Borneo International Journal eISSN 2636-9826; Vol. 6 (2); 2023; 13-19
Published by *Majmuah Enterprise*
www.majmuah.com

A Comparative Analysis of Security Measures in Social Media: Instagram and TikTok

NUR A'FYFAH ZAIMY[1] and MOHD KHAIRUDIN KASIRAN[2]

[1,2]*School of Computing, College of Arts and Sciences, Universiti Utara Malaysia (UUM), 06010 Changlun, Kedah, MALAYSIA*
Email: afyfahzaimy@gmail.com | Tel: +60145247803 |

Received: June 27, 2023
Accepted: June 30, 2023
Online Published: June 30, 2023

Abstract

This article compares the security measures implemented by Instagram and TikTok, two popular social media sites. Data security and user privacy concerns have become increasingly important as social media usage grows. The study investigates the security mechanisms these platforms employ to secure user information. It answers two research questions: (1) What security measures are implemented by Instagram and TikTok to protect users and their accounts? (2) How do these security measures compare to one another? Are there any similarities or differences? The findings show how much of a priority the platforms place on user security, including safe login passwords, two-factor authentication (2FA), effective account recovery procedures, and strict security controls for online commerce and payments. While there are some parallels, there are also clear differences in the processes taken when updating passwords and profiles and authentication techniques. Although both platforms show a dedication to user security, ongoing security protocol adaption and development are essential to fend off evolving cybersecurity threats and preserve a secure online environment.

Keywords: comparative analysis; security measures; social media

1.0 Introduction

Websites that provide the establishment of user profiles and the visibility of user relationships are referred to as social media (Boyd & Ellison, 2007); web-based applications that offer functionality for sharing, relationships, groups, conversations, and profiles are referred to as social media (Kietzmann et al., 2011). Social media such as Instagram, TikTok, Twitter, Facebook, YouTube and others have been growing at a tremendous rate, and the adoption rate of such media has been skyrocketing, which, in turn, has delivered astronomical numbers of users in less than ten years (Al-Deen & Hendricks, 2011). These platforms were first created for social interaction and amusement, but they quickly expanded into a commonplace part of every individual's everyday routine, serving purposes beyond simple communication. The attractiveness of social media stems from its inherent ability to connect individuals all over the world (Waseem & Kumar, 2017), as well as its convenience and potential for immediate information transmission. Despite such appealing features and global accessibility, however, come serious drawbacks, particularly in the realms of data security (Yadav et al., 2022) and user privacy (Cutillo & Refik, 2009).

Cutillo and Refik (2009) concurred that there are several security and privacy flaws in online social networking apps, raising serious concerns about the security of social networking platforms. On these social networking sites, individuals exchange a plethora of personal information, from location information to private photographs, making them possible targets for malevolent assaults. Social networking platforms gather user data, as Zaimy et al. (2023) claimed. The information acquired can be utilised for targeted advertising, which could raise privacy and security issues (Ullah et al., 2022). Jain et al. (2021) note that regularly updating one's whereabouts on social media can put one at risk of robbery and stalking, among other dangers. According to a Norton analysis from 2021, 14% of respondents had to deal with unauthorised activities on their social media accounts at some point in their lives (Flynn, 2021). Also, a Russian hacker allegedly sold the email addresses and passwords of 117 million LinkedIn members on a dark web marketplace in 2017, as cited by Sahoo and Gupta (2018). It is vitally important to learn more about the complex security measures used by well-known platforms in the social media landscape as we deal with these growing security risks associated with social media. Hence, this article explores in-depth security measures put in place by Instagram and TikTok, two leading competitors, to protect the security of their user information. Two main research questions will serve as the basis of this study:

RQ1: What security measures are implemented by Instagram and TikTok to protect users and their accounts?

RQ2: How do these security measures compare to one another? Are there any similarities or differences?

It believes that answering these questions will allow us to understand the current state of security measures in social media.

