Creating and Protecting Password: A User Intention

Ari Kusyanti
Department of Information Technology
Universitas Brawijaya
Malang, Indonesia

Yustiyana April Lia Sari
Department of Information System
UniversitasBrawijaya
Malang, Indonesia

***Abstract*—Students Academic Information System (SAIS) is an application that provides academic information for the students. The security policy applied by our university requires the students to renew their SAIS password based on the university's policy. This study aims to analyze SAIS users' behavior by using six variables adapted from Protection Motivation Theory (PMT), which are Perceived Severity, Perceived Vulnerability, Fear, Response Efficacy, Response Cost and Intentions. The data was collected from 288 SAIS users as respondents. The data analysis method used is Structural Equation Modeling (SEM) analysis. The study result shows that the factors affecting the intention of changing the passwords are perceived severity, fear, response efficacy, and response cost.**

Keywords—Students Academic Information Systems (SAIS); SEM; intention; PMT

I. Introduction

Students Academic Information System (SAIS) enables students to access and process their academic information, such as students' personal information, study plan, courses including exam schedules and grades, and also financial information including registration/tuition fee. Since SAIS is containing sensitive and confidential information about students, authentication process is needed to protect student's privacy and to secure student's SAIS account. Users' authentication or verification problem occurs when password to log in to the system is considered unsafe. The users often use simple and predictable words for passwords like their own names or their birth dates. To prevent unwanted parties knowing users' passwords, the university has made a new policy regarding the password-creating process [1].

Surely our university imposes its own policy concerning password-creating process for SAIS account. All new freshmen who have just received SAIS account with default username and password are required to change their passwords due to the university policy. Soon after the short notice from the university, all sophomores, juniors, and seniors also demanded to change their passwords as well. The policy requires the password to be a combination of at least 8 characters minimum of letter and number. Furthermore, suggestions and notifications will appear when a user is going to set the password, i.e. "use the combination of letters and numbers", "password is good", "password is strong", and "8 characters minimum, with letters and numbers combination". Those notifications will appear to inform the user whether he has made a good password according to the password-creating policy.

This study is similar to a study that has examined the account of students academic information systems at Carnegie Mellon University (CMU) named Andrew account. In December 2009, all Andrew accounts users received an email to change their password for the security of personal information. The password policy applied to Andrew's account contains at least eight characters, and includes at least one uppercase, one lowercase, one digit, and one symbol. The password will also be subject to a dictionary check. If the user does not change the password according to the new policy, the user becomes unable to access their Andrew account.

Several studies have examined how password policy affects user behavior. The result is that although users are aware of security issues but users rarely change their passwords [2]. A survey reported that 90% of 152 computer system users leaked their passwords. The survey also found that users tend to use simple passwords and passwords are used from time to time [3]. A survey conducted by SafeNet found that about half of the respondents wrote down their passwords and about 80% had 3 or more passwords [4].

In determining what factors influence the user to create strong password according to the policy applied, this research is using a model of Protection Motivation Theory (PMT). This model is best suited to investigate the protection motivations of users associated with user behavior in password-creating process. According to the PMT, someone wants to do something because it has its own protection motivation. Protection Motivation Theory (PMT) model consists of two processes, namely, threat-appraisal process and coping-appraisal process. Both processes have each variable that will affect the purpose of implementing strong password-creating process. Therefore, measures of behavioral intention are the typical dependent variable in the PMT. Two meta-analyses of the PMT show that it has been useful in predicting health-related intentions [5].

There is a recent studies on password-creating process by [6] entitled "Encountering Stronger Password Requirements: User Attitudes and Behaviors" which observing the attitude and behaviors related to the use and password-creating process. However, [6] did not include theoretical model that portraying the factors that affect user to create a strong password. Therefore, this research intends to use the research model taken from a study entitled "Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords" by [7], that studied about perceived severity, perceived vulnerability, fear, response efficacy, response cost which affecting intention using framework from Protection Motivation Theory (PMT). Moreover, the intention variable is adapted from the study of

[8] which is used to measure the SAIS users' intention tendencies. This research objective is to examine whether perceived severity, perceived vulnerability, fear, response efficacy, response cost influence SAIS users' intention in creating a strong password.

