Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 161 (2019) 1182–1190

Procedia Computer Science

www.elsevier.com/locate/procedia

The Fifth Information Systems International Conference 2019

Protecting Facebook Password: Indonesian Users' Motivation

Ari Kusyanti[a,*], Harin Puspa Ayu Catherina[b], Yustiyana April Lia Sari[b]

[a]*Department of Computer Science, Universitas Brawijaya*
[b]*Department of Information Systems,Universitas Brawijaya*

Abstract

Facebook is one of the social networking services that have users around 1.86 billion active users spread all over the world. To be able to enjoy various services from Facebook, a user is required to have a Facebook account. In the registration process to create a new Facebook account, the user is prompted to create a password to protect his account. The password policy service applied by Facebook requires all users to create and use a password for their Facebook account in accordance with the policies. This study aims to analyze user behavior with case study of Facebook account by using 12 construct variables adapted from Protection Motivation Theory (PMT). Data collected from Facebook users of 300 respondents. Data analysis method used is Structural Equation Modeling (SEM) analysis. From the research result, the factors that influence Facebook users' intention to protect their account are perceived vulnerability, fear, response efficacy, response cost, subjective norm, prior experience with safety hazard, threat susceptibility and personal responsibility. Meanwhile, they ignore the threat sverity, coping self-efficacy and security support from others while protecting their Facebook account.

Keywords: intention; structural equation modelling (SEM); facebook; protection motivation theory (PMT)

1. Introduction

Facebook is the most dominating social networking site in the world despite the emergence of a new social networking site [1]. In Indonesia, there are about 111 million active Facebook users hence Indonesia is the most users accessing the fourth Facebook in the world after the United States, India and Brazil [2].

* Corresponding author. Tel.: +62-81-233-799-049; fax: +62-341-577-911.
E-mail address: ari.kusyanti@ub.ac.id

1877-0509
10.1016/j.procs.2019.11.231

According to Crowd DNA teens aged from 16-19 in Indonesia are checking on their Facebook account 14 times a day and 80.9% are accessing their Facebook account every week [3, 4].

To be able to enjoy the services of Facebook, a user is required to have a Facebook account. In the registration process to create a new Facebook account, the user is prompted to create a password to protect their account.

Facebook account may contain confidential information, such as personal information, therefore it is necessary to protect the privacy and security of Facebook account. Password is a way to authenticate users in Facebook. Users often create passwords by using predictable words such as names or birthdays. To prevent a hacker guessing a user's password, Facebook creates a policy regarding password creation. All Facebook users who already have a Facebook account are required to create passwords in accordance with policies that have been set up Facebook. Facebook password policy itself consists of a minimum length of 6 characters, use a combination of numbers, letters and punctuation and combine uppercase and lowercase letters. Next will appear the kinds of notifications when the user makes a combination of passwords, among others: "Complicated", "Too Short" and "Medium". A notification that appears when a user creates a password provides information to the user whether the password that has been created complies with the policy applied.

In 2013, Facebook asks its users to immediately change the password. This request is done to anticipate the possibility of stolen account that happened to Adobe some time ago, since many users use the same password on their account on Facebook and Adobe. More than 150 million users exploited the attacker including credit card, username and password [5].

This study adapted some researchers conducted previously, i.e. a research done by [6] 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 intention 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, personal responsibility, prior experience with safety hazards and subjective norm, were adapted from a research by [7] which affected security intention by using a framework from Protection Motivation Theory (PMT). The purpose of this study is 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, in this case is intention of users of Facebook to create password.

2. Model structure and hypothesis

This research is a confirmatory research based on model and hypothesis by [6] and [7] which focus on PMT. PMT model initially intended for health-related research which presents a framework to better apprehend if and how protective actions against the threat of potential online criminal actions may be similarly motivated. The data is analyzed using Structural Equation Modelling (SEM). There are two stages in this SEM analysis: structural model and measurement model. Structural model shows the relationship between latent variables, while measurement model is used to determine the relationship connection between indicator and variables.

