International Journal of Scientific Research and Engineering Development-– Volume 7 Issue 6, Nov-Dec 2024
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

College Students' Awareness and Perceptions Towards the End-To-End Encryption In Facebook Messenger

[1]Francille C. Mapagdalita, [2]Joseph Paulo O. Galleros, [3]Marvin A. Gonzales, [4]Markdy Y. Orong
[1]College of Computer Studies, Misamis University, H.T. Feliciano St, Ozamiz City, 7200 Misamis Occidental
Email: francillemapagdalita@gmail.com
[2]College of Computer Studies, Misamis University, H.T. Feliciano St, Ozamiz City, 7200 Misamis Occidental
Email: josephpaulogalleros@gmail.com
[3]College of Computer Studies, Misamis University, H.T. Feliciano St, Ozamiz City, 7200 Misamis Occidental
Email: marvingonzales@gmail.com
[4]Doctor in Information Technology, College of Computer Studies, Misamis University, H.T. Feliciano St, Ozamiz City, 7200 Misamis Occidental
Email: markdy.orong@mu.edu.ph

----------**********----------

Abstract:

This study investigated the awareness and perceptions of college students at Misamis University in Ozamiz City, Philippines, regarding end-to-end encryption (E2EE) in Facebook Messenger. Using a quantitative approach, it explored how demographic factors like gender and program of study influenced students' understanding and views on the platform's security features. A total of 311 respondents were selected through convenience sampling. The results revealed moderate awareness of encryption, with the highest mean score of 3.29 for belief in secure transmission in Secret Conversations and the lowest of 3.06 regarding whether Messenger developers could read encrypted messages. In terms of security perceptions, students generally viewed Facebook Messenger as secure, with the highest mean score of 3.36 for overall security and the lowest of 3.14 for trust in privacy guarantees. A significant positive correlation ($r = 1$, $p < 0.01$) was found between awareness and perceptions, emphasizing the importance of awareness in shaping perceptions of digital security. Future research should explore digital literacy programs and factors like social media habits and technological exposure in influencing students' online security behaviors.

Keywords — **Awareness, Perceptions, End-to-end encryption, Facebook Messenger, Digital Security.**

----------**********----------

I. INTRODUCTION

In the digital age, social media emerged as a powerful and ubiquitous tool for individuals to curate, share, and communicate information with friends, family, and a global audience (Stone & Wang, 2019; Cladis, 2020). The widespread use and reliance on these platforms led to a significant increase in users, which surged even further during the COVID-19 pandemic under stay-at-home conditions (Nguyen et al., 2020). As society grew increasingly dependent on these digital technologies, their transformative impact on human interaction became evident, improving the speed and methods by which people conducted daily activities and enhancing productivity (Cladis, 2020). However, with the rising usage and reliance on social media platforms, associated risks escalated as well. The rapid growth of social networking led to extensive data sharing, increasing the risk of information leakage and enabling cybercrimes such as data interception, privacy invasion, copyright infringement, and fraud (Jain et al., 2021). In a world where digital interactions were pervasive, the need to protect users and secure these platforms became more critical than ever.

To address these security concerns, end-to-end encryption (E2EE) gained traction over the past

decade as one of the most widely used privacy technologies worldwide, forming a cornerstone of online user security and privacy (Scheffler & Mayer, 2023; Len et al., 2023). E2EE ensured that message content remained accessible only to the sender and intended recipient, preventing unauthorized access by service providers, government surveillance, or man-in-the-middle (MitM) attacks (Alatawi & Saxena, 2023; Chakraborti et al., 2023). Recognizing the importance of protecting users' data, major messaging platforms, including WhatsApp and iMessage, adopted E2EE by default, while others, like Facebook Messenger and Telegram, offered it as an optional feature (Song, 2024; Dechand et al., 2019; Bai et al., 2020). Initially, most instant messaging (IM) applications did not support E2EE; however, with escalating security concerns, it became the standard for secure communication, widely implemented across modern IM platforms (Beery, 2024). This shift underscored the growing emphasis on privacy and data protection as central elements of digital communication.

