Implications of Risk and Cyber Security towards Psychological Aspects of Application Users: Exploratory Study of Mobile Applications Downloading Behavior by the Generation Z

Atiqa Khaneef Harahap [1], Ngazha Syafania Munawir Putri [2], Ni Luh Made Yani [3], Farah Mulyasari[4]

{atiqa.kh@universitaspertamina.ac.id[1], 106120009@student.universitaspertamina.ac.id[2], 106120044@student.universitaspertamina.ac.id[3] , farah.mulyasari@universitaspertamina.ac.id[4]

Universitas Pertamina, Jalan Teuku Nyak Arief, Simprug, Kebayoran Lama, Jakarta, Indonesia[1,2,3,4]

Abstract. Downloading and installing mobile application means dealing with approval of access permissions on features that store various personal data on the phone. This situation creates uncomfortable feelings and dilemmas for users because of the need for applications, but on the other hand users feel confused or feel insecure by giving access permissions to parties who store various personal data. This research was conducted to understand the psychological aspects experienced by users when deciding to download the mobile application, prioritizing a qualitative approach with data collection in the form of in-depth interviews. The participants in this study were Generation Z, the most smartphone users according to the Indonesian Internet Service Providers Association (APJII). The results of this study are expected to assist young users in designing risk information that is tailored to their comfort needs and mindful behavior using technology.

Keywords: downloading, Generation Z, mobile applications, psychological aspects, risk and cyber security

1 Introduction

Smart phone applications are present to fill various activities of contemporary people's lives. Applications are used for various activities such as playing, shopping, communicating, listening to music and even studying. In other words, the application fills various needs ranging from information needs to entertainment. No wonder the application is growing and developing. App Annie noted that there were 230 billion smartphone applications downloaded globally during 2021 and Indonesia became the country with the fifth largest smartphone application market in the world [1].

The growth of the application market is not surprising as the continuous advancement of wireless technology and the growing penetration of smartphones opens up new channels for businesses with unique features to approach their customers [2]. Technological developments and smartphone penetration have opened up opportunities for developers to create applications that suit the needs of their customers. On the one hand, this progress has made it easier for many

ICONIC-RS 2022, March 31-April 01, DKI Jakarta, Indonesia

DOI 10.4108/eai.31-3-2022.2320687

people to carry out various life activities, both for personal and business purposes. Despite the many benefits of the application, the risks associated with using the application are also high such as malware, identity theft, ransomware, and stolen personal data [3].

Along with the convenience that the app offers it needs to be considered carefully as there are many mobile security issues and data privacy threats lurking. To reduce this risk, not only the technical side of system security needs to be developed but also users need to take initiatives to secure their own privacy. That is, if the user understands what it means to give permission to the application then the user is likely to be able to make safe online decisions and avoid the above risks [3].

This needs to be explored further considering that mobile device users show dramatic numbers. In Indonesia alone, mobile phone users show a dramatic number, reaching 167 million people or 89% of the total population of Indonesia [4]. As for the most age who use smartphones, based on a survey by the Indonesian Internet Service Providers Association (APJII) in 2019-2020, internet user penetration in Indonesia is dominated by the 15-19 year age group at 91 percent, followed by the 20-24 year age group at 88. 5 percent [5]. This means that the younger generation from generation Z is dominant in using smartphones which cannot be separated from software in the form of applications in it. With this dominance, generation z is in the largest proportion who will face cyber risks and security. Moreover, generation z is characteristically a generation that is often termed a digital native. Generation z are people who grew up in close contact with technology. With other katbahua, his life is filled with the use of applications for various needs.

