# Security Intention: Creating and Protecting Google Password

Ari Kusyanti
Department of Information Technology
Universitas Brawijaya
Malang, Indonesia
ari.kusyanti@ub.ac.id

Harin Puspa Ayu Catherina
Department of Information System
Universitas Brawijaya
Malang, Indonesia
harinpuspa@gmail.com

Yustiyana April Lia Sari
Department of Information System
Universitas Brawijaya
Malang, Indonesia
yustiyana.lia@gmail.com

***Abstract*— Google is a multinational company in the US that focuses on Internet product and service. To use the various services from Google, the users must own a Google account. In registering process to create a new Google account, the users are asked to create a password to protect the account. The password regulation policy made by Google requires all the users to develop a password for their Google account according to the policy applied. This study aims to analyze the behavior of the users with Google account case study by using 11 construct variable adapted from Protection Motivation Theory (PMT). The data is collected from the Google users that consists of 285 respondents. The data analysis method used in this study is structural equation modelling (SEM). The study result shows that the factor affecting the intention is perceived vulnerability and threat suspensibility.**

***Keywords*— Google, SEM, intention, PMT**

## I. INTRODUCTION

Google is one of US's multinational enterprise specifically providing the internet products and services. This company offers productivity softwares within network, includes electronic mail (e-mail), an office suite, and social media [1]. To get a charge out of a range of Google services, users are obliged to possess a Google account as its condition. During the process of making the account, the users are requested to create password for the sake of account's security.

In any Google account controlled by the users, there must be some information that is secretive, such as personal information of the users that needs authentification to secure the privacy and security of Google account owned by each user. Still, there are some problems found during the authentification or verification—identifying whether the users reserve the right to enter the system by only filling the username and passwords—since it was perceived insecure. The users often create password with predictable words such as names or date of birth. In order to avoid the villains guessing the password, the organization create new policy concerning the password. It must have minimum characters which includes capital letters and numbers which are not parts of words in a dictionary [2].

Google itself must have a policy in regards to the process of creating the password used in a Google account. The entire users of Google who own accounts are obliged to create a password based on the policy determined by Google. The policy covers: capital and small letters, numbers, symbols, and space. Additionally, Google does not allow its users to re-use the old password in the same account. Google will automatically block such predictable password. Next, various notifications will appear when the users create a combination of the old passwords, such as "Complicated", "Too Short", and "Weak". The notification pops up when the users are creating the password and gives an information whether the passwords being created has suited the policy which has been decided.

In 2014, a cite belongs to Russia published 5 million passwords from the owner of Google accounts. The report showed that around 60% of the hacked passwords are valid, owned by the users of mail google accounts. The hacked data were of importance and exhibited in Bitcoin Forum, Russia [3]. This study adapted some researches conducted previously, i.e. a research done by [4] entitled "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords" studied about perceived severity, perceived vulnerability, fear, response efficacy, response cost which is impactful towards intentention by using framework from Protection Motivation Theory (PMT). On the other hand, the variables of threat severity, coping self-efficacy, perceived security support, threat susceptibility, prior experience with safety hazards and subjective norm, were adapted from a research by [5] which affected security intention by using a framework from Protection Motivation Theory (PMT). The purpose of this research was to examine whether some factors namely perceived severity, perceived vulnerability, fear, response efficacy, response cost, threat severity, coping self-efficacy, perceived security support, threat susceptibility, prior experience with safety hazards and subjective norm could influence security intention or the attitude of users of Google accounts.

## II. MODEL STRUCTURE AND HYPOTHESIS

This study is a quantitative-confirmatory study which aims at examining research model and hypothesis as done by [4] and [5]. Data analysis in this study uses Structural Equation Modeling (SEM). SEM is used to analyze independent and dependent variables which are interrelated in shaping a model. SEM analysis was done through 2 steps, namely structural


https://sites.google.com/site/ijcsis/
ISSN 1947-5500

model and measurement model test. Structural model describes a relation between laten variables which are generally linear. The measurement model is used to measure the relation between indicator and variables.

