No. 455 | REC. 23-07-2021 | REV. 05-08-2021 | ACC. 22-09-2021

P. ISSN: 2086 - 4981
E. ISSN: 2620 - 6390
tip.ppj.unp.ac.id

Jurnal Teknologi Informasi dan Pendidikan
Volume 14, No. 2 September 2021
PG. 124 – 130 | https://doi.org/10.24036/tip.v14i2

The Effect of Privacy Concern Towards the Intention to Accept App Permission on Students Mobile Users

Alvi Geovanny[1]*, Infrisanti Wilson Tong[2], Jason Aaron Louis[3], Vincent Octarian Vianto[4]
[1234] Information System, Faculty of Computer Science, Universitas Internasional Batam,
Sei Ladi, Jalan Gajah Mada, Baloi Permai, Sekupang, Batam, Kepulauan Riau, Indonesia 29442
*Corresponding Author: alvigeovan29@gmail.com

INTISARI

Penggunaan mobile sudah menjadi bagian dari kehidupan kita sehari-hari. Namun, banyak pengguna mobile yang mengabaikan keberadaan izin aplikasi dalam aplikasi. Salah satu penyebabnya adalah kurang informasinya terkait dengan izin aplikasi. Bila pengguna tidak berhati-hati, izin aplikasi bisa disalahgunakan oleh peretas untuk mencuri data seperti SMS, foto, akses microphone, dan GPS. Tujuan penelitian ini adalah untuk mengamati perspektif mahasiswa Batam mengenai izin aplikasi sekaligus melihat akibat dari perspektif tersebut. Dasar penelitian ini menggunakan metode kuantitatif dan regresi. Penelitian ini membuktikan bahwa kekhawatiran privasi pengguna mobile memiliki pengaruh terhadap niat untuk menerima izin aplikasi, yang berarti mahasiswa Batam memiliki kecenderungan dalam mempertimbangkan privasi informasi pribadi pada mobile sebelum menerima izin aplikasi. Namun, kecemasan terhadap komputer dan juga keyakinan atas kendali tidak memengaruhi kekhawatiran privasi pengguna mobile, yang berarti mahasiswa Batam tidak memiliki kecemasan akan komputer ataupun memiliki keyakinan terhadap kendali yang mereka miliki pada privasi informasi pribadi di mobile.

Kata kunci: privasi, media sosial, izin aplikasi, mobile

ABSTRACT

Mobile usage has become a part of our daily lives. However, many users ignore the existence of app permissions in an app. One of the reasons is the lack of information related to app permissions. If users are careless, app permissions can be abused by hackers to steal their data such as SMS, photos, microphone access, and GPS. The purpose of this study is observing the perspective of Batam students regarding app permissions and the consequences. The basis of this research are quantitative method and regression. This study proves that mobile users' information privacy concerns have an influence on the intention to accept app permissions, which means that students tend to consider personal information privacy on mobile before accepting app permissions. However, computer anxiety and perceived control don't affect mobile users' information privacy concerns, which means students have neither computer anxiety nor perceived control over personal information privacy on mobile.

Keywords: *privacy, social media, app permissions, mobile*

INTRODUCTION

For the past few decades, mobile apps have grown very rapidly. Various types of mobile apps have been downloaded and installed on smartphones. Installing an app on a smartphone is easy, just by downloading and installing, and the app is ready to use[1]. This easy app installation sometimes makes users less aware that during the process of installation there is a part that must be reviewed, which is app permission.

Most smartphone users tend to ignore app permission request during the initial app launch. One of the causes is the lack of understanding of app permission request [2]. When a user first opens an app, the decision to accept app permission request must be approved first. However, most apps do not elaborate further on these app permission requests

so most users have minimal understanding on considering the risks[3]. This causes users to fail to realize the data sharing aspects of app permission such as intention, frequency, and purpose of the sharing. Without this awareness, it is difficult for users to make the right decisions in sharing data with smartphones. The carelessness with app permission can lead to unwanted outcomes, such as data being misused.

