Indonesian Generation Z's Awareness of Data Privacy in the Use of Social Media

Nathaniel Adrian, Lindawaty, Destiana Friska, Yohannes Kurniawan
Information Systems Department
School of Information Systems
Bina Nusantara University
Jakarta, Indonesia, 11480
nathaniel.adil@binus.ac.id, lindawaty@binus.ac.id, destiana.friska@binus.ac.id,
ykurniawan@binus.ac.id

Abstract

Sharing personal interest and activity in social media has become a trend nowadays. While passwords are the main access gate in social media accounts, many people still use their personal information as passwords, which inadvertently makes password vulnerable and increasing the chance for unauthorized parties to access or even control user's account. This research examines Generation Z awareness toward data privacy in multiple social media platforms. By using an online questionnaire to gather data in quantitative approach the data is summarized using descriptive statistics to gain deeper insight. The result shows most of Generation Z are quite aware of data privacy, although their behavior does not indicate any preventive action to protect their data.

Keywords
Data privacy, social media, Generation Z, awareness, and password.

1. Introduction

It is undeniable that social media has changed how people interact with each other. Beforehand, people need to be present at one place to create interaction. However, with the advantage of technology in social media, the parties and individuals that involve in the interaction are no longer required to physically present since social media enable users to share ideas, thoughts, and information through the construction of virtual networks and communication. At this time, the use of social media is not only limited as a medium to interact, but also used by businesses to reach customers since there are also some social media insights regarding the targeted consumers (Dollarhide 2021). According to the digital report 2021, published from We Are Social agency it is found that in January 2021 more than half of the Indonesia's population was an active user of social media (Kemp 2021). It is also stated that millennials and Generation Z are the dominant users of social media (Stephane 2021). Although most of the Indonesia's population already familiar with term of social media usage, however this does not mean users are fully aware of their privacy and security in social media. In fact, the Indonesian Ministry of Communication and Information revealed the Indonesian young generation show the sign of apathy when it comes to the security of personal data. As stated by the directorate general information applications in Indonesia in August 2020, the younger generation are conscious about the positive and negative impacts of the social media usage, yet they are not very mindful about their own personal data.

Social media usage has increased among young people since social media provides more ease of social interaction where users do not need to conduct any physical interaction to communicate (Allen 2020). Young people, especially Generation Z, cannot be separated from technology since they used to interact and communicate in the virtual world through the internet almost 24/7. Generation Z consists of elementary students and fresh graduates that just start to establish career opportunities. In some references, Generation Z is born from 1997, however other references stated different year of born like the end of millennium. Moreover, Generation Z has been exposed to many different technologies from their childhood and grew with it which makes them called tech-savvy (Szymkowiak et al. 2021).

This paper includes research about data privacy awareness from university student perspective in the present, which dominated by Generation Z. Furthermore, the results in this study are expected to not only acknowledge Generation Z's awareness toward data privacy in social media but also provide some insights about Generation Z tendency regarding personal information protection, especially in Indonesia.

2. Methods

In this research, the quantitative approach was utilized to collect the required data. Before distributing survey using online questionnaire, readability test was arranged to evaluate whether the participant can comprehend the questionnaire's items without misinterpretation. University students from different majors have been chosen to participate in the readability test to ensure participants familiarity with the terms that are used in the questionnaire. Following the participant's response during the readability test, some of the questionnaire's items were modified before being shared in the social media group chat through WhatsApp and Line platforms.

Table 1: Questions for every indicator included in this research

Indicators	Questions Code	Questions	Answer Options
Profiling	PR01	What social media do you use?	Facebook, YouTube, Instagram, Discord, TikTok, WhatsApp, Twitter, Line, Telegram, Others
	PR02	What is the estimate duration of your social media usage in a day?	<1 hour, 1 – 3 hours, 4 – 6 hours, >6 hours
	PR03A	How long is the password that you usually use?	Short (less than 9 characters), Medium (9 – 15 characters), Long (more than 15 characters)
	PR03B	On a scale of 1-5, how complex is the password that you usually use? **Complexity based on the combination of numbers, letters, and symbols*	1, 2, 3, 4, 5 From quite simple to overly complex
	PR04	Do you prefer to use the free Wi-Fi provided in public places instead of using mobile data?	Yes, No
Experience	EX01	Have you ever experienced phishing or hacking on your social media account?	Yes, No
	EX02	Has anyone you know ever experienced phishing or hacking on their social media account?	Yes, No
Behavioral	BV01	What type of smartphone security do you use on your lock screen?	Not using any security, PIN, Fingerprint, Face unlocks, Pattern, Password
	BV02	Do you use the same password for all social media accounts?	Yes, Mostly, No

