J. Inf. Technol. Appl. Manag. 27(2): 1~21, April 2020
https://doi.org/10.21219/jitam.2020.27.2.001

ISSN 1598-6284 (Print)
ISSN 2508-1209 (Online)

The Effect of Security Awareness Training on the Use of Biometric Authentication: Focusing on the Protection Motivational Behaviors

Seungmin Jung* · Joo Yeon Park**

Abstract

The purpose of this study is to investigate the behavioral factors affecting the security attitude and intention to use biometrics password based on the protection motivation theory. This study also investigates security awareness training to understand trust, privacy, and security vulnerability regarding biometric authentication password. This empirical analysis reveals security awareness training boosts the protection motivational factors that affect on the behavior and intention of using biometric authentication passwords. This study also indicates that biometric authentication passwords can be used when the overall belief in a biometric system is present. After all, security awareness training enhances the belief of biometric passwords and increase the motivation to protect security threats. The study will provide insights into protecting security vulnerability with security awareness training.

Keywords : Biometric Authentication Security Awareness Training Security Attitude Protection Motivation Theory

Received : 2019. 11. 29.   Revised : 2020. 03. 10.   Final Acceptance : 2020. 03. 15.

* First Author, Assistant Professor, Department of Store Management, Soongeui Women's College, e-mail : jungsm@sewc.ac.kr
** Corresponding Author, Lecturer, Discipline of Information Technology, Mathematics and Statistics, College of Science, Health, Engineering and Education, Murdoch University, 90 South Street, Murdoch Western Australia 6150, Tel : +61-8-9360-6257, e-mail : park3500@naver.com

1. Introduction

With the rapid growth of computers and telecommunications technologies, users are using a variety of information technology every day. For example, a variety of IoT devices such as home Internet sharing devices, door locks, smart home appliances, AI speakers and smart bands are commonly used in everyday life. However, while IoT device use provides a convenient living environment, it is easy to be exposed to information leaks and security threats. One of the most commonly used authentication methods to protect personal information and protect information is text passwords. However, even those who are relatively interested in cybersecurity have the hassle of setting up complicated passwords for each device, and they often do not change their passwords frequently, making the real security problem even more serious. More and more users complain about complex text password configurations and the number of different passwords on each site. Also, the illegal use of personal and corporate information using a weak authentication system has frequently occurred in recent years. In fact, many consumers say websites or systems that use only user names and passwords are too weak and unreliable, but many still use such sites. This can be seen as overlooking the vulnerability of security because it is simple and easy to use. Therefore, biometric authentication technology, which is convenient and superior secure, is attracting attention as a next-generation security technology that can supplement or completely replace unstable passwords. Biometric technology is often defined as "a technology that authenticates individuals based on their unique physical and behavioral characteristics" [Coventry, De Angeli, and Johnson, 2003]. Biometrics authentication includes a user's physical characteristics including fingerprint, palm, retina, iris, face, signature, and voice. Fingerprint identification has become a common technology in everyday life as fingerprint sensors are installed not only on smartphones but also on notebooks and other devices. Especially, biometrics has been actively used in smartphone devices which become a daily used tool for many people and perform various multi-tasks. The smartphone often requires the sensitive personal information to operate the functions such as financial transfer. Thus, the protection of privacy and security in using the smartphone became a critical issue. Smartphone manufacturers have provided a way to unlock them through fingerprinting rather than passwords or pattern locks to provide convenient usability while safeguarding users' personal information. Also, the financial sector is actively introducing biometric technology to complement the imperfect security level of financial services and to enhance user convenience.

