International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 723-732 www.ijaem.net ISSN: 2395-5252

Security measure of social media for Facebook and Twitter

Teoh Chun Hwung[1], MohdKhairudin Bin Kasiran[2]
1 Awang Had Salleh Graduate School, School of Computing, Universiti Utara Malaysia, Kedah, Malaysia
2 School of Computing,Universiti Utara Malaysia,Kedah, Malaysia..

Date of Submission: 20-07-2023 Date of Acceptance: 31-07-2023

ABSTRACT: In today's rapidly evolving digital landscape, ensuring the security of social media platforms like Facebook and Twitter has become imperative. This article delves into the comprehensive study of "Security Measures of Social Media for Facebook and Twitter," focusing on the measures implemented by these platforms to safeguard user accounts and protect sensitive information. The study will explore and emphasize the critical role of security in social media platforms and the need to address emerging challenges. A detailed review provides a robust foundation by summarizing existing research on social media security measures. The study analyzes specific security measures utilized by Facebook and Twitter, including Two-Factor Authentication, Account Recovery Processes, Privacy Settings, and Profile Information Changes. A meticulous breakdown of the procedures involved in these measures and conducts a comparative analysis between the two platforms. Moreover, the study delves into the future of security on social media platforms, discussing emerging trends and potential challenges. Emphasis is placed on the significance of user education and awareness, fostering collaboration among industry stakeholders, and adhering to ethical practices to continually enhance security measures. The discussion focuses on a comprehensive comparison of security features and strategies between Facebook and Twitter. It also delves into potential mitigation strategies to further strengthen security and protect users' accounts and personal information. Conclusively, this study synthesizes key findings and underscores the crucial need for continuous efforts in ensuring the security and trustworthiness of social media platforms. It highlights the significance of regular assessments, updates, and user education to effectively tackle emerging security threats and safeguard user data.

KEYWORDS:social media,Two-Factor Authentication, Account Recovery Processes, Privacy Settings, Profile Information Changes, Step,key findings, vulnerabilities, Ethical,Emerging trend, Challenge.

I. INTRODUCTION

Social media platforms have become an integral part of modern society, revolutionizing the way people connect, communicate, and share information. Among these platforms, Facebook and Twitter have emerged as global leaders, providing users with unprecedented access to vast networks of individuals and a multitude of online interactions. However, as the popularity of social media continues to soar, concerns about security and privacy have come to the forefront of public discourse. The advent of social media has given rise to an array of security challenges. With billions of users entrusting these platforms with their personal information, it is imperative to examine the security measures implemented by social media giants such as Facebook and Twitter. By understanding the security measures employed by these platforms, we can assess their effectiveness in safeguarding user data and mitigating risks. The rapid growth of social media platforms has transformed the way people communicate, connect, and share information. The year 2020, marked by the COVID-19 pandemic and subsequent lockdowns, witnessed a significant increase in internet usage as individuals turned to online platforms for various activities [1].

One of the primary concerns associated with social media authentication is the potential for compromised accounts and unauthorized access. Cybercriminals actively target user credentials through various techniques, such as phishing attacks and brute-force methods. The consequences of such breaches can be severe, ranging from identity theft to the dissemination of misinformation or malicious content. The effects of compromised accounts and security weaknesses extend beyond individual users and can have broader implications for the general

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 723-732 www.ijaem.net ISSN: 2395-5252

public. Privacy concerns are at the forefront, as unauthorized access to personal information can lead to privacy breaches and violations of user trust. Additionally, the misuse of user data can fuel the spread of misinformation, influencing public opinion, and impacting social discourse [2]. This aims to delve into the realm of social media security, focusing specifically on Facebook and Twitter. Through a comprehensive analysis, the security measures implemented by these platforms will be explored, with a particular emphasis on key areas such as Two-Factor Authentication, Account Recovery Process, Privacy Settings/Access Sensitive Information, and Profile Information Changes. Scrutinizing these specific security measures, valuable insights can be gained into the efforts made by Facebook and Twitter to protect user data and ensure a secure online experience.