	BV03	Do you share your social media password with people that are close to you?	Yes, No
	BV04	What is your preference regarding the privacy type on your social media accounts? **Private account or public account*	Public, Private
	BV05	I tend to use personal information (such as name, phone number, date of birth and other personal information) as my password to make it easier to remember.	Yes, No
	BV06	I often use public devices to log into my social media accounts.	Never, Almost Never, Often
Effort	EF01	Do you use additional passcode for social media? **Only applies to social media that provide additional passcode features such LINE and WhatsApp*	Yes, No
	EF02	Do you use the same password for e-mail and social media accounts?	Yes, No
	EF03	If you use a public device, do you double check that you have already logged out of your social media accounts?	Never used public device, Yes, No
	EF04	How do you save your password?	Write password on paper, Write password on smartphone/PC note, Use password manager, Share password to trusted person, Never write/save password
	EF05	I change my social media passwords regularly.	Yes, No

Table 1 shows questions and indicators used in the questionnaire. The questionnaire is distributed using a simple random sampling method. The subject of this research is university students with ages between 17 and 24 years old that are considered mature in Generation Z age range, especially in terms of technology knowledge and usage. Generation Z was born in the rise of technology which differentiates them with other generations who grew up without technology. The respondents residing in Indonesia's big city were selected because of their familiarity with technology since they use social media on daily basis. The questionnaire was open for respondents from November 9th - November 16th, 2021. The respondent's criteria consist of: (a) university students, (b) age between 17 up to 24 years old, (c) and lived in big city. For additional validation, the respondents were asked to provide their university e-mail. Furthermore, this study utilized descriptive statistics to help find insight from the data that has been collected. Mean and frequency will be calculated to summarize data.

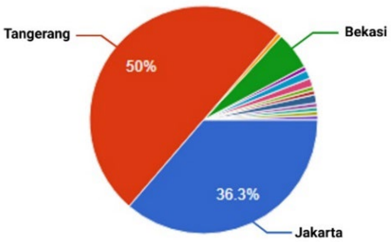

Figure 1. Respondent's Domicile

After the questionnaires were assigned, a total of 168 respondents were obtained. The respondents include university students that live in Indonesia and born between 1997 and 2004. Most respondents live in Jakarta, Tangerang, and Bekasi. Respondent's domicile distribution was shown in Figure 1.

3. Results and Discussion

Table 2. Personal experience on phishing or hack (EX01)

	Responses Number	EX01 Proportion	Cumulative Proportion
No	135	80.4%	80.4%
Yes	33	19.6%	100.0%
Total	168	100.0%	

Table 3. Perceive phishing or hack from other's experience (EX02)

	Responses Number	EX02 Proportion	Cumulative Proportion
No	55	32.7%	32.7%
Yes	113	67.3%	100.0%
Total	168	100.0%	

Based on the survey data shows in Table EX01, 19.6% of respondents have experienced phishing or hacking (EX01). Table EX02 shows 67.3% of respondents know about phishing or hacking incidents from people they know (EX02). These numbers indicate security threats like phishing or hacking are common among respondents.

Table 4. Descriptive statistic result of lock screen security usage (BV01)

	N Valid	Missing	Mean
BV01	160	8	2.43

To protect personal devices from unauthorized access, one of the most common preventive actions is to set up lock screen security. However, there are 8 out of 168 respondents who prefer to not use any type of security on their mobile phone that is categorized as missing respondents for BV01 question item. Table 4 shows a mean result of 2.43 with 160 valid respondent numbers which specifies that most Generation Z use 2 different lock screen security types on their lock screen.

