

Summer 6-27-2016

FACTORS INFLUENCING THE INTENTION TO ADOPT IDENTITY THEFT PROTECTION SERVICES: SEVERITY VS VULNERABILITY

A-Young Kim
Chungbuk National University, aa4521@naver.com

Tae-Sung Kim
Chungbuk National University, kimts@cbnu.ac.kr

Follow this and additional works at: <http://aisel.aisnet.org/pacis2016>

Recommended Citation

Kim, A-Young and Kim, Tae-Sung, "FACTORS INFLUENCING THE INTENTION TO ADOPT IDENTITY THEFT PROTECTION SERVICES: SEVERITY VS VULNERABILITY" (2016). *PACIS 2016 Proceedings*. 68.
<http://aisel.aisnet.org/pacis2016/68>

This material is brought to you by the Pacific Asia Conference on Information Systems (PACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in PACIS 2016 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

FACTORS INFLUENCING THE INTENTION TO ADOPT IDENTITY THEFT PROTECTION SERVICES: SEVERITY VS VULNERABILITY

A-Young Kim, Department of Information Security Management, Chungbuk National University, Cheongju, South Korea, aa4521@naver.com

Tae-Sung Kim, Department of Management Information Systems, Chungbuk National University, Cheongju, South Korea, kimts@cbnu.ac.kr

Abstract

Privacy of the people is becoming important due to frequent leakage of personal information from financial company, telecommunication company and portal. Leaked personal information leads to some secondary damage involving identity theft such as taking out loans or getting credit cards. By examining the influence relation of vulnerability and severity on identity theft, usefulness, social influence and herding behavior, this paper aims to analyse the effect of each variable on adoption of services. This paper will contribute to expanding the use of identity theft protection services and reduce the damage caused by identity theft.

Keywords: identify theft, identity theft protection services, the leakage of personal information

1 INTRODUCTION

Criminal incidents involving the leakage of personal information have occurred over the past years in Korea, ranging from the inadvertent leakage of personal information on Auction in 2008 to the extensive 'leakage of personal information in credit card companies (affecting 20 million card holders)' in 2014. Personal information is leaked in any contexts where such information is provided including portals, financial service providers and telecommunication service providers, and the impacts are substantial.

Date	Companies	Scale of leakage incidents (number of leaked personal information)
2014.1.20	KCB, NH card, LOTTE card, KB card	104,000,000
2012.12	BC card · KB card ISP system hacking illegality withdraw	180,000,000
2012.7	KT	8,700,000
2012.5	EBS	4,220,000
2011.7	Nate·Cyworld	35,000,000
2011.4	Hyundai capital	1,750,000
2008.9	GS caltex	11,250,000
2008.1	Auction	18,630,000

Table 1. Personal information leakage incidents in Korea¹

Leaked personal information leads to some secondary damage involving identity theft such as taking out loans or getting credit cards. Therefore, leakage of personal information entails not only psychological damage associated with privacy infringement but also a range of offences including pecuniary losses relevant to identity theft and phishing. Indeed, according to the cases of infringement on personal information reported to the Korea Internet & Security Agency (KISA) and the types of counseling provided in 2014, 'the compromise, infringement and theft of personal information including resident registration numbers' accounted for the highest percentage, or 52%. Identity theft and resultant incidents and accidents occur in diverse fields including telecommunication, finance and health care. According to the data published by the Financial Supervisory Service, the number of illegitimate bank accounts (used for phishing scams) increased from 38,437 in 2013 to 44,705 in 2014. According to the data published by the Ministry of Science, ICT and Future Planning, the damage from identify theft in the telecommunication service sector is on the rise as shown in Table 2 (The Financial News 2014). The estimated amount of damage resulting from illegitimate phones across three mobile communication service providers reached 13 billion Won from 2009 to 2013, whilst that of damage attributable to illegitimate bank accounts in the financial service sector was 116.5 billion Won in 2012 and 138.2 billion Won in 2013.

