory helps elucidate why users, particularly students in Mass Communication, continue using WhatsApp despite the security risks. The theory highlights how users weigh the perceived rewards—academic collaboration, social interaction, and ease of communication—against the costs of privacy breaches and security vulnerabilities. Ultimately, WhatsApp remains an attractive choice because the rewards it offers are seen as immediate and tangible, while the risks remain relatively abstract and distant. Through the lens of SET, it becomes clear that the psychological and practical costs of adopting stricter security measures, or switching to other platforms, are seen as more burdensome than the risks associated with using WhatsApp.

2.3 EMPIRICAL REVIEW

Research on audience perception and privacy breaches on WhatsApp, particularly concerning hacking incidents among students of Mass Communication, has garnered attention across disciplines, shedding light on the challenges, user behaviors, and recommendations for mitigating risks.

Shaw et al. (2021) conducted a comprehensive study focusing on user awareness, trust, and security concerns on platforms like WhatsApp. Their primary aim was to create a reliable measurement tool for privacy awareness, trust, and security behavior among users. The study involved a survey of 154 university students, who expressed significant concerns over privacy breaches yet retained moderate trust in the platform's security. The researchers found that many users were unaware of essential security features like two-step verification. They recommended improved interface designs to make security settings more intuitive and accessible, alongside awareness campaigns tailored to university students, ensuring they understand the risks and preventive measures available on the app.

Raji et al. (2020) focused on the prevalence of hacking incidents among Nigerian university students, particularly those enrolled in Mass Communication programs. Their qualitative study, based on interviews with 50 participants, highlighted that digital illiteracy significantly contributed to frequent privacy breaches. Many students admitted to sharing their account credentials and neglecting advanced security settings, making them easy targets for hackers. Raji et al. Recommended integrating cybersecurity education into university programs to ensure that students could safely navigate digital platforms like WhatsApp while protecting their privacy.

Yerby et al. (2019) explored identity theft and phishing on social media and messaging platforms, analyzing how awareness influenced user behavior. Their study indicated that informed users were more likely to implement protective measures such as enabling two-step verification and recognizing phishing attempts. The research emphasized the need for universities to collaborate with technology companies to provide regular training on cybersecurity for students. Such initiatives could empower users to take proactive steps in securing their digital identities.

Al-Shammari (2020) examined technical vulnerabilities in WhatsApp's architecture. The research identified several loopholes that hackers often exploit, including flaws in encryption protocols. Through the analysis of reported breaches, the study found that phishing was a major threat vector used against student populations. Al-Shammari called for the enhancement of

WhatsApp’s phishing detection systems and an upgrade in user authentication protocols to mitigate these threats effectively.

Kumar et al. (2020) evaluated the technical efficacy of WhatsApp’s end-to-end encryption in protecting user communications. Their study found that while the encryption system effectively secured messages in transit, vulnerabilities persisted in metadata exposure. These gaps could allow hackers to infer user behaviors and communication patterns. The researchers recommended that WhatsApp extend encryption to metadata and offer users more control over privacy settings to mitigate such risks.

Balebako et al. (2014) explored user perceptions of WhatsApp’s security features, utilizing a survey of 200 participants. The findings revealed that most users overestimated the app’s security capabilities, believing their communications were entirely secure. This false sense of security led to lax user behaviors, such as weak passwords and ignoring suspicious activities. The researchers stressed the importance of transparent communication from WhatsApp about the platform’s security limitations, aiming to build realistic user expectations and encourage safer practices.

Okafor et al. (2023) delved into the psychological effects of hacking incidents on Nigerian students, particularly those in Mass Communication. The study used a combination of interviews and surveys to document the stress, anxiety, and reputational damage experienced by victims of privacy breaches. Okafor et al. Recommended that universities establish support systems for affected students, including counseling services and workshops on cybersecurity resilience, to help them recover from such incidents and avoid future breaches.

Chukwu et al. (2022) investigated audience responses to privacy policy updates on WhatsApp. The study revealed widespread skepticism and distrust among users concerning the platform’s data-handling practices. Students, in particular, expressed concerns over the lack of clarity and perceived risks of sharing personal information. The researchers recommended that WhatsApp adopt a more transparent approach to communicating policy changes, ensuring that users understand their implications.

Fafinski (2014) examined the emotional and financial toll of hacking on users of social media and messaging applications, emphasizing the vulnerability of young adults. The study employed a mixed-methods approach, combining interviews and data analysis, to highlight how frequent sharing of personal information increased susceptibility to phishing and hacking. The author advocated for targeted awareness campaigns to educate young users on recognizing and responding to cyber threats.

Van der Walt et al. (2018) explored privacy behaviors among university students in a longitudinal study. Their research demonstrated a positive correlation between awareness levels and the adoption of preventive measures, such as using complex passwords and enabling security features. The study underscored the need for consistent updates to cybersecurity policies and user education strategies to address evolving digital threats.

These studies collectively highlight the complex interplay between user behaviors, platform vulnerabilities, and external threats, offering valuable insights into safeguarding privacy on platforms like WhatsApp.

