

Electronic Fraud through Social Media: A Sociological Study of Victims of Digital Crime in Sudan

الاحتيال الإلكتروني عبر وسائل التواصل الاجتماعي: دراسة سوسيولوجية لضحايا الجرائم الرقمية في السودان

Dr. Faisal Mohamed Abdel Bari^{1*}, Dr. Ashraf Mohamed Adam Adham²

¹ University of Neelain (Sudan) fisalbari@yahoo.com

² University of Neelain (Sudan) amaadham@gmail.com

Received: 09/05/2026

Accepted: 26/05/2026

Published 01/06/2026

Abstract: This study examines the phenomenon of electronic fraud through social media platforms in Sudan from a sociological perspective, with particular emphasis on victims lived experiences and the broader implications of digital crime for Sudanese society. The study seeks to identify the most prevalent forms of online fraud, analyze the social and demographic characteristics of victims, and investigate the psychological, social, and economic consequences associated with digital victimization. It further evaluates the effectiveness of legal and institutional mechanisms designed to address cyber fraud and enhance digital security.

The study adopts a descriptive-analytical mixed-methods approach combining quantitative and qualitative techniques. Quantitative data were collected through a structured questionnaire based on a five-point Likert scale, while qualitative insights were generated through semi-structured interviews with selected victims. The findings reveal that electronic fraud significantly undermines social trust and weakens interpersonal relations within digital environments. The results further indicate that cyber fraud produces varying psychological and economic effects on victims amid limited digital awareness and inadequate enforcement of cybercrime legislation. The study concludes that combating cyber fraud requires strengthening digital literacy programs, enhancing institutional and psychosocial support mechanisms for victims, and reforming legal and policy frameworks to respond more effectively to emerging digital crimes.

Keywords: Digital Crime, Cyber Fraud, Identity Theft, Cyber Extortion, Social Trust, Digital Security

* *Corresponding author : Faisal Toto e-mail : fisaltoto20@neelain.edu.sd*

1. INTRODUCTION

Over the past three decades, global societies have undergone profound transformations driven by rapid developments in information and communication technologies. These transformations have reshaped social interaction, economic activity, political participation, and cultural production across both developed and developing societies. Social media platforms have become central mechanisms through which individuals establish social relations, exchange information, construct identities, and engage in public discourse.

While digital transformation has generated important opportunities for communication, education, and economic integration, it has simultaneously produced complex social and security challenges. Among the most significant of these challenges is the rapid growth of cybercrime, particularly electronic fraud conducted through social media platforms.

Electronic fraud represents one of the most dangerous manifestations of digital crime because of its ability to exploit both technological vulnerabilities and human behavior. Fraudsters increasingly rely on psychological manipulation, impersonation strategies, deceptive communication techniques, and fake digital identities to obtain financial benefits or sensitive personal information from victims.

Within the Sudanese context, the expansion of internet access and social media usage has accelerated considerably in recent years, especially among young people. Platforms such as Facebook, WhatsApp, Instagram, and Telegram have become integrated into everyday social and economic life. However, these digital spaces have also become fertile environments for online scams, identity theft, emotional exploitation, banking fraud, and cyber extortion.

The current economic and social conditions in Sudan have further intensified the risks associated with cyber fraud. Fraudsters frequently exploit economic hardship, humanitarian crises, emotional vulnerability, and institutional weakness to manipulate victims through deceptive online interactions. Consequently, cyber fraud increasingly threatens not only individual financial security but also broader social trust, institutional legitimacy, and community cohesion.

Despite the growing prevalence of cyber fraud in Sudan, sociological research examining victims' experiences and the broader societal implications of digital crime remains limited. Existing studies have primarily focused on technological security, legal dimensions, or youth engagement with social media, leaving an important research gap concerning the social consequences of digital victimization and its impact on trust, psychological well-being, and social relationships.

