Privacy and Security of Content: A Study of User-resilience and Pre-checks on Social Media

Chukwuemeka Nwankwo
Department of Computer Science
Edo State University
Uzairue, Nigeria
pascal21.nwankwo@edouniversity.edu.ng

Francis Uwadia
Department of Cyber Security
Delta State University of Science & Technology
Ozoro, Nigeria.
uwadiaf@dsust.edu.ng

Wilson Nwankwo
Department of Computer Science
Edo State University
Uzairue, Nigeria
nwankwo.wilson@edouniversity.edu.ng

Wifred Adigwe
Department of Computer Science
Delta State University of Science & Technology
Ozoro, Nigeria.
adigwew@dsust.edu.ng

Paschal Chinedu
Department of Computer Engineering
Edo State University
Uzairue, Nigeria.
paschal.chinedu@edouniversity.edu.ng

Emmanuel Ojei
Department of Software Engineering
Delta State University of Science & Technology
Ozoro, Nigeria.
ojeie@dsust.edu.ng

2022 5th Information Technology for Education and Development (ITED) | 978-1-6654-9370-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/ITED56637.2022.10051589

Abstract— **In recent times, cybercrimes, kidnapping, and ritual killings are being enabled through the use and abuse of social media technologies and students are becoming cheap targets. Consequently, this study seeks to investigate the imperative of electronic communication styles among students via social media channels vis-a-vis the users' resilience before and during communication on social media to ensure that the message is routed to the intended recipient. In this study, we adopted the case study approach and 3500 students were drawn from different academic programmes in a known tertiary institution in Southern Nigeria. Validly completed questionnaires from 1000 students were analyzed. Findings revealed that 96% of the students who use social media are not concerned with any form of security screening before sending messages on social media networks via their smartphones.**

Keywords— data privacy, security, information theft, pre-check, social media, cyber misrepresentation

I. INTRODUCTION

Information exchange in the cyberspace has continued to soar high with the introduction of more attractive and cost-effective technologies [1]. It is almost justifiable to assert that communication channels such as social media applications and social networks had taken over the domain of information exchange across all the strata of the society [2]. It is believed that the ubiquity of social media and their adoption in various sectors globally such as governance, marketing, banking, agriculture, climate management, education, management, business, media and journalism, etc., is rapidly transforming the technology from a social technology to an instrument of economic growth [3], [4], [5], [6]. Chaffey [7] reported that as at July 2022, social media users had reached 4.70 billion users which is equivalent to 59% of the global population. It is noted that social media users grow at an astonishing rate of seven (7) new users every second with nine in every ten Internet users involved in social media communication and with each user spending an average time of two hours twenty-nine minutes [7]. Figure 1 shows the popular social media platforms and their subscriber base in millions. With focus on information exchange via text messages, chats, and voice calls; telecommunication companies now provide platform and cost-effective subscriptions for connecting subscribers and this provide alternatives to traditional voice calls. Another advantage of these channels is instant messaging features which enables timely message delivery that constitutes the hallmark for effective communication [8]. To ensure security of communications in these applications, the vendors have integrated some security features such as encryption. The use of end-to-end encryption and key exchange techniques are the main indicator in the evaluation of the security social networks [9].

