Social Media Data Privacy and Security

Project Type: Research Project

Team 5

Abril Beascoechea, Charles Degboe, Sam Martin, Ricardo Portillo, Nicholas Zhang

Table of contents

Introduction

In today's digital age, social media platforms have woven themselves into the fabric of our daily lives, serving as vital channels for communication, information sharing, and entertainment. As of 2024, the global social media user base exceeds 5.1 billion (Statista), underscoring the immense scale and influence of these platforms. This widespread adoption has ushered in an era where personal data exchanges at an unprecedented rate, raising significant concerns about data privacy and security.

The journey of social media security marks the evolution and adaptation in response to emerging threats. Early social media platforms, primarily focused on connectivity and user engagement, often lacked comprehensive security measures. This oversight led to hundreds of breaches and privacy issues, with thousands of incidents reported over the past decade alone. These breaches have highlighted the need for robust security protocols. Over time, the industry has seen the implementation of more sophisticated security measures, aimed at protecting user data and maintaining trust.

Effective security in the social media industry is crucial. With the vast amounts of personal and sensitive information shared online, the potential for misuse and exploitation by malicious actors is ever-present. Ensuring the protection of this data is not only vital for user trust but also for the platform’s integrity and continuity.

This research project aims to explore the current state of social media data privacy and security, particularly focusing on existing threats and vulnerabilities. By analyzing the strategies employed by social media companies to protect user data, this study will highlight both the

strengths and areas needing improvement. The goal is to formulate a set of recommendations that can enhance information security and mitigate the impact of various threats.

The report will begin with an overview of the current social media security standards and practices. This includes an examination of multi-factor authentication, data encryption, adherence to data privacy laws, and incident response strategies. For example, with multi-factor authentication, users can stop attempts on their account. Having MFA enabled allows users to stop these attacks and change their passwords immediately. The analysis will extend to the security approaches of major platforms such as Facebook/Meta, Twitter, and WhatsApp, identifying key similarities and differences in their methods.

Furthermore, this report will address potential threats and vulnerabilities faced by social media companies. Specific attacks, such as phishing and social engineering, along with notable case studies like the 2021 LinkedIn data breach. In this report Emerging threats, including those posed by artificial intelligence and quantum computing (World Economic Forum) will also be explored.

To provide a comprehensive view, the report will offer policy recommendations aimed at enhancing security. These will cover effective security strategies, third-party application integration, and the importance of education and awareness programs. These recommendations will be towards establishing key aspects that should be standard across the industry to ensure robust protection.

Overall, this report seeks to contribute to the ongoing efforts to secure social media platforms and protect user data. By addressing critical security challenges and proposing actionable solutions, the study aims to foster a safer digital environment for all users. We are

confident that with continued vigilance and initiative-taking measures, we can create a more secure online world where users feel confident sharing their individual experiences.

Current Social Media Security

Standards and Practices

Social media platforms are part of our everyday lives and contain extremely sensitive information in both personal and professional areas. Social Media Security refers to the proactive measures and strategies taken by users or businesses to protect their data, privacy, and confidentiality and protect organizations from the threats and risks of social media platforms. It is essential since it provides security against cyber threats and harassment, data breaches, and identity theft through various methods such as ensuring account authentication, controlling third-party access control and permissions, and raising awareness programs about common social engineering tactics. Implementing security standards is imperative to maintain the integrity of users' accounts and stop attackers from possibly getting full access to a person's or business' account contacting their friends/customers and accessing confidential information.

What are some standards and practices to follow to stay safe? The first one is implementing a strong and unique password. Your password should combine uppercase and lowercase letters, digits, and special characters to decrease the chances of cybercriminals cracking it. It should also be updated regularly and the same password shouldn't be used for different platforms while avoiding common passwords or information that could be guessed, such as birth dates and pet names.