Year	2009	2010	2011	2012	2013
Number of damage	4,008	4,094	3,847	3,882	5,200
Damage (million won)	2,513	2,347	2,354	2,341	2,789

Table 2. Identity theft damages of telecommunications services (criterion of three major telecommunications companies in Korea)

It is challenging to determine who is liable for any damage resulting from identity theft. According to Hyeong-cheol Kim, a lawyer representing the Korea Consumer Agency, quite a few cases of damage due to identity theft involve consumers' faults and are regarded as 'title lending', which is hardly

¹ www.thebell.co.kr

protected by law (Consumer Columns of the Korea Consumer Agency 2014). Thus, as the owner of personal information, one should make efforts to prevent identify theft beforehand, which is the best remedy. In the case of Korea, identity theft protection service operated by the Ministry of Science, ICT, and Future Planning and private credit evaluating company is representative as a measure of preventing identity theft. However, according to the 'Information Protection Status Survey: private sector' with 4,000 internet users conducted by the KISA in 2015, no more than 16% of respondents used the identity theft protection services to prevent any infringement on personal information. Korea's Identity theft protection service includes preventing identity theft, banking identity protection, block of self-authentication and use alarm related to telecommunication service. Telecommunication service identity theft protection is getting a text message and e-mail when registered new to various broadcasting telecommunication service (mobile communication, corded telephone, wireless internet, etc.) to check whether illegal use of other's name happened in realtime. Banking identity protection service is service that checks credit information inquiry made in realtime at finance company and provides notify corresponding breakdown and block service and prevents financial trade which customer doesn't know personally. These services are from free to over 3,000 won, and range of prevention and price is various. In this context, this paper sheds light on the variables affecting the adoption of identity theft protection services. To that end, this paper explores the literature on information protection behavior, and develops some measurement scales to determine any relationship. Ultimately, this paper contributes to raising the awareness of preventing damage from identity theft and suggests some factors mediating the adoption of identity theft protection services in practice.

2 LITERATURE REVIEW

2.1 Protection Motivation Theory and Information Protection Behavior

Protection motivation theory was first suggested by Rogers (1975) with intent to elucidate the behavioral change in line with fear appeals, and has been applied in psychology, health care and education to explicate how individuals change their attitude spontaneously towards dangerous messages and how they act subsequently. Influenced by the expectancy-value theory and cognitive processing theory, the protection motivation theory postulates certain serious fear factors cause a cognitive mediation process, which in turn impacts upon the protection motivation and leads to behavioral change (Lee 2011). Also, both personal evaluation arising from the cognitive mediation process and the resultant value determine one's behavior (Kim and Rha 2010). Rogers (1975) presented three factors of the protection motivation theory, i.e. (1) perceived severity of an event, (2) perceived vulnerability to an event, (3) perceived response efficacy to a threat. Fear appeals are assessed in terms of these three factors, whilst the protection motivation is adjusted by the cognitive process and causes some behavioral changes.

Subsequent exploration into predictors causing the protection behavior based on the protection motivation theory has been conducted. Park and Kim (2013) investigated the factors influencing SNS users to protect privacy about themselves based on Protection Motivation Theory (PMT). The results of the study are as follows; First, self-efficacy, response efficacy, perceived severity are significantly related to privacy protection awareness while perceived vulnerability is not significantly related. Second, privacy protection awareness have a positive effect on the privacy protection behavior on SNS.

Kim and Kim (2013) clarified the relationships among privacy concern/privacy protection importance and actual privacy protection behavior of online users based on privacy paradox perspective. According to the result, the antecedents of privacy concern and protection importance have statistically significant explanatory power except the relation between privacy experience and protection importance.

Kim and Jeong (2015) examined predictors of the 'disclosure' and 'protection' behaviors of privacy information, using protection motivation theory. Specifically, perceived severity was the major

predictor of privacy disclosure. Self-efficacy, knowledge, and perceived severity were predictors of privacy protection.

Park and Lee (2014) applied customer perspective to find out ways how to protect customers' privacy by themselves. It does so by examining the factors which affect customer privacy protection behaviors. Independent variables are as follows: Five variables (Perceived vulnerability, Perceived severity, Perceived response effectiveness, Perceived barriers, Privacy Rights awareness) were tested as critical variables influencing Behavioral Intention in PMT model. Privacy awareness had a moderating effect on the relationship between perceived severity and privacy protection behavior.

Woo (2014) investigated how involvement, protection motivation and intention to payment on the perceived risk of cyber security affect behavioral intention to technology acceptance and sustainable use for promoting personal information security. Research findings indicate that there are significant relationships between involvement, perceived severity, response efficacy, self-efficacy and intention to payment and the behavioral intention to technology acceptance and sustainable use for promoting personal information security. The perceived vulnerability, however, did not affect the dependant variable.

2.2 Literature on Identity Theft

Literature on identity theft largely dealt with the cases of damage and relevant mediation process. Hwang (2008) analyzed the intent of court rulings concerning illegitimate bank accounts by associating voice phishing scams with legal issues.