Applications that can be accessed easily through the installation process on the cellphone. After installing the app, the user will usually be asked for permission to access certain hardware and software on the phone in order for it to work. Many apps ask for permission to access private channels, such as camera, contacts, microphone, text messages, and external storage. In this situation, the user is actually in a situation to make important decisions that will have implications for the security of personal data. Based on the results of a survey by the National Commission on Human Rights (HAM) it is explained that the 17-25 year age group or generation Z is most worried about the security of their personal data in cyberspace [6]. This convenience has important implications for further looking at how Generation Z is aware of the risks and how to reduce the psychological discomfort that arises from the need to use applications amid feelings of insecurity due to the risks of using applications.

2 Theoritical framework and methodology

2.1 Mobile application

Mobile application is a software / set of programs that operate on mobile devices and perform certain tasks for users [7]. On mobile phones there are usually applications that are already installed but users can also download the desired application via the internet. Based on the application area, there are several categories of mobile applications, namely communication, games, multimedia, productivity, travel, and utilities [7].

2.2 Risk and cybersecurity

Cybersecurity has two important components, namely data and security. Therefore, cybersecurity can be defined as measures to prevent the loss or harm of information stored on electronic devices [8]. Measures to protect data can be anything. This means that it does not always emphasize technical development on the operating system but also one of the important elements is humans. Human awareness in making security decisions plays a big role in preventing access abuse.

2.1.1 Application permission

Access permissions on mobile applications aim to help applications become more dynamic and automatic in carrying out their functions [9]. For example, social media apps won't work properly if they don't have permission to access the camera on the device. Therefore, to maximize the function of applications that do require access to devices on mobile phones, permission is needed as a way to accommodate the relationship between developers and users.

Access permission is something that is very important because misuse of access permission can have a big impact on the security of information and data from its users. This does not mean that all access permissions should not be granted for security reasons, especially if the application is absolutely necessary. According to Pellet, access permissions can be grouped into three main categories, namely first, normal permissions, malicious permissions, and signature permissions or system permissions [9]. Normal permissions are harmless to the user, and are granted to any application that requests them. Second, malicious permissions, on the other hand are only granted with user consent consent during installation. System signatures or permissions are only allowed after inspection of the requesting application to ensure it meets the criteria requirements.

The emergence of various applications that continue to grow is part of the digital revolution. It is inappropriate to see the digital revolution as something driven by pure and transparent intentions [10]. This means that it is necessary to be vigilant in the face of technological developments, which currently even open wide access to the personal data of users who are vulnerable to being used for commercial purposes to cybercrimes.

2.3 Generation Z

Generation Z is a term used for the generation born in the period around or after 2005 and has the characteristics of a high affinity with technology [11]. In other words, Generation Z has lived with technological developments since the beginning of their lives. This condition shows that gene z as the largest population through the use of its technology will have a major impact on people's lives.

2.3.1 User awareness of application permission risks

Users install various applications on their cellphones with various types of applications needed. When the application is installed on the mobile system, the application will need access to the devices on the phone in order to function optimally. Not only on features in cellular devices but there are applications that ask for access to personal data in the form of contact lists, phone calls, photo albums and so on. most of the apps ask for access permission during the app installation process. Requested access permissions can be microphone, camera, location, contact and so on. This situation is actually an important situation that should be carefully considered by users. The permission granted can only be used for the use of such access for certain purposes. God however, users don't need the time and energy necessary to understand the risks or make an informed decision about the risks [3]. Therefore, access users do not tend to make correct security decisions because application users tend not to pay attention and understand the potential dangers of permissions requested by applications so that they do not make correct security decisions [12].

2.4 Psychological aspect of mobile application user

Users install various applications on their cellphones with various types of applications needed. When the application is installed on the phone system, the application will need access to the devices on the phone in order to function optimally. Not only on features on mobile devices, but there are applications that ask for access to personal data in the form of contact lists, phone call history, photo albums and so on. Most of the apps ask for access permission during the app installation process. Requested access permissions can be microphone, camera, location, contact and so on. This situation is actually an important situation that should be carefully considered by users. Any access permission granted can lead to misuse of such access for certain purposes. Unfortunately, however, users do not invest the time and energy necessary to understand risks or make informed decisions about risks [3]. Therefore, users tend not to make the right security decisions because application users tend not to pay attention and understand the potential dangers of the access permissions requested by the application so that they do not make the right security decisions [12].