- Definition of construct

  The definition of each constructs that used in this research is presented in Table 1.

Table 1. Definition of Construct.

Construct	Definition
Perceived Vulnerability (PV)	To measure how vulnerable the opportunity would be to a hazard caused by the creation of their account password.
Fear (FE)	To measure the emotional response of a user against a threat that can lead to a change in attitude or behavior.
Response Efficacy (RE)	To measure user confidence in recommended behaviors to prevent or mitigate the harm caused by the creation of their account password.

Response Cost (RC)	To measure the time and effort spent by users to protect their accounts from harm.
Subjective Norm (SN)	To measure the individual's perception of how others whom are important to the individual to determine how the individual should behave.
Prior Experience with Safety Hazard (PE)	To measure whether an individual has prior experience with safety hazard.
Threat Susceptibility (TSUS)	To measure vulnerabilities from threats that allow users to experience security threats.
Personal Responsibility (PR)	To measure a belief that at the right time take action to achieve the desired outcome.
Perceived Security Support (PSS)	To measure support from others who are related in terms of protection of their online accounts.
Coping Self-Efficacy (CSE)	To measure perceived capability and comfort with respect to one's behavior in doing online protection.
Security Intention (SI)	To measure how much a user's intentions are in protecting their online accounts

- Hypothesis for the Construct

Threat severity states that if a person does not assume the impact of a threat is a severity of their life then no action or intention of the protection of motivation (protection motivation) is done. Using Protection Motivation Theory, the researchers demonstrated the relation of threat severity with the protective behaviour [8]. From this statement, it can be drawn hypothesis as follows:

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

Perceived vulnerability involves vulnerability to a threat. Passwords are considered vulnerable to a threat. A hacker can use various techniques to attack user passwords. For example, hackers can use keyword-based attacks, dictionary words. People with high levels of vulnerability feel more concerned with the security or protection of their passwords [9]. From this statement, it can be drawn hypothesis as follows:

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

Fear refers to the fear triggered by the threat. Fear is an emotional response to threats that can lead to a change in attitude or behavioral intention [10]. If users are afraid of the threat of password guessing attacks or hacked, they will be more inclined to spend more effort in maintaining and updating their passwords. From this statement, it can be drawn hypothesis as follows:

H3: Fear in provider has a significant positive effect on security intention.

Response efficacy is used to evaluate how effective the recommended protection behavior is in reducing a threat. In applying protective behaviour, individuals should ensure that protective behaviors undertaken will be effective in protecting themselves from such threats [11]. From this statement, it can be drawn hypothesis as follows:

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

Response cost is used to measure costs (such as time, money and effort). Someone should do so while doing protective behavior against their online accounts. In information security, researchers found that barriers to the adoption of security practices were negatively related to public attitudes toward security policy [12]. From this statement, it can be drawn hypothesis as follows:

H5: Response cost has a significant negative effect on security intention.

Subjective norm becomes an important factor of the security-related behavior. Social influence refers to the influence of one's social network (such as family and friends) on one's behavior [13]. If someone gets a lot of influence

from one's social network (like family and friends) to conduct protective behavior against their online account then it can affect the intentions of that person to protect their online accounts. From this statement, it can be drawn hypothesis as follows:

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

Prior experience with safety hazard used to determine whether an individual has previous experience or not. In a survey at college students who had previous experience with viral infections significantly predicted an intention to use viral protection [14]. In this study, previous experiences relate to previous individuals who have experience in dealing with online threats to their online accounts. From this statement, it can be drawn hypothesis as follows:

H7: Prior experience with safety hazard has a significant positive effect on security intention.