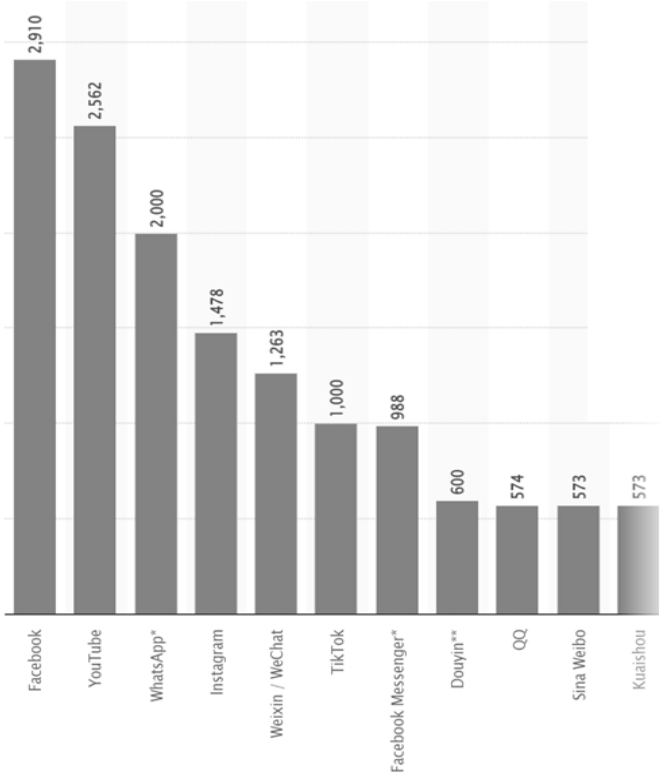

Figure 1. Popular social media and subscriber base

However, the gains recorded using these technologies are being negated by the widespread challenges the technologies inherently pose to individual users, groups, and societies [1], [10], [11], [12]. Privacy violations and security breaches have assumed terrifyingly new dimensions [13] [14] [15] as these virtual applications are emerging top vulnerable platforms for cyber-criminals and hacktivists to spoof organizations, creating malicious social media accounts for the main purpose of stealing sensitive information from customers [16]. In some quarters, they are regarded as the most popular technology with the highest security concerns especially on impersonation, identity theft, fraud, cyberbullying, and several aspects of deceit, with Facebook and Whatsapp ahead of the [17], [18], [19]. For instance, it was reported that in April 2021 533 million Facebook accounts including personal data were hacked [20]. The cost

of such could be very high as many of the users would have been exposed to various risks. Liapustin [21] notes that since 2016, the loss from email impersonation scams alone arising from business email compromise is more than 26 billion US Dollars according to the FBI. Impersonation fraud costs increased to an alarming 85 percent year-over-year, with over 2 billion US Dollars in total losses between October 2020 and September 2021 [22], [23]. Similarly, from 2015 to March 2020, 6527 cases of data breaches were reported globally involving over a billion records [24]. Also, in 2021, the United States recorded over 1862 cases of data breaches that affected over 155 million people exposing sensitive data with the average global cost of data breach in that same year reported to be 4.24 million dollars [25]. With the advent of Covid-19, and the migration to remote work via cloud platforms and social media, Verizon reports that between March to June 2020, there were over 474 cases of data breaches globally and 80% of these breaches were caused by hackers whereas in 2022, over 530 breaches have been confirmed with 82% involving human element (errors, misuse, and social engineering [26,27]. Consequently, information security and privacy violation is increasingly emerging a serious global disaster, and these issues had led to the emergence of legislations, policies, and strategies that are directed at protecting users and organizations from the unfortunate trend [28], [29], [30], [31]. This agrees with Daalen's point of view [32], which posits that information security is what is to be done and not what anyone has. The implication is that technology users have roles to play in fostering the security of their content as security is paramount in communication as it transcends every technology including social media [33], [34].

Communication is an essential part of humanity and all social and economic activities [35]. These communications occur among families, business associates, school mates, etc. irrespective of the type (written, oral, sign etc.), communication medium used, language, purpose and relevance of the communication respectively [36]. Consequent upon the ubiquity and rapid information delivery capability of smart mobile devices, confidential information could be shared through social media, text messages, voice calls etc. [37], [38]. For instance, during an urgency in communication (e.g. hospital emergency); the sender may not be careful in ensuring that the communication is relayed to the intended person. Consider a scenario where after speaking with a friend or a business partner on the phone in less than 30 minutes, another person (an impostor) uses that same phone line to send text message or a Whatsapp chat. The impostor may request urgent financial assistance while assuring you of reimbursement within a short time. Assuming that the impostor later sends their bank account information to you and this information is exactly the account detail of your business partner. If this supposed business partner has been a trusted party in the past, and you had at any time had such relationship, it is very likely that the fund would be sent. So, an innocent person may become a victim of fraud through social media because criminals can leverage on profiles, events, and records of past chats [39]. The above scenario represents a form of social engineering that is, psychologically manipulating people into involuntarily revealing sensitive information [40]. Fraudsters, kidnappers, robbers, hackers, and other cyber criminals have embraced these techniques to capture their victims. Many have become victims of such circumstances especially the less social media-savvy who may be unaware of such social engineering techniques. In Singapore, it was reported that from January to May 2020, victims were defrauded of over 2.2 million US Dollars through social media impersonation [41]. It is possible to avoid these heartbreaking evil if users could exhibit more resilience in paying attention to pre-established communication patterns and styles. Consequently, this study aims at studying the communication styles, patterns, and user resilience efforts among students in order to ascertain if there exist potential lapses that may be exploited by mischief makers and criminals in the society particularly in recent times where cyber fraud, kidnapping and ritual killing are common. The relevance of this study is to promote user resilience during communication and conversation on the social media channels and to ensure that messages are exchanged with the intended person(s) only thereby reducing crimes. The objectives of this study are:

- To investigate actions and strategies undertaken by users to ensure that their social communications are protected;
- To reveal any inherent security gaps that may be exploited by cyber criminals, kidnappers, and other criminals;
- To awaken communication security consciousness among students; and other users of social media;
- To recommend communication patterns and security screening techniques that would check social media hijacking by kidnappers, fraudsters, hacktivists, impostors, and criminals.

