JHSS (Journal of Humanities and Social Studies)
https://journal.unpak.ac.id/index.php/jhss
Volume 08, Number 01, Page 162-167
e-ISSN: 2598-120X; p-ISSN: 2598-117X

THE INFLUENCE OF INFORMATION PRIVACY AWARENESS ON PRIVACY PROTECTION BEHAVIOR IN FACEBOOK

Sulthan Muhammad Fahrezi [a*)], Candiwan [a)]

[a)] *Telkom University, Bandung, Indonesia*

[*)]*Corresponding Author: fahreziest@student.telkomuniversity.ac.id*

Article history: *received 18 July 2023; revised 02 October 2023; accepted 29 November 2023* *DOI:https://doi.org/10.33751/jhss.v8i1.8414*

Abstract. The use of the internet has become very common in today society. Based on a survey by dataindonesia.id, 68.9 percent of the 370.1 million internet users in Indonesia are social media users, and Facebook is one of the most widely used social media platforms in Indonesia, with the number of users growing to 202.2 million by July 2022. Due to this increase and the huge number of users, as well as the amount of personal information stored in it, this can be a vulnerability for Cybercriminals to exploit such as phising or scams. This research was conducted to analyze and determine what factors affect users information privacy concerns towards privacy protection behavior on Facebook. The data were collected by distributing a questionnaire to a total of 417 Facebook users in Indonesia. This research model consists of seven constructs. The research model constructs consist of User's Information Privacy Concerns, Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, Rewards, and Privacy Protection Behavior. This research was analyzed using quantitative methods by processing data through SPSS and AMOS software. The data is processed using the SEM model, which is validated with a confirmatory factor analysis test, a structural model test, and a hypothesis test. The results of this study indicate a positive correlation between User's Information Privacy Concerns and Perceived vulnerability in Privacy Protection behavior, it can be concluded that User's Information Privacy Concerns (UIPC) can affect Privacy Protection behavior (PPB) among Facebook users. Therefore, Facebook users are advised to be more concerned about their privacy information protection behaviors by avoiding any behavior that may put them at risk of privacy threats. This paper suggest users to take measures to prevent any threats to their privacy.

Keywords: security awareness; information privacy; facebook social media users; Structural Equation Modeling (SEM)

I. INTRODUCTION

In this era of globalization, technology has developed and changed to be able to support various human activities and smartphones have become one of the technologies that can connect to the internet and are most widely used [1]. According to Zlatolas the internet is a global scale network created from various networks [2]. Internet is a necessity for society. Internet users in Indonesia in February 2022 amounted to 204.7 million and reached more than 73.3% of Indonesia's population [3].

A social network is a tool for consumers that can be used to find friends, post photos or videos, create discussion forums or even play games. The most important feature is to create status messages that can be responded to by other users by giving likes or comments [4]. The object to be studied is the user of the social network Facebook. Facebook is one of the most popular social networks among various groups, especially young people, because the features offered to users are very diverse. Facebook has 202.2 million users as of July 2022 [5] The occurrence of cybercrimes is mostly found in social networks with a large number of users. Cybercriminals use phishing techniques, namely fake links that can be accessed by victims and perpetrators commit crimes such as stealing money or collecting personal data such as identity numbers through these links [6]. The article (detik.com) states that on February 2, 2023, a phishing case was found that was used to steal money and personal data belonging to DPRD members' accounts and suffered a loss of up to 654 million [7].