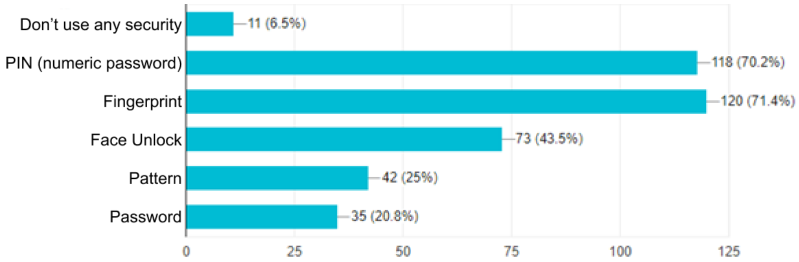

Figure 2. Lock screen security usage (BV01)

As shown in Figure .2, most respondents are using fingerprint along with PIN as their lock screen security. Face unlocks also become a favorable option among the respondent, followed with pattern and password usage. Factors that might affect respondent choices on not using any security vary between smartphone capability and respondent inconvenience to input security key repetitively.

Table 5. Descriptive statistic result of most used social media (PR01) and estimate duration of social media usage (PR02)

	N Valid	Missing	Mean
PR01	168	0	6.49
PR02	168	0	2.86

Table .5 shows mean results of 6.49 in PR01 which indicate Generation Z uses approximately 6 social media daily. As every respondent had a different answer on how many social media platforms they usually use, the result in Table 5 was processed by calculating the average number of social media platforms that respondents used. The average result of PR02 was calculated after categorizing each duration of social media usage from scale 1 to 4 based on the shortest to longest duration. The mean results of 2.86 in PR02 show that the average duration of Generation Z social media usage is from 1 to 6 hours per day.

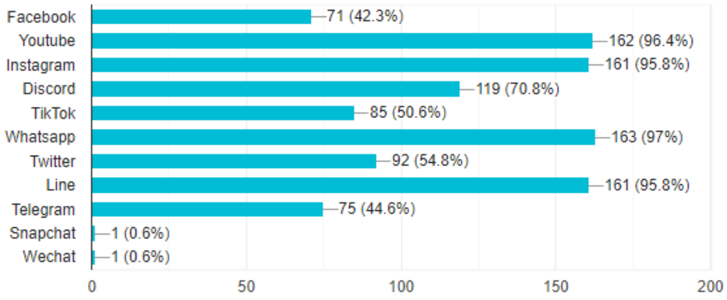

Figure 3.Most used social media (PR01)

Based on nature of connection, there are two major characteristics for social media platform which are content-based, and profile based (Voorveld et al. 2018). These characteristics are used as reference to determine the ranking of social media platform on PR01. As seen in Figure 3, YouTube became the most used content-based social media platform, followed by Instagram, Discord, and TikTok. While WhatsApp is the most used profile-based social media platform, followed by Line, Twitter, Telegram, and Facebook. Compared with other social media platforms, Facebook has a lower percentage of usage among Generation Z since they did not find content that complement their preferences on Facebook (Suwana et al. 2020).

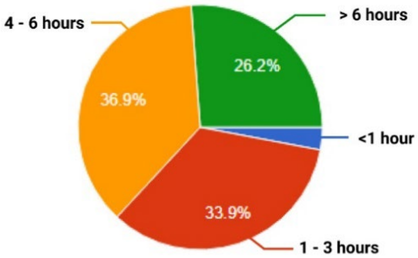

Figure 4. Estimate duration of social media usage (PR02)

In Figure 4, it shows the majority of respondent (63.1%) spend greater than 4 hours per day in social media and very few uses social media under 1 hour per day. Compared with global social media statistics research summary held in October 2021, the Generation Z social media usage is significantly more intense than average time spent by global population which is 2 hours and 27 minutes (Chaffey 2021).

Nowadays, social media is not just a communication tool but also for other purposes like entertainment, business, and networking. Since social media covers so many purposes, people spend more of their time using it which increases the use intensity of social media. The concerns of personal privacy might affect the intensity of social media usage because people who have more privacy concerns are not inclined to share their information with more people which allowing them to provide more control related with personal information (Cain and Imre 2021).

Table 6. Descriptive statistic result of password length (PR03A) and password complexity (PR03B)

	N Valid	Missing	Mean
PR03A	168	0	1.91
PR03B	168	0	3.69

The average of Generation Z preferences in creating password in Table 6 is shown with the mean of 1.91 (PR03A) and 3.69 (PR03B). The mean number in PR03A indicates medium-length passwords while mean number in PR03B specifies high complexity password. The average result of PR03A was calculated after classifying the password length usage from scale 1 to 3 sorted by short, medium, and long password. Whereas PR03B answers' result already in Likert scale form (from scale 1 to 5 based on quite simple to overly complex password), the mean result of PR03B was obtained by simply calculating it directly.