Facebook Messenger stood as one of the leading social media platforms, boasting over 1.3 billion monthly active users as of October 2019 (Rozgonjuk et al., 2020; Chang & Yen, 2020). This popular messaging application provided a versatile range of features that supported not only social interactions but also educational tools that promoted student-centered learning environments (Samani & Noordin, 2020). Among college students, Facebook Messenger gained significant traction in both their social and academic lives, offering functionalities for exchanging text messages, photos, videos, stickers, audio, files, and even interactive reactions to messages. The platform further supported voice and video calling, enhancing its utility for various forms of communication (Feng et al., 2019; Chang & Yen, 2020). This broad range of communication functionalities made Messenger an efficient and immediate tool for students seeking to connect with peers and instructors, facilitating a level of personal interaction that traditional communication channels often lacked (Giannikas, 2020).

Facebook's introduction of end-to-end encryption (E2EE) in Messenger through Secret Conversations reflected the platform's response to heightened privacy demands, yet its implementation as an optional feature required user engagement to be effective. Unlike the default messaging mode, Secret Conversations necessitated users to manually activate E2EE and to prompt their recipients to do the same. Initially limited to individual chats and calls, Secret Conversations later expanded to support E2EE in group chats and calls, enhancing privacy for a wider range of interactions (Song, 2024; Bhuse, 2023; Alatawi & Saxena, 2023). However, this user-dependent model underscored the responsibility placed on individuals to proactively manage their own privacy, a challenge given that many users lacked adequate awareness of E2EE's importance.

Despite the pervasive role of digital technology in modern life, research suggested that a gap remained in users' understanding of essential privacy practices. Studies showed that while college students—often termed "digital natives"—were familiar with technology, they did not fully grasp privacy practices. Research conducted at the University of Cape Coast in Ghana found that most students had limited understanding of data encryption (Edumadze et al., 2022), while a Swedish study noted generally low privacy concerns among students using mobile messaging applications (Tesfazion, 2020). Similarly, studies involving adult users of messaging apps revealed that many misunderstood E2EE's security features and inaccurately assessed the safety of various communication methods, sometimes believing SMS or email to be more secure than encrypted messengers (Dechand et al., 2019; Schaewitz et al., 2022; Stransky et al., 2021). This research highlighted an essential gap in user knowledge and stressed the importance of education to enhance awareness of E2EE's role in safeguarding digital interactions.

Building on these insights, this study contributed to the broader field of digital security and privacy within educational settings by focusing on Misamis University students' awareness and perceptions of end-to-end encryption (E2EE) in Facebook

Messenger. Specifically, the research examined how factors like gender and academic program impacted students' awareness and perception in the platform's security features. By shedding light on the current state of digital privacy awareness among university students, the study identified critical areas for enhancing digital literacy, aiming to better equip students for secure online interactions. Through understanding these perceptions and pinpointing awareness gaps, the findings informed educators and policymakers in developing targeted educational initiatives that promoted safer digital security practices. This effort, in turn, fostered a more secure online environment within the academic community, empowering students to navigate digital spaces with greater confidence and understanding.

II. METHODOLOGY

This study employed a quantitative approach to assess college students' awareness and perceptions of end-to-end encryption (E2EE) in Facebook Messenger at Misamis University in Ozamiz City, Misamis Occidental, Philippines. Focusing on demographic factors such as gender and program of study, the research aimed to understand how these elements influence students' awareness and perceptions of the platform's security features. Data were collected through a structured Google Forms questionnaire that gathered respondents' demographic information, E2EE awareness and perceptions of Facebook Messenger's security. Using a Likert scale, the questionnaire allowed for a quantifiable assessment of students' understanding and perceptions of E2EE.

Descriptive statistics, including mean, frequency, and percentage, were utilized to summarize demographic details and evaluate students' awareness and perceptions. To analyze the relationship between awareness and perception scores across various academic groups and genders, the study employed Pearson's Correlation Coefficient. This statistical method assesses the strength and direction of the linear relationship between awareness and perceptions, providing a robust framework for understanding these dynamics. Although the study is limited to Misamis University and the use of convenience sampling may restrict the generalizability of its findings, the results offer valuable insights into how college students perceive and understand encryption technologies, particularly in digital communication platforms like Facebook Messenger.

III. RESULTS

This section presents the findings and analysis of college students' awareness and perceptions of end-to-end encryption (E2EE) in Facebook Messenger at Misamis University, supported by tables and key discussions.