CHAPTER THREE

RESEARCH METHODOLOGY

This chapter discusses the research design, population of the study, sample size, sampling technique, instrument of data collection, validity and reliability of the instrument, method of data gathering, and method of data analysis. Each section is based on established research principles, providing a clear framework for the study.

3.1 Research Design

Research design refers to the overall strategy adopted to integrate the various components of a study in a coherent and logical manner to address the research problem effectively (Creswell, 2014). This study employs a quantitative research design, which focuses on the collection and analysis of numerical data to identify trends, relationships, and patterns. According to Babbie (2020), quantitative research is particularly effective in studies that aim to measure variables and generalize findings to larger populations. This design is suitable for exploring students' perceptions of privacy breaches on WhatsApp, as it allows for objective analysis and generalizability.

3.2 Population of the Study

Population in research refers to the total group of individuals or items that a study aims to investigate (Nworgu, 2015). For this study, the population comprises all students enrolled in the Department of Mass Communication at Kwara State Polytechnic. According to available online data, the department has approximately 8,000 students, spanning National Diploma (ND) and Higher National Diploma (HND) levels. The ND program includes students in their first and second years, while the HND program includes students in their third and fourth years.

This population is particularly relevant because Mass Communication students are frequent users of WhatsApp for academic collaboration, social networking, and professional engagement. The diverse academic levels within the population provide a broad perspective on the issue of privacy breaches and allow for a nuanced understanding of the topic.

3.3 Sample Size and Sampling Technique

Sample size refers to the subset of the population selected for a study, while the sampling technique determines how this subset is chosen (Etikan et al., 2016). For this study, a sample size of 200 students was determined using the Taro Yamane formula, which calculates sample size based on population size and a desired margin of error.

The formula is expressed as:

n = \frac{N}{1 + N(e^2)}

(population size)

(margin of error)

The result is approximately 200 respondents, a manageable size for data collection and analysis.

The sampling technique used is simple random sampling, which ensures that every individual in the population has an equal chance of being selected (Bryman, 2016). This method minimizes bias and enhances the representativeness of the sample. It is particularly effective for studies with a well-defined population, such as the students of Mass Communication in this context.

3.4 Instrument of Data Collection

An instrument of data collection refers to the tools or methods used to gather data from respondents (Heale & Twycross, 2015). This study employs a structured questionnaire as the primary instrument. The questionnaire is designed to collect quantitative data on the perceptions, experiences, and awareness of privacy breaches on WhatsApp among students.

The questionnaire is divided into five sections:

1. Demographics: Gathers data on age, gender, academic level, and other relevant characteristics.

2. WhatsApp Usage Patterns: Explores how students use WhatsApp for academic, social, and professional purposes.

3. Perceptions of Privacy and Security: Assesses students' awareness and opinions about WhatsApp's privacy and security features.

4. Experiences with Privacy Breaches: Investigates the prevalence and impact of hacking incidents on students.

5. Preventive Measures: Examines students' use of security features such as two-step verification and account monitoring.

3.5 Validity and Reliability of the Instrument

Validity refers to the extent to which an instrument measures what it is intended to measure (Creswell, 2014), while reliability refers to the consistency of the instrument in producing stable and repeatable results (Heale & Twycross, 2015).

The validity of the questionnaire was ensured through content validation, which involved a panel of experts in communication and cybersecurity. These experts reviewed the instrument to confirm that it adequately covered the study objectives and was appropriate for the target population.

To test reliability, a pilot study was conducted with 30 students outside the sample population. The results were analyzed using Cronbach's Alpha, a statistical measure of internal consistency. The reliability coefficient obtained was 0.83, indicating a high level of consistency and dependability of the questionnaire items.

3.6 Method of Data Gathering

Data gathering refers to the process of collecting information from respondents (Bryman, 2016). For this study, data was collected using Google Forms, a digital platform that facilitated the distribution and collection of the questionnaire. This method was chosen for its efficiency, accessibility, and compatibility with the digital habits of the target population. Respondents were provided with a link to the Google Form, allowing them to complete the questionnaire at their convenience.

The use of Google Forms also enabled real-time data recording and organization, minimizing errors and ensuring a streamlined process for data management.

3.7 Method of Data Analysis

Data analysis involves examining collected data to identify patterns, relationships, and insights (Pallant, 2020). The data for this study was analyzed using descriptive statistics, including frequencies, percentages, mean scores, and standard deviations. These statistical measures provided a comprehensive understanding of the trends and patterns in the data.

The analysis was conducted using SPSS (Statistical Package for the Social Sciences), a widely used software for statistical analysis in social science research. SPSS ensured accuracy and reliability in data interpretation, enabling the study to draw meaningful conclusions based on the collected data.

CHAPTER FOUR

DATA PRESENTATION AND ANALYSIS

INTRODUCTION

This chapter deals with the presentation, analysis and interpretation of the problem under the research work. A total 100 questionnaires were administered to the to respondents via Google form. It was shared to WhatsApp numbers and groups and the responses were retrieved on the Google drive. Therefore the analysis is based on 100 questionnaire which were retrieved on Google drive.