Based on a research from a Norwegian security researcher Promon, a loophole that abuses app permission named "Strandhogg" was found [4]. This vulnerability hijacks other apps and generates fake app permission requests and tricks users into thinking that the request comes from the hijacked app. After obtaining permissions, "Strandhogg" can steal data such as SMS, photos, microphone access, and GPS, thus providing access to read messages, view photos, eavesdropping, and track the victim's movements. "Strandhogg" can also display an overlay that resembles a login screen from social media apps and banks. With data such as user accounts and victim messages, hackers can bypass 2-step security verification easily.

The purpose of this study is to observe the perspective of Batam students regarding app permissions as well as to see the consequences of that perspective. Batam is the closest Indonesian city to Singapore. Singapore has access to the latest technology and technology penetration is very high. However, Batam is also a part of Indonesia that does not have high digital literacy because Batam is still a developing city. Therefore, we want to try to answer this question in a unique environment like Batam.

This study is based on the conceptual results of previous studies. One of the researches is privacy concerns of personal information on mobile devices that focuses on app permission requests. Using a survey involving 775 respondents and with SEM approach, it was found that privacy concerns about app permission requests have a significant effect and almost double the effect of factors such as prior privacy experience, computer anxiety and perceive control over technology [5].

There are also other studies that focus on privacy concerns on Facebook due to privacy literacy which can strengthen the relationship between privacy issues and other factors. This study involved about 4600 respondents which are mobile internet users and analysis approach with MPlus 8.1. The results obtained are people with low privacy literacy will still have high trust and low privacy concerns. While the level of privacy concern will be directly proportional to the more awareness of the importance of privacy [6].

Another research that we reviewed is about research that is centered on the usage of a social media, namely Instagram. This study focuses on Indonesian students as the research target and uses the Structural Equation Model (SEM) approach as the research method of choice for 545 student respondents. Although students are aware that personal information abuse often occurs, this does not hinder or affect the usage of Instagram among students. This proves that high privacy literacy does not necessarily result in privacy protection measures [7].

The basis of this research uses a survey method conducted on 340 social media users with the Structural Equation Model (SEM). It was discovered that user privacy and security concerns, trust in social media, and user awareness of privacy protection have a positive and significant impact on users' willingness to share personal information on social media sites. It was also found that when user awareness of privacy increases, users tend to maximize the usage of privacy features on their social media accounts. This way, safer use of social media requires a major shift in privacy concerns and user awareness levels. Most respondents in this research survey are students and civil servants whose age is categorized as young, so that may affect the answers to the survey. It is known that the age of the user can affect the awareness of privacy on social media [8].

Our research will also focus on privacy concerns and their relationship with app permission requests, as done by Degirmenci [5]. For the type of app that we use as a study is social media apps, as done by S. Rosenthal [6]. The method we use is a survey with instruments influenced by Degirmenci's research [5]. The target respondents are students (in Batam), like what was conducted by E. W. T. Darmaningrat [7] and V. Paramarta [8]. We will also try to contribute in the form of re-testing with student data in Batam as additional knowledge, especially regarding privacy concerns on social media.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390

METHOD

The method used in this research is quantitative. The research will be conducted on students in Batam by using the Cluster Proportional Random Sampling Method. The clusters used are six well-known universities in Batam. The research model that we use is following the research model used by Degirmenci by using the variables before privacy experience, computer anxiety, perceived control, and app permission concerns as independent variables and mobile users' information privacy concerns and intention to accept app permissions as dependent variables [5].

Prior privacy experience (PPE) refers to respondents' past experiences with privacy violations. Individuals who have experienced previous privacy violations tend to have higher privacy concerns and are less likely to share information or use information technology technologies that require data submission [9].

Computer anxiety (CA) is a feeling of anxiety that can be mediated by beliefs about the lack of ability to use a computer that is associated with the lack of mathematical and mechanical skills [10].

