Personal Data Security

Subjects: Computer Science, Information Systems

Contributor: Yohannes Kurniawan, Samuel Ivan Santoso, Regina Rolanda Wibowo, Norizan Anwar, Ganesh Bhutkar, Erwin Halim

As time goes by, information and communication technology continue to advance. Since the pandemic, the need for information and communication technology has risen to aid us in working and studying from home. One of the forms of information and communication technology is social media. Social media is where users can connect with other users in different regions, upload content as images or videos, express themselves freely, and get responses or reactions from other users (likes and comments). However, behind all those, social media can also be a place full of threats towards the personal data of its users.

Keywords: personal data ; security ; social media ; awareness ; higher education student ; information security

1. Introduction

The ongoing pandemic has changed how we perform activities or work. Everything that was previously performed directly offline is now migrating to online activities. This change triggers the need for online applications that can be used within our daily activities; these include social media. Social media can be defined as an online platform that can accommodate all forms of content in the form of images or videos sent by social media users. Most social media can be downloaded for free and can be directly used by anyone as long as they are connected to the internet.

The number of new users on social media continues to increase, as is triggered by the COVID-19 pandemic in 2019. Indonesia is one country with a fairly high number of active social media users. According to Hootsuite (We Are Social), active social media users in Indonesia in 2019 reached 130 million, or 48% penetration of the total population of Indonesia at that time, namely, 268.2 million [1]. Then, in 2022, Hootsuite (We Are Social) again uploaded data on the number of active social media users in Indonesia, which was around 191.4 million, or 68.9% of the total population of Indonesia, which was recorded as 277.7 million [2]. Both data show that the number of active social media users from 2019 to 2022 increased by 61.4 million, or around 47.2%. Other data showing the number of active social media users in Indonesia come from the Indonesia Internet Service Providers Association or *Asosiasi Penyelenggara Jasa Internet Indonesia* (APJII); the data obtained show that the internet penetration rate in Indonesia in 2021 until Q1 of 2022 reached 77%, namely, 210,026,769 people from a total population of 272,682,600 in 2021 [3]. Other data on the number of active social media users in Indonesia differentiated by age groups are 8.3% aged 0–4 years, 13.9% aged 5–12 years, 8.2% aged 13–17 years, 11.6% aged 18–24 years, 14.9% aged 25–34 years, 14.7% aged 35–44 years, 12.7% aged 45–54 years, 9.0% aged 55–64 years, and 6.8% aged 65 years and over [4]. According to APJII, the levels of active social media users in Q1 2022, if grouped by age, were 8.08% aged 5–12 years, 9.62% aged 13–18 years, 25.68% aged 19–34 years, 27.68% aged 35–54 years, and 5.97% aged 55 years and over [3].

Data obtained on the active social media users in Indonesia show that the age group that accesses social media the most is the 18–34 age group. Therefore, our research objective is higher education students who fall into this age group, being one of the groups that frequently use social media. Students use social media as a tool to find various information, or just a place to find entertainment or express themselves. However, behind those, there is a hidden threat in social media, such the theft of personal data, either intentionally or unintentionally, consciously or unconsciously. This issue raises the main concern of our research, as to whether students are aware of personal data security on social media.

Usually, identity theft on personal data occurs when the data are circulated everywhere, such as images, videos, or text written in content on social media. One case is the “Add Yours” challenge trend that went viral on Instagram Indonesia. “Add Yours” is an Instagram feature that can be used freely by its users by uploading it on their Instagram Story; if their Story is public, then other users can see it, and other users are also free to upload their own. All Instagram users can see the data collected in “Add Yours”, so many people exploit this. Then, they commit fraud by creating “Add Yours” regarding ID card photos, photos of themselves with ID cards, nicknames, addresses, mothers’ names, birth dates, and other personal data. Unfortunately, many users quickly upload the personal data mentioned earlier, and the total number of participating users can reach up to tens of millions [5].

The case mentioned above can be categorized as social engineering, because obtaining personal data involve the psychological manipulation of users who think it is a challenge or trend [6]. The case continues until financial fraud occurs, where some criminals use personal data to contact the owner and pretend to be close relatives, family, friends, or spouses. After that, the perpetrator starts to borrow money for various reasons, and finally, the victim gives the money because he believes that the acquaintance is someone close [5]. The case mentioned above has indeed occurred on

social media; other cases take the form of uploading personal data on social media in the form of pictures or videos, such as identity cards, ATM cards, house numbers, telephone numbers, places that are being occupied, and so on, which can be uploaded either intentionally or unintentionally.

