An Empirical Study of App Permissions: A User Protection Motivation Behaviour

Ari Kusyanti
Department of Information Technology
Universitas Brawijaya
Malang, Indonesia

Harin Puspa Ayu Catherina
Department of Information System
Universitas Brawijaya
Malang, Indonesia

***Abstract*—Smartphone is one of the telecommunications media that can be used anytime and anywhere. To be able to support the activity of its users, smartphone users install the application on their smartphone. When installing an application, there are permissions provided by the application about data that will be collected. However, many users choose to ignore and do not read the application permission since it is too long or difficult to understand, hence they accept the apps permissions without thinking and consequently leads to security problems. This study aims to determine the factors that affect users in reading apps permissions that have been provided by an application before they install the application. Data were collected from 292 respondents who were active in using smartphones. The data analysis method used is Structural Equation Modeling (SEM). The results of the study show that the factors that influence the user in reading the app permissions before they install the application are coping self-efficacy and personal responsibility.**

Keywords*—Protection motivation theory (pmt); application permission; smartphone; structural equation modeling (SEM)

I. Introduction

Nowadays, smartphone is one of the telecommunications media in the spotlight because it has the sophistication in various things and its effective and efficient functions that can be used anytime and anywhere [1]. A report from the Statista stated that the number of smartphone users in Indonesia in 2018 reached 70.22 million active users [2]. In fact, a few years ago the phone could only be used for the purposes of SMS and placing call only, but nowadays it has evolved into a smartphone that can be used for various purposes such as: social media, games and any other activities.

When users start installing an application, there will be an app permission displayed various data that will be accessed by the application as a perquisite. For example, an application that need to use the camera, microphone, internet, and other resources on smartphone, then Android apps will ask for permission. Apps will be installed if the user accept the apps agreement. To accept the apps permissions without thinking can have consequences, such as identity theft, disclosure of sensitive information without users noticing it, etc. Based on the initial survey that has been done in this study, users are less likely to read what is stated in the app permissions. It was found that the reasons why most users do not read the app permissions are: (1) they are too lazy to read the app permissions since it is too long (2) they think the app permissions is not important (3) reading the app permission is wasting time. The problem raises since some applications are requesting to retrieve some of the information contained on the smartphone that is mostly related to the users' sensitive information. Users are unaware of the problem that might occur in this situation.

As an example, the PlaceRaider app shows the danger of accepting permissions without reading before installing it. This app can take users' photos without permission and recreate room, hence users are vulnerable to be spied on. Another case in 2013, MouaBad malware allowed attackers to place an expensive calls without users noticing. Another malware called FireLeaker allowed the device's system database file to be accessed by attackers. They retrieved data such as phone numbers and other sensitive information and silently uploaded it to a web server managed by the attackers [3].

Based on the aforementioned reason, this study examines what factors that affect smartphone users to read app permissions by using the Protection Motivation Theory (PMT) model. The Protection Motivation Theory (PMT) model used in this study adapts from a study of Tsai et al. (2016) entitled "Understanding of online safety behaviors: A protection motivation theory perspective" which used nine variables to determine the factors that can influence the behavior of users to be able to apply protection against online security threats.

This paper is organized as follow. In section 2 provides the theoretical framework and the development of the hypotheses. Section 3 discuss the methodology and research design. Section 4 provides the results of empirical study while Section 5 includes a thorough discussion of the empirical findings. Finally, the conclusion is presented in Section 6.

II. Theoretical Framework And Hypotheses

A. Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) is used in predicting individual intentions to take protective action [4]. The factors in the research model namely response efficacy, threat severity, prior experience with safety hazard, coping self-efficacy, habit strength, perceived security support, personal responsibility, response cost, threat susceptibility and security intention.

Response efficacy is defined as the degree of user's belief regarding recommended protective behaviour whether it will be effective in terms of preventing or reducing the dangers or

threats. When applying a protective behavior, a user must be able to ensure that the protective behavior he or she is performing is effective in protecting him or her from any danger or threat that might occur.

Threat severity is defined as the extent of the consequences of a threat or a hazard caused by the absence of protective behaviour. When a user does not consider that a threat is serious, then he or she will not apply protective behavior to protect him or her.