Furthermore, this seeks to go beyond the present state of social media security and explore the future trajectory of these platforms. By considering emerging trends, potential challenges, and ethical implications, light will be shed on the ever-evolving landscape of security on social media platforms. Recommendations and insights will also be offered on how social media platforms can further enhance their security measures to address the dynamic nature of cyber threats and user expectations. By undertaking this examination of security measures on Facebook and Twitter, it is hoped that this will contribute to the ongoing discourse surrounding online security and privacy. It is believed that an informed understanding of social media security can empower users, platform administrators, and policymakers to make informed decisions and collectively foster a safer and more secure online environment.

II. LITERATURE REVIEW

In recent years, there has been a growing body of research and literature focused on security in social media authentication. Scholars and industry experts have investigated various authentication mechanisms, security protocols, and vulnerabilities specific to platforms like Twitter and Facebook.

The statistics reveal a substantial shift in internet usage patterns compared to 2018, with a greater number of individuals spending more hours online[3]. The rise in internet usage has been accompanied by a surge in popularity for social networking applications, with Facebook, YouTube, Instagram, and Twitter emerging as the frontrunners [3]. However, this increased reliance on social media platforms has also exposed users to a variety of risks and vulnerabilities, especially concerning the security of their accounts and personal information.

While statistics show a decrease in some types of cybercrimes, including virus or malicious code, spam, hacking, and intrusion, it is crucial to remain vigilant as cybercriminals continue to evolve their tactics [3]. Users' perception of security when using the internet plays a significant role in determining their confidence in social media platforms and online interactions. Several studies have examined the effectiveness of different authentication methods, such as single-factor authentication (SFA) and multi-factor authentication (MFA), in mitigating security risks. Additionally, research has highlighted the importance of secure communication channels, user data protection, and the prevention of security breaches[4].

This has also provided insights into the security features and policies adopted by social media platforms. It has emphasized the significance of robust authorization mechanisms, access control, and proactive measures to detect and respond to suspicious login attempts. By reviewing the existing literature, this can build upon the knowledge and findings of previous studies, contributing to a comprehensive understanding of security implementations in social media authentication[5].

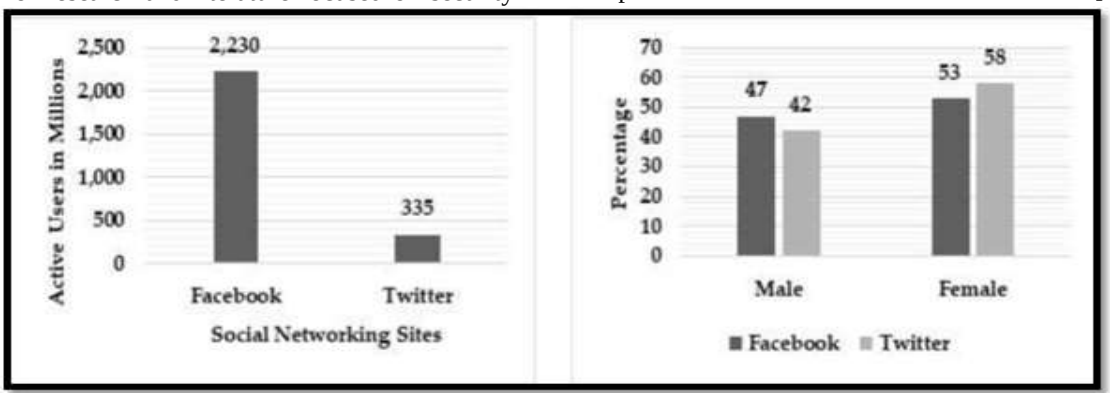

Figure 1: Active and Percentage of using Facebook and Twitter[1]

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 723-732 www.ijaem.net ISSN: 2395-5252

III. SECURITY MEASURES USED BY SOCIAL MEDIA PLATFORM

A. TWO-FACTOR AUTHENTICATION

Two-factor authentication (2FA) is an additional layer of security that can be added to Facebook and Twitter accounts. When enable 2FA, will be required to enter a code from your phone in addition to your password when log in. This helps to protect the account from unauthorized access, even if someone knows your password.

To enable Two-Factor Authentication on Facebook, follow these steps:

Facebook:

Step 1 - Go to Setting and locate the "Security and Login" option and click on it.