We have formulated some vital questions which are in consistent with the earlier stated objectives. These questions are:

- Are the students' perspectives in the use of social media connected to any inherent dangers that may arise from compromise of their communications?
- Are their communications patterns adopted by students who use social media during their studies?
- If communication styles and patterns exist, are such resilient enough to ensure that information exchange is protected and directed to the intended recipient during the communication process?
- Are there threats to privacy and content integrity that should warrant mandatory security screening while on social media?
- If threats to privacy and data security exist, to what extent can security screening and user resilience curb impersonation and criminal communication hijacking among students in tertiary institutions?

II. RELATED LITERATURE

There is tremendous increase in the use of social media and other real-time mobile communication platforms in the last decade, and the adoption of social media apps had increased astronomically since the advent of the COVID-19 pandemic due to restriction of movements globally [6] [42], [43]. Galanti etal [44] noted that many countries embraced the "Work from home" and "remote schooling" during the

corona virus outbreak. Many organizations had to strengthen their digital solutions and orientation during this time [45]. Screen time further increased consequent upon public health measures enforced by governments [46]. O'Brien [47] had noted that during this period, global retail e-commerce sales rose to 4.28 trillion US Dollars with nearly 432 billion US Dollars of that amount generated in the United States alone due to the use of social media marketing and social media platforms [48], [49]. In the higher education sector, the trend is similar. However, the use of social media technologies among staff and students dates back to the pre-COVID era. During and after the COVID-19 pandemic, many institutions had integrated smart social media solutions into their academic workflows as well as in their student support paraphernalia to further boost teaching, learning, support services, and mentoring [50]. The use of academic groups on Whatsapp, and other social apps is commonplace [51].

In relation to social interaction, Shojaee et al [52] posited that conversation orientation provides a comfort zone for people, and helps them in participating in various activities. Many students are more active with social media than while in the classroom [51]. Most users are skillful at maintaining their relationships, and managing the conflicts through the social media. Such communication takes place in different ways, and social media is emerging very popular in recent times. About two-thirds of users of social media say that the major reason for using it is to keep in touch with current friends and family members. The common choices include Facebook, Blogs, Twitter, MySpace, and LinkedIn whereas about 50% say social media helps them to reconnect with old friends [53]. Achieving a shared reality (agreement, accuracy, and congruence in beliefs and attitudes) increases the chance that family members will understand and be understood by one another [54].

Notably, on the downside of the massive adoption of social media lies the tendency to exploit and/or hijack legitimate user accounts, profiles, photos, etc on such social media platforms. Identity theft is commonplace on online platforms especially social media. Discovering that someone is being impersonated online may take some time after the impersonation and identity theft occurs. In the case of social media platforms like Facebook, whenever someone's account is compromised or completely stolen by a fraudster or hacker, and the legitimate account owner is not connected to family and close friends through other communication platforms to inform them of such theft in time, those family and friends would be communicating freely with the wrong person. This communication may lead to further theft of important information with serious consequences. Kambellari [55] noted that in the virtual world, one person can present himself in different identities and several persons can present themselves under the same virtual identity. Online impersonation can occur in two ways: either by stealing one's personal information to gain access to his online profile or by creating a completely fake profile. The fake profile might reveal information that belongs to someone else or be totally fictitious. Such flexibility in assuming one's identity online is due to the anonymity that people enjoy in the online world. Inability to elaborate proper identification tools of Internet users is one of the biggest challenges in preventing and prosecuting social media related crimes. However, creating a fake online profile is not a criminal act per se. The component that turns the lawful act into an unlawful act of online impersonation is the impostor's malicious intent to "defraud," obtain a "benefit," or "injure". Personally Identifiable Information (PII) may include name, physical home address, email address, telephone numbers, date of birth, marital status, Social Security numbers (US), National Insurance Numbers (UK), and other information relating to medical status, family members, employment, and education. These data, whether lost via data breaches or stolen piecemeal through phishing campaigns, can provide attackers with enough information to conduct identity theft, take out loans using your name, and potentially compromise online accounts that rely on security questions being answered correctly. In the wrong hands, this information can also prove to be a gold mine for advertisers without good ethical and moral policies [56].

III. METHODOLOGY

The case study approach was adopted in this study [57]. The import of this approach is to enable exhaustive investigation and particularization of the subject matter. We used the following data collection methods: structured interview, printed and online questionnaire. The population includes all undergraduates in a renown State-owned Polytechnic in Southern Nigeria. The Institution was selected based on its high multi-cultural spread. The population comprises 3500 students spread across nine (9) academic departments in the Institution. Simple random sampling was used to select 1000 students from the national diploma and higher national diploma programmes respectively. Fifteen students from each department were interviewed whereas all the students were administered questionnaires. The essence of the interview was to gain some insight as to the disposition of the students towards social media usage. The documented selected interviews were also compared to the completed questionnaires submitted by the interviewed students. Targeted social media platforms were: Facebook, Whatsapp, Instagram, Telegram, and Twitter respectively. The questionnaire was divided into four sections namely:

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 [58].
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.

