Misuse of Facebook user data

Leonel Hernández [a,1,*], Tri Juniarti Fatimah [b,2], Petrus Jack Fautngilyanan [b,3], Sayed Rahman Hamid [b,2], Setya Rahadi Pramudhita [b,3], Triyanti Simbolon [b,2]

[a] Instituciòn Universitaria ITSA, Carrera 45 # 48 -31, Barranquilla, Colombia
[b] Department of Electrical Engineering, Universitas Negeri Malang, Malang, Indonesia
[1] lhernandezc@itsa.edu.co*; [2] tri.juniarti.1805356@studens.um.ac.id; [3] jackfautngilyanan.1805356@studens.um.ac.id;
[4] sayed.rahman.1805356@studens.um.ac.id; [5] rahadisetya69@gmail.com; [6] triyanti.simbolon.1805356@studens.um.ac.id
* corresponding author

ARTICLE INFO

Article history
Received December 16, 2020
Revised January 9, 2021
Accepted January 23, 2021

Keywords
Facebook
Social media
Personal data
Misuse

ABSTRACT

Nowadays, we live when technological developments have developed rapidly, especially in the communications and information sector. One of the triggers is social media, including Facebook. In 2010, there were around 24 million Facebook users in Indonesia. In building social relationships, of course, personal information is needed from someone. The same is the case when using social media. When you want to create a Facebook account, users will be asked to provide various personal data. This functions so that users can recognize one another. Besides that, it can also help Facebook in securing user accounts. But by sharing personal data will undoubtedly pose a risk of being misused. Apart from data leaks due to Facebook's shortcomings, this is also inseparable from users' negligence in safeguarding their data. This research explores the unawareness of Facebook users in protecting their data. This research will show the consequences of a lack of attention in maintaining personal data and show how to protect personal data to increase the awareness of Facebook users in safeguarding their data.

1. Introduction

During the last decade, the Internet, particularly online news service and social media networks, have been the dominant information-sharing channels. In social media's large groups, they share similar interest forms networks that create mutual trust among the network members. information coming from a network member is accepted and propagated by the group members without much criticism. Such a free environment to make the users vulnerable and express their opinions also reveals some personal data. Third parties may collect such personal information, process it, and use it for their purposes. Advertising agencies and political parties are willing to use personal information to convince or convert individuals [1].

Social media networks create an ever-increasing array of functionalities for users to connect to make the most convenient forms of communication [2]. Facebook is one of the most popular social media platforms, with over 300 million registered users [3]. There are some benefits of using Facebook. First, Facebook was created to facilitate the exchange of knowledge among teenagers [4]. Second, Facebook is often used as a teaching and learning tool in the classroom [5]. There are 7,6 billion people on Earth, and 4,2 billion uses the Internet, which means that more than half of all Internet users are on Facebook, or to be more exact, 1/3 of the world population is on Facebook [6].

From Facebook, users can also show their identity freely for others to know more about them. However, regarding showing personal information in detail, cybercriminals will easily retrieve and misuse users' information data if users do not maintain the privacy of personal information. Cybercriminals have more opportunities to carry out their illicit activity with the exponential rise of

https:doi.org/10.31763/businta.v5i1.411

online social networking sites [7]. Hence the freedom of expressing an opinion and spreading information may be misused to propagate rumors, gossip, and misleading or false information. The question, whether such interventions affect public opinion or not is still an open debate. An information system such as TV, newspaper, blogs on the evolution of public opinion is studied.

While it is fun to share information on Facebook, it also necessitates a great deal of protection and privacy [8]. Also, the analysis of the frequency of interaction is considered. It is also shown that to use/support some concepts which are valuable or very sensitive for the society, such as religion, nationality, cultural issues, collective beliefs, can also make a profit for politicians and even the ideas adopted by the minority of the society can be supported by the majority, after such a process. Although social studies still do not have clear evidence on the influence of such misleading information flow on social preferences, false news propagation is faster and broader than the spread of true news due to the attractiveness of the false news.

Like the previous incident related to the scandal on Facebook, one of Facebook's largest-ever data leaks is the data analytics firm that partnered with Donald Trump's election team and the victorious Brexit campaign gathered millions of US voter profiles and used them to create a powerful software program to forecast and manipulate voting decisions.

2. Misuse of User Data: A literature Review

2.1. Facebook

With the advancement of technology and the proliferation of content, Facebook has become a popular social networking platform across many people. In 2010, Indonesia had approximately 24 million Facebook users, accounting for 10% of the country's total population. Facebook has evolved into a modern platform for self-presentation [9].

Users' motivations for using Facebook, privacy settings and self-disclosure, and satisfaction with Facebook's ability to fulfill their motivating needs are all critical factors [10]. In Indonesia, teenagers are among the most active users of social media. The initial impetus for them to become so involved on social media is to attract publicity, elicit input, and show their profile. However, they grow addicted to social media consumption in the long run. They can't keep away from social media events. Also, users did not consider the implications of their daily actions until they were reminded of their information's public audience, such as receiving unwelcome messages from strangers [11]. While social media has a positive side to be consumed in general, excessive use of social media has a detrimental effect. A significant number of studies have shown that teenagers' excessive use of social media leads to an uptick in self-concept incongruence when the true self and the ideal self are too far apart [12]. People who used social media to satisfy their social needs and affection were more likely to use Facebook.

Because of this influence, teens rapidly post personal information on social media networks without fully comprehending any risk involved [13]. A development that is undoubtedly fueled by the advancement of the channels they use and shifting social norms. In terms of type and purpose, a typical teen's MySpace profile in 2006 was very distinct from the 2006 edition of Facebook and the Facebook profiles that have become a staple of adolescent life today [14].