Step 2 - Within the "Security and Login" section, find the "Two-Factor Authentication" option and click on "Use Two-Factor Authentication" to proceed.

Step 3 - Select the preferred security method for Two-Factor Authentication. Facebook provides three options: "Authentication App," "Text Message (SMS)," and "Security Keys."

Step 4: If you choose the "Text Message (SMS)" option, a list of your phone numbers will be displayed. Select the desired phone number to receive the verification code via SMS. If your phone number is not listed, you can add a new one by clicking on "Add phone number.".

Step 5: After selecting the phone number, you will be prompted to re-enter your Facebook password for security verification.

Step 6: Once verified, you will receive a text message with a verification code. Enter the code in the designated "Enter Code" field. After continue you have successfully set up Two-Factor.

To enable Two-Factor Authentication on Twitter, follow these steps:

Twitter:

Step 1: Go to the "Settings & Privacy" section of your Twitter account.

Step 2: Choose "Two-Factor authentication" to open the Two-Factor Authentication settings.

Step 3: Twitter offers three options for Two-Factor Authentication: "Authentication App," "Text Message," and "Security Keys."

Step 4: If you select the "Text Message" option, you will be asked to enter your Twitter account password for security confirmation.

Step 5: After entering your password, input the phone number on which you would like to receive the authentication code via text message.

Step 6: Twitter will send a verification code to the provided phone number. Enter the received code in the "Your code" field and click "Next."

Step 7: As an additional security measure, Twitter will prompt you to save a single-use backup code. It is crucial to save this code in a secure place for future use. Two-Factor Authentication is now enabled on your Twitter account.

By following these steps, users can implement Two-Factor Authentication on Facebook and Twitter, adding an extra layer of security to their accounts. This feature ensures that unauthorized access is mitigated and that users have control over their account's security.

B. ACCOUNT RECOVERY PROCESS

The account recovery process plays a crucial role in maintaining the security of social media platforms, allowing users to regain access to their accounts in the event of unauthorized access or forgotten credentials. This section will focus on examining the account recovery processes of Facebook and Twitter, outlining the steps involved in recovering an account on each platform.

Facebook:

To recover a Facebook account, follow these steps:

Step 1: Visit the Facebook password reset site and click on "Forgot Password?" This will direct you to the account recovery page.

Step 2: Enter your registered email address or phone number associated with your Facebook account and click on "Search." Facebook will retrieve your account information.

Step 3: Choose an account recovery method. You can select either "via email" or "via SMS." If you select the email option, Facebook will send a reset code to the email address linked to your Facebook account. If you choose SMS, Facebook will text a reset code to your registered phone number.

Step 4: If you choose the email recovery option, retrieve the account code from your email and enter it in the “Enter Code” field.

Step 5: Check the "Log me out of other devices" box to log out your Facebook account from any other logged-in devices. This ensures that any unauthorized access is terminated.

Step 6: Create a new password. Enter your new password, replacing the old one, to recover your Facebook account. You can now log into your Facebook account using the new password.

Twitter:

To recover a Twitter account, follow these steps:

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 723-732 www.ijaem.net ISSN: 2395-5252

Step 1: Log in to Twitter. If your account has been temporarily limited, you may still be able to access Twitter with limited features.
Step 2: If your account is temporarily limited, click or tap on "Continue to Twitter." A countdown timer will display the remaining time until your account is automatically restored.
Step 3: If possible, remove any tweets that violate Twitter's rules before proceeding with the recovery process.
Step 4: In a web browser, visit the official appeals form for suspended and limited accounts: https://help.twitter.com/forms/general?subtopic=suspended
Step 5: Explain why you believe the suspension or limitation is in error. In the provided field, provide a detailed explanation of why you believe the suspension or limitation is incorrect or unjustified.
Step 6: Update your user information. Fill in the necessary fields with your updated information. Ensure that the provided email address is the one through which Twitter can contact you.
Step 7: If requested, upload identification. If your account suspension or limitation is due to concerns about your age or impersonation, Twitter may require you to upload identification as proof.
Step 8: Submit the form. After completing the form, click on the submit button. Twitter will communicate with you via email to inform you of their decision regarding your account. Typically, the recovery process takes a few days.