Kim (2010) investigated the title lending and identity theft occurring through the medium of illegitimate phones and bank accounts and the causality between the two to delve into the sociological significance of title lending and identity theft. The author drew on press releases concerning the National Police Agency, the Financial Supervisory Service, and the Korean Internet Safety Commission/the Korea Communications Commission as well as news articles of major daily newspapers in Korea since January 2003 regarding illegitimate phones and bank accounts to cast light on the issue, to explore the sociological significance of dealing in illegitimate phones or bank accounts, and to discuss any wise strategies applicable to preventing illegitimate phones and bank accounts from being transacted and misused for crimes based on the findings.

Han (2011) put the identity theft in telecommunication services into perspective, introduced the cases of disputes resulting from identity theft mediated by the Communication Complaints Mediation Center and the M-safer Service employed to prevent the identity theft in telecommunication services, and lastly proposed some remedies for improvement, e.g. Telecommunication service providers should exert efforts to strengthen the supervision over their agencies so as to tighten the requirements for proof of identity prior to signing the service agreements with customers, whilst policy measures should be developed to set up or reinforce a separate procedure to authenticate the identities of online subscribers in addition to the existing personal identification process. Also, the author argued more rigid provisions should be established regarding the duties of legal representatives of minor subscribers, and suggested the public awareness of the importance of handling personal information should be raised.

Cho and Ha (2015) verified the M-Safer Service's quality factors had positive effects on customer retention via customer satisfaction and trust.

3 RESEARCH MODEL AND HYPOTHESE

3.1 Model

This paper empirically investigates the factors impacting upon the intention to adopt the identity theft protection services. To that end, a model is designed as in Figure 1.

To formulate the model, this paper applies Rogers' (1983) protection motivation theory and proposes two independent variables, i.e. perceived vulnerability and perceived severity as the factors influencing the intent to adopt the identity theft protection services. In addition, TAM theory is applied to propose the perceived usefulness as the mediator affecting the intention to adopt the identity theft protection services. Moreover, this paper adds the social influence and herding behavior as variables to reinforce the protection motivation theory and TAM theory or to differentiate from existing theories.

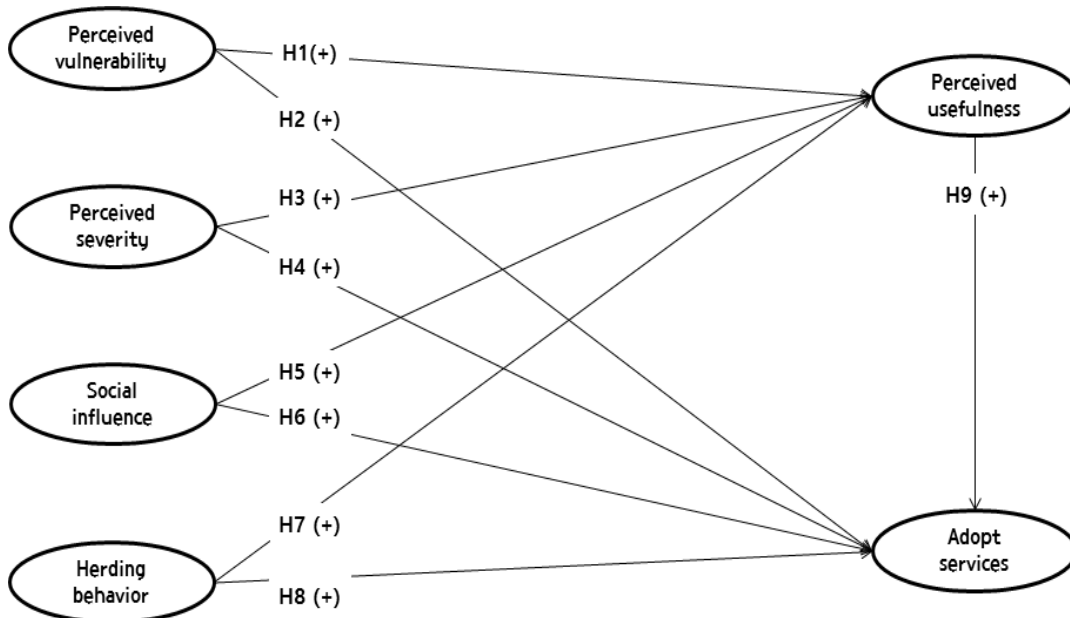


Figure 1. Research model

3.2 Hypotheses

Vulnerability is degree of possibility that threatening incident's result harm oneself (Ifinedo 2012), and in the study, operational defined vulnerability as degree of possibility that people thinking their own identity can be stolen. In this study, to resolve anxiety of my identity being stolen can use Identity theft protection service, this is because the service is thought to be useful due to it is believed to be effective counterplan of identity theft. Thus, inferred perceived vulnerability affects recognized usefulness. According to protection motivation theory, evaluation toward recognized threatening, which is, anxiety caused by perceived vulnerability activates psychological mechanism of cognitive dissonance and be a cause of taking action or attitude (Park and Lee 2014). Banks et al. (2010), Lee (2011) and Youn (2009) demonstrated that individuals who showed a high level of perceived vulnerability to any unfavorable exposure tended to act for privacy protection or increase the level of strategic behavior. Based on the foregoing study findings, the following hypotheses are set up.