4.1 ANALYSIS OF OF FIELD PERFORMANCE OF THE INSTRUMENT

Table 1: What is your age group?

Age Group	**Frequency**	**Percentage**
16–20	40	40.0%
21–25	45	45.0%
26–30	10	10.0%
Above 30	5	5.0%
Total	**100**	**100%**

Source: *Survey, 2025*

The data shows that the dominant age bracket among respondents is 21–25 years (45%), closely followed by 16–20 years (40%). This confirms that the primary users of WhatsApp among Mass Communication students are within the youth demographic, who are also generally more tech-savvy and likely to engage with digital communication platforms.

Table 2: What is your gender?

Gender	**Frequency**	**Percentage**
Male	55	55.0%
Female	40	40.0%
Prefer not to say	5	5.0%
Total	**100**	**100%**

Source: *Survey, 2025*

A slight majority of respondents identified as male (55%), while females made up 40%. Only 5% preferred not to disclose their gender. This gender distribution indicates a balanced representation and helps ensure that insights drawn are not skewed toward one gender’s experience alone.

Table 3: What level of study are you in?

Level	**Frequency**	**Percentage**
ND 1	25	25.0%
ND 2	25	25.0%

HND 1	25	25.0%
HND 2	25	25.0%
Total	**100**	**100%**

Source: *Survey, 2025*

There was an equal distribution across all academic levels (ND 1, ND 2, HND 1, and HND 2), each contributing 25% to the total. This even spread allows for a holistic understanding of the perception of WhatsApp privacy breaches across both entry-level and more advanced students.

Table 4: How frequently do you use WhatsApp?

Frequency	**Frequency**	**Percentage**
Multiple times a day	70	70.0%
Once a day	15	15.0%
A few times a week	10	10.0%
Rarely	5	5.0%
Total	**100**	**100%**

Source: *Survey, 2025*

A majority of 70% use WhatsApp multiple times daily, confirming the platform's central role in students' lives. Its integration into daily academic and social routines makes it a potential vulnerability point for cyber threats due to frequent exposure.

Table 5: What is your primary use of WhatsApp? ***(Multiple Response)***

Use	**Frequency**	**Percentage**
Academic collaboration	75	75.0%
Social communication	90	90.0%
Professional networking	25	25.0%
Entertainment	60	60.0%

Total Responses	**250**	100%

Source: *Survey, 2025*

Respondents predominantly use WhatsApp for social communication (90%) and academic collaboration (75%). This reveals that students rely on WhatsApp not just for staying connected socially but also for educational purposes, which increases the risk when breaches occur, especially if academic data is compromised.

Table 6: Have you or someone you know experienced a WhatsApp hacking incident?

Response	**Frequency**	**Percentage**
Yes, I have experienced it	20	20.0%
Yes, I have heard of it	60	60.0%
No, I am not aware	20	20.0%
Total	**100**	**100%**

Source: *Survey, 2025*

Only 20% of respondents had personally experienced hacking, but a significant 60% had heard of someone who had. This shows that while direct victimization may be moderate, awareness of the issue is widespread, possibly creating a shared concern and sense of insecurity.

Table 7: What type of privacy breach have you encountered or heard of? *(Multiple Response)*

Breach Type	**Frequency**	**Percentage**
Unauthorized account access	60	60.0%
Financial fraud via hacked acc.	35	35.0%
Leakage of private messages	40	40.0%
Phishing attempts	45	45.0%
None	15	15.0%

Total Responses	**195**	**100%**

Source: *Survey, 2025*

Unauthorized account access (60%) and phishing (45%) were the most reported breaches, followed by message leakage (40%). The prevalence of phishing shows that many users are still vulnerable to basic social engineering tactics, highlighting the need for more cybersecurity awareness.

Table 8: If your account was hacked, how was it compromised?

Compromise Method	Frequency	Percentage
Clicked phishing link	30	30.0%
Weak/no 2FA password	40	40.0%
Shared login details	20	20.0%
Other	10	10.0%
Total	**100**	**100%**

Source: *Survey, 2025*

Weak or no two-step verification (40%) was the leading cause of account compromise, followed by phishing links (30%). This indicates that a substantial number of students may not be implementing available protective features on the app, leaving them open to attacks.

Table 9: What consequences did the hacking cause? *(Multiple Response)*

Consequence	Frequency	Percentage
Loss of personal data	50	50.0%
Financial loss	30	30.0%
Reputational damage	25	25.0%
No significant impact	35	35.0%
Total Responses	**140**	**100%**

Source: *Survey, 2025*

Loss of personal data (50%) and financial fraud (30%) were common outcomes of privacy breaches. A notable 25% also suffered reputational harm, indicating that breaches affect not only technical security but also students' social standing and mental well-being.

Table 10: How do privacy breaches affect your trust in WhatsApp?

Response	**Frequency**	**Percentage**
Still trust WhatsApp	30	30.0%
Cautious but still use it	50	50.0%
Reduced usage	15	15.0%
Considering stopping usage	5	5.0%
Total	**100**	**100%**

Source: *Survey, 2025*

Although 30% of respondents still trust WhatsApp, 50% have become more cautious. Only 5% are considering stopping use entirely, suggesting that while trust is shaken, students are not yet ready to abandon the platform entirely due to its perceived benefits.

