Term Paper II

Critiqued By: Moxaben Bhupatbhai Zalawadia

Net ID: MXZ210014

Title of the Paper: Privacy and Security of Content: A Study of User Resilience and Pre-Checks on Social Media

Author of the Paper: Chukwuemeka Nwankwo, Francis Uwadia, Wilson Nwankwo, Wifred Adigwe, Paschal Chinedu, Emmanuel Ojei

Publication: IEEE Network

Abstract:
Recently, social media technologies have become a means for facilitating cybercrimes, kidnappings, and ritual killings, with students becoming vulnerable targets. As a result, this research aims to examine the importance of electronic communication styles among students when using social media platforms. It also investigates the resilience of users in ensuring that messages reach their intended recipients without any adverse consequences. The study employed a case study approach, involving 3500 students from various academic programs in a recognized tertiary institution in Southern Nigeria. Out of the collected questionnaires, 1000 were analyzed for validity. The findings highlighted that a significant 96% of students who use social media do not prioritize any form of security screening before sending messages through their smartphones on social media networks.

Section 1: Introduction

The paper discusses the increasing use of social media and its impact on information exchange, both positive and negative. On the positive side, social media has become a dominant means of communication globally and is now used for various purposes beyond social interactions, contributing to economic growth. However, the widespread adoption of social media has also given rise to numerous security and privacy challenges, making users vulnerable to cybercrimes, fraud, identity theft, and other deceitful activities. The paper focuses on the security concerns related to social media use and how individuals, especially students, can protect themselves and their communications. The research analyzes communication styles, patterns, and user resilience among students to identify potential weaknesses that criminals might exploit. The objective is to raise awareness and promote safer communication practices to reduce crimes facilitated through social media.The study poses several questions related to students' perspectives on social media use and the dangers associated with compromised communications. It also investigates the communication patterns adopted by students and their effectiveness in protecting information and reaching the intended recipients securely. The research aims to identify threats to privacy and data integrity that may necessitate mandatory security screening while using social media platforms. Ultimately, the goal is to recommend effective communication patterns and security techniques to prevent impersonation, communication hijacking, and criminal activities among students in tertiary institutions.

Following is a summarized version of the related studies:

The is a significant increase in the use of social media and mobile communication platforms over the last decade, which saw a tremendous surge during the COVID-19 pandemic due to global movement restrictions. The pandemic led to a rise in remote work, online schooling, and increased screen time as people turned to digital solutions for various activities, including retail e-commerce and education. Social media has become a prevalent means of communication, and many educational institutions integrated social media tools into their workflows to enhance teaching, learning, and support services. However, with the massive adoption of social media, there are downsides, including the exploitation and hijacking of legitimate user accounts and profiles, leading to identity theft. Impersonation and the creation of fake profiles on social media platforms are common, posing significant challenges in preventing and prosecuting such crimes. Personal Identifiable Information (PII) is often targeted, making individuals vulnerable to identity theft and other risks. Overall, the dual nature of social media – its benefits in facilitating communication and connectivity, as well as the risks associated with privacy violations and identity theft due to impersonation and misuse of personal information have been highlighted.

Section 2: Approach

The research employs a case study approach to comprehensively examine the topic. Data collection methods encompass structured interviews and both printed and online questionnaires. The study encompasses all undergraduates at a prestigious State-owned Polytechnic in Southern Nigeria, comprising 3500 students across nine academic departments. From this population, a sample of 1000 students were chosen using simple random sampling from the national diploma and higher national diploma programs. Fifteen students were interviewed from each department, and all students received questionnaires. The primary focus of the study is to analyze the students' usage and attitudes towards popular social media platforms such as Facebook, WhatsApp, Instagram, Telegram, and Twitter.