Perceived control (PE) is one of the theoretical foundations which states that the intention of an individual's actual behavior is a reflection of the influence of attitudes, views of social norms, and perceived control over an action [11]. App permission concerns (APC) matter because individuals with a higher level of concern about information privacy practices tend to refuse to participate in activities that require the submission of personal information. With increasing privacy concerns, users tend to deny app permissions, which will eventually lead to a decrease in the number of app downloads [5][12].

Mobile users' information privacy concern (MUIPC) is a variable that states that information from user data can be accessed by smartphone vendors, but users do not have clear information about the privacy policy of information that has been disclosed from users themselves [13].

Intention to accept app permissions (INT) is assumed to be influenced by the level of privacy concerns that can have an intrusive effect on the application [14][15].

The hypothesis in this study is:

H10 = Prior privacy experience does not affect mobile users' information privacy concerns.

H1a = Prior privacy experience affects mobile users' information privacy concerns.

H20 = Computer anxiety does not affect mobile users' information privacy concerns.

H2a = Computer anxiety affects mobile users' information privacy concerns

H30 = Perceived control does not affect mobile users' information privacy concerns

H3a = Perceived control affects mobile users' information privacy concerns

H40 = App permission concerns do not affect mobile users' information privacy concerns.

H4a = App permission concerns affect mobile users' information privacy concerns.

H50 = Mobile users' information privacy concerns do not affect the intention to accept app permissions.

H5a = Mobile users' information privacy concerns affect the intention to accept app permissions.

The operational definitions of variables that we used as the basis for developing the research instrument are shown in Table 1.

Table 1. Operational Definitions of Variables

Variables	Dimensions	Indicators	Data Type
Prior privacy experience (PPE)	*Prior privacy experience* (PPE)	1. How often have you personally experienced incidents whereby your personal information was used by some company or e-commerce website without your authorization? 2. How often have you personally been the victim of what you felt was an improper invasion of privacy?	Ordinal
Computer anxiety (CA)	*Computer anxiety* (CA)	1. Computers are a real threat to privacy in this country. 2. I am anxious and concerned about the pace of automation in the world. 3. I am sometimes frustrated by increasing automation in my home.	Ordinal

Perceived control (PC)	*Perceived control* (PC)	1. How much control do you feel you have over your personal information that has been released? 2. How much control do you feel you have over the amount of your personal information collected by mobile apps? 3. Overall, how much in control do you feel you have over your personal information provided to mobile apps? 4. How much control do you feel you have over who can get access your personal information? 5. How much control do you feel you have over how your personal information is being used by mobile apps?	Ordinal
App permission concerns (APC)	*App permission concerns* (APC)	If I would install this app on my mobile device, ... a. It would bother me when i am asked to accept these app permissions. b. I would think twice before accepting these app permissions. c. It would bother me to accept these app permissions.	Ordinal
Privacy concerns (PVC)	*Perceived surveillance* (PS)	If I would accept these app permissions, ... a. I believe that my mobile device would be monitored at least part of the time. b. I would be concerned that the app is collecting too much information about me. c. I would be concerned that the app may monitor my activities on my mobile device.	Ordinal
	Perceived intrusion (PI)	If I would accept these app permissions, ... a. I feel that as a result, others would know about me more than I am comfortable with. b. I believe that as a result, information about me that I consider private would be more readily available to others than I would want. c. I feel that as a result, information about me would be out there that, if used, would invade my privacy.	Ordinal
	Secondary use of personal information (SU)	If I would accept these app permissions, ... a. I would be concerned that the app may use my personal information for other purposes without notifying me or getting my authorization. b. I would be concerned that the app may use my information for other purposes. c. I would be concerned that the app may share my personal information with other entities without getting my authorization.	Ordinal
Intention to accept app permissions (INT)	*Intention to accept app permissions* (INT)	Given these app permission requests, specify the extent to which you would accept these app permissions. a. unwilling–willing b. unlikely–likely c. not probable-probable d. impossible–possible	Ordinal

To collect data from the sample, we used a Google Form-based online questionnaire to students in Batam.

