**Borneo International Journal eISSN 2636-9826**; Vol. 6 (3); 2023; 49-55
Published by *Majmuah Enterprise*
*www.majmuah.com*

# Study of Security and Privacy Measures on Twitter and Instagram

FATIN IZZATI BINTI FAMMY RIKZAN and MOHD KHAIRUDIN KASIRAN
*School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah Darul Aman, MALAYSIA*
Email: fatinizzatifammyrikzan@gmail.com | Tel: +60136068672 |

Received: August 08, 2023
Accepted: August 18, 2023
Online Published: September 01, 2023

**Abstract**

Social media is known as a very useful online platform for people to interact with each other through as long as there is Internet connection. Social media allows people to share ideas, having conversations and making contents. These types of interaction give opportunity for any user to use this platform as the business tool especially for their marketing strategy. Unfortunately, this internet-based technology comes with some vulnerability which can leads to the cyber-attacks. To avoid the occurrence of cyber-attack, the social media company offer their users with the security and privacy setting which can minimize the possibility of user's account being hacked or breach by attacker. Twitter and Instagram both are the social media with different company that provided the security and privacy setting to their users. The security and privacy settings can be modify by the users to secure their post or personal life to other stranger users. Both twitter and Instagram have their own criteria and features to set up the privacy and security settings. The comparison of the best security and privacy measure of Twitter and Instagram will be discussed in this paper.

**Keywords**: Social media; privacy setting; security; Twitter; Instagram

## 1. Introduction

Social media is a digital platform that provides multifunctional for the users to share any contents, ideas and personal thoughts through virtual networks to the community Internet presence. Nowadays, all generations have their own social media accounts to communicate with the world using the fingertips. The benefits of social media can be many but there is also risk taken especially with the cybersecurity part. Cyber-attacks are quite common in social media because the open sharing by the users via the Internet gives vulnerability to the user by allowing the attackers to make move such as data exploitation (Carpinella, 2015). Cybersecurity implementations are compulsory for any social media organizations to protect the confidentiality of the data gained from the users or company. The pattern of the security implementation might be different depending on each social media platform based on their development or function provided to the users. In this case, the comparison of the social media security implementation will be focused on the Instagram and Twitter platforms. Both social media are quite famous among users. Social media not only can be opened through the website but also by the smartphone; this makes it more convenient to be used in daily life. The security implemented is being compared, such as the type of authentication, encryption, and privacy settings used, in order to generate an analysis of the most relevant approach used to safeguard social media networks and produce future recommendations to improve the security aspect.

Cyber-attack has been known as an unauthorized act to breach the security policies of any organization's asset that cause exploiting and damage issue towards the crucial data (Li, 2021). This study of security implementation in social media is important to decrease the cyber-attack occurs especially towards the users. The awareness can be raised among the companies and users if the aware with the used of the privacy measures provided by the social media platform. Twitter and Instagram both are common social media especially in business community that currently active using the platforms to expand their products and gain more connection with customers. Based on the statistic on the cyber-attacks happened, the users need to be more alert to guarding up their security and privacy setting. Some of the vulnerabilities or threat could be face by the users in using social media are phishing attacks, identity federation challenges, malwares attack, virus, Zeus Trojan and UI address attacks (Das, 2017). These attacks are dangerous for social media users because they can exploit users' important data and used it illegally for their profits. Because of that, security and privacy measure are important in controlling the social media accounts especially in business field to avoid any loss or scam. The structure of this paper is organized with 4 different sections. Section 2 is literature review that discusses social media cybersecurity that focused on the Instagram and Twitter type of security implementation based on the previous papers study. Section 3 explains the methodology used to get the proper results of the paper case to be analysed in Section 4 which is the results of this paper case study. From the analysis, there is recommendation stated in Section 5 to improvise the study or methodology and finally there is conclusion in Section 6.

## 2. Literature Review

In this section there are several pervious papers were studied based on the related areas on the topic of security implementation in social media. The outcomes of this literature review will be the points of improvement and study of research gaps for this research paper.