3.1 Demographic Profile

The study examined the gender distribution of respondents, as presented in Table 1. The data highlights the composition of participants and provides insights into the representation of each gender within the sample.

TABLE I
RESPONDENTS' GENDER DISTRIBUTION

Gender	Frequency	Percent
Female	123	39.3
Male	190	60.7
Total	**313**	**100**

Table 1 presents the gender distribution of the respondents. Of the 313 participants, 190 (60.7%) identified as female, while 123 (39.3%) identified as male. This distribution indicates a higher participation rate among females. The predominance of female respondents suggests that gender may influence the findings on awareness and perceptions of encryption technology.

TABLE III
RESPONDENT'S PROGRAM OF STUDY DISTRIBUTION

Department	Frequency	Percent
Agriculture and Forestry	32	10.2
Arts and Science	27	8.6
Business and Man	31	9.9
Computer Studies	42	13.4
Criminology	28	8.9
Education	28	8.9
Engineering	50	16
Maritime	41	13.1
Paramedical	34	10.9
Total	**313**	**100**

While Table 2 shows the distribution of respondents by program of study, the largest group of the 313 participants came from the Engineering department, comprising 16% of the respondents, followed by those from Computer Studies (13.4%) and Maritime (13.1%). Other departments represented include Agriculture (10.2%), Paramedical (10.9%), Business and Management (9.9%), Criminology (8.9%), Education (8.9%), and Arts and Science (8.6%). This diverse distribution across academic programs offers varied perspectives on the awareness and perceptions of end-to-end encryption in Facebook Messenger. Such diversity in respondents is valuable in identifying whether specific academic backgrounds influence students' knowledge of online privacy issues and their overall trust in digital platforms, thus providing deeper insights into the factors that shape their views on secure communication.

3.2 Level of Awareness of End-to-End Encryption (E2EE) Among College Students

This section presents the mean scores and corresponding interpretations of college students' level of awareness regarding end-to-end encryption (E2EE) in Facebook Messenger. This objective aimed to evaluate the extent of students' understanding of E2EE features and their implications for secure digital communication. The findings from the analysis of mean scores are detailed in Table 3.

TABLE IIIII
RESPONDENT'S PROGRAM OF STUDY DISTRIBUTION

Statement	Mean	Interpretation
With end-to-end encryption, only my device and the recipient can read my chats.	3.18	Somewhat Aware
With Secret Conversations on Messenger, my messages are secure in transit with end-to-end encryption.	3.29	Somewhat Aware
Meta cannot read my Messenger messages with end-to-end encryption.	3.21	Somewhat Aware
Encrypted Messenger messages can be read if someone accesses my smartphone.	3.14	Somewhat Aware
Messenger developers can't read my messages, even knowing the encryption, thanks to end-to-end encryption.	3.06	Somewhat Aware
Messenger's end-to-end encryption is secure but can potentially be broken.	3.12	Somewhat Aware
With Secret Conversations, messages go directly between devices via end-to-end encryption.	3.24	Somewhat Aware
With end-to-end encryption, third parties can't read my Messenger messages in transit.	3.2	Somewhat Aware
With Secret Conversations, no one knows when or with whom I'm communicating.	3.13	Somewhat Aware
Messenger's end-to-end encryption makes messages more secure than traditional text messages.	3.25	Somewhat Aware
General Weighted Mean	**3.21**	Somewhat Aware

Note: 4.20-5.0 (Extremely Aware); 3.40-4.19 (Aware); 2.60-3.39 (Somewhat Aware); 1.80-2.59 (Slightly Aware); 1.0-1.79 (Not at all Aware)

As shown in Table 3, the general weighted mean of 3.21 indicates that respondents have a moderate level of awareness regarding end-to-end encryption in Facebook Messenger. All statements received mean scores ranging from 3.06 to 3.29, which are interpreted as "Somewhat Aware." The highest mean score, 3.29, is associated with the statement about Secret Conversations providing secure transmission, reflecting a relatively stronger understanding of this feature. On the other hand, the lowest mean score of 3.06 pertains to the belief that Messenger developers cannot read messages due to encryption, suggesting a slightly lower level of awareness in this area. These results highlight that while students are generally aware of encryption features, there are some gaps in their comprehension, particularly regarding the technical aspects. To enhance awareness, further educational initiatives and clearer communication about the security features of Facebook Messenger are recommended.