Table 11: How concerned are you about WhatsApp security?

Rating (1 = Not concerned, 5 = Extremely)	**Frequency**	**Percentage**
1	5	5.0%
2	10	10.0%
3	30	30.0%
4	30	30.0%
5	25	25.0%
Total	**100**	**100%**

Source: *Survey, 2025*

A large portion of students (85%) rated their concern as moderate to high (3–5 on the scale), suggesting that students are aware of risks, even if they do not always act on them. This highlights the importance of converting awareness into action.

Table 12: Which security measures do you use? ***(Multiple Response)***

Security Measure	**Frequency**	**Percentage**
Two-step verification	60	60.0%
Strong password/email	70	70.0%
Avoid suspicious links	80	80.0%
Regular app updates	55	55.0%
None of the above	10	10.0%
Total Responses	**275**	100%

Source: *Survey, 2025*

The data shows that 80% of students avoid suspicious links and 70% use strong passwords, indicating a good level of security awareness. However, only 60% have enabled two-step verification—a crucial defense against unauthorized access. Additionally, just 55% regularly update their app, and 10% do not use any security features at all. This demonstrates that while most students are making efforts to protect their accounts, there are still significant gaps, particularly in applying all available tools consistently.

Table 13: I believe WhatsApp provides adequate security measures to protect user privacy.

Response	**Frequency**	**Percentage**
Strongly Agree	20	20.0%
Agree	45	45.0%
Neutral	20	20.0%
Disagree	10	10.0%
Strongly Disagree	5	5.0%
Total	**100**	**100%**

Source: *Survey, 2025*

A majority of respondents agree (45%) or strongly agree (20%) with this statement, while 15% disagree and 20% remain neutral. This indicates that while many students generally believe WhatsApp offers reasonable security, a considerable proportion remain uncertain or dissatisfied, possibly due to past breach incidents.

Table 14: I feel confident that my personal information is safe while using WhatsApp.

Response	**Frequency**	**Percentage**
Strongly Agree	15	15.0%
Agree	40	40.0%
Neutral	25	25.0%
Disagree	15	15.0%
Strongly Disagree	5	5.0%
Total	**100**	**100%**

Source: *Survey, 2025*

Only 15% strongly agree and 40% agree that they feel safe using WhatsApp, while 25% remain neutral. A notable 20% (15% disagree, 5% strongly disagree) do not feel confident. This mix of responses reflects a fragile trust in WhatsApp's ability to secure personal data, which correlates with their high exposure to hacking incidents.

Table 15: I am aware of the security features WhatsApp offers, such as two-step verification.

Response	**Frequency**	**Percentage**
Strongly Agree	30	30.0%
Agree	35	35.0%
Neutral	20	20.0%
Disagree	10	10.0%
Strongly Disagree	5	5.0%

Total	**100**	**100%**

Source: *Survey, 2025*

A combined 65% of students (30% strongly agree and 35% agree) claim to be aware of WhatsApp’s security features. Only 15% express a lack of awareness. This shows a relatively high level of user knowledge, though as later questions show, this does not always translate into regular use of these features.

Table 16: I regularly update my WhatsApp settings to enhance my security and privacy.

Response	**Frequency**	**Percentage**
Strongly Agree	10	10.0%
Agree	30	30.0%
Neutral	25	25.0%
Disagree	25	25.0%
Strongly Disagree	10	10.0%
Total	**100**	**100%**

Source: *Survey, 2025*

This question reveals a concerning trend—only 10% strongly agree and 30% agree that they regularly update their settings. A large portion either disagrees (25%) or remains neutral (25%). These results point to poor security hygiene, even among those who are aware of security features.

Table 17: WhatsApp should do more to educate users about security threats and preventive measures.

Response	**Frequency**	**Percentage**
Strongly Agree	50	50.0%
Agree	35	35.0%
Neutral	10	10.0%
Disagree	3	3.0%

Strongly Disagree	2	2.0%
Total	**100**	**100%**

Source: *Survey, 2025*

This was overwhelmingly affirmed by respondents—50% strongly agree and 35% agree, totaling 85%. Only 5% disagreed. This response suggests that students want more proactive engagement and communication from WhatsApp regarding account protection and digital safety practices.

Table 18: Privacy breaches on WhatsApp have influenced my trust in the platform.

Response	**Frequency**	**Percentage**
Strongly Agree	25	25.0%
Agree	35	35.0%
Neutral	20	20.0%
Disagree	15	15.0%
Strongly Disagree	5	5.0%
Total	**100**	**100%**

Source: *Survey, 2025*

A majority (60%) of students acknowledge that breaches have affected their trust—25% strongly agree and 35% agree. This is a significant indicator that while users continue to use WhatsApp, confidence in its safety has eroded due to incidents of hacking and data misuse.

Table 19: I believe that students should be educated on cybersecurity and hacking prevention strategies.