Personal data security and social media are interrelated because the protection of personal data is important when using or accessing social media. Research related to this matter comes from several aspects or areas that are different from each other, and can also describe the conditions of social media users in a country. In this case, Lawrence Ryz et al. (2016) mentioned the evolution of a basic rule regarding data protection, namely, GDPR [7]. Radi Romansky (2014) discussed the challenges that can be faced by a social media company in maintaining the privacy of each of its users [8]. Users trust robots or Siri in providing personal data [9]. Gender plays a role in making choices to share personal data [10]. The use of social media in the health sector and the usage decisions of each user have been differentiated based on work function or role in the health sector [11]. Some research uses psychological factors to make a person pursue a higher level of security but pay the appropriate price for it [12]. There are factors affecting feelings of trust in social media [13], or FOMO attitudes [14].

2. Personal Data

Personal data are a part of the data that resides on a computer or mobile device [15]. According to the General Data Protection Regulation (GDPR), personal data are information about an identifiable individual. An identifiable person can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to their physical, physiological, mental, economic, cultural, or other social features [16].

Personal data that can be used directly to identify an individual can be categorized as Personally Identifiable Information (PII) [15]. Personally Identifiable Information (PII) may include name, date of birth, home address, gender, race, phone number, email address, political opinions, credit card number, health information, ID cards, IP address, and location data [16]. Hence, personal data are the main asset for social media, because they can be used for business or other developer purposes [17][18].

3. An Overview of Rules and Regulations for Personal Data Protection

Personal data security protects personal data and information from the possibility of unauthorized access, disclosure, disruption, deletion, corruption, modification, or destruction [19].

As mentioned by Sylwia Kosznik-Biernacka [20], personal data should be protected and secured based on the CIA triad:

- Confidentiality—The required degree of protection of the information against unauthorized access;
- Integrity—Data and information should be correct, intact, and not be manipulated;
- Availability—Data are available under the system or user requirements.

Related rules or regulations on personal data security are included in GDPR, a regulation in the European Union law on data protection and privacy in the European Union and the European Economic Area. Though it was originally published for the scope of the European Union, and is one of the world's toughest privacy and security laws, the regulation has had influence and become a great reference for many organizations and countries worldwide [16].

There are some related standards that discuss personal data security, such as [21] provides a way to protect valuable information using the base standard of ISMS (Information Security Management System), whereas [22], established by the ISACA (Information Systems Audit and Control Association), provides guidance or a framework for managing enterprise information and technology that supports enterprise goal achievement.

In Indonesia, on 20th September 2022, the UU PDP (*Undang-Undang Perlindungan Data Pribadi*) or local personal data protection law was officially formalized. The UU PDP aims to protect Indonesia's citizens' data and sets a standard for legally processing and maintaining data. The UU PDP was drafted based on the reference of the GDPR [23].

4. Functions and Threats for Personal Data Security Associated with the Use of Social Media

The use of social media has continued to increase since the COVID-19 pandemic; social media is used to share and get the latest information about the pandemic, such as diagnostic, treatment, hospital location, total infected, and follow-up protocols [24]. Another use of social media is to build personal branding by updating personal information. Some believe a personal brand will help them create a good reputation or career on social media [25].

In terms of personal branding, many social media users began to utilize social media as a place for them to seek fame and start their focus as a celebrity or content creator in various ways, one of which is uploading their data in the form of images, videos, or text [26]. Regarding images and videos, a study shows that visual content can increase the number of

views and likes, rather than just plain text; of course, the average image or video contains photos of the user and their activities [27], or even travel experiences [28]. The most frequent reason for a user to upload their data is the psychological need to get attention, or simply as a way to express themselves [29].

As explained earlier, personal data consist of several data types that refer to an individual. Social media users can sort out which data can be shared. Some users agree that phone numbers and home addresses are the most sensitive personal data and should not be made public, while other personal data are made public by some users [30].

Using personal data on social media can expose a person to becoming known to many people, but foremost, it poses cyber threats to users' personal data. Cyber threats may appear in the following forms [31].