2.0 Literature Review

2.1 Social Media Platforms

Instagram is a photo-sharing program featuring features for sharing, editing and taking photos. Because of its capabilities to help individuals create social networking based on photographs, it may also be considered a new social media based on picture interaction (Jin et al., 2015). In October 2010, the Apple Appstore officially released this mobile application. In the meantime, TikTok debuted globally in 2016 (Bhandari & Bimo, 2022). In 2023, Instagram had more than a billion monthly active members, while TikTok had already exceeded Instagram despite only being established for a short time, with almost 1.1 billion monthly active users (Tan, 2023). The benefits of these platforms come from their capacity to provide visually stimulating content that encourages user interaction, experience sharing, and interest exploration in a highly personalised way. These platforms offer distinctive chances for customer involvement, brand recognition, and e-commerce for companies and organisations. But these sites also have disadvantages, such as concerns about harassment, the spread of false information, the effects on mental health, and data privacy. Even though their algorithms are good at promoting material based on what users like, they can also create echo chambers that make it hard to hear different points of view.

2.2 User Authentication and Authorisation

Authentication is the process of verifying that someone or something is who they claim to be. Most technology systems employ some authentication to safeguard access to a program or its data. For example, when a user needs to access an online site or service, he or she must typically enter his or her username and password (Idrus et al., 2013). Then, behind the scenes, it checks the username and password entered by the user to a record in its database. If the information the user gives matches, the system considers the user valid and provides him access. Meanwhile, authorisation is the security practise determining the granted to a user or service. The purpose of authorisation in technology was to grant users or services permission to access certain data or execute a specific action (Chadwick & Otenko, 2002). More instances of authentication types will be explored further below.

a. Username and Passwords

Using a username and password or personal identification number (PIN) is the basis of password-based authentication, sometimes called knowledge-based authentication (Johnson, 2021). Moreover, according to Johson (2021), password-based authentication is today's most prevalent form of authentication. However, adversaries are most likely to exploit password-based authentication because people frequently reuse and construct passwords that are easily guessed by using dictionary words and personal information readily available to the public.

b. Two-Factor/Multi-Factor Authentication (2FA/MFA)

Two-factor authentication adds another level of security to account authorisation (Mail & Box, 2017). Contrarily, multi-factor authentication is a security procedure requiring the user to present two or more forms (Williamson & Curran, 2021) of identification before being granted access to a system or account. The user must input a code they know before logging in to the account. The code can be sent to their phone number, produced by a separate device or app, or both, and changed briefly. It makes it harder for unauthorised individuals to access a user account via a malicious device or from an unidentified location.

c. Biometric Authentication

Biometric authentication is a process of validating a person's identity based on distinctive physical or behavioural traits (Nigam et al., 2022), such as fingerprints, facial recognition, voice recognition, and iris scanning. Finance, healthcare, and government are just sectors that rely on it to keep private data safe. There are various methods for securing users using biometric authentication and making it more secure (Chang et al., 2015). Enable three-dimensional facial recognition, for example, by requesting the user to move their heads in a specified way during the authentication process. User expressions are also detectable, making them less vulnerable to an attacker or breach. According to a poll conducted at Carnegie Mellon University (Colnago et al., 2018), many users were pleased with the biometric authentication approach used to safeguard their data.

There are many benefits of using biometric authentication instead of more conventional methods like usernames and passwords. Stealing or imitating someone else's distinctive appearance or mannerisms is impossible, making this a safer option. Additionally, it is more efficient because users are not required to remember lengthy passwords or transport physical tokens such as ID cards or keys. Therefore, biometric authentication is an area that is growing quickly and could be used in numerous sectors.

2.3 Encryption

Nagaraj et al. (2015) claim that encryption is one of the most important ways to keep private information safe. Encryption keeps information private and stops it from getting out during interactions. It is widely utilised in numerous industries, including social media, to guarantee secure data storage and transmission. End-to-end encryption used by Viber and WhatsApp, which assures that only the sender and receiver can read the messages, is an example of data encryption used in social media (R, 2016). Compared to more conventional data protection techniques, data encryption provides benefits. It is more secure because it renders the data illegible to unauthorised people. Additionally, it is more dependable because it protects against unauthorised data alteration and guarantees data integrity (Rouse, 2014). Data encryption is not impenetrable and can be subject to side-channel and brute-force attacks (Bernstein & Cobb, 2021). Hence, for best security, it is crucial to employ powerful encryption methods and maintain them up to date.