There were four sections in the questionnaire:

a. Bio data, category of Phone, Online presence, and social media apps used
b. Classification of information shared on social media; Four categories namely: public, private, sensitive, and confidential respectively were considered in line with the standard private sector classification level.
c. Communication patterns and/or styles including use of slogans, “coded messages”, local dialects, etc.
d. Security pre-checks/screening actions undertaken before and during information exchange. The criteria investigated in this section include: understanding of multi-factor authentication (MFA); use of MFA against accounts; one-time passwords; tokens; group checks, profile checks, event checks, “common slogan test” before sending of main message; clicking on web links, keeping/deletion of message histories, knowledge of fake news, coupons, ads, posts, campaigns, promotions, hashtags, photos, names, descriptions, and pages.

Key Findings from the study:

- 76% of respondents own a smartphone, indicating their use of social media.
- 73% of students have at least one social media account, while 23% have no social media presence.
- 73% of students share confidential and sensitive information on social media, highlighting the need for increased user resilience in communication.
- 49.3% of respondents use communication patterns as a pre-check parameter before communication, but many retain their chat histories, which could compromise the effectiveness of such patterns.
- Overall, respondents demonstrate poor user resilience, making them susceptible to cybercriminals and hijackers.

Remedies proposed by the study include paying attention to physical activities and discussions on campus before sharing sensitive information and using questions related to recent encounters as a security pre-check.

Section 3: Pros and Cons of the Paper discussed in section 2

Pros:

1. Timely and Relevant Topic: Addresses the misuse of social media technologies and its impact on students, highlighting the increasing risks associated with cybercrimes.
2. Case Study Approach: Allows for an in-depth investigation, providing valuable insights into students' attitudes towards social media usage.
3. Large Sample Size: Inclusion of 1000 students from various academic programs enhances the reliability of findings.
4. Comprehensive Data Collection: Utilizes structured interviews and questionnaires for a holistic understanding of students' communication styles and security practices on social media.
5. Awareness and Recommendations: Raises awareness about security risks and proposes measures to promote user resilience.

Cons:

1. Lack of Methodological Details: Insufficient clarity on question formulation and data analysis methods.
2. Limited Focus on Platforms: Focuses on a few social media platforms, excluding others, reducing the scope of the study.
3. Limited Generalizability: Findings may not apply to other populations or contexts beyond the specific institution.
4. Insufficient Implications and Limitations Discussion: Fails to thoroughly discuss practical implications and study limitations.
5. Lack of Detailed Findings: Provides summary tables but lacks in-depth analysis and interpretation of the results.

Section 4:

Summary:

The paper addresses the misuse of social media technologies and their impact on students, particularly in the context of cybercrimes, kidnapping, and ritual killings. The study investigates the risks of cybercrimes and identity theft facilitated through social media, particularly among students. It adopts a case study approach with 1000 students from a Nigerian institution. The findings show that 96% of students using social media neglect security screening before sending messages. The research emphasizes the need for security awareness programs in educational institutions to promote user resilience and protect against online threats. Recommendations include paying attention to communication patterns and physical activities before sharing sensitive information on social media.

Direction: How can we extend the paper discussed in section 2

To enhance the paper on social media usage and security, researchers can explore various aspects. They can study communication patterns on social media to assess their effectiveness in preventing security breaches. Conducting a comparative analysis across institutions and regions will help understand variations in students' security awareness. Platform-specific analyses can identify vulnerabilities and suggest security improvements for specific social media platforms. Qualitative research methods like interviews and content analysis will provide deeper insights into students' attitudes towards social media security. Examining how students manage privacy settings and its impact on overall security is crucial for comprehensive findings. Lastly, involving students from diverse cultural backgrounds will facilitate a global understanding of social media usage and security practices.

References:

1. S.R. Saha & A.K. Guha. “Impact of Social Media Use of University Students". *International Journal of Statistics and Applications*, vol. 9, issue 1, pp.36-43,2019.
2. D. Aizenkot. "Cyberbullying experiences in classmates WhatsApp discourse, across public and private contexts", *Children and Youth Services Review*. vol. 110, 2020.