The outline of this research is in Section 1 explains the background of the issues raised, while Section 2 describes the research model to be used along with the formulation of the hypothesis. Afterwards, Section 3 describes the data analysis and presented in the form of data, and in Section 4 is the discussion exposure from the results of data analysis that has been done. Finally Section 5 is the exposure of the conclusions from the results of data analysis that has been obtained.

II. Model Structure and Hypothesis

This research is confirmatory research based on model and hypothesis by [7] and [8]. The data is analyzed using Structural Equation Modeling (SEM). There are two stages in this SEM analysis: measurement model and structural model. Measurement model is used to determine the relationship between indicator and variables while structural model shows the relationship between latent variables.

The variables that are used in this research are described as follows along with the hypotheses.

A. Definition of each variable

1) Perceived Severity (PS)

Generally, Perceived Severity is used to scrutinize individual's reaction to life-threatening objects. If individual does not aware about how dangerous the threat is, therefore there is no motivation to protect themself and no behavioral change. The violation of passwords can cause sensitive information and personal data leakage [7].

2) Perceived Vulnerability (PV)

When a user chose a weak password, the password is generally a common word and easily predicted [7]. The users believe that only people who has classified information or people who are distraught by the hackers whom should be aware about computer's securities [9].

3) Fear (FEAR)

Fear is an emotional response to a threat which can cause a change in attitude and behavior [10]. The anxious users will be motivated to use strong passwords. Those users tend to do anything to secure their account and change their passwords regularly.

4) Response Efficacy (RE)

Stronger passwords can protect online accounts better. Apart from using strong passwords, regularly changing password can help securing online accounts from malicious hackers [7].

5) Response Cost (RC)

According to [7] Response Cost refers user's time and work spent on creating and recreating passwords. Most users often forgot their passwords and having a hard time to remember their passwords. Using strong passwords and changing it from time to time can cause discomfort for users. That is why most users use one password for many accounts instead of creating different password for each account.

6) Intention (SI)

According to [8] intention is used to measure how strong users' intention is in protecting their online accounts.

B. Hypothesis for the Variables

Perceived by the severity assess how severe is a threat that affects individual's life. The more serious is the individual to feel the negative impact of a threat, the more he will perform the recommended actions. If individual does not consider the impact of a severe threat to his life then there is no motivation protection measures undertaken. Using the Protection Motivation Theory (PMT), researchers showed perceived severity had a significant relationship with the behavior of the protection of such implementing measures as in [11] and [12]. Thus, the hypothesis is:

H1: Perceived severity is positively related to the intention of implementing online password protection.

In protecting an online account, 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 would be very efficient [9]. Passwords can also be unpredictable after studying an individual's personal information such as birthdays, spouse or spouse's name, pet's name. Peoples who have a high degree of vulnerability felt to be more concerned with security or protection of their password [13]. Hence, the hypothesis is:

H2: Perceived vulnerability is positively related to the intention of implementing online password protection.

Fear refers to fears triggered by a threat. Fear is an emotional response to a threat that can cause a change individual's behavioral intentions [14]. If users are 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. There is a positive relationship between fear with compliance with recommended action [15]. Fears increase user intention to use strong passwords. If users are afraid password will be hacked by someone else, they will be more likely to spend a lot of effort to renew their passwords. Therefore, the hypothesis is:

H3: Fear is positively related to the intention of implementing online password protection.

Response efficacy evaluates how effective coping responses suggested in reducing the threat. In implementing behavioral protection, the individual must make sure that the protective behaviors that they do will be effective in protecting them against the threat. In addition, using strong passwords to protect online accounts, renew regular password also help protect online accounts from malicious hackers. Individuals will be more involved in the protection behavior if they believe that their extra effort to create a secure password is valuable

[16]. It is also stated that response efficacy is positively related to protection behavior. Therefore, we hypothesized:

H4: Response efficacy is positively related to the intention of implementing online password protection.

Response cost measure effort including time, money, etc., that individual must pay when doing behavioral protection. As a result, response cost reduces the possibility of selecting the recommended action. In information security, [17] found that the barriers of implementing security practices negatively related to the attitude of individual [17]. Creating and updating passwords regularly adding user inconvenience. In addition, various online accounts owned by the user cause higher costs response. This is the reason users reuse their passwords for the same account to minimize the cost of the response in using a strong password. Thus, the hypothesis is:

H5: Response cost is negatively related to the intention of implementing online password protection.