2.4 Privacy Settings

Users can manage who can view what information about them on social networking sites, internet browsers, software, and other platforms through the usage of privacy settings (Williams et al., 2019). The popularity of social media platforms increases the number of possible privacy breaches (Saeri et al., 2014). By adjusting their privacy settings, users can decide how much of their information is made public. Facebook's privacy settings, which let users decide who may view their updates and profile information, are one example of a privacy option in social media. Nonetheless, because they might result in the accidental disclosure of personal information and privacy violations, privacy settings can be perplexing and challenging for certain users to grasp. Therefore, it is crucial for users to take caution when posting anything on social media platforms because there is no assurance that the message will only reach intended audiences.

2.5 Monitoring and Moderation

Social media monitoring and moderation are similar in that they involve managing online groups and ensuring users have a safe and pleasant experience. Social media monitoring involves using tools to listen to millions of online discussions to discover what is being said about a specific brand, problem, person, or product and identify opportunities (ExpertAi, 2017). Using artificial intelligence to identify harmful content, community administrators can also accomplish this manually. Cyberbullying, hate speech, and other types of online harassment can be stopped with monitoring, which can also help guarantee that community norms are upheld. Next, the review and control of actions taken on a social media platform are called social media moderation (Armbruster, 2023). In order to maintain a vibrant and healthy community, user-generated content (UGC) on a brand's social media pages may necessitate responses, reports, or elimination. In addition to removing the offending material, moderators may warn or remove members who break community rules and assist individuals harmed by offensive material. In order to keep an online community secure and positive and to shield people from damage, moderation is crucial. Since users can freely express their thoughts and opinions on social media and other online platforms, monitoring and moderation are crucial to managing online communities.

2.6 Report and Block Features

Users can report and block other users who engage in improper or dangerous behaviour on social media or other online platforms. The report feature enables users to take action on any posts, images, or comments that are hurtful, deceptive, or malicious. Perhaps it is something incorrect or phoney. Another possibility is that the user was offended by anything someone wrote about them on the internet without their consent. On the other hand, the block feature prevents other users from interacting with individuals on that site. Sometimes it also means they cannot read any user posts or even locate their profile if they conduct a search. Thus, the block and report functions are crucial for preserving a secure and pleasant online community.

3. Methodology

Instagram and TikTok were selected for comparative analysis due to their large user bases and stature as prominent social media platforms, allowing for a comprehensive review of their security protocols. In light of the growing

concern about the security of sensitive users' data and their accounts, comparing these two platforms provides an opportunity to examine the various security procedures implemented by different organisations operating in parallel digital worlds. Due to their prominence, a thorough analysis of their security procedures might indicate movements in the industry.

A thorough observation and comparison approach was used in the attempt to understand the composition and effectiveness of security measures between two prominent social media platforms, which we will refer to as Platform X and Platform Y. The data collection is obtained through observation and in-depth analysis of the security protocols used by both platforms from the aspect of user interaction. In the beginning, both platforms' login procedures were carefully examined. The protocols implemented when users forgot their login information was also analysed to assess the resilience of their recovery processes. The third point of comparison is shopping and payment security measures because financial transactions are a crucial component that needs strict protection. Finally, the procedure for changing passwords or profiles was observed to assess the degree of user-friendliness and security built into those platforms. It is crucial to comprehend that we will only describe the protocols and procedures used by these platforms in this study. In the parts that follow, comparative results and analyses will be presented.