C. PRIVACY SETTINGS

Privacy settings are a vital component of social media platforms, allowing users to control who can access their information and ensuring a secure online experience. This section will focus on examining the privacy settings of Facebook and Twitter, providing steps to manage these settings effectively.

Facebook:
To manage privacy settings on Facebook, follow these steps:
Step 1: Access the settings menu. Scroll to the bottom of the Facebook menu and click on "Settings."
Step 2: Click on "Privacy." It is located near the top of the left column, which opens the Privacy Settings and Tools page.
Step 3: Control who can see your posts. Under "Your Activity," select the desired audience for your posts. By default, your posts are visible to the audience you select. Ensure you specify otherwise if needed when making a post.
Step 4: Manage who can find and contact you on Facebook. The bottom section of the right panel contains various options for controlling how people can search for you, add you to their friends lists, and send you messages. Adjust these settings according to your preferences.

Twitter:
To manage privacy settings on Twitter, follow these steps:
Step 1: Access the settings menu on Twitter. Click on your profile picture and select "Settings and Privacy" from the drop-down menu. This opens the Privacy Settings and Tools page.
Step 2: Click on "Privacy and Safety." It allows you to manage your privacy settings effectively.
Step 3: Manage your audience and tagging. Navigate to the "Audience and Tagging" section. Here, you can control what information others can see about you on Twitter.
Step 4: Enable tweet protection. To enhance privacy, enable the option "Protect your tweets." This restricts the visibility of your tweets to only those who follow you. If this option is selected, you will need to approve each new follower.
Step 5: Disable photo tagging. Twitter also provides the option to disable photo tagging. If you don't want others to tag you in their photos, disable this feature to prevent association with your account.

By following these steps, users can effectively manage their privacy settings on Facebook and Twitter, exerting control over who can view their posts and accessing additional options to protect their information.

D. PROFILE INFORMATION CHANGES (PASSWORD)

Ensuring the security of profile information, particularly passwords, is a critical aspect of maintaining a secure social media presence. This section will focus on examining the steps involved in changing passwords on Facebook and Twitter, highlighting the security measures implemented by these platforms.

Facebook:
To change your password on Facebook, follow these steps:
Step 1: Access the settings menu by clicking on your profile picture and selecting "Settings & Privacy."
Step 2: Click on "Security and Login" in the left panel. This will direct you to the security and login settings.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 723-732 www.ijaem.net ISSN: 2395-5252

Step 3: Locate the "Change Password" option and click on "Edit" next to it.
Step 4: Enter your current password in the top field. This ensures that the person changing the password is the authorized account holder.
Step 5: In the following field, enter your new password. To enhance the security of your account, consider using a password that is at least 12 characters long, combining numbers, letters, and special characters.
Step 6: After entering the new password, click "Save Changes." Your password will be successfully changed, enhancing the security of your Facebook account.

Twitter:
To change your password on Twitter, follow these steps:
Step 1: Access the settings menu by clicking on your profile picture and selecting "Settings & Privacy."
Step 2: Click the “Change your password” option in the menu.
Step 3: Enter your current password in the provided field. This step ensures that the person changing the password is the authorized account holder.
Step 4: Enter the new password you desire to use. It is recommended to choose a strong password that combines various characters and is not easily guessable.
Step 5: Confirm the new password by re-entering it in the subsequent field.
Step 6: Click on "Save" to save your new password. The changes will be applied immediately, securing your Twitter account with the updated password.

By following these steps, users can change their passwords on Facebook and Twitter, reinforcing the security of their profile information. It is crucial to select strong passwords and regularly update them to protect against unauthorized access.

IV. THE FUTURE OF SECURITY ON SOCIAL MEDIA PLATFORMS

A. EMERGING TRENDS IN SOCIAL MEDIA SECURITY

As social media platforms continue to evolve, so too do the challenges and threats they face in terms of security. To anticipate and address these evolving risks, it is essential to explore emerging trends in social media security. This will focus on discussing the emerging trends in social media security.

A framework that enables the real-time tracking and analysis of discussions on social media platforms. By dynamically monitoring these discussions, the framework aims to provide timely insights into emerging trends, sentiments, and influential users within the online discourse.