Threat susceptibility is used to measure vulnerabilities from threats that allow users to experience online security threats. A user who feels that they will be vulnerable to exposure to online security threats will affect the intentions of these users to improve the security of their online accounts [12]. From this statement, it can be drawn hypothesis as follows:

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

Perceived security support is used to measure the support or assistance of others against the protection of an online account from an individual. Individuals who get support or help from others in matters relating to the protection of their online accounts will be able to increase the intention of the individual to improve the security of their online accounts [15]. From this statement, it can be drawn hypothesis as follows:

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

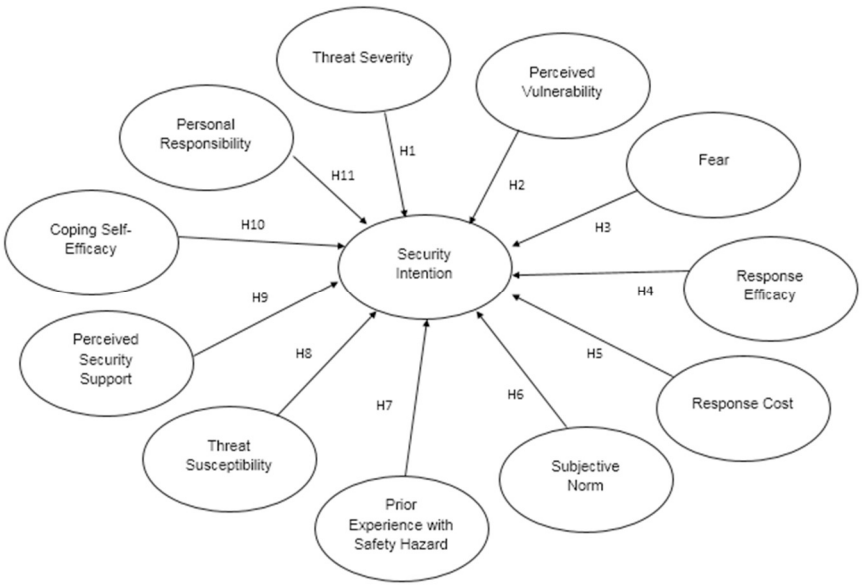

Fig. 1 Research Model.

Coping self-efficacy is used to determine the ability of someone in protecting themselves online. An individual who has the capability in protecting their online account will affect the intentions of the individual to continue to improve the security of their online account [16]. From this statement, it can be drawn hypothesis as follows:

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

Personal responsibility used to measure the belief of an individual to achieve the desired outcome. An individual who has high confidence in taking action to protect the security of their online account will directly affect the intention of the individual to continue to improve the security of their online accounts [17]. From this statement, it can be drawn hypothesis as follows:

H11: Personal responsibility has a significant positive effect on security intention.

We developed the research model as shown in Fig. 1. The model in Fig.1 will be used to depict the relationship between latent variables.

3. Data analysis

Statistical Analysis of SEM is used to analyze the collected data from questionnaire adapted from [6] and [7] with 5-point Likert scale. The respondents of this study were all people who are actively using Facebook.

- Descriptive Analysis
  Data were taken from respondents ranges from age 18 years to 24 years.
- Missing Data and Outlier
  Based on Little's MCAR, there is no missing data in this research. Mahalanobis distance is used to determine outlier data. Data which has Mahalanobis distance of more than 52.485 is considered the outlier and need to be withdrawn. From 300 questionnaires collected, there are 24 outlier data, so the eligible data to be analyzed are 276 data.
- Reliability Test
  Reliability testing is used to determine the degree of consistency of an indicator when measuring its latent variables [18]. The calculation of Cronbach alpha of each indicators is meet the cut-off criteria as presented in Table 2.

Table 2. Cronbach's Alpha Values.

Factor	Cronbach's Alpha (>0.6)
Threat Severity (TS)	0.774
Perceived Vulnerability (PV)	0.742
Fear (FE)	0.892
Response Efficacy (RE)	0.804
Response Cost (RC)	0.727
Subjective Norm (SN)	0.817
Prior Experience with Safety Hazard (PE)	0.884
Threat Susceptibility (TSUS)	0.662
Perceived Security Support (PSS)	0.717
Coping Self-Efficacy (CSE)	0.677
Personal Responsibility (PR)	0.761

- Factor Analysis

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 [18]. From the results of KMO is 0.822 and Bartlett's test of 0.000 therefore the data is considered very significant [19].