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

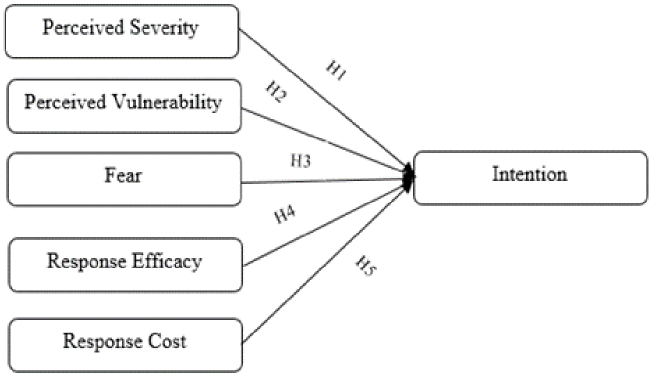

Fig. 1. Reasearch model.

The model in Fig.1 will be used to depict the relationship between latent variables. This research is analyzing six latent variables and sixteen manifested variables (indicators).

III. Data Analysis

Statistical analysis that is used for this research is SEM. SEM is used to analyze the collected data from questionnaire. The complete questionnaire can be seen in Appendix (Table 6). The respondents of this study are all students whom actively use Students Academic Information Systems (SAIS).

A. Descriptive Analysis

A total of 300 questionnaires obtained from students who are actively using Students Academic Information Systems (SIAS). The characteristic of respondents is shown in Table 1.

B. Missing Data and Outlier

Based on Little’s MCAR, there is no missing data in this study. Mahalanobis distance is used to determine outlier data. Data which has mahalanobis distance of more than 34,805 is considered the outlier and need to be withdrawn. From 300 questionnaires collected, there are 12 outlier data, so the eligible data to be analyzed are 288 data.

TABLE. I. Characteristic of Respondents

Age	Count	%	Gender	Count	%
17	2	0.67	Male	0	0
			Female	2	0.67
18	1	0.33	Male	0	0
			Female	1	0.33
19	14	4.67	Male	7	2.33
			Female	7	2.33
20	155	51.67	Male	83	27.67
			Female	72	24
21	115	38.33	Male	52	17.33
			Female	63	21
22	13	4.33	Male	6	2
			Female	7	2.33
Count	300	100		300	100

C. Reliability Test

Reliability test is performed based on Cronbach alpha for every latent variable. Details of latent variable with its corresponding Cronbach alpha can be seen in Table 2.

TABLE. II. Cronbach Alpha Value

Factor	Cronbach Alpha
Limit Value	**>0,6**
PS	0.861
PV	0.853
FEAR	0.905
RE	0.660
RC	0.729
INTENTION	0.758

D. Factor Analysis

According to [18] the test of Kaiser-Meyer-Olkin (KMO) and Bartlett’s test is used to determine whether the sample data used in the study is sufficient to analyze certain factors. The KMO result is 0.704, so it can be said to have a good criteria. Then for Bartlett’s test is 0.000, so it can be said to be highly significant in accordance with the criteria of [18] (Sig. <.001).

E. Normality Test

Normality test aims to evaluate whether the regression model, the variable spam or residuals have a normal distribution. If this assumption is violated, the statistical tests to be invalid for a number of small samples [19]. The descriptive statistics for the latent factors or constructs revealed that the values for the Skewness and Kurtosis were lower than ±2 for both statistics, which confirmed that there was no major issue of non-normality of the data [20]. Based on the tests that have been done, 288 data are normally distributed.

F. Levene’s Test

Levene’s test is used to determine whether the research data obtained is homogeneous or not [21], so it can be used for subsequent statistical analysis. Data are considered homogeneous if Sig. > 0.05 contrary, if Sig. < 0.05 then the data is considered not homogeneous. All variables in this study are said to meet homogeneous criteria.

G. Overall Model Fit

First step in SEM, which is a measurement model, is performed to determine the relationship between latent variables and its indicators by evaluating overall model fit. Overall model fit test results can be seen in Table 3. Based on

Table 3, the study has met all the determined limits. It can be concluded that the research method is fit and can be proceed for structural.