To accomplish this, the framework leverages a combination of natural language processing (NLP) techniques and machine learning algorithms. By employing topic modelling and sentiment analysis, individual posts or messages can be categorized, and their sentiment assessed. What sets this framework apart is its adaptability, continuously updating its models as new data streams in, thus reflecting the evolving nature of discussions on social media.

A comprehensive approach to dynamic social media monitoring, enabling a deeper understanding of rapidly evolving discussions. By utilizing NLP and machine learning techniques, the framework facilitates the categorization of topics, sentiment analysis, and identification of influential users. By staying updated with real-time data, this monitoring system empowers researchers and analysts to gain better insights into online conversations as they unfold [6].

These emerging trends in social media security are crucial for the future of security measures on platforms such as Facebook and Twitter. By harnessing the power of advanced technologies and monitoring techniques, social media platforms can better detect and respond to security threats, safeguard user data, and ensure a secure online environment.

B. POTENTIAL CHALLENGES AND CONSIDERATIONS

As social media continues to evolve, new challenges and considerations arise in the realm of security. This section will explore potential challenges and considerations that social media platforms like Facebook and Twitter may face in the future.

One potential challenge is the emergence of viral social media challenges. These challenges often capture the attention and participation of young adults. A research study examined the motivations behind young adults' participation in viral challenges and identified two main factors: social influence and intrinsic motivations.

Social influence plays a significant role, as young adults feel pressure to conform to the behaviour of their peers participating in these challenges. They may perceive participation as a way to fit in, gain social acceptance, or be part of a community. Additionally, intrinsic factors such as the entertainment value of the challenge, the desire

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 723-732 www.ijaem.net ISSN: 2395-5252

for attention, and the belief that the challenge will benefit others also motivate participation [7].

However, it is important to note that there can be divergent patterns between prosocial and potentially risky challenges. Prosocial challenges often foster positive behaviour and engagement, with participants motivated by social influence and a sense of community. On the other hand, risky challenges may lack the influence of social pressure and can be driven more by personal entertainment or attention-seeking desires.

Addressing these challenges and considerations requires a multifaceted approach. Social media platforms need to develop mechanisms to mitigate the risks associated with viral challenges. This can involve implementing stricter content moderation policies to identify and remove potentially harmful challenges. Additionally, platforms can promote awareness and education campaigns to inform users about the potential risks and consequences of participating in certain challenges.

Collaboration with relevant stakeholders is also essential. Social media platforms can work together with researchers, psychologists, and safety organizations to better understand the psychological and behavioural aspects behind viral challenges. By collaborating, platforms can develop effective strategies to promote responsible participation and discourage engagement in risky or harmful challenges.

User privacy is another significant consideration for the future of social media security. As technology advances, platforms must continually adapt their privacy settings and measures to protect users' personal information from unauthorized access or data breaches. Implementing stronger encryption, improving user consent mechanisms, and providing transparent privacy policies are crucial steps towards enhancing user privacy.

C. User Education and Awareness

User education and awareness play a crucial role in enhancing security on social media platforms such as Facebook and Twitter. This focuses on the importance of user education and awareness in addressing privacy concerns and protecting personal information.

The privacy concerns of social media users and identified common fears among participants. These concerns included the potential use of personal data for marketing purposes, the fear of data breaches or theft, and apprehension regarding the tracking of online activity. Social media platforms offer various privacy settings that allow users to control who can access their personal data. Users should become familiar with these settings and adjust them according to their desired level of privacy. Furthermore, using strong passwords is a fundamental measure to safeguard accounts from unauthorized access. Two-factor authentication adds an extra layer of security by requiring users to provide additional verification, such as a code sent to their mobile device, to log in. By implementing these measures, users can enhance the security of their accounts [8].

However, social media platforms should prioritize user education initiatives. This includes providing clear and easily accessible information about privacy settings, security features, and best practices for maintaining privacy. Platforms can implement user-friendly tutorials, notifications, and reminders to encourage users to review and update their privacy settings regularly.

Additionally, awareness campaigns and educational resources can help users understand the potential risks associated with sharing personal information and the importance of adopting security measures. Platforms can collaborate with privacy advocates, industry experts, and relevant organizations to develop comprehensive educational programs that address privacy concerns and promote responsible online behaviour.