Constantly disseminating personal data, it has become unconcerned with privacy. According to a study conducted by University of Iowa researchers, some third-party Facebook applications could be misusing their users' records. The study found that specific applications could be using their users' data for malware, malware, and targeted ads without their permission [15].

They believe Facebook to be a secure computing network, but this is not always the case. For example, hackers can create fake accounts or clone user accounts to steal personal users' data[13].

Also, the revelations that organizations collected user data for targeted ads, especially political advertising, with apparent success culminated in a decade of apparent indifference to data privacy at Facebook. Although Cambridge Analytica, the political consultancy and strategic communication company behind the pro-Brexit Leave EU movement, is the most well-known perpetrator, some organizations have most likely used similar strategies to gather personal data from Facebook users, including Donald Trump's 2016 presidential campaign [16].

Part of the problem is that, in 2011, Facebook told the Federal Trade Commission (FTC) in the United States that it would not exchange user data without their express permission [17]. Facebook CEO Mark Zuckerberg has since maintained that he first heard of CA from a December 2015 Guardian report breaking the news that Ted Cruz's presidential campaign was using psychological evidence focused on studies involving tens of millions of Facebook members, largely without their knowledge [18].

It is common knowledge that Facebook is not the most wholesome brand in social media. The company's downward spiral can be traced in part to the Cambridge Analytica fiasco. User data are manipulated by a particular party to influence elections in the United States at the time [19]. Therefore, another explanation that privacy standards aimed at social media sites are sometimes mistaken is that it is unlikely for the social media business to violate your privacy in the social media sense. However, social media network administrators are not specifically liable for privacy invasions caused by users. Current regulations that were structured to shield Internet service providers provide them with broad exemptions from contributory liability.

2.2. Use of Privacy Settings

The most often used privacy security techniques were excluding personal information, private email addresses, and changing the default privacy settings [20]. However, there are several ways to protect user privacy data. Although they do not guarantee it is protected, it can minimize misuse of Facebook user data. If users aren't on Facebook, Facebook can still gather a lot of information about the Facebook user. Hundreds of thousands of apps, websites, and other services submit reams of data on what Facebook users are doing on the Internet to the firm. Facebook maintains a copy of the data and will continue to use it for analytics reports and detailed success measurements for the competition.

It's also essential to protect the user's Facebook location. Facebook user's phone location services settings power the most reliable source of location data on Facebook. If a user disables their location access in the Facebook app, the information available to the company would be less precise.

Users of iPhones will go through their phone's Settings, Privacy, Location Services, and then Facebook. Then choose between "When Using the App" and "Never." Go to the Location section of their phone's settings for Android phones and press App access to location and Facebook. Then choose between "Allow only when using the app" and "Deny." These directions can differ somewhat depending on the type of phone that Facebook users have. Look for a Permissions menu on older phones.

The Facebook Login feature allows you to sign in to other websites and applications quickly and easily. However, as previously said, Facebook gains access to a little more of your personal information in return. It will also allow organizations that offer outside services access to account information, such as the name, profile, email address, and other information ordinarily available to the public. On a computer, a Facebook user can go to Settings and Privacy on the down arrow in the top right of the Facebook home, then Apps and Websites, Active, click the box next to the app's name, then Remove.

Using two-factor authentication is a good idea to secure Facebook user login operation and database. This is especially important if a user ever used the same password for several accounts or a Facebook user has a bad habit of using weak passwords. When users enable two-factor authentication in their Facebook settings, the organization will give them a verification code by text or app to prove their identity. When users enable two-factor authentication in Facebook's settings, the company will provide users a verification code via text or app to validate their identity when they log in from an unknown location, smartphone, or browser. Users can take advantage of some of the privacy rules available on Facebook and reduce activities that show or display detailed user personal data.

3. Method

The research approach used in this writing is juridical-normative research. It is a scientific procedure to find truth based on scientific logic from the normative side, whose object is the law itself. The study is focused on identifying and studying the norms or norms in a positive direction.

The use of this type of juridical-normative research in this study can be seen from two aspects, namely from the juridical and normative aspects where this research tries to examine the juridical review of the abuse of personal data on social media. Meanwhile, it is trying to analyze the problems in the rules or norms from the normative aspect.

Based on the type, the type of data used in this study is quantitative data. The data were obtained from the data collection techniques used during the research process. Based on the source, this study uses primary data. The data was obtained from the data collection techniques used during the research process. The data collection technique used in this quantitative research is data collection using a questionnaire (questionnaire). The questionnaire (questionnaire) is a data collection technique carried out by giving questions or written statements to respondents to be answered.

Data analysis was carried out by interpreting the data that had been collected. In its use consists of several stages. The first is data reduction. Data reduction is made by summarizing, selecting the main things, and focusing on essential things that support the success of the research. The second stage is the presentation of the data; in this stage, the researcher compiles a collection of information so that it is possible to conclude. The last stage is completing; in this stage, the researcher concludes the findings in descriptions or descriptions based on data that has gone through the analysis process.

Review analysis in this research uses a questionnaire or survey used as a research sample that represents the population determined by the author. The difference between people and sample is that the population is the entire population, while the sample represents it. In this research, review analysis is being used to see what testing has been conducted and what approaches have been suggested to solve a problem.

4. Results and Discussion

The Facebook user sample survey was split into demographic profile and awareness to protect personal data.

4.1. Demographic Profile

The first section aims to collect demographic profile data from participants since there are so many Facebook users that only some data can be sampled.