### 2.1 Twitter and Instagram Social Media

Twitter is a social media platform that is commonly known for its short tweets that limit the context that can be posted by users. Tweets cover various topics such as commenting on new issues or personal messages and so on. The tweets basically limit to 140-characters only for users to post something on their twitter accounts (Ma, 2014). Usually, twitter writing or post sharing is informal because of the limitation. Hashtag is one of the effective features of Twitter. The Hashtag which is known with the prefix symbol "#", enhances the tweets searched by the users in social chatting. The presence of the Hashtag can improve the Tweets to be spread fast among the Twitter community other can reflect users' personal interests or latest topic on the Twitter wall. Three factors that are crucial to this social media are user, tweet content and post timing. Instagram is a social media platform that is famous for its share photos or videos features by the users. By adding 100 million new Instagram users each year, the total number of Instagram users is clearly rising. A major milestone for Instagram, whose user base has significantly increased between 2017 and 2018, with a 200 million user differences between the two years (Zulkarnain, 2021). At first, Instagram's users only can share the photos because there is no feature for posting video media until year 2013. Based on the addition feature, the number of Instagram users becomes increased from time to time. Instagram comes with more features for users to use such as story maker, video filter, reels shared and simple notes in direct message. These features make it more interesting and attractive to be used. In Instagram, there is also opportunity for users to make friends or create personal business platform as it can be a marketing tool based in the features provided. Instagram is currently widely used by companies to promote their product or name and create good relationships with the customers or business partners (Huey, 2014).

Basically, social media requires the Internet to function because it connects people all over the world. When there is Internet, there are possibilities to connect people all over the world. When there is Internet, there is possibility of hacking activities or a risk of facing the cyber-attack by a hacker. The definition of cyber-attacks varies based on several journals (Kadivar, 2014). For example, "An exploitation of cyberspace for the purpose of accessing unauthorized or secure information, spying, disabling of networks, and stealing both data and money." (Uma & Padmavathi, 2013: p. 390). Cyber-attack usually happens when there are vulnerabilities from the organization of the social media platform or because of the user's behaviour. Cyber-attacks will affect the safety of using the Internet and other security concerns. There are five attributes of cyber-attacks which are actors, assets targeted, motivation, effect on the target and time taken. These attributes are crucial to the attackers in achieving their target towards specific victims. Attackers also use the same concepts in attacking the security of social media if there is any vulnerability.

### 2.2 Design and Implementation of Privacy and Security System in social media

Online social media are avenues for individuals to communicate in which they can produce, share, and exchange information, knowledge, and ideas in virtual communities across networks. People's interactions have increasingly changed as a result of the popularity, availability, and accessibility of social networking sites (SNSs) over the previous decade (Kumar, 2022). Social networking sites (SNSs) have revolutionized our lives in terms of pleasure, information, contact, and communication. These social networking services enable people in remote regions to communicate with one another swiftly and inexpensively. On the other hand, the security and privacy of SNS users' information has been jeopardized, and the majority of users are blind to this. The number of cyber-attacks that occur via networking sites is steadily rising. Discovering a solution that provides better security for social network members has become a significant challenge. The researcher defined that users and social networking sites themselves are the two primary causes of today's security and privacy issues on SNSs. Based on analysis, security and privacy concerns on social networking sites remain unresolved, and there is still no definite and full answer for completely eliminating those concerns on the sociability of social networking sites. But there are several efficient techniques to protect personal information when using social media platforms, such as using a unique and secure password and utilizing two factor authentications. Following several efforts, cyber security remains a key concern for many individuals. This paper focuses on the issues that current cyber security faces. It also includes the latest recent information on cyber security strategies, ethics, and developments that are changing the face of cyber security.

Based on this paper, the researchers explained that cyber-security issues are usually because of users themselves. Cyber-security treat is impossible to avoid as long as there is lack of awareness among the community. There are several strategies to protect the privacy and security of social media but in the end, it depends on the alertness of users

to overcome the cyber-attack. In conclusion, the researcher only explained the technical methodology on how to manage cyber-attacks and kept reminding of lack of awareness among the users. In future study, the researcher can highlight the steps on how to improve awareness among the users

2.3 Privacy setting on social media

The study of privacy setting on social media was referring to (Heyman, 2014). Privacy is a feature that is provided by the social media platform to their users. Privacy might be changed personally based on the users' decision without needing any permission from the social media organization. The consequence of this privacy setting is that some of the content across social media is public and other is private (Fiesler, 2017). This paper's finding was to differentiate the two different types of privacy settings which are 'privacy as subject' and 'privacy as object'. 'Privacy as subject' is defined as the management of important data about someone's identity. The users as a role who gives personal data and the way they manage their identity on social media. 'Privacy as objects' is users are invisible to the other users' which users are used as an object to the parties as their data get into the database.