By fostering user education and awareness, social media platforms can empower individuals to take ownership of their online privacy and security. Through ongoing education and improved awareness, users can make informed decisions and actively contribute to creating a more secure social media environment.

D. Collaboration and Industry Standards

Collaboration and the establishment of industry standards are vital components in shaping the future of security on social media platforms such as Facebook and Twitter. This focuses on the importance of collaboration and industry standards in ensuring the security and trustworthiness of these platforms.

The application of social media analysis in the tour and travel industry. Social media data can provide valuable insights into tourists' interests, preferences, and travel habits. By leveraging this data, tour and travel companies can enhance the customer experience, target marketing campaigns more effectively, and optimize their overall business operations. This present of a tour and travel company that successfully utilized social media

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 723-732 www.ijaem.net ISSN: 2395-5252

analysis to improve customer service. Through social media monitoring and analysis, the company identified pain points experienced by customers and subsequently developed new products and services to address these issues. Moreover, the company utilized social media platforms to actively engage with customers, fostering relationships and enhancing customer satisfaction. This has concluded that social media analysis holds significant potential for tour and travel companies [9].

However, it emphasizes the importance of responsible use of social media data. Companies must obtain the explicit consent of their customers before collecting or using their data. Additionally, transparency regarding the purpose and methods of data utilization is crucial to maintain customer trust and ensure ethical practices.

Furthermore, collaboration among social media platforms, industry stakeholders, and regulatory bodies is essential to establish and uphold industry standards for security measures. By collaborating, platforms can share best practices, identify emerging threats, and collectively work towards addressing security challenges.

Collaboration can extend beyond the platform level. Tour and travel companies can partner with social media platforms to develop guidelines and protocols for the responsible use of customer data. Additionally, collaboration with relevant regulatory authorities can lead to the development of industry standards that ensure the protection of user data and privacy.

Industry standards should encompass elements such as data protection, secure authentication methods, content moderation, and transparency in data handling. By adhering to these standards, social media platforms can enhance user trust, safeguard user data, and foster a safer online environment.

Furthermore, collaborations can facilitate knowledge-sharing and research efforts to better understand emerging security threats and devise effective countermeasures. By leveraging collective expertise, industry collaborations can contribute to the development of innovative security solutions and anticipate future security challenges.

In conclusion, collaboration and the establishment of industry standards are crucial for the future of security on social media platforms. By working together, social media platforms, industry stakeholders, and regulatory bodies can create a more secure and trustworthy environment. This collaboration will benefit users by ensuring the protection of their data and privacy, while also fostering innovation and continued growth in the social media industry.

E. ETHICAL AND PRIVACY IMPLICATIONS

Ethical considerations and privacy implications are critical aspects of the future of security on social media platforms like Facebook and Twitter. The potential ethical and privacy concerns associated with social media usage and the measures that can be taken to address them.

The privacy implications of hash-tagging on social media platforms, particularly in the context of social commerce. This highlights the concerns that widespread hash-tag usage can facilitate the tracking and identification of individuals by stalkers. Furthermore, emphasize the challenges posed by the lack of robust privacy controls on social media platforms, making it difficult for users to protect their personal information adequately. To shed light on these implications, a conducted a preliminary analysis of the trails left by hashtags, following online shopping platform product listings, consumer reviews, social-commerce policies, and influencer posts. The findings reveal that it is relatively easy to track a user's online activity by tracing the hashtag trails they leave behind. This concluded that the privacy implications of hash-tagging are a significant and valid concern. It emphasizes the need for enhanced protection of users' personal information on social media platforms. Stronger privacy controls should be implemented to empower users to have more control over their data and privacy settings [10].

Both social media platforms and users play important roles in addressing ethical and privacy concerns. Platforms should prioritize the implementation of robust privacy controls, including options for granular privacy settings and improved data handling practices. This can involve mechanisms for consent management, transparent data policies, and enhanced security measures to protect user data from unauthorized access or misuse.

Users, on their part, need to be more cautious and discerning about the information they share on social media. Being mindful of the potential consequences and risks associated with sharing personal information can contribute to maintaining individual privacy and security. Educating users about privacy best practices, potential risks, and the importance of informed consent can further empower them to make responsible choices on social media platforms.