### *A. Definition of each construct*

Threat Severity (TS)

It studies how far someone could feel the existence of negative consequence caused by the danger of IT [6] Besides, it discusses on how people would believe a threat for their lives. If someone does not aware the severity of such threat, then there will be no defending motivation which will change users' behavior. Violating the password could cause the information exposed, even the most important to the most private ones [4].

Perceived Vulnerability (PV)

When the computer users tends to choose weak password, it means that it consists of predictable words from dictionary [7]. The users believe that people with important information or people who are not bothered by the existence of hackers are those who must concern with the risks of computer [8].

Fear (FEAR)

It is an emotional response toward the menace which could change attitude or behavior [9]. It happens to the users who are afraid of improving their intention to use or create strong password. They will tend to spend their efforts in securing their account by frequently renewing their passwords.

Response Efficacy (RE)

Strong password could secure online accounts. Besides using strong key words, the renewable passwords could also help to protect online accounts from harmful hackers [4].

Response Cost (RC)

According to [4], response cost refers to the time and effort spent by the users in creating and renewing password. Most of the users often forget their password and hard to remember it. Creating strong password and renewing it gradually increase users' incovenience in using their online accounts. Thus, the users often use their password for more than one accounts to decrease their time and effort in making new password.

Subjective Norm (SN)

In pursuant to [5], subjective norm refers to individual's perception on how the other ones who are important for his/her to decide how he/she should behave. Meanwhile, according to [10], they revealed that social impacts are of social norms referring to the perception on how others would behave.

Prior Experience with Safety Hazard (PE)

As stated by [5] prior experience with safety hazard is related to the previous individual who concerns with an experience in handling online threats. On a research done by [5] prior experience with safety hazard is used to measure whether someone have an experience previously with their main computer.

Threat Susceptibility (TSUS)

According to [5], threat susceptibility is employed to measure a series of threats that are possible for the users to experience the threats on security online.

Perceived Security Support (PSS)

Based [6], perceived security support is used to measure supports from other people.

Coping Self-Efficacy (CSE)

As stated by [5] coping self-efficacy is used to assess an ability and convenience felt regarding someone's behavior in doing protection online.

Security Intentions (SI)

According to [6] security intention is used to measure how big users' intention is in protecting their online accounts.

### *B. Hypothesis for the construct*

Threat Severity including generic overview of Internet usage could pose a threat varying degrees of severity. Furthermore, the level of threat is found to be positively related to intention to adopt email security services [11]. Thus, we hypothesize:

*H1: Threat severity has a positive effect on security intention.*

Vulnerability concerns the susceptibility will be a threat. Password regarded as a vulnerability to threats. First, the hacker can employ a variety of techniques to attack the user's password. For example, hackers can use keyword-based attacks - a dictionary word, the technique of using the program to guess passwords by finding possible combinations include common words, slang and popular phrases. Since computer users tend to choose to use a bad password, word-based attacks - said the dictionary would be very efficient [7]. Passwords can also be unpredictable after studying an individual's personal information such as birthdays, spouse or spouse's name, pet's name. Hence, we hypothesize:

*H2: Perceived vulnerability has a positive effect on security intention.*

Fear refers to fears triggered by the threat. Fear is an emotional response to a threat that can cause a change in attitude or behavioral intentions [9]. It is assumed that the fear of increasing the intention to use a secure password. If the user is online afraid of the threat of attack to guess passwords or hacked by others, they will be more likely to spend more effort in maintaining and updating their passwords. Therefore, we hypothesized:

*H3: Fear has a positive effect on security intention.*

Response efficacy evaluate how effective coping responses suggested in reducing the threat. In implementing behavioral protection, the individual must make sure that the protective


https://sites.google.com/site/ijcsis/
ISSN 1947-5500

behaviors that do will be effective in protecting them against the threat. In addition to using strong passwords to protect online accounts, renew regular password also helps protect online accounts from malicious hackers. People will be more involved in the protection behavior if they believe that their extra effort to create a secure password valuable. Therefore, we hypothesized:

*H4: Response efficacy has a positive effect on security intention.*

Response cost measure a fee (eg, time, money, effort), one must pay when doing behavioral protection. As a result, response cost reduces the possibility of selecting the recommended action. In information security, the researchers found that the barriers of implementing security practices negatively related to the attitude of the people of the security policy [12]. Thus, we hypothesized:

*H5: Response cost has a positive effect on security intention.*

Subjective norm becomes an important factor of the security-related behavior. Social norms and subjective norms have been used to refer to the same concept in several studies [10]. In addition to social norms and subjective, descriptive norms referring to the attitude or behavior of online security. Because online security behavior can be calculated as planned behavior in accordance with the theory of planning behavior [13]. In the PMT models, subjective norm and deskriptiv coupled with the social norm. Based on this reasoning, we hypothesize:

*H6: Subjective norm has a positive effect on security intention.*

Prior experience (such as viral infections) is not included in the original PMT models [14]. In a survey of college students, prior experience with viral infection significantly to the intention to use virus protection [15]. In our study, prior experience with regard to previous experience in dealing with online threats. Hence, we hypothesize:

*H7: Prior experience has a positive effect on security intention.*

Threat susceptibility discusses about security threats. Therefore, we hypothesized:

*H8: Threat susceptibility has a positive effect on security intention.*

Perceived security support is one contribution that individuals perform security protection. A person can receive support from others when someone is needed to take the decision to commit acts of security protection [6]. Therefore, we hypothesized:

*H9: Perceived security support has a positive effect on security intention.*

Self - efficacy may directly or indirectly reduce the intention to open a commercial email message or attachment [16]

*H10: Coping self - efficacy has a positive effect on security intention.*

Based on the above hypotheses, we developed the research model as shown in Fig. 1.

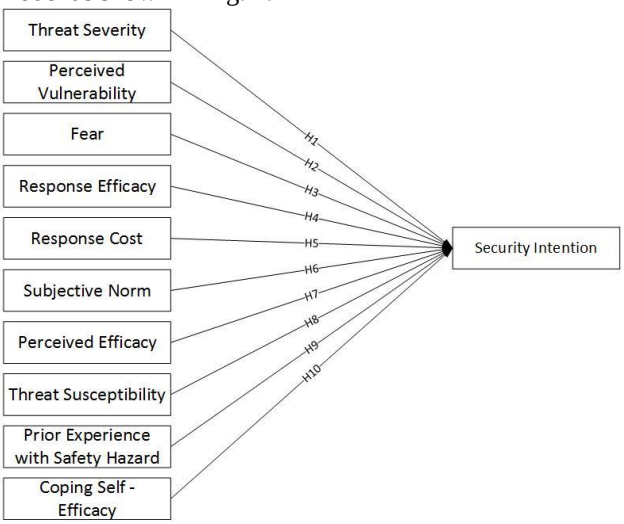


Figure 1. Research Model

Model in Fig. 1 is a model that will be used in this study, depicting the relation between laten variables. Variables investigated in this study are 12 laten variables and 36 manifets variables or the so called indicator.

## III. DATA ANALYSIS

Statistical Analysis of SEM was employed to analyse the data collected through questionnaires. There are some steps administered to answers the hypothesis as represented on methodology.

### *A. Missing data and outlier*

Test of missing data in this study did not find any missing data. While outlier test was done to find the outliers of a data by searching for the value of mahalanobis distance. The value of mahalanobis distance was measured by error level which is 62.428. This is called outlier since it must be vanished. Out of 300 data of questionnaire, there are 15 outliers so that the rest of it (285) were undergoing the analysis.

### *B. Reliability test*

This test was done by using parameter of cronbach alpha value with a limit more that 0.6. The score of cronbach alpha for each laten variable in this study can be seen on Table 1.

Table 1. Cronbach alpha value

| **Factor** | **Cronbach Alpha** |
|---|---|
| **Limit Value** | **>0,6** |
| TS | 0.885 |
| PV | 0.880 |
| FEAR | 0.772 |
| RE | 0.673 |
| RC | 0.688 |
| SN | 0.686 |


https://sites.google.com/site/ijcsis/
ISSN 1947-5500

| | |
|---|---|
| PE | 0.894 |
| TSUS | 0.881 |

*C. Overall model fit*

To examine the fitness of the data with the model, overall model fit was done. The result of this test can be seen on Table 2. Based on the result analysis of the table, the research model has filled all limits decided, so that it can be concluded that such research model was fit and ready to be used for structural model fit test.