The researcher believed that both types of privacy have a blind spot. In this paper, better understanding about the two types of privacy stated was developed. The first step was defining the perspectives that - implicitly - employ privacy as a subject then took the similar step for the privacy as object. Three types of social media were tested to analyse the privacy concepts based on the two types of privacy. The social media used were Facebook, Twitter and LinkedIn. "What type of privacy is offered most and what kind of behaviour is encouraged by default settings?" was the question provided in did the research questions.

The results from the analysis, as the total of both privacy of subject and privacy of object were compared, then it is evident users are given more control over their privacy as a subject but are constrained in their privacy as an object. The numbers control of privacy as a subject does not indicate that this form of privacy is being addressed properly. As discussed, most users manage their privacy through a variety of social methods rather than depending just on the privacy controls offered by social network companies. This shows that the privacy solutions offered do not always meet the expectations or demands of the users.

Based on this paper, the researcher defines two types of privacy which are 'privacy as object' and 'privacy as subject' by comparing the difference between interpersonal and third-party. Three social media privacy settings had been analysed to study this topic. This paper study can be improvised with the addition of Instagram social media platform privacy settings as it does not involve in the analysis.

## 3. Methodology

This paper is a study of security and privacy measures provided by social media platform. The scope of the social media platform used in this study is focus on Twitter and Instagram companies. This is because there is comparison will be held towards the analysis to get the most relevant privacy and security measures. The criteria and analysis depend on the latest update privacy measures of the social media. The privacy measures will be study by directly do analysis on the Twitter and Instagram application of researcher personal accounts. In this section the methodology on how the security and privacy measures access will be explained. Some of the security and privacy measures highlighted in this study are account login page, blocking control, posting control and personal message.

3.1 Account Login Page

Account login page is the basic security measure created by social media platforms towards the user before they can access into the account. In this section, the steps to login an account will be defined through the Twitter and Instagram application. In this paper, the login page of Twitter and Instagram procedure will be analysed to compare the level of security measure applied. The Twitter login page interface through an application is shown in Figure 1 and Figure 2 shows the login page of Instagram application. The comparison of account login page between Twitter and Instagram will be analyse by on how the procedure of login of both account to observe the level of authentication.


Figure 1: Twitter Login Page


Figure 2: Instagram login Page

3.2 Privacy Setting

Privacy setting is provided for users to control the visibility of their account from public. Their account can be set either private or public based on user's choice. The privacy setting study in this paper included the posting control, blocking setting and personal messaging. Both Twitter and Instagram privacy setting is shown in Figure 3 and Figure 4. This privacy setting of both social media will be analysed to study which has the most effective privacy measure. The comparison of the posting control, blocking setting and personal messaging will be analyse through the analysis on the features and procedure on how to set up those functions using the Twitter and Instagram mobile application.

Figure 3: Twitter Privacy Setting

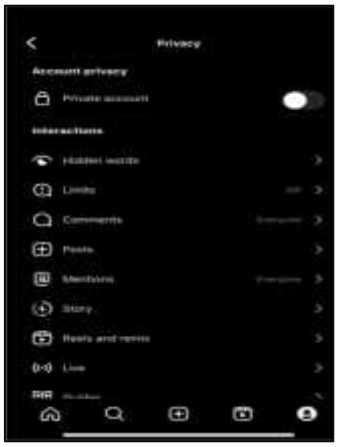


Figure 4: Instagram Privacy Setting

**4. Results and Discussion**

In this chapter the results of the comparison will be discuss to show the best security and privacy measures of those social media. In addition, in this part the name of both social media will be re-named by social media A and B. The reason behind of this rename is to avoid any bias in did the analysis and comparison between both social media company.

4.1 Login Page Procedure

For A social media login page, firstly user needs to key in the username and password. The username option given is the username, email or number phone. User can choose either one to login their account. User will directly bring into their account page if they correctly enter the username and password but if the failed, the page will tell them the password or username is incorrect. There is an option for user if they forgot their username and password which clicking on "forgot password?" button below the login box. As the user click the "Forgot Password", the page will bring to the information detail needed such as email, phone number or username. The requirement must be filled and correct information should be keyed in to avoid any failure. Then, users will get reset password link through the chosen

medium filled. After success to update the new password, user needs to go back to login page and start to login as usual.

As for social media B, first step is user need to key in the username and password to access the account. The user will directly bring to their account if the username and password is correct. The failure to put correct username and password will make it failed to access. The user needs to click the "forgot password" button as the initiative to get access to the account. After that, the user will be taken to the reset page which the user can choose either use an email address or phone number to reset the password. Then, the B system will send an email with instructions how to reset password if the user choose email. For the phone number, the user will receive verification code through SMS message for reset the password from B. Then, users can change or update their account password for login.