Currently, there were 26,675 cases of phishing attacks in the first quarter of 2023. This is an increase of 20,596 cases compared to the 4th quarter of 2022 which only had 6,106 reported phishing cases [8]. Facebook can become a target for cybercriminals due to the large amount of information and people using the platform. Based on Son & Kim's research, they found that privacy awareness in an information system influences user protection behavior to secure private information [9]. The relationship between privacy awareness and protective behavior was originally explored by Altman who suggested that people try to implement a desired level of privacy security by adopting some protective behavior [10]. Therefore, the user's information privacy awareness has a positive influence on privacy protection behavior. Rogers states that the theory of protective motivation is an individual's motivation to avoid risk that comes from three main factors: perceived severity, perceived vulnerability, and response efficacy. However, previous models cannot provide sufficient explanations to describe individual failures in adopting protective behavior [11]. Then the model was modified and the following two cognitive constructs were included: response efficacy, and rewards related to Rogers' theory. Therefore, we consider that protective motivation

Volume 08, Number 01, Page 162-167
e-ISSN: 2598-120X; p-ISSN: 2598-117X

theory can significantly explain UIPC and PPB in social networks. Unlike previous research, where several variables of privacy motivation theory, especially response efficacy and rewards were ignored. this study considers all variables to provide an overall view.

Zhang and McDowell have conducted an in-depth study where perceived severity does not motivate online users to use strong passwords [12]. However, social network users who perceive loss of information privacy as a serious risk are more likely to be concerned about the privacy of their information. Therefore, the current study proposes that there is a positive relationship between perceived severity and UIPC. As explained by Lee, LaRose, and Rifon, perceived vulnerability refers to how far users believe that threats can harm them [13]. Users' perception of the perceived vulnerability of online virus threats will involve them in protective behavior. Therefore, the current research proves that there is a positive relationship between perceived vulnerability and UIPC. According to research conducted by Woon, Tan and Low, response efficacy refers to an individual's belief that the response is believed to be effective in protecting oneself or others from threats [14]. Therefore, users who believe that the adverse consequences of loss of information privacy can be mitigated by protective measures will be more concerned about their privacy. However, Zhang & Mcdowell's research states that there is no direct correlation between response efficacy and policy towards information security measures. Therefore, this study states that there is a positive relationship between response efficacy and UIPC. As stated by Mohamad & Ahmad, Rewards relates to perceived benefits with the choice of behavior [15]. To obtain users' personal information (e.g., photos, emails, contact details, etc.), social networks use rewards (e.g., online games, applications, quizzes, etc.) as an effective approach. Once users begin to experience the benefits of a social network, they may choose to disclose their personal information in order to benefit from it. Thus, the current research suggests that there is a negative relationship between rewards and UIPC. According to Lee, Larose & Rifon, self-efficacy affects attention to information privacy, impacts behavior to apply protective measures against viruses, and influences behavior in social networks. However, other studies involving self-efficacy have revealed that it is not directly related to disclosing one's personal information [16]. Therefore, users who believe in their ability to secure their information will be more concerned about privacy. Therefore, this study hypothesizes that there is a positive relationship between self-efficacy and UIPC.

Based on the phenomena and problems that have been described by the author regarding awareness of user information privacy and user privacy protection behavior from Facebook social media users. The data is processed using the SEM model which is tested through the Confirmatory Factor Analysis Test, the Goodness of Fit Test, the Structural Model Test and the Hypothesis. Therefore, the author is interested in making a scientific work entitled "The Influence of Information Privacy Awareness on Privacy Protection Behavior on Facebook Users"