This study seeks to address this gap by examining electronic fraud through social media as both a technological and sociological phenomenon. By integrating quantitative and qualitative approaches, the study provides a comprehensive analysis of patterns of victimization, levels of digital awareness, institutional challenges, and the lived experiences of victims within Sudanese society.

Within the Sudanese context, the expansion of social media usage has created new opportunities for communication and economic interaction while simultaneously exposing individuals to increasingly sophisticated forms of online deception and exploitation. This phenomenon has become particularly alarming due to its implications for social cohesion, interpersonal trust, and individual psychological well-being.

Despite the growing prevalence of cyber fraud in Sudan, sociological research examining victims' experiences and the broader societal consequences of digital crime remains limited. Existing scholarship has primarily focused on privacy violations, youth behavior, or the technological dimensions of cybercrime, leaving a significant research gap regarding the lived experiences of victims and the social transformations associated with digital fraud. This study attempts to address this gap by examining electronic fraud through social media as both a technological and sociological phenomenon.

Research Problem

In recent years, Sudan has experienced a substantial increase in the use of social media platforms, creating new forms of communication and interaction while simultaneously facilitating diverse forms of electronic

fraud. These practices have generated serious psychological, social, and economic consequences for victims and have increasingly threatened social trust and digital security.

Against this backdrop, the present study seeks to answer the following central question:

How does electronic fraud through social media affect victims and Sudanese society, and to what extent are existing legal and social frameworks capable of limiting this phenomenon?

The study further addresses the following sub-questions:

1. What are the social and demographic characteristics of victims of digital crimes?
2. Do patterns of cyber fraud differ according to age and gender?
3. Does awareness of cyber fraud risks vary according to demographic characteristics or previous exposure to fraud?
4. How does electronic fraud affect social relationships and trust within society?
5. How do victims cope with the psychological, social, and economic consequences of cyber fraud?
6. To what extent are existing laws and official procedures effective in protecting individuals from digital fraud?

Research Objectives

The study aims to:

1. Identify the dominant forms of electronic fraud through social media in Sudan.
2. Analyze the social and demographic characteristics of victims of digital crimes.
3. Examine the psychological, social, and economic impacts of cyber fraud.
4. Assess levels of social trust and digital security among social media users.
5. Evaluate the effectiveness of legal and institutional mechanisms designed to combat cyber fraud.
6. Propose practical recommendations for enhancing digital awareness and reducing the spread of electronic fraud.

Significance of the Study

The significance of this study derives from both academic and societal considerations.

From an academic perspective, the study contributes to the growing sociological literature on digital crime within Arab and African contexts. It also provides a methodological framework integrating quantitative and qualitative approaches to examine cyber fraud from a multidimensional perspective. Furthermore, the study contributes to the development of analytical indicators related to social trust and digital security.

From a practical perspective, the study offers empirical evidence that may assist policymakers in developing more effective legal and institutional responses to cyber fraud. It also provides insights for educational institutions and media organizations seeking to design digital awareness programs targeting groups most vulnerable to online fraud.

Methodology

The study employs a descriptive-analytical methodology to examine the nature, dimensions, and consequences of electronic fraud through social media.

Research Population and Sample

The research population consists of social media users in Sudan, including users of Facebook, WhatsApp, Instagram, and TikTok. The study encompasses diverse demographic groups in terms of age, gender, educational background, and socioeconomic status.

A purposive sampling technique was adopted to ensure representation of different social groups. The sample consisted of 82 participants distributed across age and gender categories.

Data Collection Tools

Data were collected through:

1. A structured questionnaire developed by the researchers using a five-point Likert scale to measure levels of trust and digital security.
2. Semi-structured interviews conducted with a selected group of victims to explore the social and psychological dimensions of their experiences.

Data Collection Procedures

The questionnaire was distributed electronically through social media platforms while ensuring participant confidentiality. In addition, semi-structured interviews were conducted online and in person with approximately 10–15 victims.