Hypothesis 1: Perceived vulnerability will have positive effects on perceived usefulness.

Hypothesis 2: Perceived vulnerability will have positive effects on the intention to adopt services.

Kim (2015) proved that the threat severity of information security affects the perceived usefulness of information security technology. In this study, to resolve anxiety of my identity being stolen can use Identity theft protection service, this is because the service is thought to be useful due to it is believed to be effective countermeasure of identity theft. Thus, inferred perceived vulnerability affects recognized usefulness. Youn (2005) proved that personal intention and behavior to protect privacy increased in proportion to the perceived severity of any risk. Also, Cismaru (2006) proved that the intention to follow recommended behavior online increased in proportion to the perceived severity of

threatening external conditions. Based on the foregoing previous findings, the following hypotheses are established.

Hypothesis 3: Perceived severity will have positive effects on perceived usefulness.

Hypothesis 4: Perceived severity will have positive effects on the intention to adopt services.

Social influence is person's perception about others who is important to me thinks about it toward whether to do or not (Fishbein and Ajzen 1975). In this study, social influence is concept measuring how people meaningful around me perceive about usage of identity theft protection service. Rogers (1995) suggested that late adopters who would slowly adopt new products were influenced by others. In the same vein, when people purchased unfamiliar products, they were influenced by others to a great extent (Fisher and Price 1992). Oh et al. (2005) demonstrated that as an antecedent influencing the intention to adopt innovative digital home services the social influence had positive effects on adoption. Social influence has been used as variables affecting utility or use intention in various studies. Thus, this study also inferred feeling identity theft protection service's utility or social influence can affect acceptance intention and set hypothesis as the following.

Hypothesis 5: Social influence will have positive effects on perceived usefulness.

Hypothesis 6: Social influence will have positive effects on the intention to adopt services.

Herding behavior is defined as consumers imitating other consumers seeing behavioral phenomenon of others and believe they have better information about the product (Bonabeau 2004). Huang & Chen (2006) studied about herding behavior in individual decision making and they proved that herding behavior had significant effects on buying behavior in highly uncertain settings. Also, Yoo et al. (2008) empirically analyzed the herding behavior impacted on the behavioral patterns of individuals when they adopt technology. In the study, inferred that to lower uncertainty of decision making of identity protection service acceptance, if perceive that many people are using the service, people will do herding behavior and accept the service. Therefore, based on previous findings on information cascade resulting from uncertainties arising from the tendency towards herding behaviour (Banerjee 1992; Bikhchandani et al. 1992), the following hypotheses are set up regarding the effects of herding behavior on the intention to adopt services.

Hypothesis 7: Herding behavior will have positive effects on perceived usefulness.

Hypothesis 8: Herding behavior will have positive effects on the intention to adopt services.

Perceived usefulness refers to the extent to which use of a certain system improves one's job performance (Davis 1989; Davis et al. 1989). Thus, using information technology on account of a high level of perceived usefulness is attributable to one's expectation that the technology will benefit his/her job performance. Classic research on TAM (Davis et al. 1989; Mathieson 1991; Taylor and Todd 1995) argued that the perceived usefulness had the most significant effects on the adoption of information technology and user behavior. This paper focuses on the perceived usefulness only, excluding the ease of use, which is a primary factor in the TAM theory, as the factor impacting upon the intention to adopt the identity theft protection services. Previous findings suggested that perceived usefulness significantly mediates between the intention to adopt new technology or services and several factors influencing the adoption. Hence, the following hypothesis is set up.

Hypothesis 9: Perceived usefulness will have positive effects on the intention to adopt services.

4 DATA ANALYSIS RESULTS

4.1 Data Collection & Analysis

To derive and empirically validate the factors impacting upon the adoption of identity theft protection services, this paper uses a questionnaire survey. Based on previous research, the items used to measure each latent variable proposed in the research model are modified and complemented in accordance

with the present objective and content. For data collection, youths and children under 18 years of age among the survey respondents were excluded on the grounds that they were unlikely to perceive the risk of identity theft. Therefore, the questionnaire respondents are 20 years old minimum. Excluding the general demographic information of respondents, every question item was rated on a 5-point Likert scale.