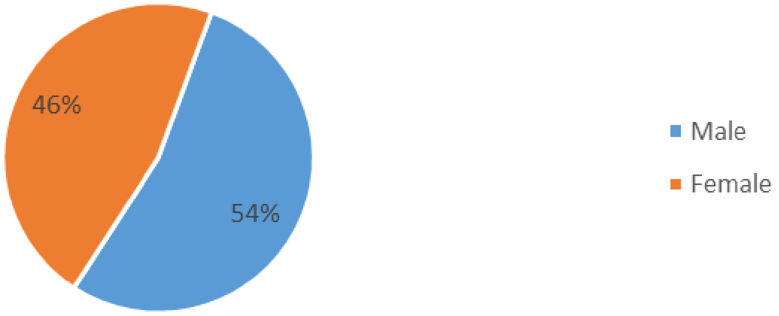

Fig. 1. Gender

Fig. 1 shows the frequency of Facebook use obtained from 28 respondents for questions about gender that Facebook users are mostly male with a percentage of 54%. The remaining 46% are women. However, based on this comparison, there is no significant difference between male Facebook users and female Facebook users, shows that using social media in Indonesia, especially Facebook is not related to gender. Both men and women all using Facebook simultaneously means that negligence in securing personal data does not necessarily occur because someone is male or female. Therefore, the objectives of this study will not be related to the gender of the user. All have the same opportunity to be negligent in safeguarding their data, not as male Facebook users or female Facebook users, but as Facebook users. Thus, negligence in protecting personal data occurs due to the lack of awareness of Facebook users regardless of gender.

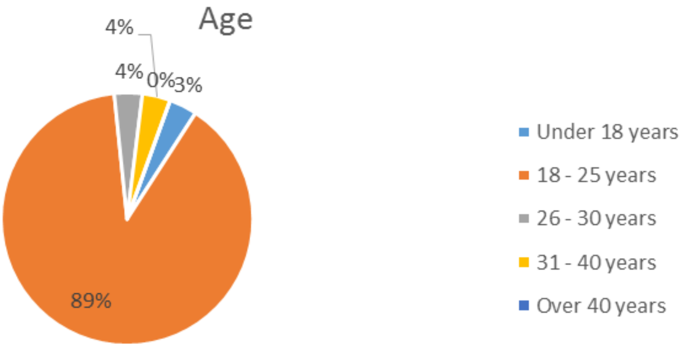

Fig. 2. Age

Fig. 2 shows the frequency of Facebook use obtained from the results of questions from 28 respondents about age, that most Facebook users are 18 to 25 years old with a percentage of 89%. Other Facebook users, namely those under 18 years old, are 3%, 26 to 30 years old there is 4%, 31 to 40 years old there is 4%, the remaining 0% are Facebook users who are over 40 years old. Based on this comparison, it appears that there is a big difference between the number of Facebook users of all ages. Adolescents, especially those between 18 and 25 years, are the most significant Facebook users among Facebook users of other generations. This shows that using social media in Indonesia, especially Facebook, is reasonably related to age. Therefore, the target of this research is Facebook users whom teenagers dominate. Negligence in securing personal data may be related to the awareness of teenagers using Facebook. All Facebook users may have an equal chance of neglecting to safeguard their data. However, people of other ages will not be able to ignore maintaining personal data because previously, they did not use social media, especially Facebook. Thus, negligence in safeguarding personal data occurs due to the lack of awareness of Facebook users, which may be related to a person's age.

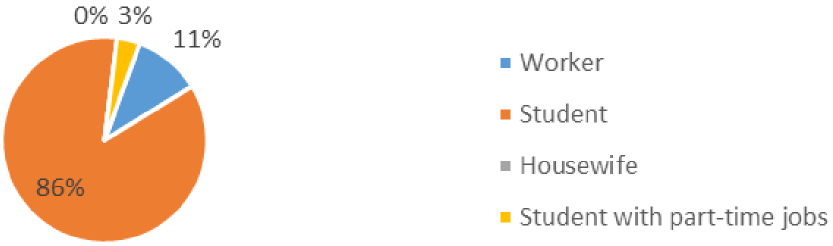

Fig. 3. Profession

Fig. 3 shows the frequency of Facebook use obtained from the results of questions from 28 respondents about the profession, that most Facebook users are students with a percentage of 89%. 11% of other Facebook users are workers, 0% are housewives, the remaining 3% are Facebook users who are students with part-time jobs. Based on this comparison, it appears that there is a significant difference between the number of Facebook users by profession. Students are the most influential Facebook users among Facebook users of other occupations, shows that using social media in Indonesia, especially Facebook, is reasonably related to the profession. Therefore, the target of this study is Facebook users whom students dominate. Negligence in securing personal data may be associated with the awareness of students using Facebook. All Facebook users may have the same opportunity to bypass their data security. However, people of different professions will not have the chance to neglect their data because they previously did not use social media, especially Facebook. Thus, negligence in safeguarding personal data occurs due to the lack of awareness of Facebook users related to one's profession.

4.2. Awareness to Protect Personal

Table 1 aims attempts to shows the value of how many Facebook users have used strategies to protect their data. We asked the respondents fifteen questions regarding this topic: Do you read Facebook's privacy policy? Do you use a VPN every time you use Facebook? Do you show your location? Have you used the setting and privacy features of Facebook? The content of your Facebook account is? , etc. All of the questions can be seen in Table 1.