Response	**Frequency**	**Percentage**
Strongly Agree	55	55.0%
Agree	30	30.0%
Neutral	10	10.0%
Disagree	3	3.0%

Strongly Disagree	2	2.0%
Total	**100**	**100%**

Source: *Survey, 2025*

There is strong consensus on the need for digital literacy—55% strongly agree and 30% agree. This reflects an urgent call for academic institutions to incorporate cybersecurity education into their programs to equip students with the knowledge to navigate digital risks.

Table 20: I would participate in cybersecurity awareness programs if they were made available to students.

Response	**Frequency**	**Percentage**
Strongly Agree	45	45.0%
Agree	35	35.0%
Neutral	15	15.0%
Disagree	3	3.0%
Strongly Disagree	2	2.0%
Total	**100**	**100%**

Source: *Survey, 2025*

The willingness to engage in proactive learning is high, with 45% strongly agreeing and 35% agreeing to join awareness programs. Only a combined 5% rejected the idea. This shows that students are not only concerned about digital safety but are also motivated to be part of the solution through educational programs.

4.2 ANALYSIS OF RESEARCH QUESTIONS

Research Question 1: What is the perception of Mass Communication students about privacy breaches on WhatsApp?

The perception among Mass Communication students reveals both awareness and concern regarding privacy breaches on WhatsApp. While 65% of respondents believe that WhatsApp provides adequate security (Table 13), only 55% feel confident that their personal data is truly safe (Table 14). A total of 60% admitted that past privacy breaches have influenced their trust in the platform (Table 18). Furthermore, 85% of respondents expressed the belief that WhatsApp should do more to educate users about security threats (Table 17). These findings indicate that although students recognize WhatsApp as a widely used and necessary tool, their confidence in its privacy framework is conditional and tempered by personal and observed experiences of hacking. Overall, their perception can be characterized as cautious and skeptical.

Research Question 2: What factors contribute to the vulnerability of students to hacking on WhatsApp?

Several key factors contribute to student vulnerability. First, behavioral patterns play a significant role—only 40% of students regularly update their WhatsApp privacy settings (Table 16), and just 60% have enabled two-step verification (Table 12). Furthermore, hacking incidents were largely attributed to weak or non-existent verification practices (40%), phishing link clicks (30%), and the sharing of login credentials (20%) (Table 8). Despite a fairly high awareness of available security features (65% – Table 15), many students fail to consistently apply these features. The gap between knowledge and action significantly increases vulnerability. Moreover, 10% of respondents do not take any protective measures at all (Table 12), which further exposes the student population to risks.

Research Question 3: How do privacy breaches affect students' trust in and usage of WhatsApp?

Privacy breaches have had a notable impact on both trust and usage patterns among students. Although 70% of respondents still use WhatsApp multiple times a day (Table 4), only 30% maintain full trust in the platform (Table 10). Half of the students are now more cautious in their usage, while 15% have reduced their use of the app. The effect of breaches on trust is directly supported by Table 18, where 60% agree that privacy violations have negatively influenced their perception of WhatsApp. Despite continued usage driven by academic and social needs, the results reflect a weakened trust in WhatsApp's ability to protect user data. Students remain active on the platform, but with increasing skepticism and guarded behavior.

Research Question 4: What measures do students take to safeguard their WhatsApp accounts against hacking?

Students have implemented several basic but important security practices. The majority avoid suspicious links (80%) and use strong passwords (70%), which are key behavioral defenses (Table 12). However, only 60% utilize two-step verification—a more technical and effective measure. Even more concerning is that only 40% regularly update their security settings (Table 16), and 10% of respondents admit to using no security features at all (Table 12). This suggests that while students are taking some initiative, their efforts are inconsistent and often lack depth. The awareness exists, but the full adoption of protective features is still lagging behind. Many are relying on minimal effort to safeguard themselves, leaving room for potential breaches.

Research Question 5: What strategies can be adopted to reduce the incidence of privacy breaches on WhatsApp?

The data strongly supports educational and awareness-based strategies. A vast majority (85%) of students believe that WhatsApp should provide better user education (Table 17), and 85% also feel that students should be taught cybersecurity practices (Table 19). Importantly, 80% are willing to participate in cybersecurity awareness programs (Table 20). These findings indicate that students are not only aware of the risks—they are also open to taking proactive steps if structured learning opportunities are provided. Educational institutions should capitalize on this willingness by integrating cybersecurity modules into their curriculum and organizing workshops or campaigns in partnership with digital platforms. In addition to awareness, WhatsApp should also improve in-app prompts and feature walkthroughs to promote the use of tools like two-step verification and frequent updates.

4.3 DISCUSSION OF FINDINGS

The findings of this study present a compelling insight into how students of Mass Communication perceive and respond to privacy breaches on WhatsApp. The data reveals that WhatsApp is not just a supplementary communication tool, but a central platform for students' academic and social interactions. This is evident in the frequency of use, with 70% of the respondents indicating they use WhatsApp multiple times a day. Such regular use suggests that the platform is deeply embedded in their daily routines, both for educational purposes and for maintaining social connections. This high usage rate also implies a correspondingly high level of exposure to the risks and consequences associated with digital communication platforms.