However, there are voices that worry about leakage of biometric information. While major banks and institutions are introducing fingerprint authentication services for security and privacy, users who are afraid of leakage are still reluctant to use biometric authentication services. Financial institutions such as banks, securities, and cards are more cautious about adopting biometrics for security because they have a lot of sensitive information. According to a report of the Bio information gathering and utilization survey shows that many biometric authentication systems are not used as many customers on average per day [Yu, 2017]. There is concern about the possibility of information abuse (55%) or theft or forgery

(51%) for the opposition to using biometric technology. Moreover, about 33% were concerned about the leakage of collected biometric information. 69% of respondents were worried about the leakage of health information collected through the biometric system in mobile devices. Another reason to avoid biometrics is unfamiliarity and inconvenience [An, 2016]. These results turn out showing that many people are aware that biometric technologies will be needed in terms of security and privacy, but still, tend to be reluctant to use them because of unfamiliar and the lack of trust in biometric technologies. Therefore, it is necessary to examine what factors increase the intention to use biometric authentication passwords and how to increase trust in biometric systems.

Early research on biometric authentication focuses on biometric characteristics based on the technology acceptance model (TAM) and user acceptance and on the biometric technology itself, including perceived usefulness and ease of use [Moody, 2004; Rosa et al., 2007]. However, Korea Consumer Agency [2016] has reported that "simplification" and "safety of authentication methods" as ranked first (40.7%) and second (22.7%), respectively, are the foremost important factors in the use of authentication methods. Therefore, it is necessary to consider both "simplification" and "safety" in studying on authentication methods. Most researches on authentication methods often have used the factors of perceived usefulness and perceived ease-of-use based on the technology acceptance model (TAM) to show the impact of the biometrics password use intention. However, few empirical studies have examined the user's intentions for biometric passwords in terms of protection motivation that includes awareness of security problem, security weaknesses of existing passwords, and security awareness training. In particular, there is little empirical analysis that focuses on security awareness training which enable to enhance security recognition in a digital environment and raise awareness on information protection. With a few recent empirical studies available, this study needs to explore key factors other than perceived usefulness and perceived ease-of-use in order to increase the use of biometrics passwords with simplicity and safety.

This study, therefore, shed a light on security awareness training and education that enhance protective motivation in using biometric authentication passwords based on the protection motivation theory. The protection motivation theory is about an individual's security cognitive process that recognizes security issues and useful to explain intention and behavior to perform a security action to protect personal computers and user systems [Ifinedo, 2012]. This theory is able to explain an individual's security cognitive process to protect security issues and identify an individual's intention to perform a security action such as choosing secured passwords [Anderson and Agarwal, 2010]. Therefore, the purpose of this study is to investigate the effect of security awareness training on protective motivational factors relate to the security attitude and intention to use biometrics authentication password. The result of this study will provide insights into protecting security vulnerability with security awareness training.

2. Theoretical Framework and Hypotheses

2.1 Protection Motivation Theory

Protection Motivation Theory is an extension of the belief model related to health in the social psychology and health domains. This is about an individual's security cognitive process that recognizes security issues. This theory is evaluated as a key theory that explains the cognitive process of the individual's protected activity and explains the motivation of protection through factors such as occurrence probability and severity for security problem [Rogers, 1983]. In addition, the theory of protection motivation can be very useful in identifying an individual's intention to perform a security action and is useful for explaining and predicting the intentions and behaviors related to the security of personal computers and user system [Anderson and Agarwal, 2010]. Liang and Xue [2009] proposed the security threat avoidance theory and studied the security behavior of personal computers. They suggested that the likelihood of occurrence and severity affect the avoidance motivation through perceived threaendts.

According to the theory, the motivation to protect is triggered by Threat Appraisal and Coping Appraisal [Rogers, 1983; Ifinedo, 2012]. The detailed components of the threat assessment consist of likelihood and severity of a security threat [Johnston and Warkentin, 2010; Vance et al., 2012]. The likelihood of a security vulnerability is the degree to which a user is aware of the likelihood of harming a malicious attack, possibly having spyware, or potentially causing harm to a security issue [Rogers, 1983]. In previous research, these factors are presented as the main variables in the research of the organization's information system security and protection of personal information, explaining the security guideline compliance and protection intention. Therefore, although physical aspects of security are also important, it is necessary to evaluate users' security perception and awareness to provide policies and guidelines for security. This is because the security awareness of the user may affect the attitude and intention to implement security behavior.