Prior experience with safety hazards is defined as the degree of user's previous experiences related to protective behaviour. When a user previously has experience in dealing with threats that occur online then he or she will apply protective behaviour.

Coping self-efficacy is defined as the degree of perceived ability and comfort with respect to user's behavior in conducting online protection. When a user is accustomed and has the ability to deal with online threats then he or she will apply the protective behaviour.

Habit strength is defined as the degree of how strong the habit of a user's ability in applying protective behavior to prevent online threats. When a user has a strong habit of applying protective behavior then he or she will continue to apply the protective behavior

Perceived security support is defined as the degree of the support from others related to applying online protective behavior. When a user is heavily influenced and can feel the support of others in applying protective behaviour, then he or she will apply protective behaviour.

Personal responsibility is defined as the degree of user's beliefs in implementing protective behavior to protect him or her. When a user has a strong belief that he or she can protect him or her from online threats then he or she will apply the protective behavior.

Response cost is defined as the degree of how much time and effort that has to spend to protect the user from online threats. A user will not implement protective behavior when he or she thinks that it takes too much effort in term of time and money.

Threat susceptibility is defined as the degree of vulnerabilities from online threats that may happen to user. A user will implement protective behavior when he or she realizes that he or she is vulnerable to online threats.

Security intention is defined as the degree of how much a user intends to apply protective behaviour. When the user feels that such protective behaviour is important then the user will likely continue to apply recommended protective behaviour.

B. Hypotheses Development

In a study conducted by [4] suggests that the response efficacy evaluates how effective the recommended protective behaviour in reducing a threat. When it comes to enforcing protective behaviour, users should ensure that protective behaviours undertaken will be effective in protecting them from threats. When a user installs an application, the user should read the app permissions provided before they install the application, because by reading the permissions is an effective protection measure to protect the user's smartphone from the perils of hackers who will take the data on their smartphone. Users who are aware that applying this protective behaviour is an effective step in reducing a threat will tend to have an intention to apply that protective behaviour. From this statement, it can be drawn hypothesis as follows:

1) Response Efficacy have a positive effect on Security Intention

Threat severity is used to measure how severe a threat can occur when protective behavior is not applied [4]. Users who consider that the impact of a threat is severe will tend to have the intention to apply protective behaviour. Currently, the use of smartphones can attract the attention of hackers to be able to break the security of the smartphone. One of them by taking data from the smartphone through a slot that is inserted through the app permissions provided when the user will install an application on the smartphone. In this study, this threat involves how severe the consequences of the occurrence of a threat when a user does not read the app permissions prior to installation. Based on the foregone review, the following hypothesis is developed:

2) Threat Severity have a positive effect on Security Intention

Based on study of [5] found that there was a significant relationship between a user's previous experience of a user's intention to apply protective behaviour. When a user has prior experience with online threats then he or she will tend to apply protective behavior. For example, on the use of smartphones when data on the smartphones had been accessed and misused by unauthorized party then a user tends to protect him or her by reading the app permissions prior to installation. Based on this the following hypothesis is developed:

3) Prior Experience with Safety Hazard have a positive effect on Security Intention

According to [5], there is a positive relationship between coping self-efficacy towards user intentions in applying protective behavior. Users who have the ability to protect the security of their data online will tend to implement protective behavior. In this study when a user has the ability to understand the importance of reading an app permissions prior to installation then he or she will not ignore the app permissions. Based on the statement, the hypothesis is drawn as follows:

4) Coping Self-Efficacy have a positive effect on Security Intention

Habit strength is used to measure how strong the habits of a user in applying protective behavior towards threats that may occur online [4]. In this case, user who has a habit and has been accustomed to protect him or her by reading the app permissions prior to installation will not ignore and will read it. According to the explanation, the hypothesis is shown as follows:

5) Habit Strength have a positive effect on Security Intention

As stated in [6] there is a positive relationship between perceived security supports to user's intention in applying protective behavior. When a user feels that he or she is

supported by others in applying protective behavior then he or she will tend to have the intention to apply that protective behavior. When a user has the support from others to read the app permissions before installing an application then he or she will tend to read it. It will also allow user to have the intention to apply protective behavior to avoid potential threats when he or she ignores the app permissions. Based on the discussion the hypothesis can be drawn as the following:

6) Perceived Security Support have a positive effect on Security Intention

In this study, personal responsibility is used to measure user's self-confidence level in implementing protective behavior. A user who knows that by ignoring the app permissions prior to application installation can cause a threat and pose a risk that could harm him or her, then the user will tend to apply the protective behavior by reading the app permissions and understand the meaning of each permission requested by the application. This can prevent the occurrence of threats that may pose a risk to the user. Based on the explanation above, the hypothesis is drawn as follows:

7) Personal Responsibility have a positive effect on Security Intention

Pursuant to [7] found that response cost has a significant relationship to user intentions in applying protective behavior. A user who feels that by applying protective behavior is a waste of time and spent a lot of effort will tend not to apply protective behavior. If a user thinks that by reading the app permissions prior to application installation is something that takes a lot of effort and spends a lot of time then he or she will tend to not read the permissions. Furthermore, even if he or she knows that by reading the app permissions constitute a protective behavior to protect him or her against the dangers and threats that occur online, he or she will ignore it. From this statement, the following hypothesis is developed:

8) Response Cost have a positive effect on Security Intention

In a study conducted by [8] found that threat susceptibility has a significant effect on user intentions in applying protective behavior. A user who feels that he or she is highly vulnerable to any possible threats that may occur online will tend to apply protective behavior to protect himself or herself against online threats. When a user is aware that he or she is vulnerable to a threat by not reading the app permissions prior to application installation then he or she will tend to read the app permissions and continue to apply protective behavior. According to the review above, it can be drawn hypothesis as follows:

9) Threat Susceptibility have a positive effect on Security Intention

Based on the hypothesis that has been formulated above, Fig. 1 depicts the research model used.

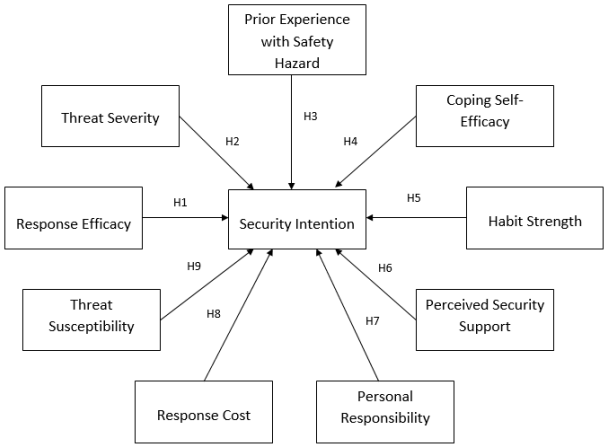

Fig. 1. Research Model

III. METHODOLOGY AND RESEARCH DESIGN

A. Measurement Development

The questionnaire used in this study consisted of two parts. The first part contains respondents' demographic data, and the second part deals with their perceptions of application permissions. All questions in this questionnaire except demographic questions, all are based on a 5-point Likert scale, coded as, 5: strongly agree, 4: agree, 3: neutral, 2: disagree, 1: strongly disagree for measuring response efficacy, threat severity, prior experience with safety hazard, coping self-efficacy, habit strength, perceived security support, personal responsibility, response cost, threat susceptibility and security intention.

The original questionnaire was in English and was not suitable for the targeted subject. Therefore a translation approach is used to ensure that the original meaning will be maintained in Indonesian version. The English version of this instrument was first translated into Indonesian by one author, and then an independent translator translated the questionnaire into English. The original English version and the translation version is then compared, revised and corrected by three experts.

The preliminary analysis was pilot study by using Cronbach's Alpha. All the multi-item scales met the cut-off criteria of 0.6 as suggested by [9]. The value of Cronbach's Alpha for each variable in this study can be seen on Table I.

IV. DATA ANALYSIS AND RESULT

A. Mahalanobis Distance

The outlier test is used to find data that has extreme value by finding the value of Mahalanobis Distance. The result of Mahalanobis Distance equals to 45.13 hence data having Mahalanobis Distance above 45.13 must be removed from data processing. In this study there were 12 data that must be removed. Data that can be used in the next analysis were 280.