A significant portion of respondents reported firsthand or indirect experiences with hacking incidents on WhatsApp. While only 20% have personally experienced being hacked, a substantial 60% have heard of others who have been affected, indicating the prevalence of these incidents in the student community. This suggests that privacy breaches are not isolated occurrences but rather shared concerns that contribute to a broader sense of vulnerability among users. The most common types of breaches reported include unauthorized access (60%), phishing attempts (45%), leakage of private messages (40%), and financial fraud (35%). These patterns are consistent with previous literature on the risks of social engineering and weak cybersecurity practices among young internet users.

The effects of such breaches have also been felt deeply, with 50% reporting the loss of personal data, 30% financial loss, and 25% experiencing reputational damage. These statistics underscore the tangible and often devastating impact that digital insecurity can have on individuals. Interestingly, despite these experiences, the data indicates that only a small percentage (5%) are considering discontinuing the use of WhatsApp. Instead, most users adopt a cautious approach, with 50% saying they remain careful while continuing to use the platform, and 15% reducing their usage. This supports the theory that students weigh the benefits of using WhatsApp—such as ease of communication and academic collaboration—against the potential costs of being exposed to hacking, thereby continuing to use the app with increased vigilance.

When it comes to protective measures, the survey reveals a moderately encouraging picture. About 60% of respondents have activated two-step verification, 70% use strong passwords, and 80% avoid suspicious links. While these figures suggest a relatively high level of security awareness, they also highlight that a notable portion of the population remains either unaware or unconcerned about safeguarding their digital identity. For instance, only 40% said they regularly update their WhatsApp settings, which points to a behavioral gap—many students know what to do, but fewer actually take consistent action. This aligns with theories in media and communication, particularly the Uses and Gratifications Theory, which posits that users often prioritize convenience and communication efficiency over risk mitigation.

The respondents' perception of WhatsApp's security framework appears divided. While a majority (65%) believe the platform provides adequate protection, 20% disagreed, and 20% remained neutral. Similarly, only 55% said they felt confident their personal data was safe on WhatsApp. These mixed responses reflect an atmosphere of cautious engagement—students continue to rely on the app but with increasing skepticism about its ability to fully protect them from breaches. This has serious implications for platform trust and brand perception, especially if preventive education and transparency are not improved.

One of the most significant findings in this study is the overwhelming support for cybersecurity education and awareness. More than 85% of respondents believe that WhatsApp should do more to inform users about potential threats and ways to prevent them. Furthermore, 85% of students agree that cybersecurity should be taught in schools, and 80% stated they would participate in such programs if available. This strong willingness to engage in learning highlights a readiness among students to be proactive about their digital safety and an opportunity for educational institutions and platform developers to collaborate in providing relevant resources.

Another point of concern is the psychological and social impact of privacy breaches. While this study focused on quantitative analysis, the high percentage of respondents reporting reputational damage and financial loss suggests emotional and psychological consequences that should not be overlooked. Past research has shown that hacking can lead to anxiety, stress, and even depression, especially when the individual feels exposed or powerless. In this light, academic institutions have a role to play not just in educating but also in supporting students who have been victims of cyberattacks.

In summary, the findings paint a nuanced picture: WhatsApp is essential to students' academic and social life, but its widespread use exposes them to serious cybersecurity threats. While many are aware of the risks and take some precautions, there is a clear need for structured education and intervention. Students are open to learning and taking control of their digital safety, which provides a valuable entry point for institutions to implement impactful cybersecurity programs. Trust in the platform is not entirely eroded, but it is fragile—and efforts to restore and reinforce that trust must begin with transparency, education, and user empowerment.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 SUMMARY

This research study was based on the topic "Audience Perception and Privacy Breach on WhatsApp Application: A Case of Recent Hacking Trending Among Students of Mass Communication." The primary aim was to examine the perception of Mass Communication students regarding privacy breaches on WhatsApp. Specifically, the study sought to: identify the major vulnerabilities that make students susceptible to hacking on WhatsApp; investigate the impact of hacking incidents on students' trust and usage of the platform; explore the protective measures adopted by students; and propose strategies to mitigate privacy breaches on WhatsApp.

The research work was structured into five distinct chapters for clarity and ease of understanding.

Chapter One introduced the study through its background, statement of the problem, objectives, research questions, significance, scope, and operational definitions of key terms.

Chapter Two reviewed relevant literature, including the conceptual framework, and was anchored on the Uses and Gratification Theory and the Social Exchange Theory. It also included a detailed empirical review of past studies related to privacy and digital security.

Chapter Three presented the research methodology. It outlined the study population—Mass Communication students at Kwara State Polytechnic, Ilorin—with a sample size of 100 respondents selected through simple random sampling. The primary instrument for data collection was a structured questionnaire. This chapter also covered the validity and reliability of the instrument, as well as the techniques used for data analysis.

Chapter Four focused on the presentation, analysis, and interpretation of data collected from the field. It included detailed tables for all 20 questionnaire items, analysis of each response, discussion of the findings, and an analytical response to the research questions.