In this research model there are seven constructs. the construct consists of User's Information Privacy Concerns, Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, Rewards, and Privacy Protection Behavior. Based on the background, study literature, problem formulation and research questions that have been explained. In this study the authors wanted to make an analysis of the influence of information privacy security awareness on privacy protection behavior on Facebook social media users. Users' information privacy concerns (UIPC) can be defined as actions to control the type, manner, and amount of personal information provided to an individual [17]. Individual perspectives on what is right in social interactions and using the Internet, especially in terms of personal information privacy practices, are discussed in UIPC [18]. Privacy protection behavior (PPB) is the user's actions to protect privacy information when deciding to use the internet network to carry out certain activities [19]. Privacy protection behavior is an individual's motivation to protect himself from risks originating from three main factors, namely perceived vulnerability, perceived severity and response efficacy [20]. Perceived severity (PS) is a person's level of awareness of the risks associated with the activities they carry out, as well as their knowledge of the potential risks that can occur when providing privacy information on internet websites [21]. Perceived severity means the perceived severity as a conscious assessment of the severity of a threatening security event [22]. According to Lee, LaRose, and Rifon, perceived vulnerability refers to the extent to which users perceive that there is a threat that may occur to them. Awareness of perceived vulnerabilities regarding online virus threats will encourage users to take protective measures [23]. According to Niu, self-efficacy is the result of interactions between self-regulation mechanisms, the external environment, individual abilities, experiences, and education [24]. Self-efficacy is also defined as the level of a person's belief in their own abilities without asking for help from others. User confidence in protecting personal information and information systems from lost or damaged data [25]. According to Woon, Tan, and Low (2005), response efficacy is a person's belief that a suggested response can protect oneself or others from harm [26]. Mohamed & Ahmad (2012) stated that rewards are rewards related to expected benefits associated with behavioral choices [27].

II. RESEARCH METHODS

This research was carried out using quantitative methods. Based on the purpose of this research is descriptive. The type of investigation used in this research is causal research which looks at a causal relationship where the independent variable affects the dependent variable. Researcher involvement, researchers do not manipulate data or intervene in data. The unit of analysis used by the researcher is individual unitization. Based on the time of implementation, the research was included in a cross-section study. By using non-probability sampling technique. Where the research sample was taken based on the number of

Volume 08, Number 01, Page 162-167
e-ISSN: 2598-120X; p-ISSN: 2598-117X

respondents taken from Facebook social media users. In this research, respondents can be rounded up to 400 respondents. The security behavior research model for social media users consists of seven model constructs, namely User's Information Privacy Concerns, Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, Rewards, and Privacy Protection Behavior.

III. RESULTS AND DISCUSSION

Confirmatory Factor Analysis test

Confirmatory Factor Analysis (CFA) functions to test a construct that has unidimensionality or indicators from the questions used, which can be used to confirm constructs or variables [29]. The purpose of CFA in this study is to evaluate the fit of the data with the model and evaluate how the constructs or variables and indicators relate to one another. The following are the results of the CFA test that has been carried out:

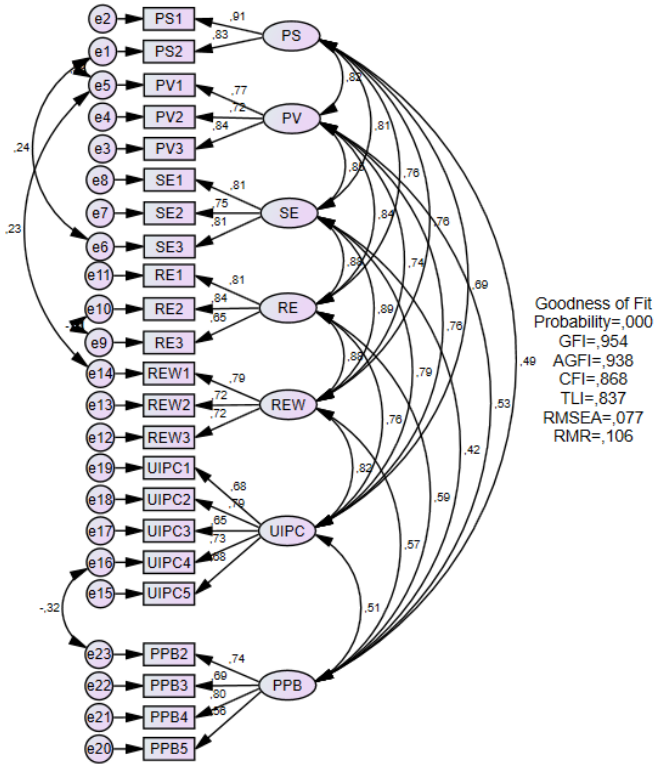

Figure 1. Confirmatory Factor Analysis (CFA) Test

Figure 1 shows the results of the CFA test which are explained in the following table 1. As shown in the table 1 , it can be concluded that the research model is appropriate. If at least one of the due diligence methods is met, then the model is considered feasible [30].