For data analysis, we used SPSS 16 using Pearson Product Correlation for validity test and Cronbach's Alpha test for reliability test. The standard we used has minimum reliability of 0.6.

The analytical method that we used is multiple linear regression. To use this method, the research model we used will be divided into 2 regressions, namely:

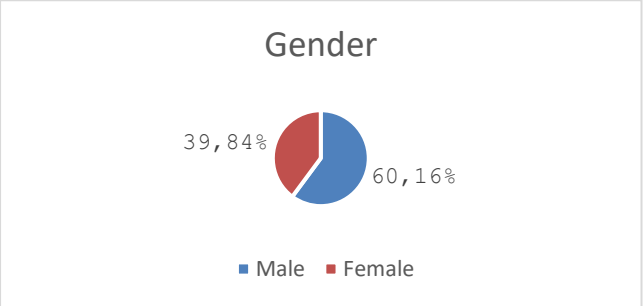
1. Regression 1 has 4 independent variables, namely Prior privacy experience, Computer anxiety, Perceived control, App permission concerns and has 1 dependent variable, namely Mobile users' information privacy concern.
2. Regression 2 has 1 independent variable, namely Mobile users' information privacy concern with 1 dependent variable, and namely Intention to accept app permissions.

RESULT AND DISCUSSION

The data that was obtained from the results of questionnaires in the Google Forms were 132 samples and 128 samples were eligible to be tested. Corresponding with Figure 1, the total number of samples obtained was dominated by men as many as 77 respondents. While women obtained were as many as 51 respondents.

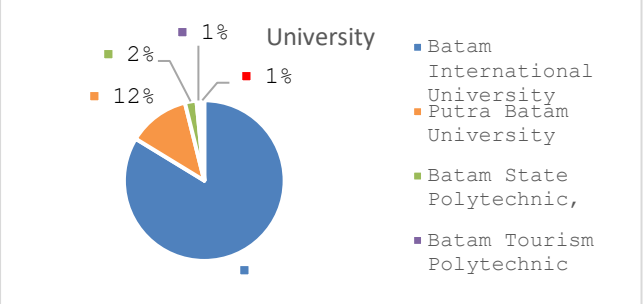
P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390

Figure 1. Distribution of Gender



In accordance with Figure 2, the number of samples obtained is dominated by students from Batam International University with a total of 108 respondents. The others consisted of 16 respondents from Putra Batam University, 3 respondents from Batam State Polytechnic, 1 respondent from Batam Tourism Polytechnic and 1 respondent from Universal University.

Figure 2. Distribution of University



Descriptive Statistic

Based on Table 2, it can be concluded that the descriptive statistics with a sample of 128 respondents, prior privacy experience has a minimum value of 1 and a maximum value of 5. The average value of prior privacy experience from these 128 samples is 2.63, which means that Batam students in general have some prior privacy experiences with privacy violations. The standard deviation value is 1.23 (below the average), which means that the spread of the data distribution is low, but the highest among other variables.

Computer anxiety has a minimum value of 1 and a maximum value of 5. The average value of computer anxiety from these 128 samples is 3.26, which means that Batam students in general have decently high computer anxiety. The standard deviation value is 1.02 (below the average), which means that the spread of the data distribution is low.

Perceived control has a minimum value of 1 and a maximum value of 5. The average value of perceived control from these 128 samples is 3.55, which means that Batam students in general have pretty high perceived controls. The standard deviation value is 0.87 (below the average), which means that the spread of the data distribution is low.

App permission concerns have a minimum value of 1.33 and a maximum value of 5. The average value of perceived control from these 128 samples is 3.69, which means that Batam students in general have pretty high app permission concerns. The standard deviation value is 0.92 (below the average), which means that the spread of the data distribution is low.

Privacy concerns have a minimum value of 1.44 and a maximum value of 5. The average value of perceived control from these 128 samples is 3.86, which means that Batam students in general have pretty high privacy concerns. The standard deviation value is 0.75 (below the average), which means that the spread of the data distribution is low.