Based on the results, the social media A and B have similarity in login into the account page. The security of this login page being analysed based on the authentication part when the user tried to login into the social media using username and passwords. Both social media provide the "Forget password" function to the users for make it easier for them reset the passwords. The details needed for verification such as email and phone number were functional as the identity confirmation of the users. As technically observed, the social media A consist of three different verification options compared to the social media B. This shows that the social media A security measures is higher compared to social media B because the more the number of verifications, it means that there is extra layer of authentications needed to login the account. It also can gives high chances for the users to get back their account. Besides, the cyber-attack vulnerabilities will be decrease as the users can immediately log in into their personal account.

4.2 Posting Control

In social media A, user usually post content of text or media file but for social media B the main post is about posting photo or video with caption addition. The posting control of A and B were analysed based on the visibility among the followers of the account. For social media A, there is only a section for user to post any tweet. Other than text, user also can post photo, video or location in that tweet. In B, the user was given three different sections to post any content which are the feed, story and reels. For availability, the post or content in social media A's privacy can be control by user through the account privacy control. If the user chooses to private the account, automatically other non-follower of non-mutual accounts do not available to see any post from the user account. Other than that, the social media A also has feature of "A Circle" which only give access to the selected users to see the content post. User can choose the content availability either for Public or "A Circle" only. To private the account, user need to log in first, then went to "Setting and Privacy" section. Next, choose the "Privacy and Safety" before clicked the "Protect your Tweet" button. The change will automatically save.

For social media B, any post on the feeds can be seen by the other people if the user set the account as public. Same with A, if the user set the account as private, only followers are able to see and interact with the posts. But, for story post for B, there is "Close friend" function which the story post only can be seen by the account chose by user as the close friends. To set the account to be private, first step user needs to log in into the social media A first. Next, went to the "Setting" part and click on "Privacy". Then, there was toggle button to turn on "Private account". When user clicked the toggle, user will be ask for confirmation as they really want to switch the account to private setting or vice versa. As the user confirmed the choice, the account automatically will be private. Based on the results analysis, the social media A and B have similar steps to private the account from public. They need to login first and changed the setting on the privacy setting section, but there was addition step from social media B which it asked users for confirmation before proceed to change the privacy setting. This confirmation makes it more comprehensive as the user will be more alert with the decision they make. So the privacy measure in posting control for social media B is better compared to social media A.

4.3 Blocking Setting

Blocking and restriction setting is a feature offered for uses to limit their interaction towards specific user or people. Basically, social media A's blocking setting come with block other user accounts function. This feature is to keep the privacy based on user preferences towards other people. To block someone account, for social media A user need to login first into the account and go to the target profile page that want to be block. There is three-dot menu symbol as more options button, click the three dot menu and select "Block" option. After that, user will be asking for confirmation if they want to block the account as confirmation message pop-up on screen. "Block" button need to be click to confirm the account block. As the account being blocked, the blocked account user cannot send any direct message, interact with user or see any past or latest activities of user on timeline. The previous comment or tagged of blocked people also will be removed from the users timeline.

For social media B, the function of blocking setting is for keep the privacy or avoiding any interaction from specific chosen user account. The steps for blocking account in B, firstly need to login into the A account. Next, directly go to the target profile account that wants to be block. Then, click on the three-dot menu icon that located on the top-right corner of the profile account page and there is dropdown menu which there "Block" button. A confirmation message will be shows directly after clicked the "Block" option button as the confirmation message for user to block the target user account. Once blocked. The target account do not has any access to view the user profile, posts or sending direct messages. In addition, all previous likes and comments from the blocked account on the user profile will be removed. In this blocking setting of social media A and B, both of them do not have any different through the steps needed. The blocked account do not has access to do interaction with the user. This privacy measure of both of the social media was similar without no specific comparison can be observed.

4.4 Personal Messaging

Private messaging in social media A and B is commonly known as direct message. Direct message function as the medium to communicate between the users privately in a chat room. Users able to make conversation between them without need to post publicly. The message can be send by direct message include text message, media sharing or voice message. For social media A, there are various types for personal messaging setting can be choose as shown in Table 1. The setting of personal messaging steps for social media A by choosing from the drop-down menu on the profile page. Then, select "Setting and Privacy" option. Next, choose "Private and safety" before go to the "Direct messages" part. On the "Direct message" section, user can choose any option based on their own choice referring to the setting types provided as in Table 1. Last but not least, the setting will be automatically save when the user selects new setting.