Table.1 Shows the general use of Facebook user

Question	Answer	Quantity	Mean	Median	Modus	Varian
Do you read Facebook's privacy policy?	Yes	12	15,3333	14	B	17,3333
	Read a little	20				
	No	14				
Total		46				
Do you show or write the information of your details on Facebook publicly?	Yes	3	20	27	B	240,3333
	Some little	32				
	Never	27				
Total		62				
Do you use a VPN every time you use Facebook?	Always	0	9,33333	1	C	234,3333
	Some	1				
	No	27				
Total		29				
Do you show your location?	Always	6	13,66667	17	C	44,3333
	Sometime	18				
	Never	17				
Total		41				
Do you click on the links or ads on your Facebook timeline?	Always	24	26	12	B	1424
	Often	80				
	Rarely	0				
	Never	0				
Total		104				
Do you use security strategies to protect your data on Facebook?	Always	32	18,25	17,5	A	121,5833
	Often	21				
	Rarely	14				
	Never	6				
Total		105				
Have you used the setting and privacy features of Facebook	Always	39	19,333	11	A	292
	Sometime	8				
	Never	11				
Total		54				
The content of your Facebook account is	Safe	15	17	15	B	67
	With restriction	26				
	Public	10				
Total		51				
You track the log of your Facebook profile activity :	Once a week	0	10	11	D	75
	1 – 2 times a month	6				
	Once a month	16				
	Never	18				
Total		40				
You monitor, or customize, your new section :	Once a week	1	21,75	7	D	1154,25
	1 – 2 times a month	1				

Question	Answer	Quantity	Mean	Median	Modus	Varian
	Once a month	13				
	Never	72				
Total		99				
Do you connect your Facebook account to other social media accounts?	Always	2	19	9	B	559
	Sometime	46				
	Never	9				
Total		57				
Are you worried if other people on Facebook don't know about your situation?	Always	0	9,75	9,5	D	66,91
	Often	9				
	Rarely	10				
	Never	20				
Total		39				
Do you connect your Facebook account to other social media accounts?	Almost all	4	17,333	16	B	197,333
	Some	32				
	No	16				
Total		60				
Do you log into a website using your Facebook account?	Always	1	21,5	14	C	664,333
	Often	4				
	Rarely	57				
	Never	24				
Total		86				
Log into Facebook using Two-Factor Authentication.	Yes	16	18	18	B	8
	No	20				
Total		36				

Table 1 shows that if the total value of each question is calculated to an average value of 60.6. It suggests that most Facebook users still do not comprehend the necessity of safeguarding data privacy on their Facebook accounts to avoid misuse of Facebook user data, as seen in the Table 1. As a result, they have not fully protected their personal information. The second section attempts to shows the value of how many Facebook users have used strategies to protect their data.

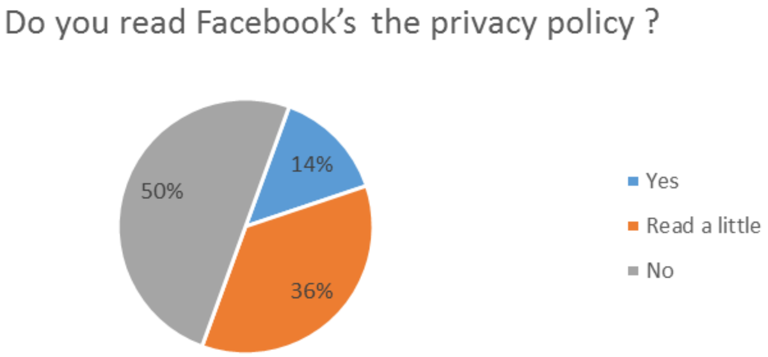

Fig. 4. Facebook User Awereness' Privacy Policy'

Fig. 4 shows that 14% of Facebook user read the Privacy Policy of Facebook, 36% read a little, and 50% do not read. Most Facebook users do not read the Privacy Policy of Facebook, but some have read it briefly. Reading the privacy policy on Facebook is very important to read and must be considered before using it on Facebook because there are several provisions such as providing an understanding of the extent to which user data is protected and Cookies policy.

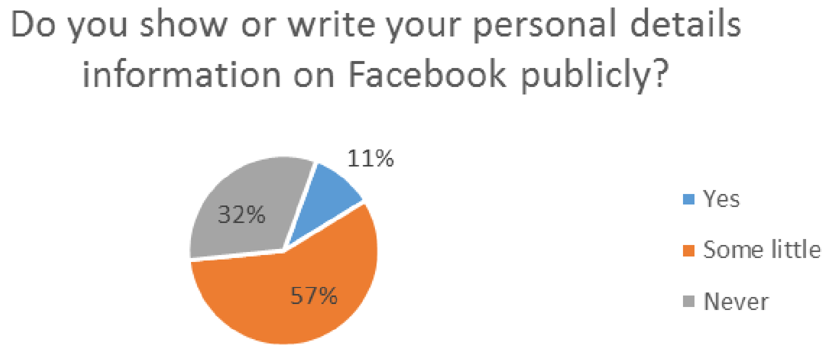

Fig. 5. Facebook User Awereness' Personal Details Information'

Fig. 5 shows that 11% of Facebook users show or write their personal detail information publicly, 57% sometimes, and 32% never do. Most Facebook users show or report personal details information on Facebook publicly. Not all user information data must be shown on social media, especially Facebook. We recommend that users continue to sort out which information data is allowed to be delivered, which cannot be directed to the Facebook account publicly.