4.0 Findings

4.1 Login Credentials

The security protocols used by platforms X and Y both show a strong focus on user safety. The application typically requests a username and password when a user tries to log in on Platform X. However, it supports two-factor authentication (2FA) to increase security. When 2FA is enabled, users must confirm their identity using a secondary means, like an authentication application, getting a code via SMS or WhatsApp and using trusted devices (a familiar device previously used to enter into the user's account). Therefore, even if an opposing party learns a user's password, they still require the second verification factor to access the account. Conversely, Platform Y also uses a similar user login system. A username or an email and password are required. Furthermore, Platform Y also provides a second level of security using 2FA. Not only does Platform Y allow SMS and authentication apps, but it also supports trusted devices and verification codes delivered to user login emails. It gives the user an additional layer of security and greatly increases the difficulty of unauthorised access.

4.2 Forgot Login Credentials

When a user on Platform X forgets their login information, it usually provides account recovery through a registered email address or phone number. A security code or password reset link is delivered upon entering the specified email address or phone number, allowing users to recover access by changing their password. In the meantime, Platform Y uses a comparable method to deal with forgotten login information. When users forget their login details, the site prompts them to input their registered email address or phone number. To establish their identification, the user requires to enter the verification code received from the platform on the designated medium. The user is advised to reset their password if the verification process is successful. Both systems adopt a user-centric strategy, ensuring the user's access to their accounts may be quickly and securely restored, minimising any harm or breaches.

4.3 Shopping and Payment Security

This section describes the measures Platforms X and Y took to ensure the safety of financial transactions within their respective platforms. Users of Platform X can choose among three different methods of payment: credit or debit cards, PayPal, a well-known online money transfer service, or a third-party online payment option like Shop Pay. When using a credit or debit card as a payment method, the transaction is often processed by a separate, secure payment gateway rather than Platform X itself. The user must input their credit or debit card information into this system before the payment can be performed safely. After that, the user must wait for the TAC code that was issued by SMS. The payment was successful once the user entered the correct TAC code provided by the financial institution.

For online transactions, PayPal offers a safe and convenient payment option. The steps are that users choose PayPal from the available payment methods throughout the checkout procedure in Platform X. To submit their login information, users are forwarded to the PayPal login page. After signing in, customers can select from the several payment options saved to their accounts, including varied credit and debit cards and bank accounts. Before finishing the transaction by selecting 'Pay Now,' users must double-check the payment information, including the total fee and billing address. Users are returned to the merchant's website for confirmation after a successful transaction. In addition, Shop Pay is an expedited transaction option made available by Shopify, the industry-leading e-commerce platform. Shop Pay enables customers to save their email addresses, credit card information, and shipping and invoice addresses

to expedite future transactions. Shop Pay uses the information to automatically fill in the details during payment, reducing the number of steps required to complete a purchase. The Shop Pay approach, however, cannot be completely explained because there was no user engagement with the program throughout this study.

Instead, Platform Y offers users four different ways to pay. These consist of Internet banking, credit or debit cards, e-Wallet services, and cash on delivery. Platform Y allows the transactions for e-Wallet services like GrabPay and Touch n Go by using secure APIs that guarantee the transmission and protection of sensitive data, including personal information and payment information. The credit or debit card information is likewise securely encrypted to prevent unauthorised access or data breaches, similar to Platform X. Moreover, Platform Y connects users to their bank's secure payment gateway for online banking transactions, where the bank manages the authentication and transaction processes. Users will be directed to the Internet banking login page, for example, the Maybank2u login page, before entering their username and password. The users also must verify their identity by confirming their security picture before logging in. Once they have verified their security picture, they can proceed to make a payment. After choosing the account, the user must accept or reject the request to make a payment in the Internet banking application. The payment will be completed if the user clicks the 'Approved' button in the Internet banking application. Upon completion of the transaction, the user will be returned to the merchant.

Consequently, each platform employs a meticulous approach to ensure that every transaction type, whether conducted via e-Wallet, online banking, or credit or debit card, is conducted securely, thereby protecting user data and nurturing user confidence in the platform's financial transactions.