Collaboration between social media platforms, users, regulatory bodies, and privacy

International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 7 July 2023, pp: 723-732 www.ijaem.net ISSN: 2395-5252

advocates is crucial in addressing the ethical and privacy implications of social media security. Open dialogues, ongoing research, and the development of industry standards can help establish guidelines and policies that protect user privacy while fostering innovation and growth in the social media industry.

The ethical and privacy implications of social media usage cannot be ignored. To ensure a secure and trustworthy social media environment, both platforms and users must proactively address these concerns. By implementing stronger privacy controls, promoting user education, and fostering collaboration, social media platforms can safeguard user privacy, promote responsible practices, and maintain the trust of their user base.

V. DISCUSSION

The discussion will compare the security measures implemented by "Social Media A" (Facebook) and "Social Media B" (Twitter) and discuss strategies for mitigating and enhancing security on these platforms.

Both social media A and social media B offer Two-Factor Authentication (2FA) as an additional layer of security. However, there are differences in the implementation of this feature. social media A provides multiple options such as authentication apps, text messages (SMS), and security keys for users to choose from. On the other hand, social media B offers authentication apps, text messages, and security keys as well, but the options available may differ slightly. Both platforms recognize the importance of 2FA in protecting user accounts from unauthorized access.

To further enhance security, both platforms can focus on promoting the adoption of 2FA by educating users about its benefits and providing clear instructions on how to enable it. Additionally, they can explore the implementation of emerging 2FA methods such as biometrics or hardware tokens to offer users more choices and strengthen security measures.

Next, the account recovery processes on social media A and social media B differ in some respects. social media A allows users to initiate account recovery by entering their email address or phone number. They provide options for recovery via email or SMS, ensuring users can regain access to their accounts. On the other hand, social media B account recovery process includes steps such as appealing limitations, verifying user information, and submitting required identification documents if necessary.

To enhance the account recovery process, both platforms can focus on improving user experiences by providing clear and user-friendly instructions during the recovery process. They should also ensure prompt and efficient response times when users submit recovery requests to minimize potential downtime and frustration. Regular assessments of the effectiveness of account recovery methods and proactive updates can further strengthen security measures.

Furthermore, social media A and social media B offer privacy settings to allow users to control the visibility of their personal information. Both platforms provide options for users to customize their privacy preferences. Social media A allows users to manage who can see their posts, control friend requests, and adjust settings related to search and tagging. Similarly, social media B offers privacy settings for account visibility, tweet protection, and the ability to manage follower requests.

To Continual improvement of privacy settings is essential for both platforms. They should regularly review and update privacy options to address evolving privacy concerns and ensure that users have granular control over their personal data. Transparent explanations of privacy settings and proactive communication about updates can enhance user awareness and promote responsible use of these features.

Moreover, both social media A and social media B allow users to change their passwords through the account settings. The process typically involves entering the current password and creating a new one. While the general process is similar, each platform may have slight variations in the interface and specific steps required.

The Platforms can further enhance security by promoting the use of strong and unique passwords. They should encourage users to adopt password management tools and provide guidance on creating strong passwords. Additionally, options for enabling multi-factor authentication during password changes can be explored to provide an extra layer of security.

In conclusion, "Social Media A" (Facebook) and "Social Media B" (Twitter) have implemented various security measures to protect user accounts and data. Both platforms offer Two-Factor Authentication, account recovery processes, privacy settings, and password change features. However, there is always room for improvement to enhance security and mitigate potential risks.

To further enhance security on social media platforms, collaboration among industry stakeholders, user education and awareness, and adherence to ethical practices are crucial. By staying

proactive, regularly evaluating and updating security measures, and prioritizing user privacy and data protection, "Social Media A" and "Social Media B" can maintain the trust and confidence of their users in an ever-evolving digital landscape.

VI. CONCLUSION

In these, the security measures implemented by two prominent social media platforms, "Social Media A" (Facebook) and "Social Media B" (Twitter). Through the examination of features such as Two-Factor Authentication, Account Recovery Processes, Privacy Settings, and Profile Information Changes, we have gained insights into the efforts made by these platforms to safeguard user accounts and protect personal information.