A. Analysis

Use of descriptive statistics enables us to represent and interpret data more efficiently through numerical calculation, graphs and/or tables [34]. Table I shows the age distribution whereas Table II depicts the gender distribution of the respondents. Table III summarizes the entire distribution. The interviewees include students from nine (9) departments. Table IV shows the distribution of respondents that use one or more types of communication patterns on social media. Table V shows the various degrees to which the respondents are involved in security screening during their communication on social media. In Table V we considered only the respondents with social media accounts, those that do not have any social media account were not included.

TABLE I: Age distribution of respondents

Department	**No. of respondents**	**Age Distribution of respondents**					
		13-18	**19-24**	**25-29**	**30-34**	**35-39**	**40-44**
Business Admin. & Management	141	57	28	24	18	11	3
Accounting	104	49	41	7	5	2	0
Science Lab. Technology	86	37	32	9	5	2	1
Computer Science	104	42	48	11	2	1	0
Civil Engineering	75	30	22	11	2	7	2
Architecture	85	43	25	12	5	0	0
Estate Management	101	32	37	21	8	3	0
Urban & Reg. Planning	132	34	43	22	30	2	1
Public Administration	172	55	57	43	13	3	2
Total	**1000**	**379**	**333**	**160**	**88**	**31**	**9**

Table II: Gender distribution

Department	Total	Gender breakdown	
		Male	Female
Business Admin. & Management	141	52	89
Accounting	104	78	26
Science Lab. Technology	86	41	45
Computer Science	104	88	16
Civil Engineering	75	73	2
Architecture	85	85	0
Estate Management	101	96	5
Urban & Reg. Planning	132	107	25
Public Administration	172	111	61
Total	**1000**	**731**	**269**

TABLE III: Student distribution.

S/N	**Department**	**NoS**	**NSP**	**SMP**	**SIS**	**PRC**
1.	Business Admin. & Management	141	120	100	92	9
2.	Accounting	104	92	81	77	4
3.	Science Lab. Technology	86	63	40	40	2
4.	Computer Science	104	102	100	95	12
5.	Civil Engineering	75	61	55	50	7
6.	Architecture	85	85	73	62	2
7.	Estate Management	101	79	52	50	1
8.	Urban & Reg. Planning	132	127	96	85	0
9.	Public Administration	172	155	134	122	3
Total		**1000**	**764**	**731**	**673**	**40**

Notes:

- 'S/N' = Serial Number
- 'NoS' = Number of respondents across all levels
- 'NSP' = Number of respondents that use smart phones
- 'SMP' = Number of respondents with social media presence
- 'SIS' = Number of respondents who share sensitive information on social media
- 'PRC' = Number of students who perform security screening before sharing sensitive information on social media.

TABLE IV. Distribution of respondents with communication patterns

Department	**Communication styles/pattern**	**%**
Business Admin. & Management	60	12.17
Accounting	27	5.48
Science Lab. Technology	35	7.10
Computer Science	57	11.56
Civil Engineering	48	9.74
Architecture	82	16.63
Estate Management	50	10.14
Urban & Reg. Planning	45	9.13
Public Administration	89	18.05
Sub-total	**493**	**49.3**

TABLE V. Distribution of respondents' security pre-checks

Security pre-check	Number of respondents	Percentage
Knowledge of Multi-Factor Authentication(MFA)	137	18.74
Use MFA in social media accounts	130	17.78
Use of one-time password	240	32.83
Use of tokens	49	6.70
Perform background group checks	226	30.92
Perform profile checks before sending messages	90	12.31
Use slogans/local dialect to verify the identity	120	16.42
Perform event checks	30	4.10
Click on shared web links without prior verification	540	73.87
Verify web links before accessing them	89	12.18
Permit account to be added to unknown groups	593	81.12
Follow online ads without verification	227	31.05
Delete chat histories	28	3.83
Maintain chat histories	**700**	**95.76**
Knowledge of fake news	637	87.14
Verify hashtags	34	4.65
Verify Posts	49	6.70
Verify names, photos, descriptions, and profiles of the other party	130	17.78
Join online campaigns	428	58.55
Verify pages	39	5.34
Share links and posts	721	98.63
Total number with social media accounts	**731**	

Figure 2 shows the percentage of students in relation to the kind of phone used. The criteria are based on:

- smart phone users
- non-smart phone users

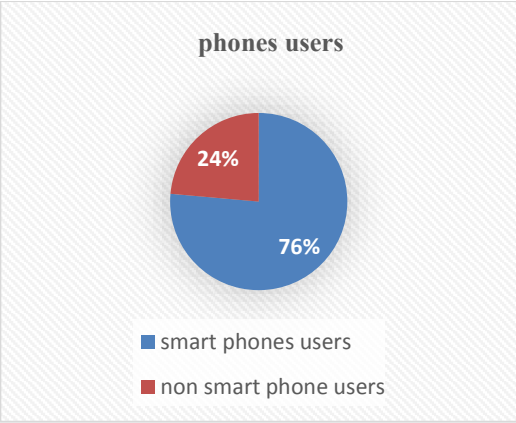

Figure 2: Category of phones used by students

Figure 3 shows the percentage of students in relation to their social media presence.

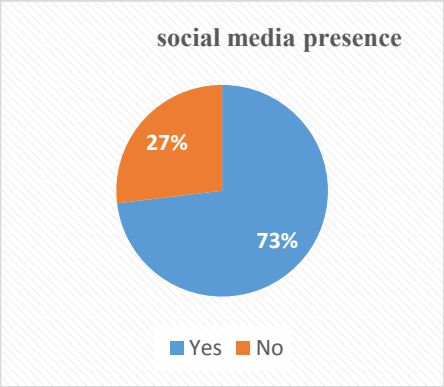

Figure 3: Social media presence

Figure 4 shows the percentage of students in relation to sharing sensitive information on social media based on 'Yes', 'No' criteria.

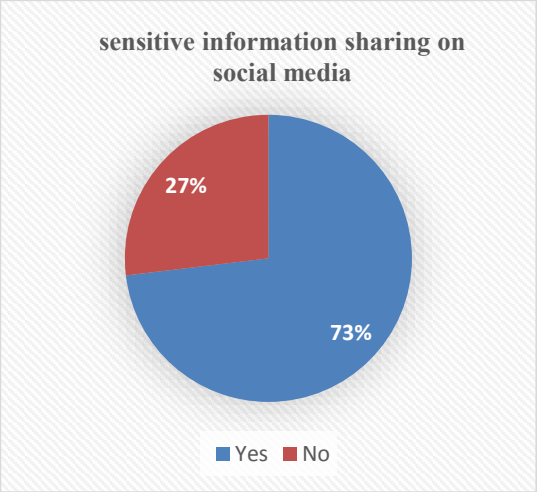

Figure 4: Sensitive information sharing on social media

IV. DISCUSSION

76% of all respondents have at least a smart phone which pre-supposes their knowledge and use of social media. Accordingly, 73% uses at least one social media platforms whereas 23% do not have any social media presence. It is instructive to note that 73% share confidential and sensitive information over the social media platform which is a ground to justify the need for more user resilience as regards the use of vital security pre-checks during communications on social media. In respect of communication pattern, 493 respondents accounting for 49.3% uses one form of communication pattern or the other which may provide a reasonable pre-check parameter prior to communication provided chat or message histories are not maintained as the hijacker or hacker can use message histories to track such patterns, however, it could be seen that majority of the respondents retain their chat histories which may greatly enhance the possibility of negating the gains that would been made through the use of appropriate communication patterns. The variability in the use of communication patterns across several departments cannot be easily explained but may be connected to the discipline. For instance, architecture deals a lot with symbolic and graphical representation which are also means of communication with the outside world. In a similar vein, public administration which recorded the highest use of

Patterns, is a social science discipline and it may correct that the discipline might have provided its students with a variety of ways to drive communication in the society. In respect of security screening, overall, there is a very poor outlook in the part of the respondents. From the statistics, it may be gathered that the respondents do not exhibit average user resilience and hijackers and cyber criminals can leverage on this poor resilience to perpetrate a lot of evil.

A. Remedies

With the proliferation of social media accounts among students in tertiary institutions, there is increased tendency of sensitive communications being hijacked and used against students, in addition to the adoption of good security pre-checks, students should pay attention to:

- **a.** Remarkable discussions or the activities that take place physically in the campus each day. For instance, after school hours when everybody must have gone home, a student launches a social media app and sees some of his colleagues' status as 'online', before that student begins to share sensitive information with the supposed colleague(s), the student can make some requests like "could you please remind me of that topic we treated at 2pm class today?"
- **b.** Before sending or requesting some supposedly confidential information from someone whom the student had met physically within the past 3 hours, the student may use questions like: "I hope you arrived Lagos safely yesterday?" if the person is smart, they would decode why such a question is asked, and this may also lead to the respondent doing own pre-check at same time.