4.4 Update Password or Profile

This section delves into the security procedures Platforms X and Y use when users want to alter their password or profile information. When a user tries to alter their password on Platform X, the platform requests that the user first input their current password for verification purposes. If a user has lost track of their current password, they can click the "Forgotten your password?" button and the platform will send them an email with a reset link. User verification is unnecessary when updating profile data in Platform X. Platform Y also has a secure mechanism to protect user profiles and login credentials. Users must enter a verification code sent to their registered phone number to update their password. After the code has been adequately confirmed, the user can update their password, subject to the requirement that it contain at least eight characters (20 characters maximum), one letter, and one number. In contrast to Platform X, Platform Y requires users to enter the verification code issued to their email or phone number to edit their profile information, such as updating their phone number and email. It is done for security purposes.

Hence, both platforms have added substantial security protocols requiring user authentication before allowing password or profile changes. These procedures are created expressly to guard against unauthorised changes to the user's profile, adding to the overall security of the user's online presence.

5.0 Discussion and Conclusion

Both platforms prioritise user safety and data security, which have similarities and differences, as shown by the thorough observation and analysis of the security protocols and practises employed by Platforms X and Y. This emphasis on security is reflected by several security solutions, such as secure login credentials, reliable recovery processes for forgotten login credentials, stringent shopping and payment security measures, and robust protocols for updating passwords or profile information. Platforms X and Y strongly emphasise user authentication regarding login information, whether through usernames, emails, or both. They also include two-factor authentication (2FA) as an additional security measure. Platform X offers 2FA support via several channels, including trusted devices, SMS codes, and authentication applications. Similar to Platform Y, 2FA is available through SMS codes, trusted devices, authentication applications, and verification codes delivered to user login emails. Both platforms' adoption of 2FA shows a common commitment to preventing unauthorised access to user accounts. Therefore, it can be concluded that both platforms work to create a user-friendly and security-focused environment.

In addition, the two platforms prioritise user-centric methods for retrieving lost credentials to regain access to accounts safely. Platforms X and Y work similarly in that users must provide their registered email address or phone number. The platforms then provide the users with a verification code that they must enter to complete the authentication process. Users are directed to reset their passwords after the successful verification process. A security code or password reset link is typically sent to a registered email address or phone number, demonstrating their focus on securely and promptly regaining user access while minimising any harm or security breaches.

The security methods used during payment and shopping transactions show Platform X and Platform Y's similarities and variances. Both platforms use secure payment gateways to safeguard user data and provide a variety of payment methods, including credit and debit cards, online banking, e-Wallet transaction, and PayPal or Shop Pay. While Platform Y uses secure APIs to guarantee the security of e-Wallet transactions, Platform X uses PayPal as a secure payment option. The encryption of credit or debit card data is also a top priority for both platforms, and Platform Y can connect users to secure payment gateways for online banking transactions. These precautions demonstrate the platforms' dedication to protecting users' personal and payment information and safeguarding financial transactions.

Finally, Platforms X and Y prioritise user authentication when altering passwords or profile information to avoid unauthorised modifications. Users of Platform X must enter their current password for Platform X to verify them, with the opportunity to change it through an email link if they forget it. On Platform X, updating profile information is not subject to user authentication. In contrast, Platform Y requires users to input a verification code sent to their registered phone number when changing their password. Similarly, Platform Y's profile updates demand that users provide the verification code delivered to their email or phone number. These controls demonstrate how they prioritise user data safety and stop unauthorised adjustments by requiring user identification and authentication before any changes can be made. Moreover, both platforms demand similar things for creating new passwords, as users must create unique and strong passwords with the combination of the alphabet (big and small letters), numbers, and symbols. This step ensures that passwords are not easily guessed or broken, providing additional security.