Table 2. Goodness of Fit Indices (GOFI) value

| Indeks | Limit | Value | Info |
|---|---|---|---|
| CMIN/DF | 1.00 < CMIN/DF < 3.00 | 1.211 | Good |
| NFI | >0.9 | 0.890 | Good |
| CFI | >0.9 | 0.978 | Good |
| RMSEA | <0.05 good fit <0.08 acceptable fit | 0.025 | Good Fit |

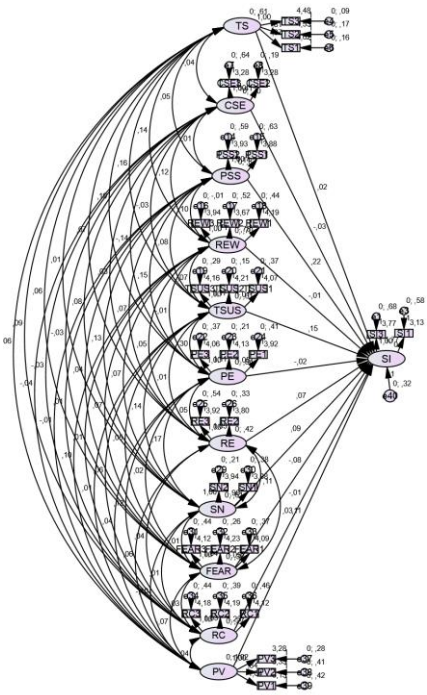


Figure 2. Stuctural model fit using Path Analysis

*D. Structural model fit*

Path Analysis method was used to do the next examination, namely structural model fit test. The test of this model was conducted to know the connection between laten variables on the model. The result of the structural model fit test can be seen through Figure 2.

Tabel 3. The Test Result of structural model and SEM hypothesis model

| Hypothesis | C.R. | P | Result |
|---|---|---|---|
| | >1.96 | <0.05 | |
| SI ← TS | .364 | .716 | Rejected |
| SI ← PV | 2.168 | .030 | Accepted |
| SI ← FEAR | -1.048 | .295 | Rejected |
| SI ← RE | .831 | .406 | Rejected |
| SI ← RC | -.063 | .950 | Rejected |
| SI ← SN | 1.248 | .212 | Rejected |
| SI ← PE | -.354 | .723 | Rejected |
| SI ← TSUS | 2.108 | .035 | Accepted |
| SI ← PSS | 1.762 | .078 | Rejected |
| SI ← CSE | -.582 | .560 | Rejected |
| SI ← REW | -.112 | .911 | Rejected |

The indicators of structural model fit test were values of estimate, critical ratio, and p-value which can be seen completely through Table 3. In pursuant to Table 3, the connection between variables with p-value less than 0.05(*) and C.R more than 1.96 has strong relation and the hypothesis is accepted.

## IV. RESEARCH RESULT

*A. Discussion on Hypothesis 1*

From the result of examining Hypothesis 1, it can be concluded that respondents did not think that a threat on violating the password are severe for their lives so that there is no change on their behavior in creating stronger password. In this research, this shows that threat severity (TS) did not have significant effect toward a factor of users' behavioral intention (INTENTION). Therefore, Hypothesis 1 in this research was rejected.

*B. Discussion on Hypothesis 2*

Based on the result of examining Hypothesis 2, the conclusion draws that the respondents were care of the existence of dictionary words they made so that they were care of the possibility of hackers' assault. This also influences users' intention in creating strong password. In this research, this shows that perceived vulnerability (PV) affects significantly toward user's behavioral intention (INTENTION). Hence, Hypothesis 2 in this research was accepted.

*C. Discussion on Hypothesis 3*

In accordance with the result of examining Hypothesis 3, it reckons that the respondents did not feel afraid of all threats which may appear by using weak and predictable password, so that it did not increase their intention in constructing strong password. This shows that, in this research, a factor of fear (FEAR) did not have compelling effects towards users' behavioral intention (INTENTION). Thus, Hypothesis 3 in this research was rejected.