A. Burglary

Robberies do not only occur online, as criminals seek victims through social media. Social media is where users can share information by posting; one example is daily activities. Criminals easily find the target they want through social media by paying attention to their daily activities. After that, the perpetrator only needs to pay attention to the valuables included in the post; then, the criminals can plan to steal the valuables.

B. Social Engineering

Social Engineering uses psychological manipulation to obtain personal data. Thus, the victim will unconsciously provide their data. Some examples include, for example, a call on behalf of a close relative or a message from a friend or relative. Usually, this type of social engineering is based on a goal that can be the theft of personal or financial information.

C. Phishing

Phishing is one of the crimes that can occur on social media. Phishing aims to trick the victim into giving their data. Phishing is usually done by sending a message to the victim containing a gift, on the condition that they provide personal data first with the reason being to verify the receipt of the gift. In addition, phishing can also take the form of a replica that resembles the address of a well-known website or institution that offers special offers or gifts to victims. Usually, phishing occurs on social media, which has the feature of allowing the sending messages either to each individual or in groups.

D. Malware

Malware is software specifically designed to damage other devices without the device owner's knowledge, and it can enter easily via attachments, messages, and links.

E. Identity Theft

Identity theft is a crime that uses someone's data for certain purposes without the permission of the owner of the personal data. Thus, any losses that may occur will be accepted by the actual owner of the information, such as losses in terms of finances, debts, loans, and so on. Social media is the best place to mine personal data because many users unknowingly upload it. One example is TikTok, a social media platform that provides short video-based content. Several TikTok videos lead to the leakage of personal data, such as the "Private school check" video, which others can use to find the user's school name and look for other information such as name, age, gender, date of birth, and address.

F. Cyber-Stalking

Stalkers in the cyber world using social media or other online media can cause irritation, harassment, and emotional anxiety in victims. Stalkers usually do not target the victim's valuables, but seek attention and commit immoral verbal acts. The stalkers will continuously see what the target is doing by looking at the posts uploaded by the target.

G. Cyber-Casing

Cyber-casing is a process used to mark or generate locations in the real world using various data types on social media. This can be done because of the features offered by social media that are intended for users who want to mark their location, perhaps while taking a picture; this feature is known as geo-tagging. Some social media already has this feature and continues to grow to the point of sharing live s, so that other users can monitor location movements using the live location feature. This threat can occur if a criminal sees and begins to mark the location points usually visited by their target, so that the perpetrator can commit a crime in the right place.

Apart from cyber-attacks that target users' data, there are other threats, such as the misuse of a person's data to attack the owner of the data on social media, such as uploading content that embarrasses or humiliates a person, tracking down a person and then physically attack the person, blackmail, bullying, discrimination, torture, commercial advertising, racism [32], and some sexual violence such as nudity content (images or videos of a person undressing), threats of rape, sex messaging, and other types of sex crimes [32][33].

5. Factors Influencing Personal Data Security Awareness

Personal data security awareness can be defined as the knowledge of security measures that can be taken to protect personal data on social media. Several things that can affect the level of awareness are age, education level, security training obtained [34], the level of psychosocial health of each user, FoMO behavior [14], or the level of user trust in social media, usually due to perceived enjoyment, benefits obtained, and status [13].

A study has been conducted to analyze user behavior in submitting personal data voluntarily; this research has concluded that users trust online agents such as robots or Siri to deliver personal data online, rather than giving it to human agents directly [9]. Another study analyzed the influence of gender on personal data security awareness and found that gender also influences the decisions made by each user to open their data [10]. Country location factors can also affect this level of awareness; this is evidenced by research conducted in Iraq and Turkey, which concluded that Iraq has a higher level of vulnerability than Turkey [35].

The security awareness level of social media users related to their data can be considered quite low due to several factors mentioned earlier. Some studies have also concluded that although younger users have a higher level of security than older users [34], there are still young users who can be quite vulnerable, because they do not know how to increase security either in general, such as using privacy settings [36], or setting strong password combinations [37]. Indonesia has a low level of security awareness amongst smartphone users, such as the results of storing important data on smartphones and installing illegal applications into them [38]. Throughout all these studies, it has been noted that there is no previous research that analyzes the level of personal data security awareness amongst higher education students (largest age group of social media users) in Indonesia. Therefore, this research will focus on analyzing the level of security awareness regarding personal data on social media amongst Indonesian students by dividing them into two types of social media users—active users (someone who actively create and shares content/information in the form of photos, videos, text, or other things that can be loaded on social media) and passive users (someone who spends time on social media looking for information, contacting relatives, friends, or entertain themselves) [39].