2.5 Methodology

This research is an exploratory qualitative research. This research is an initial study that seeks to obtain an overview of the psychological aspects of mobile application users related to understanding cyber risks and security in the context of granting access permissions in the process of downloading applications. The subjects in this study were Generation Z with an age range of 17 and over at the time this research was conducted according to a reference which indicated that Generation Z were those born around 2005 and above. The selection of research subjects was carried out using purposive sampling technique. The following is a profile of informants in this study:

Table 1. Characteristics of Informants

No.	Initials	Age	Status	Number of Apps Installed
1	TADF	21	College student at Institut Seni Indonesia Yogyakarta	40
2	AFDP	21	College student at Universitas Brawijaya	30-40
3	ARF	21	College student at Universitas Pertamina	60
4	FAU	20	College student at Politeknik Kesehatan Kemenkes Malang	39
5	SHHM	21	College student at Universitas Brawijaya	20-30
6	APA	20	College student at Universitas Pertamina	20
7	SDIP	18	College student at Universitas Pertamina	10
8	NNAS	20	College student at Universitas Pendidikan Ganesha	10-20
9	GAKCOMD	19	College student at Universitas Pertamina	38
10	CJS	20	College student at Universitas Pertamina	10 - 20

Data was collected by conducting in-depth interviews with the informants. Then, the results of the interviews will be analyzed using coding for further interpretation with the aim of achieving a rich picture of the phenomenon under study.

3 Result and discussion

This study seeks to obtain an overview of cyber risk awareness and security and the psychological impact on application users when granting access permissions when downloading applications on their mobile phones. The following are the results of the analysis obtained, namely:

Table 2. Results of Data Analysis

Application Preferences (user preferred and used app)	Applications that are widely used are social media, games, marketplaces, editing, and learning applications
Cyber Security and Risk Awareness	Users with high cybersecurity and risk awareness will consider before granting access permissions.
(perceptions of the risk of granting access permissions and their impact on cybersecurity)	Users with low cybersecurity and risk awareness tend notto do deep consideration and rely more on application service providers.
Psychological Discomfort (a state of perceiveddissonance)	Users with high cybersecurity and risk awareness will consider before giving access permissions.
	Users with low cybersecurity and risk awareness don't do deep consideration and are more dependent on application service providers.
Inconvenience Resolution Psychological (Actions taken to reduce or resolve perceived dissonance)	Users with high cybersecurity and risk awareness try to solve the psychological discomfort due to different needs and beliefs about application security in various ways: asktrusted people, learn more, set access permissions.
	Users with low cybersecurity and risk awareness tend to feel less worried and choose to rely on app trust and are comfortable with never having a bad experience with the app, seeing themselves as unimportant and no one needing their data.

Based on the results of the analysis, it was found that users have great needs for various applications such as social media, games, marketplaces, editing, and learning applications. Based on this data, it can be seen that access permissions have become an inherent part of application usage activities. The preferences of the apps used tend to require different access permissions on the camera, microphone, contacts, etc. In other words, the informants have experienced the situation of requesting access permission when installing applications on their cell phones. Awareness of cyber risks and security actually exists within each user but the levels are different. The following are the results of interviews with informant 2 ‘‘ *Kadang aku suka takut gitu kayak diminta akses itu, kaya kases kamera. Itu mereka juga ada kan suka minta aplikasi saat digunakan atau kaya kapan saja bisa diakses. Aku kadang suka mikir dulu nih tiga* kali *ini buat apa, kadang suka worry juga sih takut salah klik dan mereka bisa mengakses data-data di hp kita. Tapi emang sih aku baca yang kebijakan privasi itu, karena harus sih biar nggak worry juga kalo misal nantinya udah setuju gitu. (Sometimes I'm afraid that I'm being asked to access something like to access my camera. They also like to ask for applications when they are used or when they can be accessed. I sometimes like to think about what these three things are for, sometimes I like to worry, I'm afraid of making a wrong click and they can access the data on our cellphones. But I actually read the privacy policy even though I have to agree later).* This statement indicates that the use of the application poses a risk to the security of his data. This high risk awareness leads to psychological discomfort in the form of the need to use the application and the belief that the application can be harmful.