The survey was conducted from November 4 to December 7, 2015 in Chungbuk National University, using the face-to-face interview and Google Docs. Among the 170 copies of questionnaire returned, 2 copies were excluded from the analysis due to insincere responses. Therefore, a total of 168 copies of questionnaire were used for the statistical data analysis.

4.1.1 Demographics

Demographic characteristics of the present sample is as follows. The sample comprises 88 males (52.38%) and 80 females (47.62%), indicating a nearly even gender distribution. The respondents in the sample group are mostly in their 20s.

Type		Frequency	Percentage(%)
Gender	Male	88	52.38
	Female	80	47.62
Age	20s	159	94.64
	30s	6	3.57
	40s	2	1.19
	50s	1	0.6
	60s	0	0
Occupation	Homemaker	0	0
	White collar job	8	4.76
	Blue collar job	5	2.98
	Public official	1	0.6
	Student	131	77.97
	Self-employed	0	0
	Professional(professor, doctor, lawyer, etc.)	5	2.98
	Technician	11	6.55
	Agriculture, fisheries, animal husbandry	0	0
	Etc.	7	4.16

Table 3. Descriptive statistics of the sample

4.1.2 Use of identity theft protection services

This study investigated the awareness and usage of the identity theft protection services for the respondents. Respondents who have heard of or are aware of the identity theft protection services account for 59.53%. 33 respondents use the services (19.64%), whereas 135 respondents (80.35%) do not, indicating most people do not use such services. The most widely used service is 'Blocking personal identification and the notification service.' As for the reasons for not using the identity theft protection services, 66.67% of respondents answered 'I do not know much about the services.'

4.2 Model Verification

Smart PLS 2.0 is used to test the hypotheses with the sample consisting of 168 respondents. Prior to verifying the hypotheses, this paper analyzes the measurement model to assess the reliability and validity of measurement items. Each latent variable's CR (Composite Reliability) and Cronbach's α are 0.7 or higher. Also, each latent variable's AVE (Average Variance Extracted) is 0.5 or higher as suggested by Fornell and Larcker (1981) and Chin (1998). The factor loading of constructs is 0.7 or higher, which is the reference point suggested by Fornell and Larcker (1981). The discriminant

validity is verified based on whether the square roots of AVE marked on the diagonal axis of the correlation coefficients between constructs are greater than the correlation coefficients between other constructs (Fornell and Larcker 1981). According to the analysis, the smallest square root of AVE is greater than the greatest correlation coefficient, which indicates good discriminant validity.

	herding behavior	social influence	usefulness	adopt services	severity	vulnerability	AVE	Composite credibility	Cronbach's Alpha
herding behavior	0.833						0.695	0.872	0.779
social influence	-0.013	0.859					0.739	0.934	0.913
usefulness	0.273	0.274	0.854				0.730	0.915	0.876
adopt services	0.186	0.418	0.633	0.880			0.774	0.932	0.902
severity	0.289	0.171	0.269	0.306	0.951		0.905	0.966	0.947
vulnerability	0.254	0.223	0.362	0.362	0.616	0.924	0.853	0.959	0.942