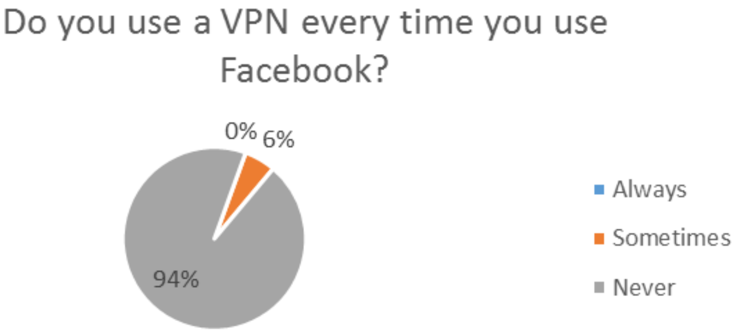

Fig. 6. Facebook User Awereness' Use a VPN'

Fig. 6 shows that 0% of the Facebook user always use a VPN every time log in Facebook, 6% sometimes, and 94% never do. Most Facebook users never use a VPN to log in to Facebook. The use of a VPN has several benefits: it encrypts users 'internet traffic, keeps users' online activities from surveillance, and allows users to browse in privacy. This can maintain user privacy every time they access Facebook using a VPN. Although this is not sure to protect, it can prevent user privacy surveys every time they access Facebook using a VPN.

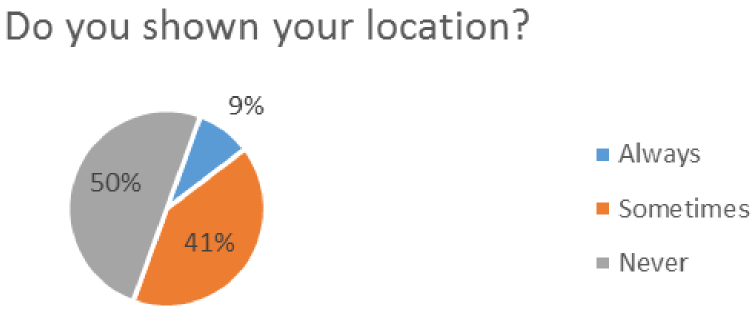

Fig. 7. Facebook User Awereness' Shown Location'

Fig. 7 shows that 9% of the Facebook user always shown their location, 41% sometimes, and 50% Never do. Facebook users showed their place, but most have it for a while. Maintaining location information is very important because it prevents other people from monitoring user activity.

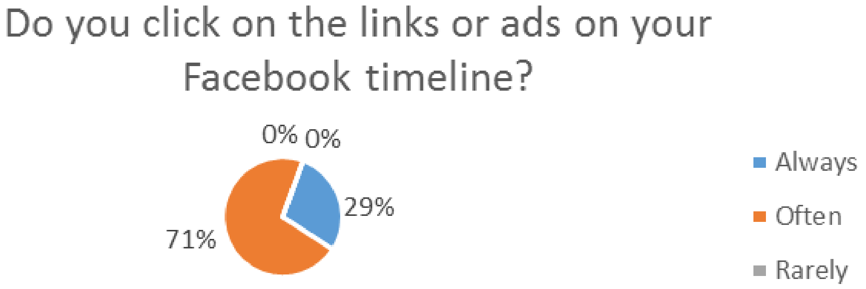

Fig. 8. Facebook User Awereness' Link or Ads'

Fig. 8 shows that 29% of the Facebook user always click on links or ads on Facebook timeline, 71% often, 0% rarely, and 0% never do. The Facebook users always click on the links or ads on Facebook timelines, but most have it often. Most Facebook users have already clicked on a link or ads from their home page. It is advisable to never click on links or ads from the home page because it prevents information data theft through the links or ads.

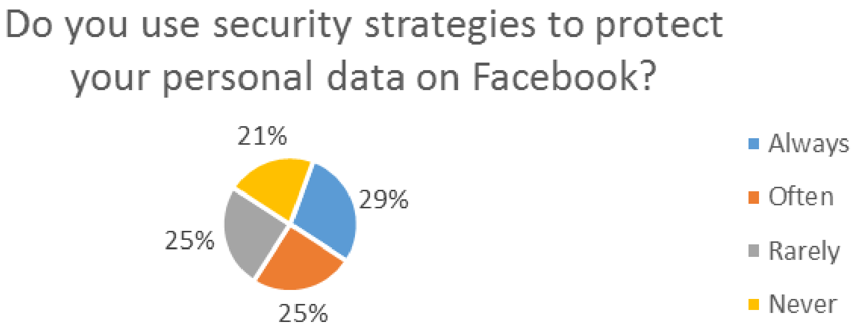

Fig. 9. Facebook User Awereness' Security Strategies'

Fig. 9 shows that 29% of the Facebook user always use security strategies to protect their data on Facebook, 25% often, 25% rarely, and 21% never do. The diagram above shows that many people have used strategies to protect their data. Because personal data protection is not a minor issue, it is better to protect users' data, such as securing accounts, not displaying detailed personal information, monitoring login activities, etc.

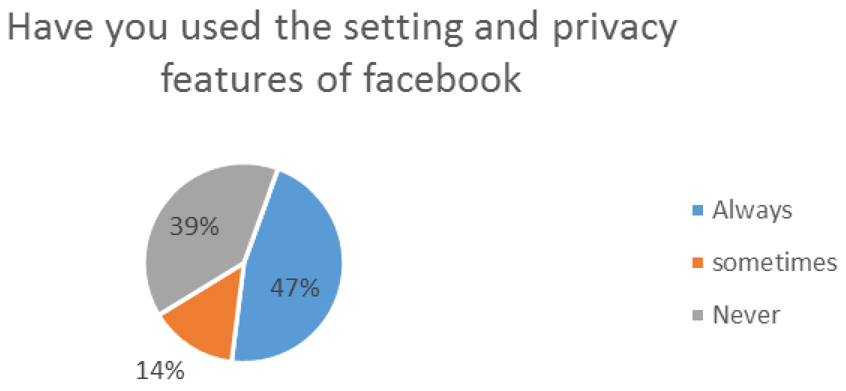

Fig. 10. Facebook User Awereness' Setting and Privacy Features'

Fig. 10 shows that 47% of the Facebook user continuously use the setting and privacy features, 14% sometimes, and 39% never have. Some Facebook users used the setting and privacy features, but some others never use them. Users must take advantage of existing security systems and settings in Facebook's features to protect their data.