V. CONCLUSION

This study focuses on the privacy and security of content relayed through social media amid rising security concerns such as fraud, kidnapping, ritual killing, and other social vices connected with the cyber space especially the social media and social networks. The emphasis is on security screen and user resilience. Findings in this study revealed that user resilience among students is still poor and this may have been connected to several social vices as had been mentioned earlier in this paper. As had been noted earlier, security is what the user of a technology does and not what they have. Consequently, we conclude that security awareness programmes on social media and social networks may be necessary in tertiary institutions to educate the younger population on how to strengthen their personal security not only on social media but in the cyber space generally.

RECOMMENDATION

We recommend that sensitization programmes on security be organized for students in our tertiary institutions. The programmes must deal with security issues in social media communications.

We also recommend that the subject matter should be extended to the other establishments and the world at large.

ACKNOWLEDGMENT

The authors appreciate the support given by Staff and Students of Abia State Polytechnic Aba during this study.

REFERENCES

[1]. W. Nwankwo, K.C. Ukaoha. "Socio-Technical perspectives on Cybersecurity: Nigeria's Cybercrime Legislation in Review", *International Journal of Scientific and Technology Research*, vol. 8, issue 9, pp. 47-58, 2019.

[2]. W. Nwankwo & C. Umezuruike. "Institutionalizing Social Network Solutions in Tertiary Educational Institutions", *Journal of Applied Science, Information and Computing*, vol. 1, issue 1, pp. 20-28, 2020.

[3]. J. I. Criado & J. Villodre. "Revisiting social media institutionalization in government. An empirical analysis of barriers", Government Information Quarterly, vol. 39, Issue 2, 2022.

[4]. F. Platania, C. T. Hernandez, & F. Arreola, "Social media communication during natural disasters and the impact on the agricultural market". Technological Forecasting and Social Change, vol. 179, 2022.

[5]. A.J. Kucharczuk, T. L. Oliver, & E. B. Dowdell. "Social media's influence on adolescents′ food choices: A mixed studies systematic literature review". *Appetite*, vol. 168, 2022.

[6]. W. Nwankwo, B.S. Olanrewaju, P.U. Chinedu & T.C. Olayinka, "The Role of Social Information Technology in curbing Corruption", *American Journal of Embedded Systems and Applications*, vol. 6, issue 1, pp. 56-68, 2018.

[7]. Chaffey. (2022). *Global social media statistics research summary 2022*[Online]. Available: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

[8]. T. Dittloff. (2020). *The Importance of timely communication* [Online]. Available: https://fullsailleadership.com/the-importance-of-timely-communication/

[9]. R. M. Ali & S.N. Alsaad, "Instant messaging security and privacy secure instant messenger design", *3rd International Conference on Sustainable Engineering Techniques (ICSET 2020) IOP Conf.* Series: Materials Science and Engineering 881,2020

[10]. W. Nwankwo. "A Review of Critical Security Challenges in SQL-based and NoSQL Systems from 2010 to 2019", *International Journal of Advanced Trends in Computer Science and Engineering*, vol.9,issue 2, pp.2029-2035,2020

[11]. P.U. Chinedu, W. Nwankwo, D.Aliu, S.M. Shaba, & M.O. Momoh. "Cloud Security Concerns: Assessing the Fears of

Service Adoption". *Archive of Science and Technology*, vol. 1, issue 2, 2020. pp. 164-174.

[12]. A. Daniel, S.M. Shaba, M.O. Momoh, P.U. Chinedu, & W. Nwankwo. "A Computer Security System for Cloud Computing Based on Encryption Technique", *Computer Engineering and Applications,* vol. 10, issue 1, pp.41-53, 2021.

[13]. P.U. Chinedu, W.Nwankwo, F.U. Masajuwa, & S. Imoisi, "Cybercrime Detection and Prevention Efforts in the Last Decade: An Overview of the Possibilities of Machine Learning Models". *Review of International Geographical Education (RIGEO)*, vol. 11, issue 7, pp.956-974, 2021.

[14]. W. Nwankwo & C.C. Njoku, "Adoption of Internet Voting Platform: Containing Data Injection Threats with Structured LINQ". *Nigerian Research Journal of Engineering and Environmental Sciences*, vol. 4, issue 2, pp.724-739, 2019.

[15]. W. Nwankwo & A.S. Olayinka. "Implementing a risk management and X-Ray cargo scanning document management prototype", *International Journal of Scientific and Technology Research*, vol.8, issue 9, pp. 93-105, 2019.

[16]. Groupsence. (2022). *Social media account impersonation: cyber criminals posing as your brand are a significant risk to your organization.*[online] Available: https://www.groupsense.io/social-media-account-impersonation.

[17]. K.V. Schyff, S. Flowerday, & P.B. Lowry. "Information privacy behavior in the use of Facebook apps: A personality-based vulnerability assessment", *Heliyon*, vol.6, issue 8, 2020.