Structured Equation Modeling Test

The value of the parameter estimation coefficient is used in the structural model test to test and evaluate the hypotheses that have been modeled. The proposed hypothesis is accepted if the critical ratio value (C.R) is greater than the critical value of 1.65 and the significance level is p <0.05 [31].

Table 1. Results of the CFA Goodness of Fit test

Goodness of Fit Indices	Results	Cut – Off Value	information
Probability	0,000	≥ 0,05	Tidak Fit
GFI	0,954	≥ 0,90	Good Fit
AGFI	0,938	≥ 0,90	Good Fit
CFI	0,868	≥ 0,90	Marginal Fit
TLI	0,837	≥ 0,90	Marginal Fit
RMSEA	0,077	≤ 0,08	Good Fit
RMR	0,106	≤ 0,05	Tidak Fit

Conversely, if the CR value cannot reach its critical value at a significance level of p <0.05, then the hypothesis is rejected. Following are the results of the structural model test:

Table 2 The results of the structural model test

			Estimate	S.E.	C.R.	P	Label
UIPC	<---	PS	,024	,076	**,313**	**,755**	
UIPC	<---	PV	,413	,138	**2,996**	**,003**	
UIPC	<---	SE	-,395	,283	**-1,395**	**,163**	
UIPC	<---	RE	,091	,205	**,445**	**,656**	
UIPC	<---	REW	,749	,246	**3,043**	**,002**	
PPB	<---	UIPC	,432	,036	**12,008**	***	

Based on table 2 it is concluded that the value test of the critical ratio (CR) is more than 1.65 and the p value is less than 0.05. There are only 2 relationships between variables because the other variable relationships have a CR value below 1.65 or a p value greater than 0.05.

Based on the results carried out using the AMOS software from the data of Facebook user respondents on information security awareness, privacy and user behavior, the following results were found Based on the results of hypothesis testing conducted by researchers, the perceived severity (PS) hypothesis has no effect on user's information privacy concerns (UIPC) because it obtains a critical value of 0.313 or less than 1.65 and obtains a p value of 0.755 or greater than 0 ,05. This is not in line with previous research where the severity felt by users affects awareness of privacy information (Larose, 2005). Meanwhile, (Crossler, 2010; Dinev & Hart, et al, 2004) explains that users feel that losing private information and private photos through social networks will cause serious problems for them [32][33]. So it can be concluded that the severity felt by Facebook users in Indonesia does not really have an impact on information security awareness of users' privacy on the Facebook social network.

Based on the results of hypothesis testing conducted by

Volume 08, Number 01, Page 162-167
e-ISSN: 2598-120X; p-ISSN: 2598-117X

researchers, the perceived vulnerability (PV) hypothesis has a significant positive effect on user's information privacy concerns (UIPC) because it obtains a critical value of 2.996 or greater than 1.65 and obtains a p value of 0.03 or smaller than 0.05. This is in line with previous research that users feel they have the potential to experience online security problems such as privacy disturbances or virus attacks on social networks (Adhikari & Panda, 2018; Dinev et al, 2004; Afandi et al, 2017; Rogers, 1975) so that users feel risk and feel insecure when sharing personal information on the social network Facebook [34][35][36]. So it can be concluded that users can feel the vulnerability of information and security problems that can occur to them thereby affecting user awareness of information privacy on social networks.

Based on the results of hypothesis testing conducted by researchers, the Self-efficacy (SE) hypothesis has no effect on user's information privacy concerns (UIPC) because it obtains a critical value of -1.935 or less than 1.65 and obtains a p value of 0.163 or greater from 0.05. This is not in line with previous research (Dienlin & Trepte, 2014) [37]. This explains that users feel unsure about the ability to protect their personal information on social networks. In previous research (Larose, Lee & Rifon, 2005) users do not need help to activate privacy protection features on social networks. However, in this study, users are not confident about the privacy protection used on social networks. So it can be concluded that Facebook users in Indonesia doubt their ability to protect private information on social networks.