B. Kaiser--Meyer-Olkin and Barlett Test of Spericity

Kaiser-Meyer-Olkin Measure (KMO) was used to determine sampling adequacy [10]. The value of KMO in this

study was 0.845 (>0.5) which means that factor analysis is feasible to do.

C. Normality Test

Normality test was used to determine whether the data to be used is normally distributed or not [10]. In this study, the normality test results of 0.068 (>0.5) which indicated that the data used in this study was normally distributed.

D. Homogenity Test

Levene test in this research was used to examine homogeneity of the data. This test was used to evaluate the similarities of variance throughout the data, with an assumption that a variance of a variable must be stable in all levels. Using Levene test would have the same variance if the Sig. value is > 0.05 [10]. In this research, all variables were considered homogeneous.

TABLE I. CRONBACH'S ALPHA VALUE

Factor	Value
Response Efficacy (RE)	0.775
Threat Severity (TS)	0.735
Prior Experience with Safety Hazard (PEW)	0.824
Coping Self-Efficacy (CSE)	0.905
Habit Strength (HS)	0.727
Perceived Security Support (PSS)	0.745
Personal Responsibility (PR)	0.824
Response Cost (RC)	0.675
Threat Susceptibility (TSUS)	0.721
Security Intention (SIN)	0.882

E. Measurement Model Fit

Measurement model fit was useful to determine the manifest variable (indicator) actually has a relationship with the latent variable (construct). This test was done by using Confirmatory Factor Analysis (CFA) method. Measurement model fit test results can be seen in Table II. Based on Table II, all values in this study met the specified criteria. Therefore the analysis can be continued at the structural model fit stage.

F. Structural Model Fit

Structural model fit was performed to evaluate the relationship between variables that have a causal relationship or mutual relationship influence. This test was done by using Path Analysis method and the result showed in Table III.

Based on the results of structural model from 9 hypotheses that have been tested, there are 7 rejected hypothesis and 2 accepted hypothesis.

The impact of coping self-efficacy (p=***) and personal responsibility (p=0.036) on security intention were significant at p=0.05. Thus, H4 and H7 can be accepted. Meanwhile, respond efficacy, threat susceptibility, prior experience with safety hazard, habit strength, perceived security support, response cost and threat susceptibility have no significant impact on the intention to read the application permission, and thus H1, H2, H3, H5, H6, H8 and H9 were rejected.

TABLE II. GOODNESS OF FIT INDEX VALUE

Index	Criteria	Value	Result
Chi-Square	> 0.05	807.91	Good
CMIN/DF	1<CMIN/DF< 3	1.616	Good
GFI	> 0.8	0.810	Good
RMSEA	< 0.08	0.059	Acceptable Fit

TABLE III. HYPOTHESES RESULTS

	Hypotheses	P < 0.05	Result
H1	SIN ← RE	.601	Rejected
H2	SIN ← TS	.347	Rejected
H3	SIN ← PEW	.331	Rejected
H4	SIN ← CSE	***	Accepted
H5	SIN ← HS	.371	Rejected
H6	SIN ← PSS	.785	Rejected
H7	SIN ← PR	.036	Accepted
H8	SIN ← RC	.108	Rejected
H9	SIN ← TSUS	.824	Rejected

V. DISCUSSION

A. Discussion on Hypothesis 1

In testing hypothesis H1, the results failed to support the proposition. Respondents feel that they are not convinced by reading the app permissions prior to application installation is an effective way in preventing or reducing the dangers and threats that may occur. They assume that there will be no danger or threats that occur even if they do not read the permissions of an application. Thherefore they have no intention to read the permissions of an application before they install the application. Therefore, in this study response efficacy (RE) had no significant effect on security intention (SIN).

The finding may further imply [11] which suggested that when users feel that the protective behavior to be applied is not an effective way of protecting them from the dangers and online threats then they will tend to have no intention in applying such protective behavior.