Intention to accept app permissions has a minimum value of 1.75 and a maximum value of 5. The average value of perceived control from these 128 samples is 3.56, which means that Batam students in general have pretty high intentions to accept app permissions. The standard deviation value is 0.7 (below the average), which means that the spread of the data distribution is low, and it is the lowest among other variables.

Table 2 Descriptive Statistic

VAR	NUM	AVG	MAX	MIN	STDEV
PPE	128	2.63	5	1	1.23
CA	128	3.26	5	1	1.02
PC	128	3.55	5	1	0.87
APC	128	3.69	5	1.33	0.92
PVC	128	3.86	5	1.44	0.75
INT	128	3.56	5	1.75	0.7

Validity Test and Reliability Test

The results obtained from the validity test using Pearson Product Correlation and the reliability test using Cronbach's Alpha test with a minimum reliability standard of 0.6; all research variables are declared valid and reliable.

Coefficient of Determination test (R^2 Test)

The results obtained in the Coefficient of Determination test, regression 1 shows a value of 0.599 and Adjusted R2 shows a value of 0.359. It means that the prior privacy experience variable, computer anxiety variable, perceived control variable, and app permission concern variable simultaneously have an influence on the mobile users' information privacy concerns variable by

40%, while 60% is influenced by external variables not examined.

While regression 2 shows a value of 0.063 and Adjusted R2 shows a value of 0.055. This means that the variable mobile users' information privacy concerns have an influence on the intention to accept app permissions by 5.5%, which means that there are variables that are not examined that have an influence of 94.5% on the intention to accept app permissions.

F-Test

The results obtained in the F-test, regression 1 and regression 2 have sig values of 0.00 and 0.04. With sig < 0.05; then the hypothesis is accepted, which means that every independent variable in regression 1 and regression 2 simultaneously affects the dependent variable.

t-Test

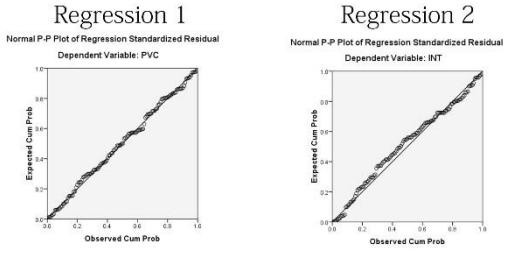
The results obtained in the t-test, regression 2 obtained a sig value as shown in Table 3. The variable mobile users' information privacy concerns obtained a sig value of 0.004. This shows that the variable mobile users' information privacy concerns influence the variable intention to accept app permissions.

Classic Assumption Test

a. Normality test

From the 2 normal p-plot graphs in regression 1 and regression 2 (see Figure 3), it is known that the distribution of plot points follows and approaches the diagonal line so that it can be concluded that the data is normally distributed.

Figure 3. P-Plot Graph for Regression 1 and Regression 2



b. Multicollinearity Test

Based on the multicollinearity test, the tolerance value for regression 1 and regression 2 reach more than 0.1 and the VIF value for regression 1 and regression 2 was less than 10.0. This shows that regression 1 and regression 2 are free from multicollinearity.

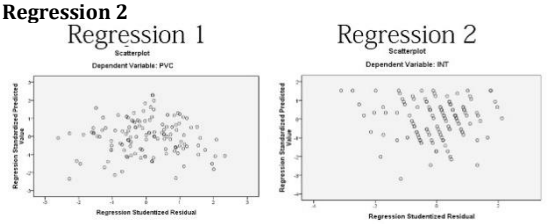
Variables	Coefficient B	Sig	Hypothesis
PPE	0.135	0,007	$H1_0$ rejected, $H1_a$ accepted
CA	0,110	0,071	$H2_0$ accepted, $H2_a$ rejected
PC	0,094	0,166	$H3_0$ accepted, $H3_a$ rejected
APC	0,292	0,00	$H4_0$ rejected, $H4_a$ accepted

Variables	Coefficient B	Sig	Hypothesis
PVC	0.135	0,004	$H1_0$ rejected, $H1_a$ accepted

c. Heteroscedasticity Test

From the 2 normal scatter plots in regression 1 and regression 2, it is known that the spread of the plot points is seen that the scattering data points do not form a certain pattern and their position is in a state of distribution. Thus, it can be concluded that regression 1 and regression 2 are free from heteroscedasticity cases.