TABLE. III. GOODNESS OF FIT INDICES (GOFI) VALUES

Indeks	Criteria	Value	Info
Chi-square	>0,05	250,362	Good
CMIN/DF	1.00 < CMIN/DF < 3.00	2,813	Good
GFI	>0.9	0.913	Good
RMSEA	<0.05 good fit <0.08 acceptable fit	0.078	Acceptable Fit

Convergent validity is the extent to which observed variables of a particular construct share a high portion of the variance in common [22]. In addition, [18] suggested that average variance extracted (AVE) estimation should be greater than 0.5. AVE results can be seen in Table 4, in which all variables are said to meet the criteria.

TABLE. IV. AVE RESULTS

Construct	AVE
PS	0.608
PV	0.728
FEAR	0.563
RC	0.443
RE	0.603
INTENTION	0.631

H. Structural Model Fit

The next step in SEM is structural model fit. Path analysis is used to perform the advanced test which is structural model fit. This test is used to determine the relationship between latent variable to the model. The results of structural model fit can be seen in Table 5.

TABLE. V. STRUCTURAL MODEL RESULTS AND SEM MODEL HYPOTHESIS

Hypothesis	P	Result
	<0.05	
INTENTION ← PS	.004	Accepted
INTENTION ← PV	.055	Rejected
INTENTION ← FEAR	***	Accepted
INTENTION ← RE	***	Accepted
INTENTION ← RC	***	Accepted

The indicators of structural model fit test are the value of estimate, critical ratio, and p-value which can be seen completely in Table 5. In pursuant to Table 5, the relationship between variables with p-value less than 0.05(*) has a strong relation and the hypothesis is accepted.

IV. RESEARCH RESULT

A. Discussion on Hypothesis 1

Hypothesis 1 is accepted. It can be concluded that the respondents considered the threat of severe violations password for his life, so that users tend to change their behavior by using a strong password. It shows that in this study that Perceived Severity (PS) has significant influence over users' intention in creating password (INTENTION). Therefore, in this study Hypothesis 1 is received.

B. Discussion on Hypothesis 2

As Hypothesis 2 is rejected, it shows the respondents do not concern about their password-creating process to protect their accounts. They also do not aware about possible danger from hackers. The result shows that there is no change in user behavior in creating a strong password. Therefore, the Perceived Vulnerabilty (PV) does not affect significantly users' intention in creating password (INTENTION).

C. Discussion on Hypothesis 3

Hypothesis 3 is accepted which means that the respondents are alarmed about the harm and the threats from the use of weak passwords. This can increase users' intention to create stronger password in order to secure their accounts. It proves that fear (FEAR) significantly affect users' intention in creating password (INTENTION).

D. Discussion on Hypothesis 4

Hypothesis 4 is accepted which shows that the respondents are aware that the use of strong passwords can secure their accounts from hackers. This can increase their intentions to create stronger passwords. It proves that Response Efficacy (RE) can significantly affect users' intention in creating password (INTENTION).

E. Discussion on Hypothesis 5

Hypothesis 5 is accepted, it can be concluded that the respondents consider that frequently updated password is not just waste of time and requires no effort, they believe it can improve their security so that it can affect respondents' intentions in creating stronger passwords. It shows that in this study the Response Cost (RC) has a significant influence on users' intention in creating password (INTENTION).

V. CONCLUSION

Based on the data analysis it can be concluded that factors affecting users to create strong passwords are; perceived severity, fear, response efficacy, and response cost. Respondents considered the threat of severe password violations so that users tend to change their behavior by creating a strong password. The respondents had fear to the threats that could be caused by the easily predicted passwords; hence the strong passwords are created. Respondents are sure that creating powerful and strong passwords would protect their account from the hackers; that increasing respondents' intention in creating strong ones. The respondents consider that frequently updated password is not just waste of time and requires no effort, they believe it can improve their security so that it can affect respondents' intentions in creating stronger passwords.

Although this research is only focused on Students Academic Information System (SAIS), many other applications, such as social network account, e-commerce account, email account, etc., also require a strong password to protect it. In that sense, this research only represents a first step in the direction of evaluating users' intention in protecting their account. In ongoing and future work, it can be extended to a broader scope and platforms.

In addition, the result of this research can raise users' security awareness in term of protecting their online accounts as the security awareness is an important necessity for any organization, including university. Users are needed to be informed regarding their online safety to prevent a lot of potential problems that could damage the infrastructure and the organization as a whole.