This is the statetemen of Informant 10 ‘‘*Perasaan takut pasti pernah lah ya, apalagi ada kasus-kasus TokoPedia itu pasti pernah takut datanya kecuri atau diambil diubah-bah gitu pasti pernahlah. (There must have been a feeling of fear, yes, especially when there were cases that TokoPedia must have been afraid of having its data stolen or taken and changed)* This statement shows a sense of discomfort because of the dissonance between the need which means the necessity to use and his belief in the security of the application used. Thiscondition encourages the user to take certain resolution actions that are considered to be able toresolve the feeling of discomfort, as stated by Informant 2 below ‘‘*Sering banget sih, kadang kan ada aplikasi yang baru banget downloadnya dan mereka minta akses kan, kadang aku sukamikir ini jawabnya apa ya? Cara aku ngatasinnya biasanya aku naya temen. Kayak eh tau nggak aplikasi ini semisal aku ngeklik setuju dataku bakalan aman nggak kayak gimana-gimana gitu kan. Kadang tuh nanya sama temenku, atau sama kakak yang emang udah ada aplikasinya,jadi kan worrynya berkung juga kan, kadang mereka juga tuh minta apakah saat aplikasi digunakan saja, kadang aku tuh nge klik itu doang jadi as aplikasi digunain aja jadi mereka bisa akses apa yang mereka mau.‘‘ (Very often, sometimes there are applications that have just been downloaded and they ask for access, right, sometimes I like to think about this, what is the answer? The way I solve it is usually I ask a friend. Like, do you know this application, for example, if I click agree, my data will be safe, it's not like that, right? Sometimes I ask my friends, or my sibling, who already has the application, so I don't worry that much. Sometimes they also ask if I only use the application, sometimes I just click on it so I could use the application so they can access anything that they want. There is nothing to do).*

Other users whose risk awareness is low is reflected in the statement of Informant 3 ‘‘*Ya mungkin ada* beberapa *yang aku baca cuma enggak semuanya gitu loh, jadi aku bacanya mager banget mungkin kayak langsung aku centang-centang gitu. Kan ada pilihannya gitu kan ya‘‘. (Yes, maybe there are some that I read, but not all of them are like that, so I read it really slow, maybe I immediately checked it. There's a choice, right).* This statement shows that the user is aware of the risks that may occur in granting access permissions to the applications used. This awareness leads to worry following the statement to Informant 3 *“Jujur sebenernya rasa khawatirnya pasti ada‘‘.* (*Honestly, there's a lot to be worried about*). However, because the level is notlarge enough, the user does not take special steps to solve it and chooses to leave it because of the need for the application. This can be seen from the statement of Informant 3*‘‘Nanti rasa takut kita ini nanti bakal kalah sama rasa keinginan kita yang besar ini tadi. Ya mungkin kalaukhawatir aku pasti ada tapi ya balik lagi itu tadi namanya orang pengen dan butuh itu ya maugimana lagi‘‘. (Later this fear of ours will lose to our sense of this great desire earlier. Yes, maybe if I'm worried I'll be there, but then again, that's what people want and need, so what can I do)*