Table 4. Internal consistency and discriminant validity verification

4.3 Verification of the Structural Model

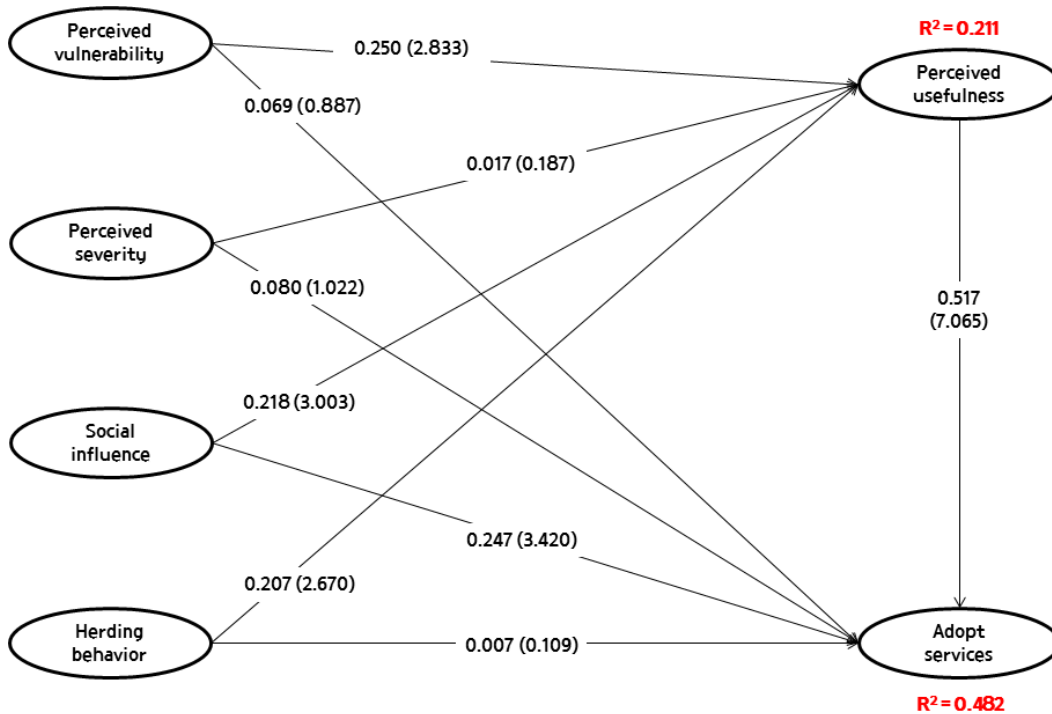


Figure 2. PLS test of the research model

After the proposed model is validated, the 9 hypotheses are tested. To test the hypotheses, the path coefficient between constructs is determined by PLS. Also, the t-value of each path coefficient is yielded by the bootstrapping of PLS to test each hypothesis. As a result, hypotheses 1, 5, 6, 7 and 9

lead to significant t-values of path coefficients. Thus, as in Table 3, hypotheses 1, 5, 6, 7 and 9 are supported. On the other hand, hypotheses 2, 3, 4 and 8 are rejected.

The explanatory power of a path model in PLS analysis is represented by the explained variance, R^2 (Chin and Gopal 1995). According to the analysis of R^2 in the PLS of the present model, the explanatory power of the perceived usefulness and the intention to adopt services is 21% and 48%, respectively, which are 10% higher than the power of test suggested by Falk and Miller (1992).

Hypothesis		Path coefficients	t-value	Result
H1	Perceived vulnerability → Perceived usefulness	0.250	2.833	Supported
H2	Perceived vulnerability → Adopt services	0.069	0.887	Not supported
H3	Perceived severity → Perceived usefulness	0.017	0.187	Not supported
H4	Perceived severity → Adopt services	0.080	1.022	Not supported
H5	Social influence → Perceived usefulness	0.218	3.003	Supported
H6	Social influence → Adopt services	0.247	3.420	Supported
H7	Herding behavior → Perceived usefulness	0.207	2.670	Supported
H8	Herding behavior → Adopt services	0.007	0.109	Not supported
H9	Perceived usefulness → Adopt services	0.517	7.065	Supported

Table 5. Summary of the results

5 CONCLUSION

5.1 Discussion of the Finding

The findings shed light on the following.

First, concerning the variables relevant to the perceived vulnerability to identity theft, people feel the usefulness of the identity theft protection services when they perceive that identity theft occurs easily. Also, the perceived usefulness leads to the intention to adopt such services.

Second, it is hypothesized here that the perception of negative results due to identity theft will have significant effects on the perceived usefulness of and the intention to adopt the identity theft protection services. Yet, the t-values indicating the effects of the perceived severity on the perceived usefulness and the intention to use such services are 0.187 and 1.022, respectively, which reject the hypothesis. The perceived severity did not affect the dependant variable in this study. People are highly aware of the seriousness of the incident due to identity theft, but does not think it's going to happen to them. Therefore, it can be interpreted as they do not feel the need to use the service. Thus, to induce people to adopt the identity theft protection services, it is more important to promote the fact that identity theft can occur easily than to highlight the severity of identity theft.

Third, the variables relevant to the social influence of identity theft protection services measure the extent to which others influence one's use of identity theft protection services. This paper shows that greater social influence leads to the perceived usefulness of and the intention to adopt the identity theft protection services. Importantly, most people feel the usefulness when they use such services and intend to adopt the services, whereas from the perspective of social influence people intend to adopt the identity theft protection services, on seeing those who are important to them recommend or use such services, regardless of the perceived usefulness.