**Table 1: Social media A Personal Messaging Setting Types**

| Personal Messaging Types | Direct Message Description |
|---|---|
| Everyone | Publicly open to any users on social media A to send direct message |
| Friends | Only for users that follow each other can send direct message |
| Friends of Friends | Only for people followed by the user and their friends can send direct message |
| Only people you follow | Only for people that follow by the user even they are not follow back can send direct message |
| Only people you mention | Only the people that being mentioned by user can send direct message |
| None | Nobody can send direct message to user except for previous people that being allowed |

For social media B, there are three types of personal messaging settings which are shown in Table 2. To change the personal messaging settings, firstly the user need to login and click on the three lines horizontally on the top right of profile page. Then, choose "Setting" from the menu options. Next, choose "Privacy" option and click on "Messages" section. After that, user can choose any option based on the types of personal messaging setting as shown in Table 2. Lastly, the setting will save automatically as the user changed it.

**Table 2: Social media B Personal Messaging Setting Types**

| Personal Messaging Type | Direct Message Description |
|---|---|
| Everyone | All users on social media B able to send direct messages |
| People you follow | Only people followed by user can send direct messages |
| Off | Nobody able to send direct messages to user |

Based on the personal messaging setting of social media A and B, the social media A given more options to users to change the privacy setting compared with the social media B. Social media A has six different options while social media B only has three options for user. The more options given can make user be more specific in filtering other people to reach their direct message inbox. This privacy crucial to avoid cyber-attack to happen such as phishing attack that can be done using a single link shared. In this personal messaging setting, social media A's privacy level is better compared to social media B.

## 4. Conclusions

Security and privacy setting in social media are crucial for user to protect themselves from any cyber-attack. The higher level or more option provided by the social media company towards the users can make the users account be more safety. The security measures of Twitter and Instagram had been analysed based on their setting and function provided. Each of them has different level of strength in security and privacy level depending on the features analyzed. If the security and privacy level is higher, the user's chances to be attack by the hacker are lower. Social Media Company needs to be more alert and improve any vulnerability to avoid cyber-attack to happen.

## Acknowledgments

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Online Business, Financial and Technology. This work was supported by Universiti Utara Malaysia.

## References

Carpinella, R. (2015). Cybersecurity and social media. *Hudson Whitman/Excelsior College Press.*

Das, R. P. (2017). Cyber security for social networking sites: Issues, challenges and solutions. *International Journal for Research in Applied Science & Engineering Technology (IJRASET),, 5*(4), 833-838.

Deore, M. P. (2017). Hybrid encryption for database security. *Inter. Res. J. Eng. Technol*, 4.

Fiesler, C. D. (2017). What (or who) is public? Privacy settings and social media content sharing. *Proceeding of the 2017 ACM conference on computer supported cooperative work and social computing*, (pp. 567-580).

Handayani, F. (2015). Instagram as a teaching tool? Really? . *Proceedings of ISELT FBS Universitas Negeri Padang* (pp. 320-327). Padang: Universitas Negeri Padang.

Heyman, R. D. (2014). Evaluating social media privacy settings for personal and advertising purpose. *info, 16*(4), 18-24.

Huey, L. S. (2014). How Instagram can be used as a tool in social network marketing. *Center for Southern New Hampshire, 7*(4), 122-124.

Kadivar, M. (2014). Cyber-attack attributes. *Technology Innovation Management Review, 4*(11).

Kumar, R. K. (2022). Design and implementation of privacy and security system in social media. *International Journal of Advanced, 13*(4), 5081-5088.

Li, Y. L. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186.

Ma, Z. S. (2014). Tagging your tweets. A probabilistic modeling of hashtag annotation in twitter. *Proceedings of the 23rd ACM international conference on conference on information and knowledge management*, (pp. 999-1008).

Reno, J. (2013). Multifactor authentication: Its time has come. *Technology Innovation Management Review, 8*.

Zulkarnain, N. H. (2021). A REVIEW OF PURCHASE INTENTION ON INSTAGRAM AMONG UNIVERSITI TEKNOLOGI MALAYSIA LOCAL UNDERGRADUATES'STUDENTS. *International Journal of Modern Trends in Social Sciences, 4*(15), 114-120.