- Normality Test

Normality test is used to determine the normal distribution of the cumulative sample [19]. In this study all data are normally distributed.

- Levene Test

Levene's test is used to determine whether the research data obtained is homogeneous or not [19]. So, it can be used for subsequent statistical analysis. Data are considered homogeneous if the value (Sig. > 0.05), but if the value (Sig. < 0.05) then the data is considered not homogeneous. In this study all data are homogeneous.

- Measurement Model Fit

Measurement fit model to find out the level of compatibility between variable manifest and latent variables. In testing the measurement model, Confirmatory Factor Analysis (CFA) Method is used. Measurement model fit test results can be seen in Table 3.

Table 3. Goodness of Fit Index.

Index	Criteria	Value	Info
Chi-square	>0.05	244.647	Good
CMIN/DF	1.00 < CMIN/DF < 3.00	1.421	Good
GFI	>0.9	0.905	Good
RMSEA	<0.05 good fit	0.038	Good Fit
	<0.08 Acceptable Fit		

- 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 4.

Table 4. Structural Model Fit Result.

Hypothesis	P-Value <0.05	Info
SI ← TS	0.348	Not accepted
SI ← PV	0.044	Accepted
SI ← FE	***	Accepted
SI ← RE	0.012	Accepted
SI ← RC	0.047	Accepted
SI ← SN	***	Accepted
SI ← PE	***	Accepted
SI ← TSUS	0.005	Accepted
SI ← PSS	0.978	Not accepted
SI ← CSE	0.068	Not accepted
SI ← PR	0.002	Accepted

The indicators of structural model fit test were values of p-value which can be seen completely in Table 3. In pursuant to Table 4, the connection between variables with p-value less than 0.05(*) has strong relation and the hypothesis is accepted. In this study, there are 8 hypotheses accepted and the 3 hypotheses are not accepted.

4. Research result and discussion

- Discussion on Hypothesis 1

Hypothesis 1 is not accepted. From the test results of Hypothesis 1, it can be concluded that the respondents does not consider the threat of violation or hacking password is a thing that is severe for his life so that it can lead to changes in the intentions of user behavior in creating strong passwords. It shows that in this research hazard or threat factor (TS) does not has a significant influence on interest factor of user behavior (INTENTION). Therefore, in this study The results of this study are similar to the results of research conducted by [6] which states that online account users consider the severity of password violations does not necessarily make a user to take greater effort in protecting their passwords.

- Discussion on Hypothesis 2

Hypothesis 2 is accepted. From the test results of Hypothesis 2, it can be concluded that the respondents concern about the dictionary words on the composition of the passwords they create, hence it affects the intentions of respondents in creating strong passwords. It shows that in this research the vulnerability factor (PV) has a significant influence on user behaviour creating strong password (INTENTION).

The results of this study are similar to the results of research conducted by [14] which states that an individual who notices the composition of their passwords automatically they also concern about the possibility of attacks from hackers. Individuals who pay attention to the composition of their password will make secure passwords in improving the security of their online accounts.

- Discussion on Hypothesis 3

Hypothesis 3 is accepted. It can be concluded that respondents have a feeling of fear of all threats that can happened by the use of weak and predictable passwords, therefore increasing user intentions in creating strong passwords. It shows that in this research the fear factor (FEAR) has a significant influence on user behavior in creating strong password (INTENTION).

The results of this study are similar to the results of research conducted by [6] which states that an individual who has a fear of threats that can occur by using a weak password will automatically make the individual to increase their intention to protect the account online by using a strong password.

- Discussion on Hypothesis 4

From the test results of Hypothesis 4 that is accepted, it is concluded that respondents have confidence when using strong passwords will protect their accounts from malicious hacker, hence it is increasing user intentions to create strong passwords. It shows that in this study Response Efficacy (RE) has a significant influence towards user behavior (INTENTION).

The results of this study are similar to the results of research conducted by [6] which states that when a user is aware of and assumes that security measures can protect their online accounts, they are more likely to adopt such security measures.