Based on the results of hypothesis testing conducted by researchers, the response efficacy (RE) hypothesis has no effect on user's information privacy concerns (UIPC) because a critical value is obtained of 0.445 or less than 1.65 and a p value of 0.656 or greater than 0 is obtained. ,05. This is in line with research conducted by Adhikari & Panda (2018) and Mohamed & Ahmad (2012). but this is not in line with previous research (Woon, Tan & Low, 2005) where users are confident in their ability to protect private information on social networks. so users take action to enable privacy protection features on social networks and cannot effectively control privacy information using privacy protection features on social networks (Zhang & Mcdowell, 2009). The results of the researchers found that users were unable to take effective measures in protecting privacy on social networks.

Based on the results of hypothesis testing conducted by researchers, the rewards hypothesis (REW) has a negative effect on user's information privacy concerns (UIPC) with a critical value of 3.043 or greater than 1.65 and a p value of 0.002 or less than 0 is obtained. 05, the REW variable significantly affects UIPC. This is not in line with previous research (Adhikari & Panda, 2018; Mohamed et al, 2012) but is in line with research conducted by Crossler (2010) and Zhang & Mcdowell (2009). that users provide their personal information when getting rewards. This shows a negative influence on the awareness of the security of user information privacy on social networks. Researchers found that Facebook users in Indonesia tend to provide information privacy if given rewards such as being able to join a community or being able to reconnect with old relatives.

Based on the results of hypothesis testing conducted by researchers, the user's information privacy concerns (UIPC) hypothesis influences privacy protection behavior (PPB) because a critical value is obtained of 12.008 or greater than 1.65 and a p value of 0.000 is obtained or less than 0. ,05. This shows that there is a positive and significant effect of the UIPC variable on PPB. This is in line with previous research (Adhikari & Panda, 2018; Son & Kim, 2008; Mohamed & Ahmad, 2012) where when users are aware of the vulnerabilities that can occur in their privacy information, users tend to protect their privacy information. facebook in this study, when users are rewarded in exchange for sharing their privacy information, users tend to reduce their privacy protection behavior.

IV. CONCLUSION

The purpose of this study is to determine the level of user awareness of information about how they maintain their privacy when using the social network Facebook. Data has been collected from 417 Facebook users in Indonesia. Structural Equation Modeling (SEM) analysis, which was processed using SPSS and AMOS applications. After processing and analyzing the data is complete, the following results were found The construct of the research model on Facebook social network users uses 7 model constructs namely Perceived Severity, Perceived Vulnerability, Self-Efficacy, Response Efficacy, Rewards, User's Information Privacy Concerns and Privacy Protection Behavior it is found that the results of the relationship analysis of model 2 constructs have a positive effect, and 4 no effect. Model constructs that have no effect are perceived severity, self-efficacy, rewards and response efficacy model constructs on user's information privacy concerns. While the model constructs that have a positive influence are Privacy vulnerability (PV) to user's information privacy concerns (UIPC), Rewards (REW) on user's information privacy concerns (UIPC), User's information privacy concerns (UIPC) on Privacy Protection Behavior. Based on the results of data processing and analysis, it can be concluded that User's Information Privacy Concerns (UIPC) affect Privacy Protection Behavior (PPB). The research results show that privacy vulnerability (PV) has a positive and significant impact on user's information privacy concerns (UIPC). Users of the social network Facebook are aware of the harm that can be done to the privacy of their information but lack the ability to take effective privacy protection measures. The Rewards variable (REW) influences user's information privacy concerns (UIPC) so it can be concluded that Facebook users tend to provide their privacy information when given rewards such as being able to join the community. This makes it vulnerable to threats that can be received by users. Users are better off maintaining privacy protection behavior and protecting privacy information from threats that can occur when using Facebook