B. Discussion on Hypothesis 2

Hypothesis 2 was rejected. Based on the results of hypothesis testing 2, it can be concluded that respondents assume that the danger or threat caused by not reading the app permissions prior to application installation is not a severe threat. They also assume that even if they do not read the app permissions before they install the application there will be no serious threats that will occur. Thus, it makes them have no intention of reading the app permissions before they install the application. It established that in this study threat severity (TS) did not have significant influence on security intention (SIN).

The results of this study together with the results of research conducted by [4] who argued that when a user feels that a threat does not have a negative impact on the user then the user will tend to not have any intention in applying protective behavior.

C. Discussion on Hypothesis 3

With regards to H3, the results supported a negative relationship which indicates that respondents have no prior experience related to the hazards or threats caused by not reading the app permissions before they install the application. In previous experience, they feel there is no danger or threat that occurs because they do not read the permissions of an application. Thus, they have no intention of reading the app permissions as a protective behaviour. Therefore, in this study prior experience with safety hazard (PE) had no significant effect on security intention (SIN).

Prior literature [12] suggested that when users have no prior experience that could adversely affect their use of online applications, they will tend to have no intention of implementing protective behavior.

D. Discussion on Hypothesis 4

The results of hypothesis H4 supported the proposition that that respondents assume that when they have the ability to know about how severe a danger or threat that might occur when they choose not to read the app permissions before they install the application, it will make them have the intention to continue reading the app permissions as an act to protect themselves online. A significant direct association was found between coping-self efficacy (CSE) and security intention (SIN).

Similarly, previous literature [11] argued that when users have the ability to know and use an application and they have a sense of comfort in using it then the user will tend to continue to have intention in using the application.

E. Discussion on Hypothesis 5

In testing hypothesis H5, the results revealed a negative relationship. Respondents feel they do not have a habit to understand or read the app permissions before they install the application, even they tend to ignore it. It proved that most respondents in this study did not have a habit to read the app permissions before they installed the application. Thus, reading the app permissions is not considered as a protective behaviour. It indicated that in this study habit strength (HS) did not have significant influence towards security intention (SIN).

The finding is supported by [13] who suggested that when users do not have a strong habit of applying protective behavior then the user will tend to have no intention in implementing the recommended protective behavior.

F. Discussion on Hypothesis 6

Hypothesis 6 was accepted. Based on the results of hypothesis testing 6, it can be concluded that respondents do not have support from other parties related to the hazards or threats caused by not reading the app permissions before they install the application. If users do not have support from other parties, they will tend to feel that there is no danger or threat that occurs because they do not read the app permissions. This is because there is no single party around those who are exposed to such dangers or threats. Therefore, respondents have no intention in reading the app permission as a protective behavior. This revealed that in this study perceived security support (PSS) did not have significant influence on security intention (SIN).

The results of this study are similar to those of [4] who suggested that when users feel that no party around them can adversely affect or harm them on the use of an online application then they will tend to have no intention in implementing the protective behavior.

G. Discussion on Hypothesis 7

As it has been hypothesized, Hypothesis H7 supported the proposition that respondents have high confidence and responsibility in protecting themselves against the dangers or threats caused by reading the app permissions before they install the application. Respondents have a sense of confidence and responsibility arising from their own consciousness that by reading the app permissions is considered an act to protect themselves from possible dangers or threats. Thus, it encourages them to have an intention to read the app permissions prior to application installation. This study posited a significant relationship between coping-personal responsibility (PR) and influence on security intention (SIN).

This result confirmed previous literature [4] who argued that when a user has a high sense of responsibility in protecting themselves against threats or dangers online it will encourage the user to have intentions in implementing protective behavior.

H. Discussion on Hypothesis 8

Hypothesis 8 was not supported. Respondents consider having to read the app permissions before they install the application is a very time-consuming and requires a lot of effort. Furthermore, it is not guaranteed that they will be suffered from dangers or threats that may occur. They also find it uncomfortable to read the app permissions hence they have no intention of reading the app permissions prior to application installation. This study posited a negative relationship between response cost (RC) and security intention (SIN).

This is consistent with previous findings [14] which suggested that when users feel they need to take a lot of effort in using an application then they will tend to have no intention in using the application.