The second practice to implement to stay safe is enabling two-factor authentication. Two-factor authentication (2FA) amplifies your security by requiring the user to submit a second form of verification, like a special code sent to their email, in addition to their password. This

way, even if the initial credentials are compromised, the risk of unauthorized access to your account is significantly reduced. Complementing 2FA, which adds an extra layer of security, with a long and complex password greatly enhances your account security minimizing the risk of a cyber attack.

Another crucial practice an organization should follow is to educate and train employees on security awareness. Users in general and, more importantly, employees need to be aware of common social engineering tactics. Most security breaches can be avoided if businesses hold regular training sessions to inform personnel on newly developed security risks and recent potential hazards on social media, and how to identify, react, and mitigate them. An example would be recognizing phishing attempts and not clicking suspicious links or divulging sensitive information. By fostering a culture of security awareness, the organization can significantly reduce the risk of social media-related breaches.

Other practices to keep in mind are regularly monitoring your account, Updating your software, and being cautious with third-party apps. Monitoring your account is vital to detect any suspicious activities like posts or messages that the user didn't create. Most social media nowadays notify the user with a security alert when there is a suspicious login. For example, Instagram has a section where you can view all the devices that are currently logged into your account and their location. Keeping your software and apps up to date is important since they often come with a security patch that addresses vulnerabilities. Outdated software can be a significant security risk, providing an easy target for cybercriminals. Third-party apps can be a potential entry point for malicious actors. If the user is going to grant permission to an external app, they should be completely sure it comes from a reputable source and review the access request it makes. If possible, limit the permissions to only what is strictly necessary for the app

to function, since it can help mitigate risks. Additionally, periodically reviewing and revoking access to apps that are no longer needed is a good practice.

Data Encryption

What is data encryption? Data encryption converts data into a secure format to protect information from malicious actors and make sure that it can only be accessed by authorized users. This way, even if the email, database content, or file is intercepted, it remains confidential. An example of encryption is cryptography, which works through a complex mathematical algorithm (data encryption cipher) to substitute one character for another. It transforms normal data into a sequence of unrecognizable random characters known as "ciphertext". To get the information's original state, a process of decryption is required which involves having the "key" that the authorized user has. Some benefits of data encryption are maintaining data integrity, protection of data across many devices, remote office security, cloud data security, and protection of intellectual property from duplication or reverse engineering.

Adherence to Data Privacy Laws & Legislature

These laws mandate how data should be handled, stored, and protected while imposing penalties for organizations that don't comply. Many countries have adopted general data privacy laws for their government and private-sector activities that handle personal data. International standards have broad principles regarding the collection and storage of information. Organizations must be transparent about their data collection practices, obtain explicit consent from users, and provide options for users to manage their privacy settings. In general, personal information should be lawfully obtained. Implementing these regulations not only helps avoid legal repercussions but also enhances the credibility and trustworthiness of the organization.

Modern Security Strategies/Systems

In today's world, we have many big social media platforms, and they all have similarities and differences in how they protect their users' information. In the wake of digital transformation, social media platforms have assumed a role that influences communication, information sharing, and social interaction. As such, these platforms are bound to hold loads of personal data, raising a strong need for versatile security and privacy strategies to safeguard their users against threats of all kinds. The modern concepts of security and privacy strategies that Facebook, Twitter, and Instagram hold, work on are complex mixes of traditionally pervasive cybersecurity measures and more recent innovative approaches, including encryption for data anonymization and machine learning for threat detection. We will compare and contrast how these platforms actually take their security and privacy strategies forward, showing the protection given to the users and the treatment of their data.

The use of encryption is one major way that goes across the security strategies at major social media platforms. In protecting data at rest and in transit, this is very important. For example, Facebook provides end-to-end encryption in its messaging service, where messages can only be read by the sender and the receiver. At the same time, Twitter practices encrypted data transfer between users and its servers by using HTTPS, in which the information is cryptographically blinded in case of in-process eavesdropping attacks or man-in-the-middle attacks (Twitter, 2023). Instagram encrypts all moved data from the user to its servers so as to provide all users with safe, secure, and private communication among themselves (Instagram, 2023).