APPENDIX

TABLE. VI. COMPLETE QUESTIONNAIRE

Item	**Construct Indicator (measured on five-point, Likert-type scale)**	**References**
Perceived Severity	1. How severe do you think the consequence will be if someone guessed your passwords? 2. How severe do you think the consequence will be if someone cracked your passwords? 3. How severe do you think the consequence will be if someone obtained your passwords?	Adapted from [23] cited in [7]
Perceived vulnerability	1. What are your chances of someone guessing your passwords? 2. What are your chances of someone cracking your passwords? 3. What are your chances of someone obtaining your passwords?	Adapted from [24] cited in [7]
Fear	1. The thought of having someone guess my passwords makes me nervous 2. The thought of having someone crack my passwords makes me nervous 3. The thought of having someone obtain my passwords makes me nervous	Adapted from [25] cited in [7]
Response Cost	1. If I use strong passwords, they will be difficult for me to remember. 2. If I update my passwords often, they will be difficult for me to remember 3. If I use unique password on each account, they will be difficult for me to remember	Adapted from [11] cited in [7]
Response Efficacy	4. I can protect my online accounts better if I use strong passwords 5. I can protect my online accounts better if I update my passwords often 6. I can protect my online accounts better if I use unique passwords for each online accounts	Adapted from [26] cited in [7]
Intention	1. I intend to make a strong password 2. I intend to use strong password in the future 3. I intend to update the password as often as possible	[8]

REFERENCES

[1] Tim UPPTI (2007) Buku Panduan Layanan Teknologi Informasi Untuk Mahasiswa. Malang.

[2] P. Inglesant and M. A. Sasse. The true cost of unusable password policies: password use in the wild. In ACM Conference on Human Factors in Computing Systems 2010, pages 383{392, 2010.

[3] J. Leyden. Office workers give away passwords for a cheap pen. The Register, 2003.

[4] SafeNet. 2004 annual password survey results. SafeNet, 2005.

[5] Floyd, D. L., S. Prentice-Dunn, and R. W. Rogers. 2000. A meta analysis of research on protection motivation theory. Journal of Applied Social Psychology 30: 407–429.

[6] 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.

[7] 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

[8] Shin, D.H., (2010) The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Vol. 22 No. 5, pp 428-438

[9] 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.

[10] 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.

[11] Woon, I. M. Y., G. W. Tan, and R. T. Low. 2005. A protection motivation theory approach to home wireless security. Proceedings of the 26th International Conference on Information Systems, Las Vegas, NV, December 11–14, 367–380.

[12] Lee, Y., and K. R. Larsen. 2009. Threat or coping appraisal: Determinants of SMB executives' decision to adopt anti-malware software. European Journal of Information Systems 18: 177–187.

[13] 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.

[14] 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.

[15] Sutton, S. R. 1982. Fear-arousing communications: a critical examination of theory and research. In Social psychology and behavioral medicine, ed. J. R. Eiser, 303–337. London: Wiley.

[16] Gurung, A., X. Luo, and Q. Liao. 2009. Consumer motivation in taking action against spyware: An empirical investigation. Information Management and Computer Security 17 (3): 276–289.

[17] 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.

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

[19] Ghozali, Imam. 2005. Aplikasi Analisis Multivariate dengan program SPSS, Badan Penerbit Universitas Diponegoro, Semarang.

[20] Chandio, F. H. 2011. Studying Acceptance of Online Banking Information System: A Structural Equation Model. London: Brunel University.

[21] Levene. 1960. Contributions to Probability and Statistics. Standford University Press. CA.

[22] Hair, et al. 2006. Multivariate Data Analysis 6th Ed. New Jersey: Pearson Education

[23] Plotnikoff, R. C., and N. Higginbotham. 2002. Protection motivation theory and exercise behavior change for the prevention of coronary heart disease in a high-risk, Australian representative community sample of adults. Psychology, Health and Medicine 7 (1): 87–98.

[24] Pechmann, C., C. Zhao, M. E. Goldberg, and E. T. Reibling. 2003. What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message theme. Journal of Marketing 67:1–18.

[25] Milne, S., S. Orbell, and P. Sheeran. 2002. Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. British Journal of Health Psychology 7:163–184.

[26] Maddux, J. E., and R. W. Rogers. 1983. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology 19 (5): 469–479.