There are some general password formulation guidelines embedded in some platform to help the user in formulating their password. However, some users may ignore the guideline since it required additional effort to meet the security objectives criteria. Moreover, directly adjusting the password formulation using the guideline could cause some users to become frustrated (Grobler et al. 2020). Based on detailed data, the respondents are inclined to use medium to short passwords that fulfil minimum password length requirement. Respondents are more likely to use complex passwords. Yet, the complexity of their password is based on their perspective since this research cannot explore the password complexity furthermore due to respondent's privacy.

Table 7. Using the same password on all social media accounts (BV02)

	Responses Number	BV02 Proportion	Cumulative Proportion
No	39	23.2%	23.2%
Mostly	100	59.5%	82.7%
Yes	29	17.3%	100.0%
Total	168	100.0%	

Based on Table 7, 59.5% of the respondents use the same password in most social media account, while 23.2% of the respondents expressed that they use different password for each social media accounts and 17.3% revealed that the password used in every social media account is the same. This result might be affected by the limitation of user's capability to create a new combination of password or similar authentication method, which influence users to reuse their password (Grobler et al. 2020).

Table 8. Share password with other people (BV03)

	Responses Number	BV03 Propostion	Cumulative Proportion
No	137	81.5%	81.5%
Yes	31	18.5%	100.0%
Total	168	100.0%	

In term of password confidentiality, most respondents did not share their social media account's password to other people even with their close relatives (BV03). Based on Table 8, only 18.5% respondents stated that they shared their social media password to those they trusted. These users may find it is convenient to share their social media accounts' password with selected people as an act of trust, yet they do not consider the privacy risk. Prior studies revealed that there were some cases about account abuses as the side effect of password sharing, where abusers exploit the user's access on their social media and force them to log out of their accounts. This condition would become more out of control if the user reused the same password for all social media accounts. Many devices and applications automatically save the user's login information which makes it harder to remove unwanted access from account (Obada-Obieh et al. 2020). However how high the risk level of account abuses may depend to whom the users' account access is granted.

Table 9. Use personal information as password (BV05)

	Responses Number	BV05 Proportion	Cumulative Proportion
No	64	38.1%	38.1%
Yes	104	61.9%	100.0%
Total	168	100.0%	

Table 9 shows that most of the respondents did not use their personal information to create their password for social media account (BV05). Only 37.5% of the respondents used their personal information in their password. Respondent's decision to not use personal information as their password might be influenced by user's knowledge about how vulnerable it is. Many studies stated that since people actively use social media and share their interests, personal information becomes more detectable and predictable to many people (Tülek et al. 2020).

Table 10. Using social media password for e-mail password (EF02)

	Responses Number	EF02 Proportion	Cumulative Proportion
No	83	49.4%	49.4%
Yes	85	50.6%	100.0%
Total	168	100.0%	

Based on Table 10, more than half respondents (50.6%) use the same password for their e-mail and social media account. Yet, the rest of the respondents still show lack of awareness by using the exact same password for e-mail and social media accounts.

Table 11. Descriptive statistic result of password-saving method (EF04)

	N Valid	Missing	Mean
EF04	117	51	1.32

Table 11 shows the mean of 1.32 which indicates that most Generation Z only use 1 method to save their password (EF04). The average result in Table 11 was generated by calculating the amount of password-saving method used by 117 out of 168 respondents, while the rest of respondents who stated they never write or save their password are excluded.

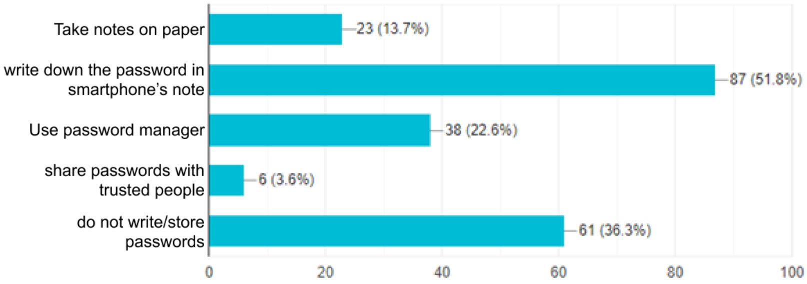

Figure 5. Password saving method (EF04)