REFERENCES

Volume 08, Number 01, Page 162-167
e-ISSN: 2598-120X; p-ISSN: 2598-117X

[1] Gischa, S. (2020, February 24). Globalisasi: Perubahan Perilaku Masyarakat Halaman all - Kompas.com. KOMPAS.com. https://www.kompas.com/skola/read/2020/02/24/130000469/globalisasi-perubahan-perilaku-masyarakat?page=all

[2] Zlatolas, L. N., Welzer, T., Hericko, M., & Hölbl, M. (2015). Privacy antecedents for SNS self-disclosure: The case of Facebook. Computers in Human Behavior, 45, 158–167. https://doi.org/10.1016/j.chb.2014.12.012

[3] S. (2022, November 2). Digital 2022 - We Are Social USA. We Are Social USA. https://wearesocial.com/us/blog/2022/01/digital-2022/

[4] Ali, A. T., Kamran, A., Ahmed, M. M., Raza, B., & Ilyas, M. (2019). Privacy Concerns in Online Social Networks: A Users' Perspective. International Journal of Advanced Computer Science and Applications, 10(7). https://doi.org/10.14569/ijacsa.2019.0100780

[5] Rizaty, M. A. (2022, August 9). Pengguna Facebook di Indonesia Capai 202,2 Juta pada Juli 2022. Dataindonesia.id. https://dataindonesia.id/digital/detail/pengguna-facebook-di-indonesia-capai-2022-juta-pada-juli-2022

[6] N. Naurah, "Serangan Phishing di Indonesia Terus Meningkat, Ini Datanya," GoodStats, Jul. 13, 2023. [Online]. Available: https://goodstats.id/article/serangan-phishing-di-indonesia-terus-meningkat-ini-statistiknya-U8VdY

[7] I. W. S. Suadnyana, "Anggota DPRD Klungkung Diduga Kena Phising gegera Klik Link di Facebook," Detikbali, Feb. 02, 2023. [Online]. Available: https://www.detik.com/bali/hukum-dan-kriminal/d-6548064/anggota-dprd-klungkung-diduga-kena-phising-gegera-klik-link-di-facebook

[8] N. Naurah, "Serangan Phishing di Indonesia Terus Meningkat, Ini Datanya," GoodStats, Jul. 13, 2023. [Online]. Available: https://goodstats.id/article/serangan-phishing-di-indonesia-terus-meningkat-ini-statistiknya-U8VdY

[9] J.-Y. Son and S. W. Kim, "Internet Users' Information Privacy-protective Responses: A taxonomy and a nomological model," Management Information Systems Quarterly, vol. 32, no. 3, p. 503, Jan. 2008, doi: 10.2307/25148854.

[10] Altman, I. (1975). The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding. Monterey, Calif. : Brooks/Cole Publishing Company.

[11] Rogers, R. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change1. The Journal of Psychology, 91(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

[12] Zhang, L., & McDowell, W. H. (2009). Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. Journal of Internet Commerce, 8(3–4), 180–197. https://doi.org/10.1080/15332860903467508

[13] Lee, D., LaRose, R., & Rifon, N. J. (2008). Keeping our network safe: a model of online protection behaviour. Behaviour & Information Technology, 27(5), 445–454. https://doi.org/10.1080/01449290600879344

[14] Woon, I. M. Y., Tan, G. W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In International Conference on Information Systems. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1237&context=icis2005

[15] Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Computers in Human Behavior, 28(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

[16] LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005, May). Online safety strategies: A content analysis and theoretical assessment. Paper presented at the 55th Annual Conference of the International Communication Association, New York, NY.