Figure 4. Normal Scatter Plot for Regression 1 and Regression 2



d. Autocorrelation Test

Based on the autocorrelation test, the Durbin-Watson value in regression 1 was obtained at 1.727 compared to the Durbin-Watson table where the dL value is 1.6476 and the dU is 1.7763. Due to the Durbin-Watson value was obtained by regression 1 between dL and dU, it couldn't be concluded with certainty. The autocorrelation test in regression 1 was carried out using the run test method. Based on the results of run test regression 1, the asymp value. Sig obtained 0.478 which is greater than 0.05; it could be concluded that regression 2 is exempt from the autocorrelation.

The results of the autocorrelation test of regression 2, the Durbin-Watson value was obtained at 1.739 compared to the Durbin-Watson table whose dL value

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390

was 1.6957 and the dU value was 1.7271. Because the Durbin-Watson value obtained by regression 2 is greater than dU, it could be concluded that regression 2 was free from autocorrelation.

CONCLUSION

The purpose of this observation is to understand the perspective of students at Batam on app permissions and the factors that affects it. This observation was done with quantitative method that was held with online questionnaire.

According to the data that has been received, this observation has proven that mobile users' privacy concerns have an influence on the intention to accept application permission, however computer anxiety and perceived control does not affect user's privacy concern. It means that students in Batam reconsider the safety of their information privacy in their mobile phone before deciding to download the app, yet they do not have any concern with the amount of control they have on their personal information or worry about computer technology regarding to the privacy of their information. This provides a different conclusion with the observation from Degirmenci [3] whereas privacy concerns on application permission requests have a significant impact twice as much as the influence of factors such as prior privacy experience, computer anxiety, and perceived control over technology.

This study also proves that mobile users' privacy concerns have little effect on their willingness to accept app permission. Batam students do not have big concerns when receiving app permission requests from mobile apps, so the possibility of accepting app permission is greater. This provides a conclusion that is comparable to [5] where although students are aware that the use of personal information incorrectly often occurs, it does not hinder or affect the use of applications among students.

Factors such as prior privacy experience, computer anxiety, perceived control, application permission concerns have an impact on privacy concerns of mobile users' personal information, meaning students are aware of privacy security. However, mobile users' information privacy concerns do not have a significant impact on their willingness to receive applications. This leaves students with little concern about the impact on privacy of information and has the possibility of willingly accepting application permissions in the end. This is because Batam students prioritize the functionality of the mobile application rather than paying attention to their privacy. Therefore, when an app permission request appears prior to the installation of an app, it is very easy for them to allow it without a second thought.

This research can be a reference for readers who want to know about the level of concern about the privacy of personal information on mobile devices for students in Batam. Therefore, we suggest for users of mobile apps to start considering factors such as prior privacy experience, computer anxiety, perceived control, application permission concerns, and the mobile users' information privacy concerns before accepting the app permission request.

SUGGESTION

Based on the results of the research discussion and the conclusions above, the suggestions given to future researchers are as follows:

1. The variables used in this study have a small impact, therefore future research can add other variables related to the intention to receive application permission to discover factors that can affect the intention to receive application permissions.
2. This research was only conducted on students in Batam. Should the results be closer to the actual conditions, future research is expected to increase the number of populations that are not only specifically for Batam students.

REFERENCE

[1] A. D. Samala, B. R. Fajri, and F. Ranuharja, "Desain Dan Implementasi Media Pembelajaran Berbasis Mobile Learning Menggunakan Moodle Mobile App," *J. Teknol. Inf. dan Pendidik.*, vol. 12, no. 2, pp. 13–19, 2019, doi: 10.24036/tip.v12i2.221.