*D. Discussion on Hypothesis 4*

Based on the result of examining Hypothesis 4, it can be revealed that the respondents were not sure whether the use of strong password will protect their accounts from dangerous hacker's assault, so that it did not increase users' intention in making strong passwords. This showed that, in this research, response efficacy (RE) did not have significant impacts toward


https://sites.google.com/site/ijcsis/
ISSN 1947-5500

the factor of users' behavioral intention (INTENTION). That is why, Hypothesis 4 in this research was rejected.

### *E. Discussion on Hypothesis 5*

In line with the result of examining Hypothesis 5, the conclusion shows that the respondents thought that renewing the password frequently is a waste of time and effortful, so that it did not affect users' intention in creating strong password. This showed that, in this research, it did not affect a factor of users' behavioral intention (INTENTION). Therefore, Hypothesis 5 in this research was rejected.

### *F. Discussion on Hypothesis 6*

Confirming the test result of Hypothesis 6, it can be drawn that the respondents guessed that the other people who mean a lot to them did not influence their intention in creating strong password. This revealed that, in this research, a factor of subject norm (SN) did not significantly affect the users' behavioral intention (INTENTION). Hence, in this research, Hypothesis 6 was rejected.

### *G. Discussion on Hypothesis 7*

From the test result of Hypothesis 7, the conclusion shows that the respondents thought that an experience they have done or once happened in the previous time, did not affect users' intention in creating strong password. This yields a fact that, in this research, a factor of prior experience with safety hazard (PE) did not give crucial effects toward a factor of users' behavioral intention (INTENTION). Thus, Hypothesis 7 in this research was rejected.

### *H. Discussion on Hypothesis 8*

According to the test result of Hypothesis 8, it can be drawn that the respondents perceived that the possibility of online threats could influence their intention in creating strong password. This showed that, in this research, a factor of threat susceptibility (TSUS) significantly affects users' behavioral intention (INTENTION). Therefore, Hypothesis 8 in this research was accepted.

### *I. Discussion on Hypothesis 9*

In pursuant to the test result of Hypothesis 9, it can be concluded that the respondents thought that supports from the others did not give impact to their intention in creating strong password. This showed that, in this research, a factor of perceived security support (PSS) did not give significant effects toward a factor of users' behavioral intention (INTENTION). Therefore, in this research, Hypothesis 9 was rejected.

### *J. Discussion on Hypothesis 10*

Based on the test result of Hypothesis 10, it can be drawn that the respondents perceived that by having an ability and convenience in doing online protection did not affect their intention in creating strong password. This revealed that, in this research, coping self-efficacy (CSE) did not have any significant effects towars users' behavioral intention (INTENTION). Hence, Hypothesis 10 in this research was rejected.

## V. CONCLUSION

According to the result of analysis in this research, it can be concluded that there are two factors affecting the users in creating strong password, namely: perceived vulnerability and threat suspensibility. The respondents were aware of the existence of words from dictionary as the composition of password they made so that they were also care about hackers' threat which possibly happens. The respondents thought that online threats which might possibly happen could influence their intention in creating strong password.

## APPENDIX

| Item | Construct Indicator (measured on five-point, Likert-type scale) | References |
|---|---|---|
| Security Intention | 1. It is possible for me to take a step - security measures to protect my google account<br>2. I would change my password more often | [17], [6] |
| Threat Severity | 1. How dangerous for you a malware if the information is used to commit a crime against me<br>2. How dangerous for you a malware if it makes my computer run slower<br>3. How dangerous for you a malware if it caused the system to crash from time to time | [6] |
| Coping Self-efficacy | 1. Taking a step - a step necessary security completely under my control<br>2. I have the knowledge and resources to take action - password required security measures | [17] |
| Perceived Security Support | 1. I was able to install and use protective software even if there was no one around to tell me what to do<br>2. I was able to install and use protective software even if I do | [6] |