3.3 Level of Perception of End-to-End Encryption (E2EE) Among College Students

This section presents the mean scores and corresponding interpretations of college students' perceptions regarding end-to-end encryption (E2EE) in Facebook Messenger. The objective of this

analysis was to evaluate how students perceive the security features of E2EE and their implications for ensuring secure digital communication. The results from the mean score analysis is presented in Table 4.

TABLE IV
STUDENTS' LEVEL OF PERCEPTION ON END-TO-END ENCRYPTION (E2EE)

Statement	Mean	Interpretation
I find the latest version of Facebook Messenger trustworthy.	3.14	Neutral
I trust the honesty of the latest Facebook Messenger version.	3.22	Neutral
I believe the latest version of Facebook Messenger is secure.	3.36	Neutral
I believe only I and the recipient(s) can read messages in Facebook Messenger's Secret Conversations.	3.19	Neutral
I believe others cannot send messages pretending to be me in Facebook Messenger.	3.18	Neutral
I believe no one can secretly modify messages between me and the recipient(s) in Facebook Messenger.	3.17	Neutral
I believe that if someone hacks my phone, they won't be able to read my messages in Facebook Messenger's Secret Conversations.	3.29	Neutral
I believe only I and the recipient(s) are aware of the messages sent in Facebook Messenger.	3.14	Neutral
I believe Facebook Messenger only collects the personal information strictly needed.	3.22	Neutral
I believe Facebook Messenger will not use my personal information for other purposes without my authorization.	3.21	Neutral
General Weighted Mean	**3.21**	Neutral

Note: 4.20-5.0 (Strongly Agree); 3.40-4.19 (Agree); 2.60-3.39 (Neutral); 1.80-2.59 (Disagree); 1.0-1.79 (Strongly Disagree)

In Table 4, respondents generally exhibit a moderate level of agreement regarding their perceptions of Facebook Messenger's security features, with all statements receiving mean scores between 3.14 and 3.36, which are interpreted as "Neutral." The highest mean score, 3.36, corresponds to the belief that the latest version of Facebook Messenger is secure, suggesting that students perceive the platform as relatively secure and trustworthy. Conversely, the lowest mean score of 3.14 pertains to respondents' trust in the latest version of Facebook Messenger and their belief that only the user and recipient(s) are aware of the messages, indicating a slightly lower level of confidence in these areas. These findings suggest that while students generally perceive Facebook Messenger as secure and trustworthy, there are variations in their confidence regarding specific security features. The general weighted mean of 3.21 confirms that, overall, respondents show a neutral level of agreement with the security features of Facebook Messenger. To enhance user perception, continued efforts to emphasize the platform's security and privacy measures are recommended.

3.4 Relationship Between Awareness and Perceptions of End-to-End Encryption (E2EE) in Facebook Messenger

This section presents the analysis of the correlation between college students' awareness and perceptions of end-to-end encryption (E2EE) in Facebook Messenger. The objective of this analysis was to evaluate the strength and direction of the relationship between students' understanding of E2EE features and their perceptions of its security implications for digital communication. The findings from the correlation analysis are summarized in Table 5.

TABLE V
CORRELATION BETWEEN THE COLLEGE STUDENTS' AWARENESS AND PERCEPTIONS TOWARDS END-TO-END ENCRYPTION IN FACEBOOK MESSENGER

Variables	r	Interpretation	p-value	Interpretation
Level of Awareness	1	Perfect Linear	0	Significant
Level of Perception				

*Scale: 0 - ±0.29 = No linear Relationship, ±0.30 - ±0.49 = Weak linear Relationship, ±0.50 - ±0.69 = Moderate linear Relationship, ±0.70 - ±0.99 = Strong linear Relationship, ±1 = Perfect linear Relationship (*N = 42)*

In Table 5, Pearson product moment correlation r is being used to determine the correlation between the college students' awareness and perceptions towards th end-to-end encryption in facebook messenger. It shows they are significantly related since the p-value which is equal to 0.000 is lesser than the level of significance at 0.05 and both variables have a perfect linear relationship. This implies that the null hypothesis is rejected.