Another common security measure is MFA. MFA adds another security layer beyond simply the username and password. Both Facebook and Instagram, as well as Twitter, offer

MFA—usually a second verification step, such as a code sent to the user's mobile phone or an authentication app. This helps to curb possible risks that password compromises would pose to users on the increased unauthorized access front.

Data anonymization and minimization are cross-cutting techniques. These techniques reduce the general quantum of personal data that platforms keep and handle. Thus, Facebook uses techniques to make user data anonymous for advertising, where no identifiable personal details are passed to the advertiser (Facebook, 2023). Twitter and Instagram also practice data minimization by minimizing the data that is collected to only what is actually needed for the service, as well as anonymizing it wherever possible, to be able to protect the users from violations of privacy (Twitter, 2023; Instagram, 2023).

While these platforms may be similar in some of the collected practices, the difference is a lot in how they treat the user data. For example, Facebook is on record to have come under fire regarding user data collection, especially the sharing of third-party data and targeted advertising practices (Guardian, 2022). In line with this sentiment, Facebook has even set controls on access and improved transparency, as users can now learn an explanation of how and with whom their information will be shared. On the contrary, Twitter has followed a much more privacy-leaning agenda traditionally. It enforces stronger controls over shared data, with less aggressive data monetization, as published by Twitter (2023).

While Instagram does show some similarities with the latter in its approach to data handling, it has also invented a number of quite unique features associated with sharing, thereby letting people distribute more remotely. For instance, the "Close Friends" feature offers users more control in terms of privacy and visibility related to personal content uploads. This reveals another subtle attitude towards controlling user data. Another important factor is related to the

application of machine learning and artificial intelligence in threat detection and mitigation. They have invested heavily in artificial intelligence, which aids in detecting and removing harmful content such as hate speech, misinformation, or spamming in real-time (Facebook, 2023). This proactive approach helps in quickly identifying and mitigating threats, protecting users from potential harm. Twitter does use AI in one area: for similar reasons, though it does combine it with a heavier reliance on users reporting undesirable content back to the company for follow-up and human moderation. In contrast, Instagram uses this technology for the majority of its content, including the moderating of indecent content as well, in addition to general safety and positive experience reasons.

Most of these efforts are also quite variable, and so is the transparency across the aisle on user awareness. Facebook has suppliers in various initiatives that aim to educate users about privacy settings and use of data, including quite elaborate help centers and privacy checkups. Twitter's transparency reports expose detailed information about government requests for user data and requests for content takedown, thereby instigating an air of accountability and openness. Instagram also has a robust privacy setting, offered to the users, with control for letting them know about changes in privacy settings in different apps (Instagram, 2023).

Although some of the foundational security strategies taken by Facebook, Twitter, and Instagram are quite similar, such as encryption, multi-factor authentication, and data anonymization, in reality, the way they handle user data, threat detection, and transparency diverges radically. All these differences emanate from the distinctive qualities and challenges of each platform in trying to juggle vocal user privacy and impactful business objectives together with stringent regulatory needs. As social media continues to evolve, these platforms should

rinse and repeat the strategy to protect user data that keeps trust in an ever changing complicated digital landscape.

Potential Threats and Vulnerabilities

Due to the nature of their data and the value it has, social media companies can face a plethora of different threats as attackers attempt to gain unauthorized access to data or sensitive information. In particular, specific attacks like phishing and social engineering can be especially prevalent on social media.