In conclusion, by putting strong security measures in place, Platforms X and Y show a strong commitment to user safety. They are comparable regarding how login credentials are employed, how to retrieve forgotten login information, and how to secure online purchasing and payments. Additionally, user authentication is given priority on both platforms for profile and password updates. However, several noticeable variations exist, like the unique authentication techniques used and the additional security precautions each platform employs. Overall, Platforms X and Y's security procedures demonstrate their commitment to safeguarding user accounts and promoting user trust in their platforms. Thus, it is advised that users proceed with caution and fully utilise the security features offered by the platforms. Besides, in response to shifting cybersecurity threats and the ever-evolving sophistication of cyberattacks, Platforms X and Y should keep innovating and adapting their security procedures. Users' trust and confidence will grow due to ongoing security protocol improvements, promoting a safe and dependable online experience.

Acknowledgments

The authors acknowledge all personnel of the School of Computing who contributed to this study's invention. This study was conducted for the Online Business, Financial Technology and Cybersecurity Project.

References

Al-Deen, H. S. N., & Hendricks, J. A. (2011). Social Media Usage and Impact. In *Lexington Books*.

Armbruster, C. (2023). *Social Media Moderation: Why It's Essential and How To Do It*. BrandBastion. https://blog.brandbastion.com/social-media-moderation#:~:text=Social media moderation refers to a healthy and positive community.

Bernstein, C., & Cobb, M. (2021). *Advanced Encryption Standard (AES)*. TechTarget. https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

Bhandari, A., & Bimo, S. (2022). Why's Everyone on TikTok Now? The Algorithmized Self and the Future of Self-Making on Social Media. *Social Media + Society*, *8*(1). https://doi.org/10.1177/20563051221086241

Boyd, D. M., & Ellison, N. B. (2007). No Title. *Journal of Computer-Mediated Communication*, *13*(1), 210–230. https://doi.org/10.1111/j.1083-6101.2007.00393.x

Chadwick, D. W., & Otenko, O. (2002). The PERMIS X.509 Role Based Privilege Management Infrastructure. *Symposium on Access Control Models and Technologies*. https://kar.kent.ac.uk/13778/1/PermisChad.pdf

Chang, I.-P., Lee, T.-F., Lin, T.-H., & Liu, C. M. (2015). Enhanced Two-Factor Authentication and Key Agreement Using Dynamic Identities in Wireless Sensor Networks. *Sensor Networks*, *15*(12), 29841–29854. https://doi.org/10.3390/s151229767

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Cranor, L., & Christin, N. (2018). It's Not Actually That Horrible": Exploring Adoption of Two-Factor Authentication at a University. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 1–11. https://doi.org/10.1145/3173574.3174030

Cutillo, L. A., & Refik, M. (2009). Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust. *IEEE Communications Magazine*, *47*(12), 94–101.

ExpertAi. (2017). *What is Social Media Monitoring and How Does it Work*. Expert Ai. https://www.expert.ai/blog/social-media-monitoring-definition/

Flynn, S. (2021). *How Often Are Social Media Accounts Hacked*. https://www.makeuseof.com/how-often-are-social-media-accounts-hacked/

Idrus, S. Z. S., Cherrier, E., Rosenberger, C., & Schwartzmann, J.-J. (2013). A Review on Authentication Methods. *Australian Journal of Basic and Applied Sciences*, *7*(5), 95–107. https://hal.science/hal-00912435/document

Jain, A. K., Ranjan, S. S., & Kaubiyal, J. (2021). Online Social Networks Security and Privacy: Comprehensive Review and Analysis. *Complex & Intelligent Systems*, *7*, 2157–2177. https://doi.org/https://doi.org/10.1007/s40747-021-00409-7

Jin, Y. J., Han, K., Shih, P. C., & Lee, D. (2015). Generation Like: Comparative Characteristics in Instagram. *CHI 2015 - Proceedings of the 33rd Annual CHI Conference on Human Factors in Computing Systems*, 4039–4042. https://doi.org/10.1145/2702123.2702555

Johnson, K. (2021). *Use these 6 user authentication types to secure networks | TechTarget*. TechTarget. https://www.techtarget.com/searchsecurity/tip/Use-these-6-user-authentication-types-to-secure-networks

Kietzmann, J., Hermkens, K., McCarthy, I. P., & Silvestre, B. (2011). Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media. *Business Horizons*, *54*(3), 241–251. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2519365