References

1. Hootsuite (We Are Social): Indonesian Digital Report 2019. 2019. Available online: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2019/ (accessed on 29 October 2022).
2. Hootsuite (We Are Social): Indonesian Digital Report 2022. 2022. Available online: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2022/ (accessed on 29 October 2022).
3. Hasil Survei Profil Internet Indonesia 2022. 2022. Available online: https://apjii.or.id/content/read/39/559/Laporan-Survei-Profil-Internet-Indonesia-2022 (accessed on 29 October 2022).
4. Data Digital Indonesia Tahun 2022. 2022. Available online: https://www.kompasiana.com/andidwiriyanto/620fe14651d76471ad402f76/data-digital-indonesia-tahun-2022?page=1&page_images=1 (accessed on 29 October 2022).
5. Tren Baru Challenge Share Instagram Ternyata Berbahaya Penipuan? Waspada Bagikan Data Pribadi! 2021. Available online: https://kuyou.id/homepage/read/27591/tren-baru-challenge-share-instagram-ternyata-berbahaya-penipuan-waspada-bagikan-data-pribadi (accessed on 29 October 2022).
6. Social Engineering, Ancaman Manipulasi Psikologis di Balik IG Story Add Yours. 2021. Available online: https://kumparan.com/kumparannews/social-engineering-ancaman-manipulasi-psikologis-di-balik-ig-story-add-yours-1wyWX9hcPJR (accessed on 29 October 2022).
7. Ryz, L.; Grest, L.; Ontrack, K. A New Era in Data Protection. Comput. Fraud Secur. 2016, 2016, 18–20.
8. Romansky, R. Social Media and Personal Data Protection. Int. J. Inf. Technol. Secur. 2014, 6, 65–80.
9. Sundar, S.S.; Kim, J. Machine Heuristic: When We Trust Computers More than Humans with Our Personal Information. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow, UK, 4–9 May 2019.
10. Lina, X.; Wang, X. Examining gender differences in people's information-sharing decisions on social networking sites. Int. J. Inf. Manag. 2020, 50, 45–56.
11. Pianese, T.; Belfiore, P. Exploring the Social Networks' Use in the Health-Care Industry: A Multi-Level Analysis. Int. J. Environ. Res. Public Health 2021, 18, 7295.
12. Mahmoodi, J.; Curdova, J.; Henking, C.; Kunz, M.; Matic', K.; Mohr, P.; Vovko, M. Internet Users' Valuation of Enhanced Data Protection on Social Media: Which Aspects of Privacy Are Worth the Most? Front. Psychol. 2018, 9, 1516.
13. Sundaram, A. Social media security and privacy protection concerning youths. 'How to be safe, secure and social'. Int. J. Bus. Innov. Res. 2019, 18, 453–471.
14. Reer, F.; Tang, W.Y.; Quandt, T. Psychosocial well-being and social media engagement: The mediating roles of social comparison orientation and fear of missing out. New Media Soc. 2019, 21, 1486–1505.