- Discussion on Hypothesis 5

From the test results of Hypothesis 5 that is accepted, it shows that respondents assume that frequent renewal of passwords can be a waste of time and require effort, so that it affects the intentions of respondents in creating strong passwords. Based on the result, Response Cost (RC) has a significant influence towards user behavior in creating strong password (INTENTION). The results of this study are similar to the results of research conducted by [5] when users feel uncomfortable and have to pay by spending time and effort, they are usually reluctant to adopt the recommended security measures.

- Discussion on Hypothesis 6

Hypothesis 6 is accepted. Based on the result, it can be concluded that the respondent considers the person who is considered important to the respondent can influence their intention in creating strong password. It concluded that Subjective Norm (SN) has significant influence towards user behavior (INTENTION).

The results of this study are similar to the results of research conducted by [20] who suggested that the existence of social influences such as: friends or family of a user can influence a user to continue security measures. If a friend or family of an individual advises that the user increases security measures in protecting their online account, then the user will increase the security measures and vice versa.

- Discussion on Hypothesis 7

Hypothesis 7 is accepted, which shows that the respondent considers that their prior experience regarding online attack that has been done or never happened before can affect the intention of the respondent in creating strong password. It shows that in this research experience factor that has been done before (PE) has a significant influence on interest factor of user behavior (INTENTION).

The results of this study are similar to the results of research conducted by [7] who argued that individuals who have had previous experience in terms of protecting their online accounts will always have the intention of continuing to protect their online accounts.

- Discussion on Hypothesis 8

Hypothesis 8 is accepted, therefore it can be concluded that respondents consider the possibility of online threats can affect the intentions of respondents in creating strong passwords. It shows that in this research Threat Sustability (TSUS) has a significant influence towards user behavior to create strong password (INTENTION).

The results of this study are similar to the results of research conducted by [21] which states that respondents who experienced an online attack on their online accounts will automatically increase the intentions to improve the security of their online accounts.

- Discussion on Hypothesis 9

Hypothesis 9 is not accepted, which shows that respondents assume that support from others can not affect the intentions of respondents in creating strong passwords. It shows that in this research the support factor of others, Perceived Security Support (PSS) does not have significant influence towards user behavior (INTENTION).

The results of this study are similar to the results of research conducted by [7] argues that even if there is support or help from others it does not mean that the user have the intention of continuing to improve the security of their online accounts. In terms of improving the security of their online accounts, they do not need the support or assistance of others, they can do it on their own.

- Discussion on Hypothesis 10

Hypothesis 10 is not accepted. It can be concluded that respondents assume that having the ability and comfort in doing online protection can not affect the intention of the respondent in creating strong password. This indicates that in this study the perceived ability and comfort factor associated with a person's behavior in doing online protection (CSE) does not have a significant influence on their interest in creating strong password (INTENTION). The results of this study are similar to the results of research conducted by [7] which argues that eventhough a user has the ability to increase security measures to protect their online accounts, it does not necessarily they have any intention of continuing to improve security measures to protect their online accounts.

- Discussion on Hypothesis 11

From the test results of Hypothesis 11 which is accepted, it shows that respondents is confident in taking action to improve security measures in protecting their online accounts by creating strong passwords. This indicates that in this study Personal Responsibility (PS) has a significant influence towards user behavior to create strong password (INTENTION).

The results of this study are similar to the results of research conducted by [7] which states that having confidence in taking action to improve security measures in protecting an online account affect a user to continue to improve the security of their online account.

5. Conclusion

Based on the results of data analysis it can be concluded that there are 7 factors that affect users in creating password on Facebook account, namely: perceived vulnerability, fear, response efficacy, response cost, subjective norm, prior experience with safety hazard, threat susceptibility and personal responsibility. The result of this research will raise users' awareness towards user behaviors in protecting their online accounts. Deeper investigation may be required like adding some constructs from different model to obtain a better comprehension on protecting online accounts.