There have been several large scale cyber attacks against social media in the last few years that have impacted millions of people. In 2021, the business focused social media LinkedIn suffered a major data breach where the personal information of 700 million users was leaked onto the darkweb. This included things such as full names, physical addresses, email addresses, and phone numbers. LinkedIn reported that the cause of the data leak was through the misuse of the LinkedIn API, which allowed the attacker to access user data. Despite this, LinkedIn suggested that the "incident was not a data breach per se, but rather a case of data scraping involving public profile information" (Baek, 2023). Other major incidents that have happened in the last few years are 2023 Twitter/X data leak and the 2022 WhatsApp data leak, with 200 million and 500 million users respectively, having their personal data leaked. In many cases, user data was the focus of the attack, which highlights the value of social media user data sets in our modern society.

Common Attack Types

Arguably the most common attack that faces social media and its users is phishing and other social engineering based attacks. Impacting millions of users annually, these attacks center around getting users to unknowingly click malicious links or reveal sensitive personal information, these types of attacks prey on human error rather than attacking a network or system. As attackers continue to target users, phishing attacks become more and more complex with attackers targeting multiple users in an organization through multiple means of communication. Furthermore, phishing attempts are becoming harder and harder to distinguish from real messages as attempts become more and more sophisticated. Regarding social media, attackers often utilize a site's messaging system to target users, through means such as impersonating known individuals or organizations. These tactics can also potentially harm the public image of the organizations that attackers choose to impersonate.

Another common attack type is the Distributed Denial of Service attack, which aims to disrupt normal network operations and deny access to regularly available online resources and services. With the use of large numbers of internet access enabled devices under the control of an attacker, the target system or network can become temporarily overwhelmed by requests sent by the botnet of attacker controlled devices. Just like other websites or networks, social media websites can also be targeted by DDoS attacks.

In 2016, the internet domain name system provider Dyn, which provided services for many prominent businesses, organizations, and social media companies, was targeted by a DDoS attack. The botnet responsible for the attack was made of computers and other internet of things devices that were all infected with the Mirai malware. The Guardian reported that "Dyn estimated that the attack had involved "100,000 malicious endpoints", and the company, which is still investigating the attack, said there had been reports of an extraordinary attack strength of

1.2Tbps" (Reed, 2016). With this, the perpetrator was able to disrupt website access for users across North America and Europe. Sites such as Facebook, Twitter, Tumblr, Reddit and others were all affected by this attack.

In addition to the two attack types mentioned earlier, social media companies are susceptible to other attacks as well. Malware, ransomware, and attacks to 3rd party applications that work with social media platforms are all potential threats that social media companies must keep in mind. Because of their interconnected nature, social media companies must also be aware of potential vulnerabilities in the external systems, API's, and organizations that they interact with.

Emerging Threats

As new technologies develop, attackers have access to new methods to attack users. Arguably the biggest new threat is the use of artificial intelligence.Whether it be AI generated phishing emails, deep fakes, or more, the full capability of artificial intelligence in conducting malicious activity is yet to be discovered. Artificial intelligence gives attackers the ability to conduct larger scale attacks at an even more complex level than what is currently available. The FBI has recently made announcements urging businesses to become vigilant of the threats of artificial intelligence, particularly AI based phishing and social engineering attacks that use AI generated video, audio, or other media to trick users and employees (FBI, 2024).

With the rapid development of artificial intelligence, social media companies must develop new strategies to counter these emerging threats. Despite this, many organizations seem to not be fully prepared for the potential impacts of artificial intelligence. In May 2024, Forbes found in a survey on 700 global IT security professionals that "Around 48% of IT

decision-makers are not confident they have the technology in place to defend against AI attacks" (Kite-Powell, 2024). This suggests that organizations may still need to "catch up" to the new threat of artificial intelligence.

On a more general scale, the development of quantum computing poses potential threats to traditional encryption systems such as RSA and ECC, commonly used by social media companies and other organizations. Quantum computing processes data and operates at a much faster rate than traditional computers, which puts the validity of contemporary cyber security systems. Although these technologies have not been fully developed, they emphasize the notion that organizations must continue to improve and modernize their cybersecurity practices.