[18]. D. Aizenkot. "Cyberbullying experiences in classmates WhatsApp discourse, across public and private contexts", *Children and Youth Services Review*. vol. 110, 2020.

[19]. The Guardian. (2019 May). *Social media fraud rose by 43% in 2018*" [online]. Available: https://guardian.ng/technology/social-media-fraud-rose-by-43-in-2018/

[20]. T. Bull. (2021 Sept.). *How to Keep Your Facebook Account from Being Hijacked* [online]. *Available: ttps://www.tworivercomputer.com/facebook-account-hacked/*

[21]. Liapustin, M. (2022). *Email security and impersonation protection*[online].Available: https://trustifi.com/email-security-and-impersonation-protection/

[22]. L.F. Freedman. "Privacy Tip #312 -Impersonation fraud increased during pandemic". *The National Law Review*, vol. 12., Issue 232, 2022.

[23]. S. Zeebaree, S. Ameen, & M.S. Mohammed. "Social Media Networks Security Threats, Risks and Recommendation". A Case Study in the Kurdistan Region", vol. 13, pp 349-365,2020

[24]. N. Foecking, M. Wang, & T. L. D. Huynh. "How do investors react to the data breaches news? Empirical evidence from Facebook Inc. during the years 2016–2019", *Technology in Society*, vol. *67*, issue 101717, 2021.

[25]. IBM (2022). *Cost of a Data Breach Report* [online]. Available: https://www.ibm.com/downloads/cas/3R8N1DZJ.

[26]. Verizon. (2020). *Money makes the cyber-crime world go round - Verizon Business 2020 Data Breach Investigations Report*[online] Available: https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report

[27].Verizon Inc, (2022). *2022 Data Breach Investigations Report.* Available: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

[28]. N. Goyal, M. Howlett, & A. Taeihagh. "Why and how does the regulation of emerging technologies occur? Explaining the adoption of the EU General Data Protection Regulation using the multiple streams framework". *Regulation & Governance*, vol. 15, issue 4, pp. 1020-1034. 2021.

[29]. A. Kifordu, W. Nwankwo, & W. Ukpere, "The Role of Public Private Partnership on the Implementation of National Cybersecurity Policies: A Case of Nigeria", Journal *of Advanced Research in Dynamical and Control Systems*, vol. 11, issue 8, pp.1386-1392, 2019.

[30]. P.U. Chinedu, W. Nwankwo, B.S. Olanrewaju, & T.C. Olayinka, "Cloud-Based Virtual Organization Framework for Optimizing Corporate Value Chain". *International Journal of Discrete Mathematics,* vol. 3, issue 1, pp. 11-20,2018.

[31]. W. Nwankwo & A. Kifordu, "Strengthening Private Sector participation in Public Infrastructure Projects through Concession Policies and Legislations in Nigeria: A Review". *Journal of Advanced Research in Dynamical and Control Systems, vol.*11, issue 8, pp.1360-1370, Special Issue, 2019

[32]. O. Daalen. "In defense of offense: information security research under the right to science" *Computer Law & Security Review*. vol. 46, 105706. 2021.

[33]. L. Chen, S. Suo, X. Kuang, Y. Cao, & W. Tao, "Secure Ubiquitous Wireless Communication Solution for Power Distribution Internet of Things in Smart Grid", IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), pp. 780-784,2021.

[34]. W. Nwankwo & O. Famuyide, "A Model for Implementing Security and Risk Management Data Warehouse for Scanning Operations in Nigeria", *International Journal of Engineering Research and Technology*,vol. 5, issue 5, pp.581-593, 2016.

[35]. A. Berea. (2019). *A complex systems perspective of communication from cells to societies*{Online]. Available: https://www.intechopen.com/chapters/65763

[36]. S. Z. Zhao, T. T. Luk, N. Guo, etal. "Association of Mobile Instant Messaging Chat Group Participation with Family Functioning and Well-Being: Population-Based Cross-sectional Study". *J Med Internet Res*. Vol.23, Issue 3, 2021.

[37]. P. M. Etwire, S. Buah, M. Ouédraogo et al. "An assessment of mobile phone-based dissemination of weather and market information in the Upper West Region of Ghana". *Agric & Food Security,* vol.6, Issue 8.

[38]. W. Kuang. (2018). Mobile Phone Media and Its Public Opinion Management. Social Media in China[Online]. Available: https://link.springer.com/chapter/10.1007/978-981-13-0914-4_7#citeas.

[39]. J.W. Emma, B. Amy, & N. Adam. "Individual differences in susceptibility to online influence: A theoretical review". *Computers in Human Behavior*, vol. 72, pp. 412-421, 2017.