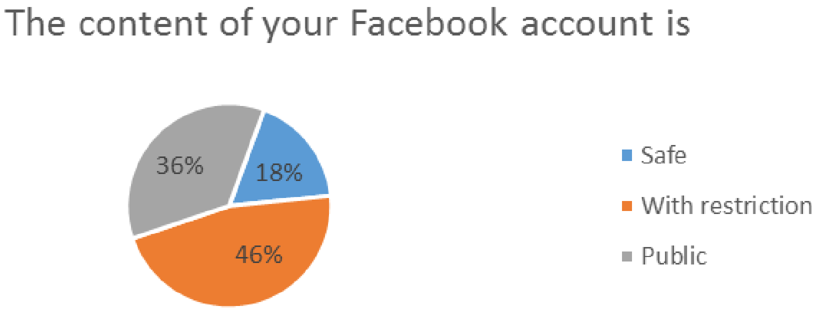

Fig. 11. Facebook User Awereness' Content'

Fig. 11 shows that 18% of the Facebook user safe their Facebook content, 46% with restriction, and 36% public. Most Facebook user save their Facebook content. Content on Facebook accounts for users is better not shown to the public but safely or with restriction. This is to prevent the theft of personal information from users.

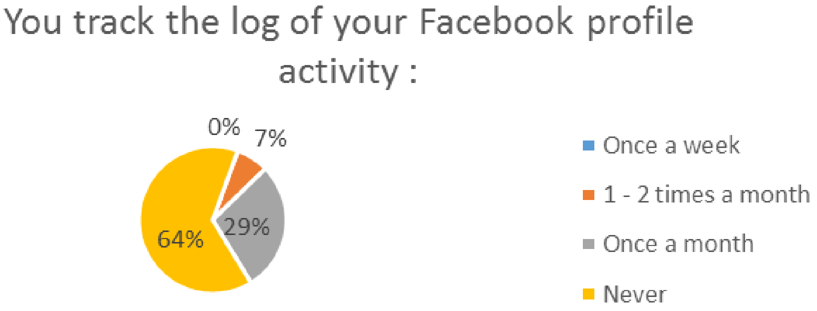

Fig. 12. Facebook User Awereness' Track'

Fig. 12 shows that 0% of the Facebook user track their profile activity, 7% track for 1 or 2 times a month, 29% once a month, and 64% Never do. Most Facebook users never track their profile activity. This indicates that 64% or most Facebook users do not monitor their login profile account activity. This is very important if to prevent misuse of personal data because users monitoring login profile activities can prevent cybercriminals from trying to log in using user accounts.

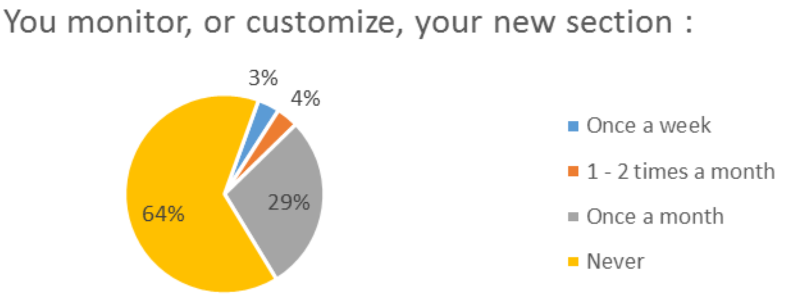

Fig. 13. Facebook User Awereness' New Section'

Fig. 13 shows that 3% of the Facebook user monitor or customize their new section, 4% do it 1 or 2 times a month, 29% one a month, and 64% never do. The most Facebook user never monitor or customize their new section. Most of the users did not have to watch and are not customizing their new page. It is recommended that users always observe and adjust their page to prevent showing their data on their Facebook account.

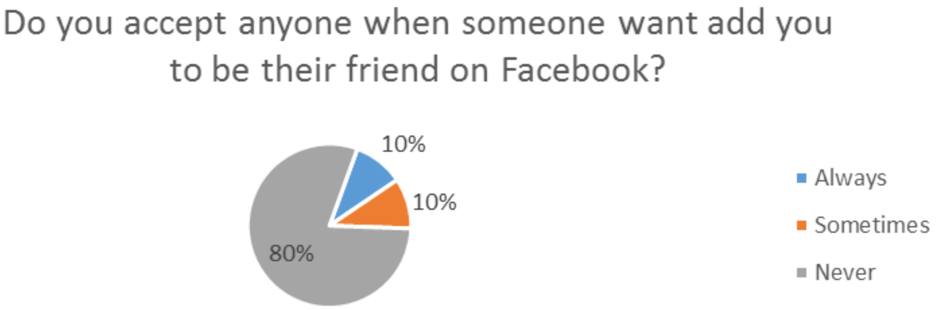

Fig. 14. Facebook User Awareness 'Accept Anyone'

Fig. 14 shows that 10% of the Facebook user accept anyone when someone adds them as a friend on Facebook, 10% sometimes, and 80% never do. Most Facebook users never take when someone adds them as a friend on Facebook. When a stranger or an unknown person adds a user to their friend on Facebook, it is better not to accept it because it prevents them from tracking activity or user accounts through friends unless they have set the security of their personal information to protect their data.