Mail, A. O. L., & Box, D. (2017). *Two factor authentication*. https://www.cfins.com/wp-content/uploads/2021/05/2FA-Instructions.pdf

Nagaraj, S., Dr., G. S. V. P. R., & Srinadth, V. (2015). Data Encryption and Authentication Using Public Key Approach. *International Conference on Computer, Communication and Convergence (ICCC 2015)*, 126–132. https://doi.org/10.1016/j.procs.2015.04.161

Nigam, D., Patel, S. N., Vincent, P. M. D. R., Srinivasan, K., & Arunmozhi, S. (2022). Biometric Authentication for Intelligent and Privacy-Preserving Healthcare Systems. *Journal of Healthcare Engineering*. https://doi.org/10.1155/2022/1789996

R, A. (2016). *Social Media and the Encryption Challenge | Manohar Parrikar Institute for Defence Studies and Analyses*. Manohar Parrikar Institute for Defence Studies and Analyses. https://www.idsa.in/idsacomments/social-media-and-the-encryption-challenge_arul-r_220416

Rouse, M. (2014). *Data Encryption Key*. Techopedia. https://www.techopedia.com/definition/5660/data-encryption-key-dek

Saeri, A. K., Ogilvie, C., La Macchia, S. T., Smith, J. R., & Louis, W. R. (2014). Predicting Facebook Users' Online Privacy Protection: Risk, Trust Norm Focus Theory and the Theory of Planned Behavior. *The Journal of Social Psychology*, *154*(4), 352–369. https://doi.org/10.1080/00224545.2014.914881

Sahoo, S. R., & Gupta, B. B. (2018). Security Issues and Challenges in Online Social Networks (OSNs) Based on User Perspective: Principles, Algorithm, Applications, and Perspectives. In *Computer and Cyber Security* (pp. 591–606). https://doi.org/10.1201/9780429424878-22

Tan, C. (2023). *TikTok vs Instagram Users & Stats in 2023*. IncrediTools. https://increditools.com/tiktok-vs-instagram/

Ullah, I., Boreli, R., & Kanhere, S. S. (2022). Privacy in Targeted Advertising on Mobile Devices: A Survey. *International Journal of Information Security*. https://doi.org/10.1007/s10207-022-00655-x

Waseem, A., & Kumar, R. (2017). A Study on Positive and Negative Effects of Social Media on Society. *International Journal of Computer Sciences and Engineering*, *5*(10), 351–354. https://www.researchgate.net/profile/Waseem-Akram-19/publication/323903323_A_Study_on_Positive_and_Negative_Effects_of_Social_Media_on_Society/links/5ab1c064a6fdcc1bc0bfefef/A-Study-on-Positive-and-Negative-Effects-of-Social-Media-on-Society.pdf?forcedefa

Williams, M., Nurse, J. R. C., & Creese, S. (2019). Smartwatch Games: Encouraging Privacy-Protective Behaviour in a Longitudinal Study. *Computers in Human Behaviour*, *99*, 38–54. https://doi.org/10.1016/j.chb.2019.04.026

Williamson, J., & Curran, K. (2021). The Role of Multi-factor Authentication for Modern Day Security. *16Semiconductor Science and Information Devices*, *3*(1), 16–23. https://doi.org/10.30564/ssid.v3i1.3152

Yadav, U. S., Gupta, B. B., Peraković, D., Peñalvo, F. J. G., & Ivan, C. (2022). Security and Privacy of Cloud-Based Online Online Social Media: A Survey. In *Sustainable Management of Manufacturing Systems in Industry 4.0* (pp. 213–236). EAI/Springer Innovations in Communication and Computing. https://doi.org/https://doi.org/10.1007/978-3-030-90462-3_14

Zaimy, N. A., Saip, M. A., & Fikri, M. (2023). Cybersecurity Threat in Social Media: A Bibliometric Analysis. *Borneo International Journal*, *6*(1), 80–86.