Effective Security Strategies

Companies need to be able to employ effective security strategies to ensure their company's quality and integrity. The most important and biggest thing a company can do is to make sure to implement 2-factor authentications. Two-factor authentication (2FA) is a security process that requires you to verify your identity in two ways before accessing your account or device. Typically, this means entering your password (something you know) and then providing a second form of proof, like a code sent to your phone (something you have), making it harder for unauthorized users to gain access. To a company that is working with very sensitive data, like a database with customers' information, protecting this is necessary to retain customers and uphold the integrity of the company. Something you can also do that goes hand in hand with 2-factor authentication is to make all of your employees use strong password protocols. This would include using a combination of an uppercase letter, and special symbols, and making your password at least 8 characters long. To go into more actual company protocol, the company

would need to make sure that it utilizes common security policies, these can be things like network security, email security, mobile device policies, and so much more. The last basic thing a company needs to maximize security is an effective crisis plan. Sometimes things are out of anyone's control and will cause a disruptive environment. Having a plan to get everyone back on track and minimize damages is key.

3RD Party Application Integration

What is 3rd Party Application Integration exactly? Third-party integration is when a company connects an external software or service to its systems, allowing them to work together and share data. This lets the company use features from the external software without having to create them from scratch, improving efficiency and functionality. A company could use this principle to adopt something called centralized observability. Centralized observability involves gathering and analyzing data from various IT sources into a single platform, enabling comprehensive monitoring and understanding of system performance. A company would usually download an app or software from another platform that allows this to happen. When using applications like this, it’s important to adopt zero-trust principles. A zero-trust principle is simply ensuring that everyone is never assumed to be the person they say they are, so verification is always required. This is an important principle to understand since third-party applications can be less secure if the proper steps are not followed. All interactions involving third-party applications need to be continuously monitored and logged for unusual or suspicious activity, enabling rapid detection and response to threats. With all of that said, it’s important to stay informed about the applications that you use as the company could publish an updated version with better functions, that if you aren’t paying attention, you may miss.

Education and Awareness

The last key topic to touch on is the importance of education and awareness. Employees need to stay informed about common safety measures and measures about specific software or models that the company may be using, and there are multiple great ways to achieve this. Senior management needs to be involved in any training/ education that goes on, who knows better than the people who have been working in the field for years and years? When training modules are implemented, it's important to make these interactive and not just an arrow click through multiple pages of reading. Some ways to make the training more engaging might include quizzes, polls, or even real-world scenarios. On the topic of training modules, it is important to make tailored training. If there is an obvious weakness across the company, it would make sense to tailor the training more towards that. Another thing that would be a good idea is to get assessments of individuals to individualize training, this has also proven to be very effective.

Conclusion

Ultimately, social media companies find themselves in a unique position when it comes to handling data security. They are both responsible for the protection of the personal information of millions of users and facilitating the exchange of information between users. As technologies and threats evolve, social media companies must continue to develop effective counter measures to protect users and their personal data.

References

Baek, D. S. (2023, December 10). *LinkedIn Data Breach (700m) in 2021*. LinkedIn. https://www.linkedin.com/pulse/linkedin-data-breach-700m-2021-david-sehyeon-baek--ex85c

Begeny, K. (2020, September 3). *Best practices for building an effective security awareness program*. The SHI Hub. https://blog.shi.com/cybersecurity/security-awareness-training-best-practices/

Canada, C. S. E. (2022, January 12). *Security considerations when using social media in your organization ITSM.10.066*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/security-considerations-when-using-social-media-your-organization-itsm10066

CybSafe. (2022, August 23). *10 key topics to cover in cyber security awareness training*. CybSafe. https://www.cybsafe.com/blog/ten-key-topics-in-cyber-security-awareness-training/

Defining AI hacking: The rise of ai cyber attacks. Sangfor Technologies. (n.d.). https://www.sangfor.com/blog/cybersecurity/defining-ai-hacking-rise-ai-cyber-attacks#:~:text=This%20means%20that%20AI%20is%20often%20used%20to%20generate%20false,injecting%20malware%20into%20the%20network