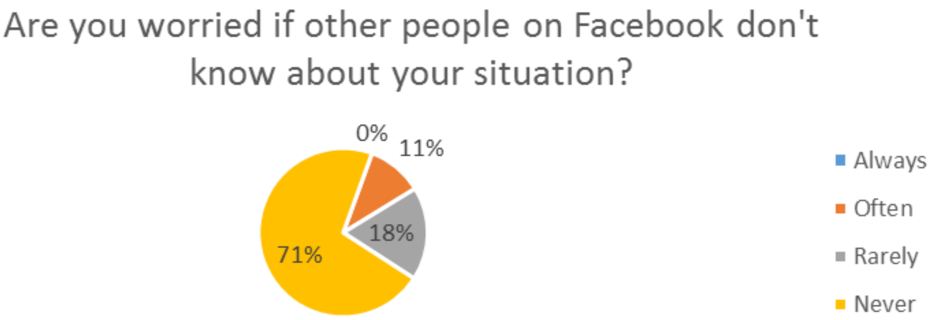

Fig. 15. Facebook User Awareness 'Worried'

Fig. 15 shows that 0% of the Facebook user always worried if other users do not know about their situation, 11% often, 18% rarely, and 71% never concerned. Most Facebook users never worried if other users do not know about their situation. This is pretty good because not everyone should know what users are doing. Moreover, to show obvious information on what the user is doing now.

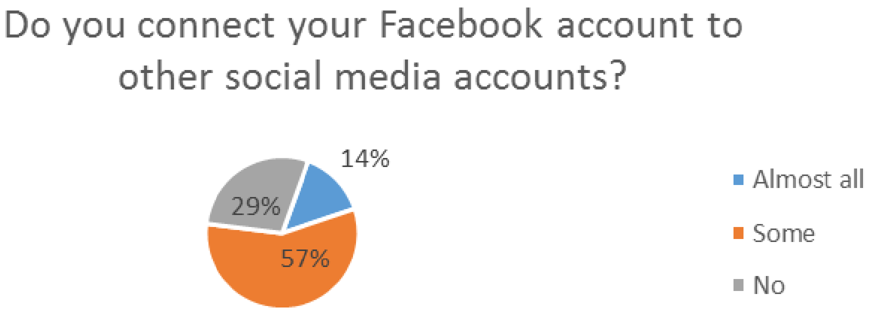

Fig. 16. Facebook User Awereness' Connect to Others'

Fig. 16 shows that 14% of the Facebook user connect their Facebook account to almost all of their social media accounts, 57% to some social media accounts, and never do. It is better to log in to other social media. It is better not to use a Facebook account because it prevents theft of personal data through JavaScript trackers or the like.

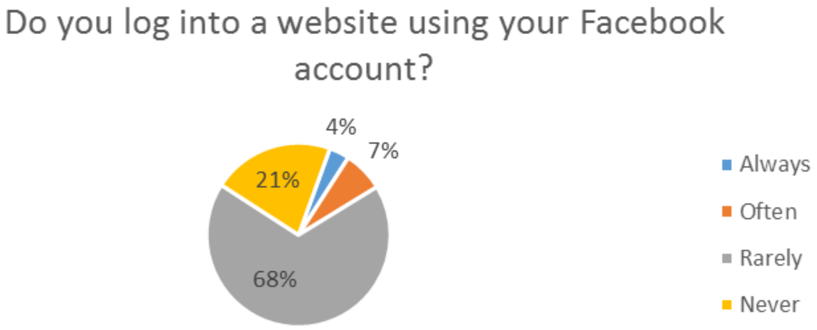

Fig. 17. Facebook User Awereness' Log In Using Facebook'

Fig. 17 shows that 4% of the Facebook user always log into a website with their Facebook account, 7% often, 68% rarely, and 21% never do. Like not using Facebook to log in to other social media, websites are also not recommended to log in using a Facebook account because it prevents data theft from happening through the website.

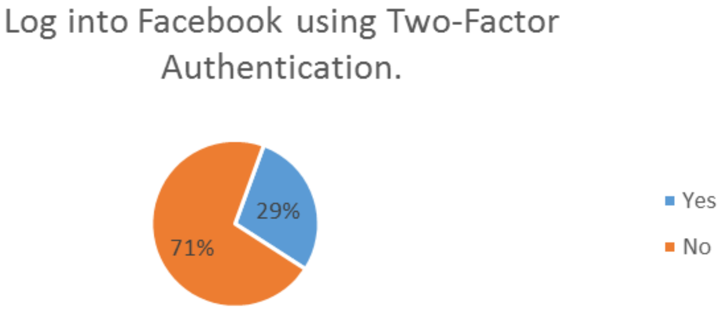

Fig. 18. Facebook User Awereness' Two-Factor Authentication'

Fig. 18 shows that 29% of Facebook users log in with Two-Factor Authentication, and 71% never log in. Most Facebook users never log in with Two-Factor Authentication. It can be seen from these data that most Facebook users do not use Two-Factor Authentication to log in to their Facebook account. Two-Factor authentication can provide double security for social media accounts, especially Facebook. This does not guarantee that personal data will not be stolen, but at least when someone else tries to enter the user's Facebook account before verifying the code employing a phone number.