Statistical Analysis

The data were analyzed using the Statistical Package for the Social Sciences (SPSS Version 25). The study employed descriptive statistics, frequencies, percentages, means, standard deviations, Cronbach's Alpha reliability testing, independent sample t-tests, cross-tabulations, chi-square analysis, and ANOVA tests.

The reliability and validity analysis demonstrated acceptable psychometric properties for the research instrument. Cronbach's Alpha coefficient reached 0.70, indicating acceptable internal consistency, while the validity coefficient reached 0.84, reflecting satisfactory construct validity.

Literature Review and Theoretical Framework

The growing body of international scholarship on cybercrime demonstrates that electronic fraud has become one of the defining social risks associated with digital transformation and technological modernization. Researchers increasingly emphasize that digital technologies have reshaped patterns of criminal behavior by enabling transnational forms of deception capable of targeting large populations through virtual environments.

Contemporary sociological perspectives argue that cyber fraud is not merely a technological issue but also a social phenomenon rooted in changing patterns of trust, communication, and social interaction. According to Manuel Castells' theory of the network society, modern communication systems increasingly operate through interconnected digital networks that reshape social relations and institutional structures. Within such environments, trust becomes more fragile because individuals interact with unknown actors without conventional mechanisms of social verification.

Social capital theory also provides an important framework for understanding the consequences of electronic fraud. Putnam conceptualizes

trust as a fundamental component of social cohesion and collective solidarity. Repeated exposure to digital deception weakens interpersonal trust and contributes to social anxiety and suspicion, particularly within online communication environments.

Routine activity theory further explains the emergence of cyber fraud by arguing that crime occurs when motivated offenders encounter suitable targets in the absence of effective guardianship. Social media platforms create ideal conditions for cybercrime by increasing accessibility to victims while reducing social monitoring and institutional control.

Previous studies conducted in Arab and African contexts reveal that cyber fraud is strongly associated with rapid digital expansion combined with weak digital literacy and insufficient legal protection. Studies conducted in Algeria, Oman, and Sudan indicate that fraudsters often exploit emotional vulnerability, economic hardship, and social trust to manipulate victims.

Research by Al-Tayeb (2018) demonstrated that Sudanese youth increasingly face risks related to privacy violations and digital exploitation through social media platforms. Ahmed (2018) further emphasized the relationship between social transformation and the development of cybercrime within Sudanese society.

Similarly, ethnographic research conducted by Basma and Amal (2025) highlighted the emotional and psychological dimensions of cyber fraud victimization, including anxiety, stress, and social isolation. Other studies stressed the inadequacy of existing legal frameworks and the inability of many institutions to respond effectively to rapidly evolving forms of digital crime.

Despite these scholarly contributions, relatively few sociological studies have focused specifically on victims of electronic fraud within Sudanese society. Existing literature often prioritizes legal and technological dimensions while overlooking the lived experiences of victims and the broader impact of cyber fraud on social trust and community relations.

Accordingly, the present study contributes to the literature by adopting an integrated sociological perspective that combines social trust theory, digital awareness analysis, institutional evaluation, and victim-centered inquiry.

2. Theoretical Framework

2.1 Conceptualizing Electronic Fraud

Electronic fraud is considered one of the most significant contemporary forms of cybercrime associated with rapid technological transformation and digital communication. It involves the unlawful use of digital systems and online networks to obtain financial or material benefits through deception, identity theft, manipulation of information, or unauthorized access to private systems (Khawla & Sarah, 2025, p.12).

From a sociological perspective, electronic fraud reflects the capacity of offenders to exploit digital environments to create new forms of deception based on manipulation of trust, emotional vulnerability, and social relationships. Consequently, cyber fraud constitutes a multidimensional phenomenon combining technological, psychological, and social dimensions (Haraki, 2023, p.50).

In the Sudanese legal framework, cyber fraud is criminalized under the Information Crimes Act, which penalizes fraudulent activities conducted through digital networks or computer systems using false identities or deceptive methods for financial gain (Sudan, 2005, p.3).