[17 Van De Garde-Perik, E., Markopoulos, P., De Ruyter, B., Eggen, B., & IJsselsteijn, W. W. (2008). Investigating Privacy Attitudes and Behavior in Relation to Personalization. Social Science Computer Review, 26(1), 20–43. https://doi.org/10.1177/0894439307307682

[18] Malhotra, N. K., Kim, S. W., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. Information Systems Research, 15(4), 336–355. https://doi.org/10.1287/isre.1040.0032

[19] Edwards, K. J. (2015). Examining the Security Awareness, Information Privacy, and the Security Behaviours of Home Computer Users. In ProQuest LLC eBooks. https://eric.ed.gov/?id=ED567975.

[20] Haryono, S. (2016). Metode SEM Untuk Penelitian Manajemen Amos Lisrel PLS. http://catalogue.ubharajaya.ac.id/slims/index.php?p=show_detail&id=40746

[21] Edwards, K. J. (2015). Examining the Security Awareness, Information Privacy, and the Security Behaviours of Home Computer Users. In ProQuest LLC eBooks. https://eric.ed.gov/?id=ED567975

[22] LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005, May). Online safety strategies: A content analysis and theoretical assessment. Paper presented at the 55th Annual Conference of the International Communication Association, New York, NY

[23] Lee, D., LaRose, R., & Rifon, N. J. (2008). Keeping our network safe: a model of online protection behaviour. Behaviour & Information Technology, 27(5), 445–454. https://doi.org/10.1080/01449290600879344

[24] Niu, H. (2010). Investigating the effects of self-efficacy on foodservice industry employees' career

Volume 08, Number 01, Page 162-167
e-ISSN: 2598-120X; p-ISSN: 2598-117X

commitment. International Journal of Hospitality Management, 29(4), 743–750. https://doi.org/10.1016/j.ijhm.2010.03.006

[25] Rhee, H., Kim, C., & Ryu, Y. H. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & Security, 28(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

[26] Woon, I. M. Y., Tan, G. W., & Low, R. (2005). A Protection Motivation Theory Approach to Home Wireless Security. In International Conference on Information Systems. http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1237&context=icis2005

[27] Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Computers in Human Behavior, 28(6), 2366–2375. https://doi.org/10.1016/j.chb.2012.07.008

[28] Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. Journal of Global Marketing, 31(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

[29] Sari, P. K., Candiwan, & Trianasari, N. (2014). Information security awareness measurement with confirmatory factor analysis. In 2014 International Symposium on Technology Management and Emerging Technologies. https://doi.org/10.1109/istmet.2014.6936509

[30] Haryono, S. (2016). Metode SEM Untuk Penelitian Manajemen Amos Lisrel PLS. http://catalogue.ubharajaya.ac.id/slims/index.php?p=show_detail&id=40746

[31] Haryono, S. (2016). Metode SEM Untuk Penelitian Manajemen Amos Lisrel PLS. http://catalogue.ubharajaya.ac.id/slims/index.php?p=show_detail&id=40746

[32] Crossler, R. E. (2010). Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data. https://doi.org/10.1109/hicss.2010.311

[33] Dinev, T., & Hart, P. '. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. Behaviour & Information Technology, 23(6), 413–422. https://doi.org/10.1080/01449290410001715723

[34] Adhikari, K., & Panda, R. K. (2018). Users' Information Privacy Concerns and Privacy Protection Behaviors in Social Networks. Journal of Global Marketing, 31(2), 96–110. https://doi.org/10.1080/08911762.2017.1412552

[35] Dinev, T., & Hart, P. '. (2004). Internet privacy concerns and their antecedents - measurement validity and a regression model. Behaviour & Information Technology, 23(6), 413–422. https://doi.org/10.1080/01449290410001715723

[36] Afandi, I. (2017). Analisis Hubungan Kesadaran Keamanan, Privasi Informasi, Dan Perilaku Keamanan Pada Para Pengguna Media Sosial Line

[37] Dienlin, T., & Trepte, S. (2014). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. European Journal of Social Psychology, 45(3), 285–297. https://doi.org/10.1002/ejsp.2049