I. Discussion on Hypothesis 9

Hypothesis 9 was unaccepted. From the test result of Hypothesis 9, it can be concluded that respondents assume when they decide not to read the app permissions before they install the application there will be no high vulnerability to threats or dangers that may occur and harm them. They also assume that even if they do not read the app permissions, they will not be vulnerable to threats, hence they have no intention to read the app permissions before installing an application. The result found a significant relationship between treat susceptibility (TSUS) and influence on security intention (SIN).

The finding of this study with regard to threat susceptibility is consistent with previous studies [4] who argued that when users feel that they will not be vulnerable to threats caused by the use of an application then they will tend to not apply protective behaviour.

VI. CONCLUSIONS

This study aims at contributing in this viewpoint by determining the factors that influence users to read the app permissions before they install an application. Based on the results of the study, there are 2 factors that are found, namely: coping self-efficacy and personal responsibility. With regards to coping self-efficacy, respondents will read the app permissions prior to application installation as an effective way to prevent or reduce the dangers and threats that may occur since they have the ability to understand the importance of reading an app permissions as a protective behaviour. Meanwhile, concerning personal responsibility, respondents have high confidence and responsibility in protecting themselves against dangers or threats by reading the app permissions prior to installation. Additionally, the result of this study can raise users' awareness and inform them in term of protecting themselves by reading the app permissions before installing an application.

REFERENCES

[1] Gary B. S., Thomas J. C., & Misty E. V., 2007. Discovering Computers: Fundamental 3rd.

[2] Statista. 2018. Number of smartphone users in Indonesia from 2011 to 2022 (in millions)* https://www.statista.com/statistics/266729/smartphone-users-in-indonesia/

[3] Benedetti, F. F. 2014. Stop ignoring Android app permissions. https://en.softonic.com/articles/stop-ignoring-android-app-permissions

[4] Tsai et al. 2016. Understanding of online safety behaviors: A protection motivation theory perspective. *Computers & Security* Journal. Volume 59, June 2016, Pages 138-150

[5] Lee D, LaRose R, Rifon NJ. 2008. Keeping our network safe: a model of online protection behaviour. Behav Inf Technol;27(5):445–54. doi:10.1080/01449290600879344.

[6] Luarn P, Lin H-H. 2005. Toward an understanding of the behavioral intention to use mobile banking. Comput Human Behav;21(6):873–91. doi:10.1016/j.chb.2004.03.003.

[7] Liang H, Xue Y. 2010. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J Assoc Inf Syst;11(7):394–413.

[8] Zahedi FM, Abbasi A, Chen Y. 2015. Fake-website detection tools: identifying elements that promote individuals' use and enhance their performance. J Assoc Inf Syst;16:448–84

[9] Hair Joseph F. Jr., Black William C., Babin Barry J., Anderson Rolph E. & Tatham Ronald L. 2006. Multivariate Data Analysis, 6th edn, Pearson Prentice Hall, Pearson Education, Inc., Upper Saddle River, New Jersey 07458.

[10] Field, A., 2009. Discovering statistics using spss. 3rd ed. [e-book]. Sage Publications. Web Page: http://fac.ksu.edu.sa/sites/default/files/ktb_lktrwny_shml_fy_lhs.pdf

[11] Pahnila, S., Siponen, M., and Mahmood, A. 2007. Which Factors Explain Employees' Adherence to Information Security Policies? An Empirical Study. Pacific Asia Conference on Information Systems (PACIS)

[12] Hsieh, J. Y., & Liao, P. W. 2011. Antecedents and Moderators of Online Shopping Behaviour in Undergraduate Students. Social Behavior and Personality.

[13] Shin, K-h., Kim, G., and Lee, C., Y., 2014. A Study on Behavioral Intention and Use Behavior of Sharp (#) Mail Initial Experienced Users. Contemporary Engineering Sciences, Vol. 7, 2014, no. 30, 1657 – 1663

[14] Jeong, B. K., and Yoon, T. E. 2013. An Empirical Investigation on Consumer Acceptance of Mobile Banking Services. Business and Management Research ISSN 1927-6001 (Print) ISSN 1927-601X (Online)