Social Media Platforms

Social media platforms refer to internet-based digital applications that enable individuals to communicate and interact through the exchange of texts, images, videos, and audio content. These platforms include Facebook, WhatsApp, Instagram, Snapchat, LinkedIn, YouTube, and similar applications used for both personal and commercial purposes (Bouchaala & Al-Alimi, 2024, p.102).

Digital Crime

Digital crime encompasses both traditional crimes committed through digital means and emerging crimes directly associated with modern communication technologies, including hacking, data manipulation, identity theft, cyber extortion, and online fraud. Contemporary forms of digital

deviance increasingly challenge existing legal and technological mechanisms designed to control cybercrime (Nuh, 2022, p.53).

Forms of Electronic Fraud through Social Media

The study identifies several dominant forms of cyber fraud commonly practiced through social media:

Chat Room Fraud

This form of fraud occurs through online conversations and chat platforms where offenders establish trust-based relationships with victims before requesting financial assistance or sensitive personal information.

Social Media Fraud

Fraudsters create fake accounts or compromise legitimate profiles on platforms such as Facebook, WhatsApp, and Instagram to distribute deceptive links, fake promotions, or fraudulent investment opportunities.

Fake Website Fraud

Fraudulent websites are designed to imitate legitimate institutions in order to deceive users into disclosing personal or financial information through counterfeit payment or registration forms.

SMS Fraud

This type involves deceptive text messages claiming to originate from banks or companies and often includes malicious links or urgent requests for account verification.

Previous Studies

Although sociological research on cyber fraud in Sudan remains limited, several related studies provide useful contextual insights.

Al-Tayeb (2018) examined Sudanese youth attitudes toward the misuse of social media in violating individual privacy. The study demonstrated that social media platforms, despite their positive communicative functions, have increasingly become tools for privacy violations and social insecurity.

Basma and Amal (2025) explored electronic fraud and victim-offender dynamics through an ethnographic study conducted in Algeria. Their findings highlighted the psychological and social effects of cyber fraud, including anxiety, social isolation, and emotional distress.

Ahmed (2018) investigated the relationship between social change and the development of cybercrime in Sudan, emphasizing the role of social, economic, and cultural transformations in facilitating electronic crimes.

Majid (2025) analyzed mechanisms for combating cyber fraud and identified major deficiencies within legislative and judicial frameworks related to cybercrime.

The current study differs from previous research by focusing specifically on the experiences of cyber fraud victims within Sudanese society and by examining the sociological consequences of digital crime on social trust and community relations.

3. Field Study

3.1 Extended Analytical Discussion

The findings of this study must be understood within the broader context of digital transformation and social instability experienced in Sudan during recent years. The spread of electronic fraud reflects structural changes in communication patterns, economic practices, and forms of social interaction within contemporary Sudanese society.

One of the central findings of the study is the increasing normalization of cyber fraud within everyday digital interactions. Exposure to online scams is no longer perceived as an exceptional experience but rather as a recurring social risk associated with routine engagement on social media platforms. This finding aligns with contemporary theories of digital risk society, which argue that modern technological systems generate new forms of insecurity that affect individuals across different social categories.

The study further demonstrates that cyber fraud disproportionately affects younger age groups, particularly university students and digitally active youth populations. This result can be interpreted sociologically through the concept of digital immersion, whereby younger individuals spend extensive periods engaging with online platforms for educational, economic, and social purposes. Increased digital exposure inevitably creates more opportunities for interaction with deceptive content, fraudulent advertisements, and manipulated social identities.

At the same time, the results reveal an important contradiction between awareness and practice. Although many participants demonstrated

substantial knowledge regarding common methods of electronic fraud, this awareness did not always translate into effective protective behavior. This gap between knowledge and practice reflects a broader sociological pattern frequently observed in studies of risk behavior and digital security.