[2] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, "Little brothers watching you:" raising awareness of data leaks on smartphones," *SOUPS 2013 - Proc. 9th Symp. Usable Priv. Secur.*, 2013, doi: 10.1145/2501604.2501616.

[3] F. Ranuharja, G. Ganefri, B. R. Fajri, F. Prasetya, and A. D. Samala, "Development of Interactive Learning Media Edugame Using

Addie Model," *J. Teknol. Inf. dan Pendidik.*, vol. 14, no. 1, pp. 53–59, 2021, doi: 10.24036/tip.v14i1.412.

[4] M. Kan, "Android Malware Abuses App Permissions to Hijack Phones," 2019. .

[5] K. Degirmenci, "Mobile users' information privacy concerns and the role of app permission requests," *Int. J. Inf. Manage.*, vol. 50, pp. 261–272, Feb. 2020, doi: 10.1016/j.ijinfomgt.2019.05.010.

[6] S. Rosenthal, O. C. Wasenden, G. A. Gronnevet, and R. Ling, "A tripartite model of trust in Facebook: acceptance of information personalization, privacy concern, and privacy literacy," *Media Psychol.*, vol. 23, no. 6, pp. 1–25, 2019, doi: 10.1080/15213269.2019.1648218.

[7] E. W. T. Darmaningrat, H. M. Astuti, and F. Alfi, "Information Privacy Concerns Among Instagram Users: The Case of Indonesian College Students," *J. Inf. Syst. Eng. Bus. Intell.*, vol. 6, no. 2, p. 159, 2020, doi: 10.20473/jisebi.6.2.159-168.

[8] V. Paramarta, M. Jihad, A. Dharma, I. C. Hapsari, P. I. Sandhyaduhita, and A. N. Hidayanto, "Impact of user awareness, trust, and privacy concerns on sharing personal information on social media: Facebook, twitter, and instagram," *2018 Int. Conf. Adv. Comput. Sci. Inf. Syst. ICACSIS 2018*, pp. 271–276, 2019, doi: 10.1109/ICACSIS.2018.8618220.

[9] C. B. Foltz and L. Foltz, "Mobile users' information privacy concerns instrument and IoT," *Inf. Comput. Secur.*, vol. 28, no. 3, pp. 359–371, 2020, doi: 10.1108/ICS-07-2019-0090.

[10] T. D. Dos Santos and V. F. De Santana, "Computer anxiety and interaction: A systematic review," 2018, doi: 10.1145/3192714.3192825.

[11] E. Princi and N. C. Krämer, "Out of Control – Privacy Calculus and the Effect of Perceived Control and Moral Considerations on the Usage of IoT Healthcare Devices," *Front. Psychol.*, vol. 11, no. November, 2020, doi: 10.3389/fpsyg.2020.582054.

[12] A. N. Septikasari, M. Maison, and ..., "Interactive E-book for Physics Learning: Analysis of Students' Characters and Conceptual Understanding," *... J. Sci. ...*, vol. 04, no. March, pp. 25–36, 2021, doi: 10.24042/ijsme.v4i1.7664.

[13] E. O. Kurniawati, A. Kusyanti, and R. I. Rokhmawati, "Analisis Faktor-Faktor yang Memengaruhi Pemahaman Privasi Informasi pada Pengguna Smartphone di XYZ dengan menggunakan Mobile User ' s Information Privacy Concerns (MUIPC)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 4, pp. 1358–1365, 2018.

[14] V. M. Wottrich, E. A. van Reijmersdal, and E. G. Smit, "The privacy trade-off for mobile app downloads: The roles of app value, intrusiveness, and privacy concerns," *Decis. Support Syst.*, vol. 106, pp. 44–52, 2018, doi: 10.1016/j.dss.2017.12.003.

[15] M. J. Tsai, C. Y. Wang, and P. F. Hsu, "Developing the Computer Programming Self-Efficacy Scale for Computer Literacy Education," *J. Educ. Comput. Res.*, vol. 56, no. 8, pp. 1345–1360, 2019, doi: 10.1177/0735633117746747.

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390