From the two examples of user statements, it can be seen that the awareness of cyber risk and security actually exists within them. However, the amount of psychological discomfort felt also varied, some were very worried, some just felt afraid. The magnitude of the perceived discomfort prompts different resolution actions to be taken. Users who experience high discomfort characterized by high anxiety or fear tend to take another step of asking certain trusted individuals or learning more about the app. However for users who experience low discomfort they are only mildly concerned and are less likely to take further action and build comfort by relying on the app's level of trust, referring to never having had a bad experience of abuse by the app, or seeing themselves as unimportant so they won't be data theft targets

4 Conclusion and recommendation

This research is a preliminary study to understand the psychological aspects of the behavior of installing mobile applications, especially granting access permissions on mobile devices. Through this research, it can be concluded that there is psychological discomfort experienced by users when granting access permissions to the application. The magnitude of this psychological discomfort is what prompts different solutions for each user. This research was conducted in a small scope to get an in-depth picture of the behavior of granting access permissions on installed applications. Therefore, further research is needed to examine each aspect more deeply by considering the important elements that were not examined in this study so that further specific communication strategies can be developed to increase awareness to use mobile applications consciously in generation z.

References

[1] Pahlevi R. Indonesia jadi pasar aplikasi smartphone terbesar ke-5 di dunia [Internet]. Katadata; 2022 January 14. Available from: https://databoks.katadata.co.id/datapublish/2022/01/14/indonesia-jadi-pasar-aplikasi-smartphone-terbesar-ke-5-di-dunia

[2] Gokgoz ZA, Ataman MB, Bruggen GH. There's an app for that! Understanding the drivers of mobile application downloads. Journal of Bussiness Research. 2021;123:423-437. Available from: https://doi.org/10.1016/j.jbusres.2020.10.006.

[3] Moore SR, Ge H, Li N, Proctor RW. Cybersecurity for android applications: Permissions in Android 5 and 6. International Journal of Human- Computer Interaction. 2018;35(7):1-11. Doi: 10.1080/10447318.2018.1489580.

[4] Hanum Z. Kemenkominfo: 89% Penduduk indonesia gunakan smartphone. Media Indonesia; 2021 Maret 7. Available from: https://mediaindonesia.com/humaniora/389057/kemenkominfo-89-penduduk- indonesia-gunakan-smartphone.

[5] Milana R. Kaum muda, media sosial dan nasionalisme [Internet]. Revolusi Mental; 2021 Maret 9. Available from: https://revolusimental.go.id/kabar-revolusi-mental/detail-berita-dan-artikel?url=kaum-muda-media-sosial-dan-nasionalisme#

[6] Bayu DJ. Generasi Z paling mengkhawatirkan keamanan data pribadi di internet [Internet]. Katadata; 2020 December 29. Available from: https://databoks.katadata.co.id/datapublish/2020/12/29/generasi-z-paling- mengkhawatirkan-keamanan-data-pribadi-di-internet.

[7] Islam MDR, Mazumder T. Mobile application and its global impact. International Journal of Engineering. 2010;10(6):2-78.

[8] Konke A, Shoemaker D, Siglar K. The Complete Guide to Cybersecurity Risks and Controls. Boca Raton: Taylor & Francis Group;2016.

[9] Jutail MA, Al-Akhras M, Albesher A. Associated risk in mobile applications permissions. Journal of Information Security. 2019;10(2):69-90.

[10] Harley D, Morgan J, Frit H. Cyberpsychology as everyday digital experience across the lifespan. United Kingdom: Palgrave Macmillan; 2018.

[11] Koulopoulos T, Keldsen D. The gen Z effect. Brookline: Bibliomotion Inc; 2014.

[12] Felt AP, Ha E, Egelman S, Haney A, Chin E, Wagner D. Android permission: attention, comprehension, and behavior. In: Symposium on Usable Privacy and Security (SOUPS); Washington DC; 2012. Doi:10.1145/2335356.2335360.

[13] West RL, Turner LH. Introducing communication theory analysis andapplication. 6th Edition. New York: McGraw Hill Education; 2014.