Participants often recognized the dangers associated with suspicious links and deceptive online communication while simultaneously continuing to engage in unsafe digital practices due to convenience, emotional trust, curiosity, or economic pressure. Such findings suggest that digital awareness campaigns focusing exclusively on theoretical information may be insufficient unless accompanied by practical behavioral training.

The qualitative interviews conducted with victims provide particularly significant sociological insights. Fraudsters appear highly capable of exploiting dominant social and cultural values within Sudanese society, especially values associated with trust, solidarity, and rapid social assistance. Many fraudulent operations relied on impersonating relatives living abroad, humanitarian organizations, or trusted institutions in order to manipulate victims emotionally and financially.

These findings illustrate how cyber fraud adapts to local cultural contexts. Rather than relying solely on technical deception, fraudsters strategically manipulate culturally embedded patterns of social trust and collective responsibility. Consequently, electronic fraud in Sudan cannot be analyzed purely as a technological issue; it must also be understood as a socially embedded form of exploitation.

The findings additionally demonstrate that women experience unique forms of vulnerability within digital environments, particularly in relation to emotional manipulation and cyber extortion. Many female victims refrain from reporting incidents because of fears associated with social stigma, reputational damage, and cultural judgment. This finding reveals the intersection between digital victimization and gendered social norms within Sudanese society.

The psychological consequences identified in this study are equally significant. Victims frequently reported anxiety, stress, emotional insecurity, embarrassment, and declining confidence in online interaction. In several

cases, exposure to fraud generated broader forms of social withdrawal and reduced willingness to participate in digital communication.

Such outcomes indicate that cyber fraud extends beyond financial loss to produce deeper social and emotional consequences that affect social integration and psychological well-being. These findings support sociological arguments that cybercrime contributes to the erosion of social capital and collective trust.

Another important finding concerns the perceived inadequacy of institutional and legal responses to cyber fraud. Participants consistently expressed skepticism regarding the effectiveness of existing cybercrime legislation and the capacity of institutions to investigate and prosecute offenders.

This skepticism reflects broader structural challenges associated with technological modernization in developing societies. While digital communication technologies evolve rapidly, legal systems and institutional mechanisms often struggle to adapt at comparable speed. In Sudan, these challenges are intensified by economic instability, limited technological infrastructure, and insufficient cybercrime expertise.

The findings further reveal that many fraudulent operations originate outside national borders, complicating efforts to identify perpetrators and enforce legal accountability. Consequently, cyber fraud increasingly represents a transnational phenomenon requiring coordinated international and regional cooperation.

From a sociological perspective, the study highlights the transformation of trust within digitally mediated societies. Traditional forms of trust based on kinship, direct social interaction, and community familiarity are increasingly challenged by anonymous digital communication environments where identity verification becomes difficult.

The erosion of trust identified in this study may therefore have long-term implications for social cohesion and digital participation. If individuals increasingly perceive online environments as unsafe or deceptive, they may reduce engagement with digital systems that are becoming essential for education, commerce, and social participation.

The findings also suggest that digital inequality plays a major role in

shaping vulnerability to cyber fraud. Individuals with limited digital literacy, weak technological knowledge, or restricted access to cybersecurity resources are more likely to become targets of online scams. This demonstrates that cyber fraud is not distributed randomly across society but rather reflects broader inequalities in access to knowledge, technology, and institutional protection.

The study therefore emphasizes the need for a multidimensional response to electronic fraud that integrates sociological understanding, technological development, legal reform, and public awareness strategies.

3.2 Results and Discussion

Demographic Characteristics of Participants

The sample was relatively balanced by gender, with males representing 52% and females 48% of participants. In terms of age distribution, the majority of participants (88%) belonged to the 18–29 age category, reflecting the strong engagement of youth with digital environments.

Students constituted 93% of the sample, indicating the predominance of digitally active youth populations within the research context.

Exposure to Electronic Fraud

The findings indicate that 54% of participants had previously experienced electronic fraud, while 46% reported no prior exposure. This result demonstrates the widespread prevalence of cyber fraud within the Sudanese digital environment.