IV. DISCUSSION

This study examines college students' awareness and perceptions of end-to-end encryption (E2EE) in Facebook Messenger at Misamis University, with a focus on the role of demographic factors, particularly gender and program of study, in shaping their understanding and attitudes towards encryption technologies.

Research has shown that demographic factors such as gender and educational background can significantly affect technology perceptions and readiness. Studies indicate that men and women may approach technology differently, which can lead to variations in their understanding and attitudes toward security measures like E2EE (Blasko et al., 2020). In this study, gender differences were explored to identify any patterns in how male and female students perceive E2EE in Facebook Messenger. However, while gender may influence technological perceptions, the findings from this study suggest that other factors, such as the students' program of study, may play an equally crucial role.

The representation of students from technical programs, such as Engineering, Computer Studies, and Maritime, indicates that their educational background may have a substantial impact on their awareness of encryption technologies. Students in technical fields often have more exposure to cybersecurity concepts, which may enhance their understanding of E2EE compared to their peers in non-technical disciplines. This aligns with existing research showing that students from technical fields, like Information Technology and Engineering, typically exhibit higher levels of cybersecurity awareness (Blasko et al., 2020). In contrast, students from non-technical fields, such as Business and Education, may prioritize different aspects of digital security, like privacy or ethical considerations, which can influence their perceptions of encryption technologies (Senthilkumar & Easwaramoorthy, 2017).

The findings of this study reveal that college students at Misamis University possess a "somewhat aware" level of awareness regarding E2EE in Facebook Messenger, with a general weighted mean score of 3.21. This aligns with prior research, which has shown that users are generally aware of online security threats but often lack familiarity with specific terms like "end-to-end encryption" (Schaewitz et al., 2022). The highest mean score, 3.29, is associated with students' awareness of the secure transmission of messages in Secret Conversations, suggesting a relatively stronger understanding of this E2EE feature. This is consistent with research by Singh et al. (2022), which emphasizes the importance of clear communication about encryption features to build user trust. However, the lowest mean score of 3.06, regarding the belief that Messenger developers cannot read messages due to encryption, points to a gap in students' understanding of the limitations and potential vulnerabilities of E2EE systems. Alaqra et al. (2023) noted that while users may understand the general goal of encryption, they often lack knowledge of the technical details involved. This gap highlights the need for educational initiatives that clarify both the benefits and limitations of E2EE to improve students' understanding of the technology.

Regarding perceptions, students showed a "neutral" level of agreement on the security features of Facebook Messenger, with a general weighted mean score of 3.21. This indicates that while students view the platform as generally secure, their confidence in its security features varies. The highest mean score of 3.36, reflecting the belief that the latest version of Facebook Messenger is secure, suggests a positive perception of the platform's security measures. This finding aligns with previous studies indicating that users tend to trust platforms with robust security features (Schaewitz et al., 2022). However, the lowest mean score of 3.14, related to respondents' trust in Facebook Messenger's privacy assurances, suggests some hesitation in fully trusting the platform. This is

consistent with studies that highlight user skepticism regarding the privacy practices of social media platforms, particularly in light of past controversies involving data breaches and privacy violations (Demjaha et al., 2018). Additionally, the belief that "no one can secretly modify messages" received a mean score of 3.17, suggesting that students may not fully understand the potential vulnerabilities within messaging systems. Research by Van Ouytsel et al. (2022) underscores the importance of user education on the limitations of encryption and the possibility of security breaches.

The relationship between students' awareness and perceptions of E2EE was analyzed using Pearson's correlation coefficient. The results indicate a perfect linear relationship ($r = 1$) between the two variables, with a statistically significant p-value of 0.000. This suggests that higher awareness of E2EE is strongly correlated with more positive perceptions of its security features. These findings are consistent with previous research, such as Kher et al. (2019), which highlights the critical role of awareness in shaping user attitudes toward cybersecurity measures. As students become more informed about the mechanisms and benefits of E2EE, their perceptions of its effectiveness and necessity in digital communication are likely to improve. This relationship emphasizes the need for educational programs that enhance awareness of encryption technologies. By improving students' understanding of E2EE, institutions can foster more positive attitudes toward its implementation, encouraging more proactive engagement with security features among users.