References

[1] Emarketer. (2016a) "Facebook Remains the Largest Social Network in Most Major Markets." *Emarketer*. Available from: http://www.emarketer.com/Article/Facebook-Remains-Largest-Social-Network-Most-Major-Markets/1013798.

[2] Reza, J. I. (2017) "Indonesia Negara ke-4 dengan Pengguna Facebook Teraktif di Dunia [Title in English: *Indonesia is the Fourth Largest Facebook Users*]." Available from: http://tekno.liputan6.com/read/2926217/indonesia-negara-ke-4-dengan-pengguna-facebook-teraktif-di-dunia.

[3] Crowd DNA. (2014). "Coming of Age on Screens." *Facebook IQ.* Available from: http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/).

[4] Emarketer. (2016) "Facebook Remains the Largest Social Network in Most Major Markets." *Emarketer*. Available from: http://www.emarketer.com/Article/Facebook-Remains-Largest-Social-Network-Most-Major-Markets/1013798.

[5] Mahardy, D. (2013) "Adobe Diserang, Facebook Minta Pengguna Ganti Password." Available from: http://tekno.liputan6.com/read/745380/adobe-diserang-facebook-minta-pengguna-ganti-password?page=22&toDate=2014-02-05+06%3A30%3A00. [Accessed 7th August 2017].

[6] 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.

[7] Tsai, S.H., et al. (2016) "Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective."

[8] Woon, I. M. Y., G. W. Tan, and R. T. Low. (2005) "A Protection Motivation Theory Approach to Home Wireless Security", in *Proceedings of the 26th International Conference on Information Systems, Las Vegas, NV,* December 11–14. pp. 367–380.

[9] Weirich, D., and M. A. Sasse. (2001) "Pretty Good Persuasion: A First Step Towards Effective Password Security in The Real World", in *Proceedings of the 2001 Workshop on New Security Paradigms, Cloudscrofl, NM, September*. pp. 10–13.

[10] 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.

[11] 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.

[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] Lai, F, D. Li, and C-T. Hsieh. (2012). "Fighting Identity Theft: The Coping Perspective." *Decision Support Systems* **52 (2)**: 353–63. doi:10.1016/j.dss.2011.09.002.

[14] Lee, D., R. LaRose, and N.J. Rifon. (2008) "Keeping Our Network Safe: A Model of Online Protection Behaviour." *Behav Inf Technol*. **27 (5)**: 445–54. doi:10.1080/01449290600879344.

[15] Liang, H, and Y. Xue. (2010)."Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective." *J Assoc Inf Syst* **11 (7)**: 394–413.

[16] LaRose, R., and N.J. Rifon. (2006) "Changing Online Safety Behavior: Experiments With Online Security and Privacy", *Paper presented in the International Communication Association,* Dresden, Germany.

[17] LaRose, R., N. J. Rifon, and C. Wirth. (2007) "Online Safety Begins with You and Me: Getting Internet Users to Protect Themselves", *Paper presented at the 57th International Communication Association Conference*, San Francisco, CA.

[18] Yamin, S., and H. Kurniawan. (2009) *Structural Equation Modeling: Belajar Lebih Mudah Teknik Analisis Data Kuesioner dengan Lisrel-PLS* [Title in English: *Structural Equation Modeling: Easy to Learn the Analysis of Questionnaires Using LISREL-PLS*], Jakarta, Salemba Infotek.

[19] Field, A. (2009). *Discovering Statistics Using SPSS,* 3rd Ed., Sage Publications. doi= http://fac.ksu.edu.sa/sites/default/files/ktb_lktrwny_shml_fy_lhs.pdf.

[20] Hsu, C. L., and J. C. C. Lin. (2007) "Acceptance of Blog Usage: The Roles of Technology Acceptance, Social Influence and Knowledge Sharing Motivation."

[21] Klein, R. H., and E. M. Luciano. (2016). "What Influences Information Security Behavior? A Study With Brazilian Users." *JISTEM - Journal of Information Systems and Technology Management* **13 (3)**.