Financial fraud emerged as the most common form of cyber fraud, accounting for 50% of reported cases, followed by emotional fraud and identity-related fraud.

Most participants who experienced fraud reported a single exposure, although a smaller proportion experienced repeated victimization, suggesting the existence of vulnerable groups characterized by limited digital protection or inadequate awareness of preventive measures.

Digital Awareness and Behavioral Patterns

The findings reveal generally high levels of awareness regarding cyber fraud risks, with most participants demonstrating familiarity with

fraudulent methods, suspicious links, and the importance of protecting personal information.

However, the study also identified a gap between theoretical awareness and practical digital behavior, particularly in relation to verifying the credibility of online sources and identifying sophisticated fraud techniques.

Age and Gender Differences in Exposure to Fraud

The results demonstrate statistically significant differences between age groups regarding exposure to electronic fraud. Younger participants, particularly those aged 18–29, reported the highest rates of victimization due to their intensive engagement with digital platforms.

Similarly, statistically significant differences were identified between males and females in relation to exposure to cyber fraud. Although exposure levels were relatively close, males appeared more vulnerable to financial and transactional fraud, while females were more likely to encounter emotional or socially manipulative forms of fraud.

Impact of Electronic Fraud on Social Trust

The findings indicate that cyber fraud significantly affects social trust and interpersonal relations within digital environments. Participants reported increased suspicion and reduced confidence in online interactions following exposure to fraudulent experiences.

These findings align with social capital theory, which emphasizes trust as a fundamental component of social cohesion. Repeated exposure to cyber fraud contributes to the erosion of social trust and weakens confidence in digital communication networks.

Psychological, Social, and Economic Consequences

The study reveals that electronic fraud generates substantial psychological effects, including anxiety, stress, insecurity, and social withdrawal. Victims also reported economic losses and diminished trust in digital transactions.

Interestingly, the results indicate that these psychological and social impacts were relatively consistent across demographic groups, suggesting that cyber fraud represents a broadly shared social experience rather than an isolated individual problem.

Effectiveness of Legal and Institutional Frameworks

Participants generally expressed dissatisfaction with the effectiveness of existing laws and institutional procedures in combating electronic fraud. The findings suggest that current legal frameworks are unable to keep pace with the rapid evolution of cybercrime techniques.

The study further identified significant demand among participants for stronger legal measures, improved institutional capacity, and more effective mechanisms for tracking fraudulent digital accounts, particularly those operated from outside Sudan.

Interview Findings

Qualitative interviews provided deeper insight into the lived experiences of victims. Participants reported that fraudsters frequently exploit the current economic and social conditions in Sudan by impersonating relatives abroad, humanitarian organizations, or telecommunications companies offering financial rewards.

Victims also described the widespread use of fake banking notifications and deceptive phone calls requesting confidential account information under the pretext of updating digital applications.

The interviews further revealed that many victims refrain from reporting incidents due to social stigma, particularly women subjected to cyber extortion who fear reputational damage and public shame.

In addition, participants highlighted technical limitations faced by official institutions in tracking fraudulent accounts and investigating cross-border cybercrime operations.

Recommendations

Based on the empirical findings and sociological analysis of this study, several recommendations can be proposed to reduce the prevalence of electronic fraud and strengthen digital security within Sudanese society.

- First, educational institutions should integrate digital literacy and cybersecurity education into school and university curricula. Digital awareness programs must move beyond theoretical information and focus on developing practical skills related to identifying fraudulent content, protecting personal information, and verifying online

identities.