15. Rodgers, N.S. Understanding Personal Data in the World of Social Media. Undergraduate Honors. Program Thesis, Utah State University, Logan, UT, USA, 2020.
16. General Data Protection Regulation. GDPR.eu. 2016. Available online: https://www.gdpreu.org/the-regulation/key-concepts/personal-data/ (accessed on 8 November 2022).
17. Borzykh, P. Concept of Personal Data in Social Media Environment: Effect of General Data Protection Regulation and Trade Secrets Directive. 2022. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105982 (accessed on 8 November 2022).
18. Tskhovrebashvili, N. Economic and Social Exchange of Personal Data and the Risks of Their Protection. Vectors Soc. Sci. 2021, 1, 53–68.
19. National Institue of Standards and Technology. nist.gov. US Government. Available online: https://csrc.nist.gov/glossary/term/infosec (accessed on 8 November 2022).
20. Kosznik-Biernack, S. The Analysis of Risks to Personal Data Security. Secur. Dimens. 2020, 34, 256–267.
21. ISO. 2022. Available online: https://www.iso.org/isoiec-27001-information-security.html (accessed on 8 November 2022).
22. ISACA. isaca.org. 2019. Available online: https://www.isaca.org/resources/cobit#:~:text=COBIT%202019%20is%20a%20framework,that%20supports%20enterprise%20goal%20ach (accessed on 8 November 2022).
23. Hasanah, M. Viva Tekno. Viva News. 21 September 2022. Available online: https://www.viva.co.id/digital/digilife/1523677-membandingkan-sanksi-pada-uu-pdp-dan-gdpr-uni-eropa#:~:text=Dalam%20pembuatannya%20regulasi%20ini%20mengacu%20pada%20General%20Data,landasan%20hukum%20terkait% (accessed on 8 November 2022).
24. González-Padilla, D.A.; Tortolero-Blanco, L. Social media influence in the COVID-19 Pandemic. Int. Braz. J. Urol. 2020, 46, 120–124.
25. Vițelar, A. Like Me: Generation Z and the Use of Social Media for Personal Branding. Manag. Dyn. Knowl. Econ. 2019, 7, 257–268.
26. Al-laymoun, O.H.; Aljaafreh, A. Examining Users' Willingness to Post Sensitive Personal Data on Social Media. Int. J. Adv. Comput. Sci. Appl. 2020, 11, 451–458.
27. Li, Y.; Xie, Y. Is a Picture Worth a Thousand Words? An Empirical Study of Image Content and Social Media Engagement. J. Mark. Res. 2019, 57, 1–19.
28. Oliveira, T.; Araujo, B.; Tam, C. Why do people share their travel experiences on social media? Tour. Manag. 2020, 78, 104041.
29. Sutarno, K.; Estadimas, B.; Taliya, A.; Wardoyo, D.; Hapsari, I.C.; Hidayanto, A.N. Factors Influencing User Intention in Opening Personal Data on Social Media. In Proceedings of the 2020 Fifth International Conference on Informatics and Computing (ICIC), Gorontalo, Indonesia, 3–4 November 2020.
30. Cain, J.A. How Much for My Name? Privacy Perceptions and Motivations for Sharing Personal Information on Social Networking Sites. J. Soc. Media Soc. 2021, 10, 140–161.
31. Soomro, T.R.; Hussain, M. Social Media-Related Cybercrimes and Techniques for Their Prevention. Appl. Comput. Syst. 2019, 24, 9–17.
32. Kröger, J.L.; Miceli, M.; Müller, F. How Data Can Be Used Against People: A Classification of Personal Data Misuses. 2021. Available online: https://ssrn.com/abstract=3887097 (accessed on 8 November 2022).
33. Pendergrast, T.R.; Jain, S.; Trueger, N.S.; Gottlieb, M.; Woitowich, N.C.; Arora, V.M. Prevalence of Personal Attacks and Sexual Harassment of Physicians on Social Media. JAMA Intern. Med. 2021, 181, 550–552.
34. Koyuncu, M.; Pusatli, T. Security Awareness Level of Smartphone Users: An Exploratory Case Study. Mob. Inf. Syst. 2019, 2019, 2786913.
35. Cengiz, A.B.; Kalem, G.; Boluk, P.S. The Effect of Social Media User Behaviors on Security and Privacy Threats. IEEE Access 2022, 10, 57674–57684.
36. Padmavathi, D.J.; Mohanlal, S.A.K. A Study on Extent of Awareness Among College Students in Security and Privacy Issues in Social Media. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. 2021, 7, 676–682.
37. Alqahtani, M.A. Factors Affecting Cybersecurity Awareness among University Students. Appl. Sci. 2022, 12, 2589.
38. Amin, M.; Tasmil; Herman; Bahrawi; Alam, N.; Dhahir, D.F.; Hadiyat, Y.D. Security and privacy awareness of smartphone users in Indonesia. J. Phys. Conf. Ser. 2021, 1882, 012134.
39. Verduyn, P.; Gugushvili, N.; Massar, K.; Täht, K.; Kross, E. Social comparison on social networking sites. Curr. Opin. Psychol. 2020, 36, 32–37.