Based on Figure 5, saving passwords on smartphone's notes has become the most common choice due to its simplicity and easiness to be accessed. Users can choose between offline or online notes depending on their preference yet both choices come with their own advantages and disadvantages. Storing passwords in online notes allow users to access files and applications on multiple devices, but this condition might cause a security gap and endanger saved passwords. Offline notes eliminate this security gap, but there is a chance that users cannot recover password if their device experiences problems. Password manager provides more efficiency for users since it enabled the users to create and save all their passwords on multiple platforms which allows auto login to their accounts. However, password manager also had its limitations like the risk of the password manager being hacked and revealing all of passwords that are being used. Writing the password on paper and store it at the safe place could provide more security than using password manager, but this option is less effective compared to password manager. Sharing passwords with trusted people could be an alternative option for keeping the password, yet the assurance cannot be measured. Some people choose to not write down their password because of these risks, therefore they rely on their capability to remember their password. Yet, there is a chance the user may forget their password if it is not extensively used. But forgetting may not be a problem since some platforms has the 'forgot my password' feature to reset their password.

Table 12. Frequently changing social media password (EF05)

	Responses Number	**EF05 Proportion**	**Cumulative Proportion**
No	138	82.1%	82.1%
Yes	30	17.9%	100.0%
Total	168	100.0%	

Result in Table 12 shows that only 17.9% of respondents change their social media password regularly while 82.1% do not change their social media password very often (EF05). Changing password for every one to three months is recommended to enhance the account security, but many people might find changing password regularly become a tedious task, therefore people tend to cut corners which resulting in simpler and shorter password (Madnick 2020).

Table 13. Use of additional passcode on social media (EF01)

	Responses Number	**EF01 Proportion**	**Cumulative Proportion**
No	89	53.0%	53.0%
Yes	79	47.0%	100.0%
Total	168	100.0%	

Additional passcode enables more protection for users' social media account (EF01), however not all social media platforms provide this feature. Some users might find using additional passcode on some social media accounts are tiresome since they must re-enter the passcode if they want to access their social media every time. As seen in Table 13, only 47% of respondent stated that they used the additional passcode feature on certain social media platforms as further effort of securing data. Whereas 53% of respondent voiced that they do not use this feature.

Table 14. Preference on using Wi-Fi instead of mobile data (PR04)

	Responses Number	**PR04 Proportion**	**Cumulative Proportion**
No	90	53.6%	53.6%
Yes	78	46.4%	100.0%
Total	168	100.0%	

In regard of public Wi-Fi usage as shown in Table 14, 53.6% of respondents prefer to use mobile data instead of public network. Many factors could influence this result, such as inconvenience to login, slow internet speed, and security awareness. Even though majority of respondent still prefer using mobile data, there are still 46.4% respondent prone to security risk due to public Wi-Fi usage. Based on previous research, public Wi-Fi may cause harm to the users privacy such as personal data stealing including financial information, password, file, and pictures (Poojary and Suresh 2021).

Table 15. Log in social media account on public device (BV06)

	Responses Number	BV06 Proportion	Cumulative Proportion
Often	9	5.4%	5.4%
Almost Never	86	51.2%	56.5%
Never	73	43.5%	100.0%
Total	168	100.0%	

In public places like airports, library, and school, public devices like PCs or tablets are provided for free usage. Based on Table 15, 51.2% of the respondent stated that they rarely use public device to access their social media accounts, 43.5% of respondents revealed that they never used public device to log in their social media account, and only 5.4% respondents declared that they often use public device to access their social media accounts (BV06). The use of public devices has been known to be unsafe and may raise the risk of data stealing since there is a possibility for people to install spyware without us knowing. This kind of malicious software can monitor and capture data via users' activity trace log, keystrokes logging, and screen capture (Steinberg 2020).

Table 16. Ensuring personal social media access on public device (EF03)

	Responses Number	EF03 Proportion	Cumulative Proportion
No	7	4.2%	6.5%
Yes	101	60.1%	100.0%
Never use public device	60	35.7%	
Total	168	100.0%	

Results in Table 16 show that 60.1% of the respondent always double check their social media access before leaving the public device completely, 4.2% respondent stated that they do not always double check their social media access on public device, and 35.7% are not using the public device to access their social media accounts (EF03).