- Second, media institutions and civil society organizations should implement continuous public awareness campaigns targeting the most vulnerable social groups, particularly youth, women, and individuals with limited technological experience. These campaigns should address both technical and psychological dimensions of cyber fraud.
- Third, the Sudanese government should strengthen cybercrime legislation and update legal frameworks to keep pace with rapidly evolving digital threats. Legislative reform should include clearer definitions of digital crimes, stronger penalties for offenders, and improved mechanisms for international cooperation in cybercrime investigations.
- Fourth, specialized cybercrime units should receive greater technical and institutional support to improve their ability to investigate digital crimes, track fraudulent accounts, and respond rapidly to cyber threats.
- Fifth, psychological and social support services should be established for victims of cyber fraud, particularly victims of cyber extortion and emotional manipulation who may experience severe social and psychological consequences.
- Sixth, social media companies and financial institutions operating within Sudan should strengthen digital protection mechanisms and collaborate with governmental authorities to identify suspicious activities and fraudulent accounts.
- Finally, future sociological research should continue examining the relationship between digital transformation and social trust within Arab and African societies, particularly in contexts characterized by political instability and rapid technological change.

4. CONCLUSION

This study demonstrates that electronic fraud through social media has evolved beyond a purely technical issue to become a significant sociological phenomenon affecting social relations, trust structures, and perceptions of security within Sudanese society.

Cyber fraud not only exposes individuals to financial losses and privacy violations but also produces profound psychological and social consequences, including diminished trust in digital interactions, increased feelings of insecurity, and social isolation.

The findings reveal structural weaknesses in digital awareness and institutional capacity, rendering individuals increasingly vulnerable to digital exploitation. Youth and women appear particularly vulnerable due to their patterns of digital engagement and social interaction within online environments.

The study therefore recommends:

1. Expanding digital literacy and awareness programs within schools and universities.
2. Strengthening cybercrime legislation and enforcement mechanisms.
3. Establishing psychological and social support networks for victims of digital crime.
4. Enhancing the technical capacities of security and cybercrime institutions.
5. Developing integrated national strategies combining sociological knowledge with public policy interventions to ensure a safer and more equitable digital environment in Sudan.

5. Bibliography List:

1. Ahmed, Safaa Mohamed Nour Eid. (2018). Social Change and Its Relationship to the Development of Cybercrime: A Field Study on Victims at the Emerging Crimes Prosecution Office in Khartoum North. Master's Thesis in Sociology, Al-Neelain University, Faculty of Graduate Studies.
2. Al-Sudan, Government of Sudan. (2005). Information Crimes Act of 2007. Khartoum.
3. Al-Tayeb, A. A. (2018). Sudanese Youth Attitudes toward the Exploitation of Social Media in Violating Individual Privacy. *International Journal of Social Communication*, 5(3), 188–212.
4. Basma, F., & Amal, T. (2025). Electronic Fraud between Victim and Offender and Its Role in the Development of Criminality: An

- Ethnographic Study of Victims of Digital Crime in Algeria. *Journal of Human and Social Studies*, 14(2), 187–200.
5. Boushaala, A., & Al-Alami, A. (2024). Social Media and Its Impact on Algerian Community Security: An Analytical Study. *Al-Haqiqa Journal for Social and Human Sciences*, 23(2), 98–117.
 6. Haraki, H. (2023). The Reality of Electronic Fraud in E-Commerce. *Journal of Social Change*, 8(2), 45–60.
 7. Khawla, T., & Sarah, J. (2025). Electronic Fraud in Islamic Jurisprudence and Algerian Law: A Comparative Study. Master's Thesis, Faculty of Humanities and Social Sciences, Mohamed Boudiaf University of M'sila, Algeria.
 8. Majid, A. H. (2025). Mechanisms for Limiting the Crime of Electronic Fraud. *Iraqi University Journal*, 73(7), 179.
 9. Mohammed, S. J., & Al-Ma'shani, M. B. (2023). Criminal Confrontation of Electronic Fraud in Omani Legislation. *Academic Researcher Journal in Legal and Political Sciences*, 6(1), 171–185.
 10. Nuh, A. (2022). Digital Ethics and Their Contribution to Preventing Digital Crime. *Journal of Legal and Political Sciences*, 13(2), 44–65.