The comparison between "Social Media A" and "Social Media B" revealed similarities and differences in the implementation of security measures. Both platforms recognize the importance of Two-Factor Authentication as an additional layer of protection. They offer users various options to secure their accounts, such as authentication apps, text messages, and security keys. Account recovery processes differ slightly, but the goal remains the same – ensuring users can regain access to their accounts in a secure manner.

Privacy settings are available on both platforms, empowering users to control the visibility of their personal information. Users can customize their preferences to manage who can see their posts, control friend requests, and adjust settings related to search and tagging. Additionally, password change features enable users to update their credentials and strengthen account security.

To further enhance security on social media platforms, there are several considerations. Both platforms can focus on promoting the adoption of Two-Factor Authentication, improving the account recovery process, enhancing privacy settings, and encouraging the use of strong and unique passwords. Continuous collaboration among industry stakeholders, user education and awareness, and adherence to ethical practices are crucial for maintaining the security and trustworthiness of these platforms.

It is essential to recognize that security measures on social media platforms should evolve with the ever-changing threat landscape. Regular assessments, updates, and enhancements are necessary to address emerging security challenges and protect user data from unauthorized access, privacy breaches, and potential misuse.

As users of social media platforms, individuals also play a significant role in safeguarding their own security. Being mindful of the information shared, adopting best practices for password management, and staying informed about privacy settings are essential steps to protect personal data and privacy.

In conclusion, the security measures implemented by "Social Media A" and "Social Media B" demonstrate a commitment to ensuring user security and privacy.

However, there is always room for improvement and the need to adapt to the evolving digital landscape. By prioritizing collaboration, user education, and continuous efforts to enhance security measures, social media platforms can maintain user trust, protect personal information, and create a safer online environment.

VII. ACKNOWLEDGEMENT

The authors would like to thank all Schoolof Computing members who were involved in thisstudy. This study wasconducted for the purpose ofOnline Business, Financial Technology &CybersecurityResearchProject. This work was supported by UniversitiUtara Malaysia.

REFERENCE

[1] C. Malaysia, “Cybersecurity Malaysia,” MyCert (Malaysia Computer Emergency Respond Team), 2023.

[2] Norton, “2019 data breaches: 4 billion records breached so far,” A look at 2019 data breaches, 8 August 2018.

[3] C. A. M. C. Malaysia, “Internet Users Survey 2020,” SURUHANJAYA KOMUNIKASI DAN MULTIMEDIA MALAYSIA, 2020.

[4] S. D. Octopus, “What is two factor authentication (2FA)?: Security wiki,” 15 August 2021. [Online]. Available: https://doubleoctopus.com/security-wiki/authentication/what-is-2fa/#security-wiki-content.

[5] C. S. D. H. S. Thapa, “Security Analysis of User Authentication and Methods,” Security Analysis of User Authentication and Methods, August 2022.

[6] A. L. N. A.-C. J. C. R. M. A. A. A. Maya Srikanth, “Dynamic Social Media Monitoring for Fast-Evolving Online Discussions,” KDD '21: Proceedings of the 27th ACM SIGKDD Conference on Knowledge Discovery & Data Mining, p. 3576–3584, August 2021.

[7] R. R. H. Z. K. C. M. P. J. W. Jaclyn Abraham, "Applying Behavioral Contagion Theory to Examining Young Adults," ACM Transactions on Social Computing, vol. 5, no. 1-4, pp. 1-34, 2022.

[8] K. G. Jeremy McHatton, "Mitigating Social Media Privacy Concerns - A Comprehensive Study," IWSPA '23: Proceedings of the 9th ACM International Workshop on Security and Privacy Analytics, p. 27–32, April 2023.

[9] I. N. A. N. Yohannes Kurniawan, "Social Media Analysis in Tour and Travel Industry," ICGSP '22: Proceedings of the 6th International Conference on Graphics and Signal Processing, pp. 55-62, July 2022.

[10] G. D. J. H. Bethany Sumner, "Preliminary Analysis of Privacy Implications Observed in Social-Media Posts Across Shopping Platforms," ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security, pp. 1-10, 2022.