Table 17. Preference of social media privacy type (BV04)

	Responses Number	BV04 Proportion	Cumulative Proportion
Public	64	38.1%	38.1%
Private	104	61.9%	100.0%
Total	168	100.0%	

Regarding social media privacy as shown in Table 17, 61.9% respondents more inclined to have a private social media account rather than the public one (BV04). Private type account enables users to gain more control to whom their contents are being viewed. Since the audiences that allowed to view are based on users' consent motive and preference, the motive of public or private account toward privacy remained unclear (Ravn et al. 2019). However, it should be noted that once the content information is already shared in social media platforms the owner has lost control and privacy of their content regardless of using private or public accounts setting (Click 2020).

4. Conclusion

This research is held to identify Generation Z privacy awareness towards social media password and security, since Generation Z is quite intense on using social media compared to other generations. Besides password, lock screen security is also included in this research. Lock screen security is important since devices automatically save login information for most applications, which makes people who have access to the phone can immediately access social media and other apps instantly after they go through lock screen security. The result from the survey shows most Generation Z use fingerprint and PIN for lock screen security on their smartphone.

Through this research, it is found that more than half respondents are already aware of data privacy. Based on the survey result, passwords used in social media apps are preferred to be medium-length (9 to 15 characters) with medium-high complexity. Most respondent prefer to use mobile data instead of public network (Wi-Fi) and only few of them use public devices. For the most of part, people who used public devices always make sure they have logged out their account before leaving the device.

Number of respondents that aware of data privacy is not much different from those who are not. The average of social media use by Generation Z is six applications. By using multiple apps, many people resort to use the same password and one third of respondents even used their personal information in their password. Although many respondents who already experienced phishing or hacking, they still do not put any preventive effort to secure their social media account. It is shown through survey results where many respondents are using the same passwords for all social media accounts and e-mail.

Slightly over half of respondents choose not to use additional passcode for their social media accounts and seldom change their social media passwords. This research found the Generation Z that have not experienced phishing and hacking tend to differentiate their password on social media and e-mail their password which put Generation Z in the gap category for those who are very attentive and those who are very ignorant with their privacy.

Acknowledgements

This work is supported by The Ministry of Education, Culture, Research, and Technology, Republic of Indonesia as a part of Program Kompetisi Kampus Merdeka Grant to Bina Nusantara University in 2021.

References

Allen, S., Social media's growing impact on our live*s*., Available: https://www.apa.org/members/content/social-media-research, September 29, 2021.

Cain, J. A., and Imre, I., Everybody wants some: Collection and control of personal information, privacy concerns, and social media use, *New Media & Society*, pp. 1-20, 2021.

Chaffey, D., Global social media statistics research summary 2022, Available: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/, January 27, 2022.

Click, C., Social Media Privacy, Available: https://www.sans.org/newsletters/ouch/social-media-privacy/, September 21, 2021.

Dollarhide, M., Social Media, Available: https://www.investopedia.com/terms/s/social-media.asp, October 31, 2021.

Grobler, M., Chamikara, M. A., Abbott, J., Jeon, J. J., Nepal, S., and Paris, C., The importance of social identity on password formulations, *Personal and Ubiquitous Computing*, vol 25, no. 12, pp. 813–827, 2020.

Kemp, S., Digital 2021: Indonesia, Available: https://datareportal.com/reports/digital-2021-indonesia, September 11, 2021.

Madnick S., Do you have password headaches? You are not alone, and it is unnecessary!, 2020

Newlands, G., Lutz, C., Tamo`-Larrieux, A., Eduard Fosch Villaronga, R. H., and Scheitlin, G., Innovation under pressure: Implications for data privacy during the covid-19 pandemic, *Big Data & Society*, vol. 7, no. 2, pp.1-14, 2020.

Obada-Obieh, B., Huang, Y., and Beznosov, K., The burden of ending online account sharing, *CHI '20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems,* pp. 1-13, Honolulu, Hawaii, USA, April 25-30, 2020.

Poojary, and Suresh, P., Safety measures to be maintained while using public wi-fi, *International Journal of Research Publication and Reviews*, vol. 2, no. 4, pp. 64-66, 2021.

Ravn, S., Barnwell, A., and Neves, B. B., What is "Publicly Available Data"? Exploring blurred public–private boundaries and ethical practices through a case study on Instagram, *Journal of Empirical Research on Human Research Ethics*, vol. 15, no. 1-2, pp. 40-45, 2019.