Fourth, the variables relevant to the herding behavior towards the identity theft protection services measure the extent to which 'others' choice or behavior influences 'my' choice or behavior and whether it has significant effects on the intention to adopt the services. That is, it is hypothesized that frequently seeing others use the identity theft protection services will cause one to perceive the usefulness or will impact upon his/her intention to adopt such services. Herding behavior affects the

perceived usefulness of identity theft protection services, but does not directly lead to the intention to adopt such services as the social influence does.

5.2 Implications of the Study

To delve into the factors influencing the intention to adopt identity theft protection services, a range of variables are employed in this paper. It is empirically proved that the perceived vulnerability to identity theft triggers the perceived usefulness of identity theft protection services and leads to the adoption of such services. Also, the perceived vulnerability to, rather than the perceived severity of, the identity theft increases the perceived usefulness of such services. Interestingly, people are significantly influenced by others in adopting the identity theft protection services. When others recommend or encourage using the identity theft protection services, one comes to perceive the usefulness of such services, and furthermore intends to adopt such services regardless of the perceived usefulness. This analysis finding agrees with the aforementioned response to the question of 'whether to use the identity theft protection services in the future,' where the highest percentage (62.22%) of respondents answer 'I will use identity theft protection services once many others do.'

To raise the adoption of identity theft protection services, it is necessary to inform the public of the fact that identity theft may easily cause incidents and damage. The findings will hopefully be conducive to raising the public awareness of identity theft protection and broader adoption of relevant services so as to minimize any damage. According to the present survey results, respondents do not use identity theft protection services primarily because they are 'not aware of the services', which suggests the need to inform the public of how easily identity theft could occur and to promote the identity theft protection services. Currently, the government-led M-Safer, which is a free identity theft protection service developed for the telecommunication service sector, is available and need be promoted so as to increase the public awareness. Moreover, it is necessary to develop effective methods to increase the use of identity theft protection services for financial transactions and personal identification. Identity theft protection services are intended to protect one's properties and creditability. Given the increasing non face-to-face transactions, it is expected to be frequent at identity theft incidents. Thus, identity theft protection services will prove more useful than ever before.

5.3 Limitation of the Study

Despite the foregoing implications, this paper has the following limitations. First, as the sample is limited to students in their 20s, diverse opinions are not considered. The perceived usefulness of, or the intention to adopt, the identity theft protection services may vary with age groups. Further studies need to analyze different age groups with larger samples and diversify the survey questions to derive more significant implications. Second, this paper fails to consider diverse variables representing the intention to adopt the identity theft protection services. In addition to the perceived vulnerability, perceived severity, social influence and herding behavior, other factors influencing the intention to adopt the identity theft protection services should be extensively taken into account. Third, different types of identity theft protection services exist. The perceived usefulness or intention to adopt such services may vary with different services. Hence, it is necessary to comparatively analyze the identity theft protection services across diverse sectors, e.g. finance, telecommunication and personal identification. Fourth, In part to derive hypotheses it may lack a logical basis. In a further study it is necessary to clarify relationship of the variables.

6 ACKNOWLEDGEMENTS

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Korean Government (NRF-2011-0025512). This work was

supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2015S1A5A2A01009763).

References

- Bae, S.Y. (2008). America FTC '2007 Consumer Fraud and Identity Theft Complaint Data' of the Main contents and Implications. *Monthly Trend of Consumer Policy* (Korea Consumer Agency), 2, 1-18 (in Korean).
- Banerjee, A. V. (1992). A simple model of herd behavior. *The Quarterly Journal of Economics*, 797-817.
- Banks, M. S., Onita, C. G., & Meservy, T. O. (2010). Risky Behavior in Online Social Media: Protection Motivation and Social Influence. In *AMCIS* (p. 372).
- Bikhchandani, S., Hirshleifer, D., & Welch, I. (1992). A theory of fads, fashion, custom, and cultural change as informational cascades. *Journal of political Economy*, 992-1026.
- Bonabeau, E. (2004). The perils of the imitation age. *Harvard Business Review*, 82(6), 45-54.
- Chin, W. W., & Gopal, A. (1995). Adoption intention in GSS: relative importance of beliefs. *ACM SigMIS Database*, 26(2-3), 42-64.
- Chin, W. W. (1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, 295(2), 295-336.
- Cho, J.H. and Ha, G.R. (2015). An Empirical Study on the Effects of M-Safer Service Quality on Customer Satisfaction, Trust and Customer Retention. *Entrue Journal of Information Technology*, 14.2, 113-130 (in Korean).
- Cismaru, M. (2006). Using protection motivation theory to increase the persuasiveness of public service communications.
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.
- Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: a comparison of two theoretical models. *Management science*, 35(8), 982-1003.
- Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*. University of Akron Press.
- Fisher, R. J., & Price, L. L. (1992). An investigation into the social context of early adoption behavior. *Journal of Consumer Research*, 477-486.
- Fishbein, M., & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley, 6.
- The Financial News. (Oct. 14, 2014). Identity theft, damages 12.3 billion won and compensation six billion won. Retrieved from <http://www.fnnews.com/news/201410141010274025> (in Korean).
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research*, 39-50.
- Han, J.Y. (2011). Dispute Resolution Cases on Identity Theft. *Journal of Law & Economic Regulation*, 4(2), 116-119 (in Korean).
- Huang, J. H., & Chen, Y. F. (2006). Herding in online product choice. *Psychology & Marketing*, 23(5), 413-428.
- Hwang, J.I. (2008). A study on the fake deposit bank pass-book and tele-financial fraud crime. *Korean Association of Public Safety and Criminal Justice Review*, 17(4), 443-476 (in Korean).
- Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83-95.
- Kim, S.H. and Lee, G.S. (2015). An Empirical Study on Influencing Factors of Using Information Security Technology. *The journal of Society for e-Business Studies*, 20(4), 151-175(in Korean).
- Kim, S.H. and Park, H.S. (2013). An Analysis of Influence Factors on Privacy Protection Awareness and Protection Behavior and moderating Effect of Privacy Invasion Experience. *The Journal of Internet Electronic Commerce Research*, 13(4), 79-105 (in Korean).