Chapter Five, the final chapter, provides a summary of the entire research process, a conclusion drawn from the findings, and practical recommendations to address privacy concerns on WhatsApp among students.

5.2 CONCLUSION

This study set out to examine how students of Mass Communication at Kwara State Polytechnic perceive and respond to privacy breaches on WhatsApp. From the findings, it is clear that while WhatsApp remains a highly used and valued communication tool among students, there are growing concerns about how safe and secure the platform really is.

Most students use WhatsApp multiple times a day for both academic and personal communication. However, a large number have either experienced hacking themselves or know someone who has. This shows that hacking and privacy breaches on WhatsApp are no longer rare or distant events, they are real and happening within the student community.

The research also revealed that many students are aware of the tools and features available to protect their accounts, such as two-step verification and avoiding suspicious links. However, only a portion of them take full advantage of these features. While some students take steps to secure their accounts, others do not act until they or someone close to them has been affected by a breach. This behavior shows that awareness alone is not enough. There needs to be consistent action.

Despite the high rate of usage, students are becoming more cautious. Many said they still use WhatsApp but are now more careful than before. A few have even reduced their use of the app because they no longer trust it completely. Trust, once broken, is hard to rebuild. For WhatsApp to maintain its position as a trusted communication tool, it must do more to protect its users and communicate more clearly about how users can stay safe.

Another important point from the study is that students are open to learning more about digital safety. Most of them believe that there should be more education and training on how to avoid hacking and keep personal information safe. They are willing to attend awareness programs and learn how to use the platform more responsibly.

In conclusion, the problem of privacy breaches on WhatsApp is not just a technical issue, it is also a matter of awareness, behavior, and education. If students are properly guided and supported, they can protect themselves better. At the same time, WhatsApp and educational institutions have a responsibility to create a safer digital environment through proper communication, stronger features, and useful training.

5.3 RECOMMENDATIONS

From the findings of this research, it is clear that privacy and security concerns on WhatsApp are real and affect students directly. To address the issues discovered in this study, the following recommendations are made:

1.WhatsApp should increase user education.

The platform should do more to teach users, especially students, how to use security features like two-step verification. WhatsApp can include short guides or reminders within the app to encourage users to take simple steps that will make their accounts more secure.

2. Schools should organize digital safety awareness programs.

Higher institutions should hold seminars, workshops, and training sessions to teach students about online safety. These programs should cover topics like phishing, password protection, and how to recognize and report suspicious activities.

3. Digital safety should be added to the school curriculum.

Since students use online platforms every day, digital literacy should be taught as part of their general education. Topics like privacy, responsible use of social media, and how to avoid cyber threats should be included in classroom discussions.

4. Students should take responsibility for their online safety.

Every student must play an active role in protecting their own privacy. This includes not sharing login details, using strong passwords, ignoring unknown links, updating apps regularly, and enabling features like two-step verification.

5. Support systems should be provided for victims of hacking.

Some students may feel confused or discouraged after being hacked. Schools should have a support system, such as IT help desks or counselors, who can assist students and guide them on what to do next.

6. WhatsApp should send warnings about common scams

Whenever new hacking methods or scams are reported, WhatsApp should notify users and provide tips to avoid falling victim. This can help users stay informed and alert before any damage is done.

If these recommendations are followed, both students and the institutions that serve them can work together to create a safer digital environment. These steps will help reduce the risk of privacy breaches and improve how students manage their digital lives.

REFERENCES

Al-Shammari, H. (2020). Security vulnerabilities in WhatsApp: Challenges and solutions. Journal of Cybersecurity Studies, 5(3), 150–160.

Balebako, R., Jung, J., Lu, W., Cranor, L. F., & Nguyen, C. (2014). “Little Brothers Watching You”: User perceptions of data collection and use on social network sites. Proceedings of the Eighth Symposium on Usable Privacy and Security, 1–15.

Babbie, E. R. (2020). The Practice of Social Research (15th ed.). Cengage Learning.

Bryman, A. (2016). Social Research Methods (5th ed.). Oxford University Press.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. American Journal of Theoretical and Applied Statistics, 5(1), 1–4.

Fafinski, S. (2014). Psychological effects of cyber hacking: A study of victims. Journal of Internet Security, 6(2), 87–102.

Heale, R., & Twycross, A. (2015). Validity and reliability in quantitative research. Evidence-Based Nursing, 18(3), 66–67.

Kshetri, N. (2017). Categorizing hacking activities: An overview of threats and consequences. Cybersecurity Journal, 9(4), 200–214.

Kumar, A., & Rajput, P. (2020). Analyzing end-to-end encryption in WhatsApp communications. Journal of Network Security, 12(2), 34–48.

NITDA. (2024). Advisory on protecting WhatsApp accounts from cyber threats. Retrieved from https://nairametrics.com/2024/11/13/nitda-issues-advisory-on-protecting-whatsapp-accounts-from-cyber-threats/

NITDA. (2024). Recommendations for safeguarding WhatsApp accounts. Retrieved from https://guardian.ng/news/nitda-advises-nigerians-on-response-to-whatsapp-breaches/

Sharma, V., Rana, N. P., & Dwivedi, Y. K. (2020). WhatsApp and the spread of misinformation: Examining its implications. Journal of Digital Communication Studies, 7(1), 45–62.