V. CONCLUSIONS

This study examined the level of awareness and perceptions of Misamis University college students concerning end-to-end encryption in Facebook Messenger. The findings indicate that students possess a moderate understanding of encryption features, with notable variations in their comprehension of specific technical aspects. Similarly, their perceptions of Messenger's security demonstrate moderate agreement, with higher confidence in the platform's overall security features and relatively lower trust in its handling of personal information and privacy assurances.

A significant positive correlation ($r = 1$, $p < 0.01$) was found between awareness and perceptions, underscoring the influence of knowledge in shaping user attitudes toward secure communication technologies. These findings highlight the need for targeted educational interventions to bridge gaps in understanding and deepen students' awareness of encryption and its role in protecting privacy and security. Furthermore, the study emphasizes the importance of integrating cybersecurity awareness into educational curricula, especially in technical programs. As students' awareness of E2EE grows, so does their confidence in its security features, suggesting that educational efforts can play a key role in improving students' trust in encrypted messaging services. By fostering digital literacy, this study advocates for preparing students to navigate the complexities of cybersecurity, thereby contributing to a more secure digital communication environment in an increasingly interconnected world.

VI. RECOMMENDATIONS

The study recommends implementing digital literacy programs to enhance students' understanding of encryption and online security. These initiatives could include workshops, seminars, and integrating cybersecurity topics into academic courses. Efforts should focus on improving access to reliable information and increasing exposure to secure technologies. Collaboration with technology providers can further foster trust and equip students with the skills to navigate digital platforms securely. Additionally, universities should tailor educational approaches to address demographic differences in students' awareness and perceptions of digital security, ensuring targeted efforts across disciplines. Future research should assess the effectiveness of these programs and explore factors influencing students' behaviors regarding online security.

REFERENCES

[1] Alaqra, A. S., Karegar, F., & Fischer-Hübner, S. (2023). Structural and functional explanations for informing lay and expert users: the case of functional encryption. Proceedings on Privacy Enhancing Technologies, 2023(4), 359-380. https://doi.org/10.56553/popets-2023-0115

[2] Alatawi, M., & Saxena, N. (2023a). SoK: An Analysis of End-to-End Encryption and Authentication Ceremonies in Secure Messaging Systems. Proceedings of the 16th ACM Conference on Security and Privacy in Wirelessand Mobile Networks, 187–201. https://doi.org/10.1145/3558482.3581773

[3] Alatawi, M., & Saxena, N. (2023b). SoK: An Analysis of End-to-End Encryption and Authentication Ceremonies in Secure Messaging Systems. Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 187–201. https://doi.org/10.1145/3558482.3581773

[4] Bai, W., Pearson, M., Kelley, P. G., & Mazurek, M. L. (2020). Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 210–219. https://doi.org/10.1109/EuroSPW51379.2020.00036

[5] Beery, T. A. (2024). WhatsApp with privacy? Privacy issues with IM E2EE in the Multi-device setting. 18th USENIX WOOT Conference on Offensive Technologies (WOOT 24), 11–16. https://www.usenix.org/conference/woot24/presentation/beery

[6] Bhuse, V. (2023). Review of End-to-End Encryption for Social Media. International Conference on Cyber Warfare and Security, 18, 35–37. https://doi.org/10.34190/iccws.18.1.1017

[7] Blasko, D. G., Lum, H. C., & Campbell, J. P. (2020). Gender differences in perceptions of technology, technology readiness, and spatial cognition. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 64(1), 1395-1399. https://doi.org/10.1177/1071181320641333

[8] Chakraborti, A., Suciu, D., & Sion, R. (2023). Wink: deniable secure messaging. Proceedings of the 32nd USENIX Conference on Security Symposium.

[9] Chang, M. S., & Yen, C. P. (2020). Evidence Gathering of Facebook Messenger on Android. Int. J. Netw. Secur., 22, 828–837. https://api.semanticscholar.org/CorpusID:221178656

[10] Christina Giannikas. (2020). Facebook in tertiary education: The impact of social media in e-Learning. Journal of University Teaching and Learning Practice. https://api.semanticscholar.org/CorpusID:216312001

[11] Cladis, A. (2018). A shifting paradigm: An evaluation of the pervasive effects of digital technologies on language expression, creativity, critical thinking, political discourse, and interactive processes of human communications. E-Learning and Digital Media, 17, 204275301775258. https://doi.org/10.1177/2042753017752583