FBI. (2024, May 8). *FBI warns of increasing threat of cyber criminals utilizing Artificial Intelligence*. FBI. https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/fbi-warns-of-increasing-threat-of-cyber-criminals-utilizing-artificial-intelligence

Fornetix. (2022, August 31). *End-to-end encryption strategies for Social Media*. https://www.fornetix.com/articles/end-to-end-encryption-strategies-becoming-the-norm-for-social-media/

Guardian News and Media. (2018, March 17). *How Cambridge Analytica turned Facebook "likes" into a lucrative political tool*. The Guardian.

https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm

Hetler, A. (2024, April 23). *6 common Social Media Privacy Issues: TechTarget*. WhatIs. https://www.techtarget.com/whatis/feature/6-common-social-media-privacy-issues

IMI https://www.identitymanagementinstitute.org/app/uploads/2021/03/logo-.jpg. (2024, March 13). *Cybersecurity Quantum Attack*. Identity Management Institute®. https://identitymanagementinstitute.org/cybersecurity-quantum-attack/

Kite-Powell, J. (2024, July 24). *This new report looks at how to fight AI and identity fraud*. Forbes. https://www.forbes.com/sites/jenniferkitepowell/2024/05/16/this-new-report-looks-at-how-to-fight-ai-and-identity-fraud/

Newberry, C. (2024, June 13). *Social Media Security: Risks, best practices, and tools for 2024*. Social Media Marketing & Management Dashboard. https://blog.hootsuite.com/social-media-security-for-business/#:~:text=Phishing%20and%20scams,common%20type%20of%20phishing%20scam

Newberry, C. (2018, August 8). *8 Social Media Security Tips to Mitigate Risks*. Hootsuite Social Media Management. https://blog.hootsuite.com/social-media-security-for-business/

Nicko, John, & Chester. (2023, April 24). *LinkedIn data leak – what we can do about it*. Scrubbed. https://scrubbed.net/blog/linkedin-data-leak-what-we-can-do-about-it/

Log in or sign up to view. (2024). Facebook.com. https://www.facebook.com/security

Powell, L. (2023, September 18). *The Dark Side of social media: Privacy concerns and solutions*. Medium. https://medium.com/@th3Powell/the-dark-side-of-social-media-privacy-concerns-and-solutions-94ef401dd41d

Prey. (2023b, August 23). *Encrypting data: Best practices for security*.

https://preyproject.com/blog/data-encryption-101

Privacy Settings & Information | Instagram Help Center. (n.d.). Help.instagram.com. *https://help.instagram.com/196883487377501*

Reed, B. (2016, October 26). *DDoS attack that disrupted internet was largest of its kind in history, experts say*. The Guardian. https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

Safety and security. (n.d.). https://help.x.com/en/safety-and-security

Sandoval, K. (2023, December 12). *7 Practices to Secure Third-Party API Usage | Nordic APIs |*. Nordic APIs. https://nordicapis.com/7-practices-to-secure-third-party-api-usage/

Statista, (2024), Number of social media users worldwide from 2017 to 2024, Statista, Retrieved August 6, 2024, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Suresh, A. (2024, May 7). *10 best practices for Social Media Security: Pro tips*. Sprinklr. https://www.sprinklr.com/blog/social-media-security-best-practices/

The most common social media privacy issues. NordVPN. (2024, July 18). https://nordvpn.com/blog/social-media-privacy-issues/

Third party apps. Third Party Apps - Workplace - Documentation - Meta for Developers. (n.d.). https://developers.facebook.com/docs/workplace/third-party-apps/introduction/

World Economic Forum, (2024, April), Quantum computing and the future of cybersecurity, World Economic Forum, Retrieved August 6, 2024, from https://www.weforum.org/agenda/2024/04/quantum-computing-cybersecurity-risks/