[40]. O. Kubovic. (2021). *Impersonation*: *When an attacker is posing as the CEO*[Online] Available: https://digitalsecurityguide.eset.com/en-us/impersonation-when-an-attacker-is-posing-as-the-ceo

[41]. J. Lim. (2020). *Social media impersonation scams double in 2 months, with victims losing $2.2m*[online]. The StraitsTimes Singapore. Available: .https://www.straitstimes.com/singapore/courts-crime/amount-social-media-impersonation-scam-victims-lost-doubles-to- 22m-in-2.

[42]. J. Abbas, D. Wang, Z. Su, & A. Ziapour. "The Role of Social Media in the Advent of COVID-19 Pandemic: Crisis Management, Mental Health Challenges and Implications", *Risk Manag Healthc Policy*, vol. 14, pp. 1917-1932, May 2021.

[43]. M.N. Khan, MA. Ashraf, D Seinen, K. Khan, & L.R.A. Ullah(May 2021). "Social Media for Knowledge Acquisition and Dissemination: The Impact of the COVID-19 Pandemic on Collaborative Learning Driven Social Media Adoption". *Frontiers in Psychology* vol. 12.Available: www.frontiersin.org/articles/10.3389/fpsyg.2021.648253

[44]. T. Galanti, G. Guidetti, E. Mazzei, S. Zappalà, & F. Toscano. "Work from home during the COVID-19 outbreak: The Impact on Employees' Remote Work Productivity, Engagement, and Stress", *Journal of Occupational and Environmental Medicine, vol.* 63, issue 7, Jul. 2021.

[45]. W.A. Tri, I.G. Artatanaya, & B. John. "Working from home effectiveness during Covid-19: Evidence from university staff in Indonesia". *Asia Pacific Management Review,* vol. 27, Issue 1, pp. 50-57, Mar. 2022

[46]. A. Pandya & P. Lodha (Jul. 2021). "Social Connectedness, Excessive Screen Time during COVID-19 and Mental Health: A Review of Current Evidence", *Frontiers in Human Dynamics.* vol. 3. Available https://www.frontiersin.org/articles/10.3389/fhumd.2021.684137/full

[47] C. O'Brien. (2021). *The Future of Marketing After Covid 19[*Online*]*. Available: https://digitalmarketinginstitute.com/blog/the-future-of-marketing-after-covid-19

[48] D. Öztamur,İ. SarperKarakadılar, "Exploring the Role of Social Media for SMEs: As a New Marketing Strategy Tool for the Firm Performance Perspective", *Procedia - Social and Behavioral Sciences*, vol. 150, pp.511-520, Sept. 2014.

[49] A. N. Sulthan, R. Evangelin, & V. Shanmugam. Influence of Social Media marketing in post COVID-19. *Design Engineering*, issue 7, pp. 6370-6377, 2021. Available: https://www.researchgate.net/publication/354886494_Influence_of_Social_Media_marketing_in_post_COVID-19

[50]. W. Nwankwo, U.P. Chinedu, D. Aliu, M.S. Saliu, O.M. Momoh, C.P. Nwankwo, & A. Wilfred. "Integrated FinTech Solutions in Learning Environments in the Post-COVID-19 Era". *IUP Journal of Knowledge Management,* vol. 20, issue 3, pp. 1-22. 2022.

[51]. 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.

[52]. S. Shojaee, M. S. Khakhaninejad, & M. Najafi. "Family communication patterns of individuals with and without disabilities". *Health psychology research*, vol. *6, issue* 1, 2018.

[53]. H. Russell. (2011). *Using social media to keep in Touch [*Online*]. Available:* https://www.pewresearch.org/facttank/2011/12/2/using-social-media-to-keep-in-touch/

[54]. D. R. Samek & M.A. Rueter. "Associations between Family Communication Patterns, Sibling Closeness, and Adoptive Status". *Journal of marriage and the family,* vol. 73, issue 5, 2011.

[55]. E. Kambellari. (2017). *Online Impersonation: I Have a Right to Be Left Alone. You Can't Mandate How I Use My Privacy Toolbox [*Online*]* Available: https://www.researchgate.net/publication/332382876_Online_Impersonation_I_Have_a_Right_to_Be_Left_Alone_v_You_Can't_Mandate_How_I_Use_My_Privacy_Toolbox/citation/download

[56]. O. Charlie, (2019). *Cybersecurity 101: Protect your privacy from hackers, spies, and the government*[Online] Available: https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government

[57] W. Nwankwo & K. Ukhurebor. "Big Data Analytics: A Single Window IoT-enabled Climate Variability System for all-year-round Vegetable Cultivation". *IOP Conference Series: Earth and Environmental Science,* vol. 655, Issue 1, 2021.

[58] J.M. Stewart, M. Chapple, & D. Gibson. CISSP Study Guide, Sixth Edition, *Indianapolis*: John Wiley & Sons, 2012.