[12] Dechand, S., Naiakshina, A., Danilova, A., & Smith, M. (2019). In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception. 401–415. https://doi.org/10.1109/EuroSP.2019.00037

[13] Demjaha, A., Spring, J., Becker, I., Parkin, S., & Sasse, M. A. (2018). Metaphors considered harmful? an exploratory study of the effectiveness of functional metaphors for end-to-end encryption. Proceedings 2018 Workshop on Usable Security. https://doi.org/10.14722/usec.2018.23015

[14] Edumadze, J., Kissiedu, A., Mensah, S., & Biney, B. (2022). Assessing Mobile Device Security Awareness Among First-Year Undergraduate Students in Ghana: The Case of The University of Cape Coast. European Journal of Education and Pedagogy, 3, 249–255. https://doi.org/10.24018/ejedu.2022.3.6.503

[15] Feng, S., Wong, Y. K., Wong, L. Y., & Hossain, L. (2019). The Internet and Facebook Usage on Academic Distraction of College Students. Comput. Educ., 134, 41–49. https://api.semanticscholar.org/CorpusID:86848118

[16] Herbert, F., Becker, S., Schaewitz, L., Hielscher, J., Kowalewski, M., Sasse, A., ... & Dürmuth, M. (2023, April). A world full of privacy and security (mis) conceptions? Findings of a representative survey in 12 countries. In Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (pp. 1-23).

[17] Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex & Intelligent Systems, 7(5), 2157–2177. https://doi.org/10.1007/s40747-021-00409-7

[18] Len, J., Ghosh, E., Grubbs, P., & Rösler, P. (2023). Interoperability in End-to-End Encrypted Messaging. IACR Cryptol. EPrint Arch., 2023, 386. https://api.semanticscholar.org/CorpusID:257857826

[19] Nguyen, M. H., Gruber, J., Fuchs, J., Marler, W., Hunsaker, A., & Hargittai, E. (2020). Changes in Digital Communication During the COVID-19 Global Pandemic: Implications for Digital Inequality and Future Research. Social Media +

Society, 6(3), 2056305120948255. https://doi.org/10.1177/2056305120948255

[20] Rozgonjuk, D., Sindermann, C., Elhai, J. D., & Montag, C. (2020). Fear of Missing Out (FoMO) and social media's impact on daily-life and productivity at work: Do WhatsApp, Facebook, Instagram, and Snapchat Use Disorders mediate that association? Addictive Behaviors, 110, 106487. https://doi.org/https://doi.org/10.1016/j.addbeh.2020.106487

[21] Samani, E., & Noordin, N. (2020). Getting Connected with Facebook Messenger: Exploring Meaningful Interactions through Online Chats in the ESL Context.

[22] Schaewitz, L., Lohmann, C., Fischer, K., & Sasse, A. (2022). Bringing Crypto Knowledge to School: Examining and Improving Junior High School Students' Security Assumptions About Encrypted Chat Apps (pp. 43–64). https://doi.org/10.1007/978-3-031-10183-0_3

[23] Scheffler, S., & Mayer, J. R. (2023). SoK: Content Moderation for End-to-End Encryption. Proc. Priv. Enhancing Technol., 2023, 403–429. https://api.semanticscholar.org/CorpusID:257378585

[24] Song, S. (2024a). Keeping Private Messages Private: End-to-End Encryption on Social Media. In Boston College Intellectual Property and Technology Forum (Vol. 2020, pp. 1–12). unav.

[25] Song, S. (2024b). Keeping Private Messages Private: End-to-End Encryption on Social Media. In Boston College Intellectual Property and Technology Forum (Vol. 2020, pp. 1–12). unav.

[26] Stone, C. B., & Wang, Q. (2019). From Conversations to Digital Communication: The Mnemonic Consequences of Consuming and Producing Information via Social Media. Topics in Cognitive Science, 11(4), 774–793. https://doi.org/https://doi.org/10.1111/tops.12369

[27] Stransky, C., Wermke, D., Schrader, J., Huaman, N., Acar, Y., Fehlhaber, A., Wei, M., Ur, B., & Fahl, S. (2021, October). On the Limited Impact of Visualizing Encryption: Perceptions of E2E Messaging Security.

[28] Tesfazion, H. (2020). The use of instant messaging applications among swedish students and their security awareness (p. 43).