Stutzman, F., Gross, R., & Acquisti, A. (2013). Privacy concerns and awareness in social media platforms. Journal of Information Privacy, 8(3), 205–220.

Symantec. (2020). Hacking trends and the state of cybersecurity: Annual review. Retrieved from https://www.symantec.com

Taddicken, M. (2014). Factors influencing the willingness to disclose personal data on social media. Journal of New Media Research, 6(3), 215–231.

Tufecki, Z. (2008). Grooming, gossip, Facebook, and MySpace: What can we learn about these concepts in the age of online social networks? Social Science Computer Review, 26(4), 515–528.

Walther, J. B., Van Der Heide, B., Kim, S., Westerman, D., & Tong, S. T. (2008). The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep? Human Communication Research, 34(1), 28–49.

Weerakkody, N. (2009). Research Methods for Media and Communication. Oxford University Press.

Yin, R. K. (2018). Case Study Research and Applications: Design and Methods (6th ed.). SAGE Publications.

AUDIENCE PERCEPTION AND PRIVACY BREACH ON WHATSAPP APPLICATION: A CASE OF RECENT HACKING TRENDING AMONG STUDENTS OF MASS COMMUNICATION

QUESTIONNAIRE

Dear Participant,

I am Olanrewaju Hawal Muhammed with Matriculation number HND/23/MAC/FT/139, a student of Mass Communication at Kwara State Polytechnic. I am conducting a research study titled "Audience Perception and Privacy Breach on WhatsApp Application: A Case of Recent Hacking Trending Among Students of Mass Communication." This study aims to examine how students perceive privacy breaches on WhatsApp, their experiences with hacking incidents, and the impact on trust and security awareness.

Your participation in this survey is crucial as it will provide valuable insights and contribute significantly to the study. The questionnaire is divided into sections for clarity, and your responses will remain anonymous and used solely for academic purposes. Kindly answer honestly and select the options that best reflect your views. Your time and cooperation are deeply appreciated.

Thank you.

SECTION 1: BIODATA QUESTIONS

1. What is your age group?

16-20 [ ] 21-25 [ ] 26-30 [ ] Above 30 [ ]

2. What is your gender?

Male [ ] Female [ ] Prefer not to say [ ]

3. What level of study are you in?

National Diploma (ND) 1 [ ] National Diploma (ND) 2 [ ] Higher National Diploma (HND) 1 [ ] Higher National Diploma (HND) 2 [ ]

4. How frequently do you use WhatsApp?

Multiple times a day [ ] Once a day [ ] A few times a week [ ] Rarely [ ]

5. What is your primary use of WhatsApp? (Select all that apply)

Academic collaboration [ ] Social communication [ ] Professional networking [ ] Entertainment [ ]

SECTION B

6. Have you or someone you know experienced a WhatsApp hacking incident?

Yes, I have experienced it [ ] Yes, I have heard of it happening to others [ ] No, I am not aware of such incidents [ ]

7. What type of privacy breach have you encountered or heard of? (Select all that apply)

Unauthorized account access [ ] Financial fraud via hacked accounts [ ] Leakage of private messages or media [ ] Phishing attempts via suspicious links [ ] None [ ]

8. If your account was hacked, how was it compromised?

Clicked on a phishing link [ ] Weak password/no two-step verification [ ] Shared login details unknowingly [ ] Other _______________

9. What consequences did the hacking cause? (Select all that apply)

Loss of personal data [ ] Financial loss [ ] Damage to reputation [ ] No significant impact [ ]

10. How do privacy breaches affect your trust in WhatsApp?

I still trust WhatsApp and continue using it [ ] I am cautious but still use WhatsApp [ ] I have reduced my usage [ ] I am considering stopping using WhatsApp [ ]

11. How concerned are you about the security of your WhatsApp account? (Rate from 1 to 5, where 1 = Not concerned and 5 = Extremely concerned)

12. Do you use any of the following security measures on WhatsApp? (Select all that apply)

Two-step verification [ ] Strong password for linked email accounts [ ] Avoiding suspicious links and messages [ ] Regularly updating the app [ ] None of the above [ ]

SECTION C: PERCEPTIONS OF SECURITY AND PRIVACY

(For questions 13-20, select: Strongly Agree, Agree, Neutral, Disagree, Strongly Disagree)

Statement	SA	A	N	D	SD
13. I believe WhatsApp provides adequate security measures to protect user privacy.					
14. I feel confident that my personal					

information is safe while using WhatsApp.					
15. I am aware of the security features WhatsApp offers, such as two-step verification.					
16. I regularly update my WhatsApp settings to enhance my security and privacy.					
17. WhatsApp should do more to educate users about security threats and preventive measures.					
18. Privacy breaches on WhatsApp have influenced my trust in the platform.					
19. I believe that students should be educated on cybersecurity and hacking prevention strategies.					

20. I would participate in cybersecurity awareness programs if they were made available to students.					