https://sites.google.com/site/ijcsis/
ISSN 1947-5500

| | | |
|---|---|---|
| | not ever use a package like that before | |
| Threat Susceptibility | 1. It is very likely that my account will be hacked in the future<br>2. Possible my google account hacked<br>3. There is a possibility that my account hacked | [6] |
| Prior Experience with Safety Hazards | 1. My google account hacked<br>2. The message of my google account hacked<br>3. Become victims of scams that my account hacked | [5] |
| Response Efficacy | 1. I can protect my online account better if I use strong passwords<br>2. I can protect my online account better if I frequently update my password<br>3. I can protect my online account better if I use a unique password for every my online account | [4] |
| Subjective Norm | 1. Friends - friends that affect the behavior I would have thought that I should take steps - steps to create a strong password<br>2. Another important person for me would think that I should take steps - steps to create a strong password | [17] |
| Fear | 1. I was nervous when someone guesses My password<br>2. I was nervous when someone hijacked my password.<br>3. I was nervous when someone obtain my password | [4] |
| Response Costs | 1. If I use a strong password, it would be difficult for me to remember.<br>2. If I frequently update my password, I'd be hard to remember.<br>3. If I use a unique password for each account, I'd be hard to remember | [4] |
| Perceived Vulnerability | 1. How big is the chance of someone guessing your password?<br>2. What are the chances someone hijacked your password?<br>3. How big is the opportunity for someone to gain your password? | [4] |

## REFERENCES

[1] Google. Tentang Google. 2016. Web Page: https://www.google.co.id/intl/id/about/ [Retrieved on 12 December 2016]
[2] Shay, R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, L.M., Bauer, L., Christin, N., Cranor, L.F., Encountering Stronger Password Requirements : User Attitudes and Behaviors, 2010.
[3] Ridwan,. A. Hacker Bobol Jutaan Akun Pengguna Gmail. 2014. Web Page: http://techno.okezone.com/read/2014/09/11/55/1037630/hacker-bobol-jutaan-akun-pengguna-gmail [Retrieved on 12 December 2016]
[4] Zhang, Lixuan and McDowell, William C.(2009) 'Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords', Journal of Internet Commerce, 8: 3, 180 — 197
[5] Tsai, S.H. et al. Understanding online safety behaviors: A protection motivation theory perspective. 2016
[6] Liang H, Xue Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective. J Assoc Inf Syst 2010;11(7):394–413.
[7] Campbell, J., D. Kleeman, and W. Ma. 2007. The good and not so good of enforcing password composition rules. Information Systems Security 16 (1): 2–8.
[8] Weirich, D., and M. A. Sasse. 2001. Pretty good persuasion: A first step towards effective password security in the real world. Proceedings of the 2001 Workshop on New Security Paradigms, Cloudscrofl, NM, September 10–13.
[9] LaTour, M. S., and H. J. Rotfeld. 1997. There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself. Journal of Advertising 26:45–59.
[10] Johnston AC,Warkentin M. Fear appeals and information security behaviors: an empirical study. MIS Q 2010;34(3):549–66.
[11] Herath T, Chen R,Wang J, Banjara K,Wilbur J, Rao HR. Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. Information Systems Journal 2012;doi:10.1111/j.1365-2575.2012.00420.x.
[12] Herath, T., and H. R. Rao. 2009. Protection motivation and deterrence: A framework for security policy compliance in organizations. European Journal of Information Systems 18:106–125.
[13] Ajzen I. The theory of planned behavior. Organ Behav Hum Decis Process 1991;50:179–211.
[14] Rogers RW. A protection motivation theory of fear appeals and attitude change. J Psychol 1975;91(1):93–114. doi:10.1080/00223980.1975.9915803.

[15] Lee D, LaRose R, Rifon NJ. Keeping our network safe: a model of online protection behaviour. Behav Inf Technol 2008;27(5):445–54. doi:10.1080/01449290600879344.
[16] Chen R,Wang J, Herath T, Rao HR. An investigation of email processing from a risky decision making perspective. Decision Support Systems 2011;52(1):73–81. doi:10.1016/j.dss.2011.05.005.
[17] Anderson CL, Agarwal R. Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q 2010;34(3):613–43. doi:10.1016/j.chb.2004.12.002.


https://sites.google.com/site/ijcsis/
ISSN 1947-5500