5. Conclusion

Based on the results of our research, it is known that personal data or personal information is personally identifiable data based on such information regarding specific individuals. Personal data is misused for the personal and political interests of particular individuals. One of the media with the most significant number of users and holds various users' Information is Facebook. Unfortunately, many users are not careful in protecting their data. 64.3% of Facebook users do not monitor login activity on their accounts, and 71.4% of Facebook users do not use Two-Factor Authentication to log in.

Facebook must protect the personal data of its users as stated in the Privacy Policy, and Facebook has also agreed to the Statement of Rights and Responsibilities. However, this only applies if the user's data occurs between the user and Facebook. If the problem occurs between the user and fellow users, then Facebook is not responsible. Therefore, users need to be more careful in safeguarding their data and not underestimating the misuse of personal data. Users also need to pay attention to data provisions and policies from media and social networks before agreeing to and providing personal data. Users can take advantage of both the security facilities provided by Facebook and trusted facilities from outside Facebook to protect their data. However, it would be better if social network users do not have to share all personal data. Share what is necessary for the social network by knowing the purpose for which the data is requested.

References

[1] S. Gündüç, “The Effect of Social Media on Shaping Individuals Opinion Formation,” in *International Conference on Complex Networks and Their Applications*, 2020, pp. 376–386.

[2] T. Limba and A. Šidlauskas, “Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook,” *Entrep. Sustain. Issues*, vol. 5, no. 3, pp. 528–541, Mar. 2018.

[3] M. Laliberté, É. Samson, C. Beaulieu-Poulin, A. C. Larrivée, M. Charbonneau, and D. E. Feldman, “Facebook and physiotherapy: current uses and misuses,” *Physiotherapy*, vol. 101, pp. e809–e810, May 2015.

[4] M. T. Kincheloe, D. Weed, and C. W. Lack, “Facebook and psychology: Use and misuse of social networks,” in *Recent advances in clinical medicine book series: Recent advances in biology and biomedicine*, 2010, pp. 80–83.

[5] M. J. Bugeja, “Facing the facebook,” *Chron. High. Educ.*, vol. 52, no. 21, 2006.

[6] T. Vranešević, N. Perić, and T. Marušić, “Perception of Social Media as a Source of Relevant Information,” *Zagreb Int. Rev. Econ. Bus.*, vol. 22, no. 1, pp. 133–144, May 2019.

[7] P. Patel, K. Kannoorpatti, B. Shanmugam, S. Azam, and K. C. Yeo, “A theoretical review of social media usage by cyber-criminals,” in *2017 International Conference on Computer Communication and Informatics (ICCCI)*, 2017, pp. 1–6.

[8] Senthil Kumar N, Saravanakumar K, and Deepa K, “On Privacy and Security in Social Media – A Comprehensive Study,” *Procedia Comput. Sci.*, vol. 78, pp. 114–119, 2016.

[9] H. Pangastuti, “Hubungan antara narsisme dengan presentasi diri pada pengguna jejaring sosial facebook,” Universitas Muhammadiyah Surakarta, 2015.

[10] W. P. Special and K. T. Li-Barber, “Self-disclosure and student satisfaction with Facebook,” *Comput. Human Behav.*, vol. 28, no. 2, pp. 624–630, Mar. 2012.

[11] H. R. Lipford, A. Besmer, and J. Watson, “Understanding Privacy Settings in Facebook with an Audience View,” *UPSEC*, vol. 1, pp. 1–8, 2008.

[12] P. Felita, C. Siahaja, V. Wijaya, G. Melisa, M. Chandra, and R. Dahesihsari, “Pemakaian Media Sosial dan Self Concept Pada Remaja,” *J. Ilm. Psikol. MANASA*, vol. 5, no. 1, pp. 30–41, 2016.

[13] P. Nyoni and M. Velempini, “Privacy and user awareness on Facebook,” *S. Afr. J. Sci.*, vol. 114, no. 5/6, May 2018.

[14] M. Madden *et al.*, “Teens, social media, and privacy,” *Pew Res. Cent.*, vol. 21, no. 1055, pp. 2–86, 2013.

[15] G. Dillon, “Study Finds Some Facebook Apps Misuse User Data; TikTok Looks to Quell Privacy Concerns,” *ExchangeWire*, 2020. [Online]. Available: https://www.exchangewire.com/blog/2020/07/02/study-finds-some-facebook-apps-misuse-user-data-tiktok-looks-to-quell-privacy-concerns/. [Accessed: 17-Oct-2020].

[16] D. Patterson, “Facebook data privacy scandal: A cheat sheet,” *TechRepublic*, 2020. [Online]. Available: https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/. [Accessed: 17-Oct-2020].

[17] BBC, “Facebook’s data-sharing deals exposed,” *BBC news*, 2018. [Online]. Available: https://www.bbc.com/news/technology-46618582. [Accessed: 17-Oct-2020].

[18] N. Lomas, “Facebook data misuse and voter manipulation back in the frame with latest Cambridge Analytica leaks,” *TechCrunch*, 2020. [Online]. Available: https://techcrunch.com/2020/01/06/facebook-data-misuse-and-voter-manipulation-back-in-the-frame-with-latest-cambridge-analytica-leaks/. [Accessed: 17-Oct-2020].

[19] Z. Muhammad, “Facebook’s Dangerous Misuse of User Data Revealed,” *Digital Information World*, 2019. [Online]. Available: https://www.digitalinformationworld.com/2019/04/leaked-documents-show-mark-zuckerberg-abused-user-data.html. [Accessed: 17-Oct-2020].

[20] A. L. Young and A. Quan-Haase, “Information revelation and internet privacy concerns on social network sites,” in *Proceedings of the fourth international conference on Communities and technologies - C&T ’09*, 2009, p. 265.