Steinberg, S., The latest ways identity thieves are targeting you and what to do if you are a victim, Available: https://www.cnbc.com/2020/02/27/these-are-the-latest-ways-identity-thieves-are-targeting-you.html, November 23, 2021.

Stephane, C., Riset ungkap lebih dari separuh penduduk Indonesia "Melek" media sosial. Available: https://tekno.kompas.com/read/2021/02/24/08050027/riset-ungkap-lebih-dari-separuh-penduduk-indonesia-melek-media-sosial, October 5, 2021.

Suwana, F., Pramiyanti, A., Mayangsari, I. D., Nuraeni, R., and Firdaus, Y., Digital media use of generation z during covid-19 pandemic, vol 19, no. 3, pp. 327-240, 2020.

Szymkowiak, A., Melovic, B., Dabic, M., and Jeganathan, K., Information technology and gen z: The role of teachers, the internet, and technology in the education of young people, *Technology in Society*, vol. 65, no. 5, pp 1-10, 2021.

Tülek, N. M., Kuşkon, M., Sezgin, I., and Levi, A., Disclosure of personal information in passwords on social media, *2020 28th Signal Processing and Communications Applications Conference (SIU)*, October 5-7, 2020

Voorveld, H. A., Noort, G. V., Muntinga D., G., and Bronner, F., Engagement with social media and social media advertising: The differentiating role of platform type, *Journal of Advertising*, vol. 47, no. 1, pp. 38-54, 2018.

Biographies

Nathaniel Adrian is an undergraduate student at Bina Nusantara University, currently in his fourth year pursuing his degree in Information Systems. By having an interest in business and technology, he chose Business Intelligence as his stream. In 2021, he started his career by joining Teravin Technovations to become a Business Analyst as an intern. Teravin Technovations is a service company for IT (Information Technology) & Information System related with banking as target market. While working there, his job desk focuses on UI/UX, diagram, and business analysis. He gained both experience in soft skills and technical competence from working there for one year. Intrigued by UI/UX design done by professional, he learned more on UI/UX skill. In recent years, his interest in investing also grew and he tried all short of investing opportunity and technique in purpose to learn and hoping to gain stable income from it.

Lindawaty is a university student at Bina Nusantara University in Indonesia, where she is majoring in Information Systems. Since high school, she had an interest in business management and information technology, which led her to learn more about data analytics to find business insight. This interest led her to take Business Intelligence stream in her major. In her first year as a university student, she is actively participating in the Information Systems Student Association as Media and Information activist. In the beginning of 2020, she was assigned as Vice Coordinator for Media and Information division for Alam Sutera campus region. In 2021, she joined Kalbe Farma as an intern for Business Intelligence Analyst role. Through this internship, she got to see real implementation of data analytics in the business sector. Worked as a Business Intelligence Analyst, she learned about data pre-processing, text mining, machine learning, analytics using Python and SQL, and dashboard making using Tableau. Besides doing internship, she also become a part-time teacher at KodeKiddo, where she tutors kids about coding and algorithm to enhance their computational thinking.

Destiana Friska is a student at Bina Nusantara University in Indonesia, majoring in Information Systems program. In her first year as a university student, she participated in some activities like visiting children charity foundation for education workshop and become a volunteer to help the event continuity on seminar. She also joined the mentorship program at Bina Nusantara University to assist other university students in learning activities. To complete her major in Information System, she pursuit one of Information System streaming on Applied Database course where she learned the requirement in database system and how to use the basic of Oracle Database technology. Later in early 2021, she started her internship program as Oracle Developer at Enseval Putera Megatrading Ltd., an Indonesian company that specialized in trading and distribution for pharmaceutical goods, medical equipment, and other related products. During her internship, she learned how to utilize the Oracle Database technology for ERP (Enterprise Resource Planning) software program to integrate the core business process inside the company.

Yohannes Kurniawan is an associate professor at Bina Nusantara University, he has more than 10 years of experience in academics and industries, he has helped a lot of organizations to accelerate their digital transformation. Yohannes' extensive expertise in Knowledge Management, Digital Business, User Experience, Information System Security and Information System Development makes him become the Subject Matter Expert for UX and Educational Technology at BINUS CREATES. His research interests vary from Implementing Human Information Behavior Concept for Design and Knowledge Management System impact in Hospital.