- Kim, S.E. (2010). A Sociological Research about the problem of a borrowed identity, identity theft in Korea. In Proceedings of special Conference on The Korean Sociological Association, 43-77 (in Korean).
- Kim, J.K. and Kim, S.H. (2013). Privacy Protection Behavior of Online User: Based on Privacy Paradox Perspective. *The Journal of Internet Electronic Commerce Research*, 13(1), 41-64(in Korean).
- Kim, J.H. and Rha, J.Y. (2010). Analysis of Consumer Privacy Protection Behaviors in online. In Proceedings of spring Conference on Korean Society of Consumer Studies, 1-10 (in Korean).
- Kim, H.J. and Jeong, S.H. (2015). Disclosure and Protection of Online Privacy Information among Older Adults. *Journal of Cybercommunication Academic Society*, 32(3), 49-79 (in Korean).
- KISA. (2015). 2015 Information Protection Status Survey: private sector (in Korean).
- Korea Consumer Agency. (Jan. 22, 2014). *Consumer Columns* 569 (in Korean).
- Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, 50(2), 361-369.
- Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, 19(5), 469-479.
- Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information systems research*, 2(3), 173-191.
- Oh, J.I., Won, J.J. and Lee, J.S. (2005). An Empirical Study on the Potential Users Adoption of Digital Home Services. In Proceedings of spring Conference on the Korea Society of Management Information Systems, 1-8 (in Korean).
- Park, C.O. and Lee, S.W. (2014). A study of the User Privacy Protection Behavior in Online Environment: Based on Protection Motivation Theory. *Journal of Internet Computing and Services*, 2, 59-71 (in Korean).
- Park, H.S. and Kim, S.H. (2013). An Empirical Study on SNS users' Privacy Protection Behaviors. *Management and Economics (Keimyung university Industrial Management Institute)*, 46(2), 69-91 (in Korean).
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change¹. *The journal of psychology*, 91(1), 93-114.
- Rogers Everett, M. (1995). *Diffusion of innovations*. New York, 12.
- Ryu, I. and Choi, H.R. (2008). The Effect of Social Influence on Flow, Perceived Usefulness and Intention to Use in Online Community. *The Journal of Information Systems*, 17(2), 113-135 (in Korean).
- Taylor, S., & Todd, P. (1995). Assessing IT usage: The role of prior experience. *MIS Quarterly*, 561-570.
- Woo, H.J. (2014). Exploring the Relationship between the Perceived Risk to Cyber Security and the Behavioral Intention to Technology Acceptance and Sustainable Use for Promoting Personal Information Security. *Journal of Communication Science*, 14(2), 220-257 (in Korean).
- Yoo, C.W. et al. (2008). The Effect of Herding Behavior and Perceived Usefulness on Intention to Purchase e-Learning Content: Comparison Analysis by Purchase Experience. *Asia Pacific Journal of Information Systems*, 18(4), 105-130 (in Korean).
- Youn, S. (2005). Teenagers' perceptions of online privacy and coping behaviors: a risk-benefit appraisal approach. *Journal of Broadcasting & Electronic Media*, 49(1), 86-110.
- Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs*, 43(3), 389-418.