2.2 Research Model and Hypotheses

Information security awareness training refers to a series of activities to raise the awareness of information security while at the same time enhancing the user's understanding of information security [Jemal, 2014]. By enhancing information security awareness, user scan recognize the importance of information security and can suppress the possibility of information infringement while obeying information security norms. In this sense, the education and training in enhancing information security awareness are the most direct and cost-effective means by which users can acquire the latest technical information regarding the security issue [Albrechtse and Hovden, 2010]. So many organizations are fostering training programs for information security awareness.

Security awareness training increases the level of understanding in security problems that the existing passwords could embed potentially and enhance the protect motivation to avoid problems. Awareness of potential security problem is defined as the degree to which a user is aware of the likelihood of harming a malicious attack, possibly having spyware, or potentially causing harm to a security issue [Rogers, 1983]. The protection motivation consists of factors such as a security vulnerability, likelihood and severity of a security threat [Johnston and Warkentin, 2010]. In previous research, these factors are presented as the main variables in the study of the organization's information system security and protection of personal information, explaining the security guideline compliance and protection intention [Vance et al., 2012].

According to the study of Liang and Xue [2009], the perception of security vulnerability and severity could increase protection motivation to avoid the security threat. That is because the security awareness of the user may affect the attitude and intention to implement security behavior. Kim and Kang [2008] showed that the degree of prior knowledge-related to privacy protection influences the choice of secure passwords to protect information. Security awareness program and campaigns also have a positive effect on the perception of a security vulnerability which resultsin reducing the weak password usage and security threat [Yim, 2014; Eminagaoglu et al., 2010]. James et al. [2006] also argued that an individual's understanding of importance or need for security has a positive effect on using biometric devices. The field experiment by Kim et al. [2018] has shown that in groups that have completed security education, security awareness training has a positive effect on employee's security behaviors through the awareness of potential risks. These findings suggest that organizations need to consider providing regular training programs. The study of Lee and Kim [2015] analyzes the effect of most underlying security education in security activities on security capabilities of enterprise and it indicates that security education has a positive (+) correlation with security capabilities. Also, Heo and Ahn [2020] argued that security education has a moderating effect between awareness of security policies and security behavior and Yun [2016] argued that technical support is also important, but by improving the cybersecurity awareness and security expert knowledge through the cybersecurity education to workers is important to raise the security level. In addition, the research of Kang and Chang [2014] found that information security education to increase awareness of information security had a positive impact on information security behavior, mediating an understanding of information security policy. Above all, if there is a lack of sufficient understanding of security policies and lack of knowledge of security risks, then the training of industrial security does not affect the security-related behavior [Lee and Chae, 2014]. In the research of Chang and Kang [2012], the information security education has a significant impact on information security awareness, such as the importance of password security, and information security education has also been proven to have a significant impact on perceived information security risks. Therefore, the following hypotheses were set up based on previous studies.

H1: Security awareness training has a positive effect on the awareness of potential security problems.

H2: Security awareness training has a positive effect on the security vulnerability of existing passwords.

H3: Security awareness training has a positive effect on the perceived privacy of biometric passwords.

H4: Security awareness training has a positive effect on the trust in a biometric password.

According to motivation theory, threat assessment is an essential factor that induces motivation and positively affects protection behavior [Rogers, 1983]. Users of smartphones and personal computers recognize that security threats are more likely to occur, and if they determine that the security problem is severe, users are aware that the current security system is not stable and cannot be relieved. That positively affects the user's security attitude toward biometrics password [Kim and Kim, 2014]. In other words, as the awareness of security risks expand, the more secure in threats and information leakage [Shaw et al., 2009]. Security vulnerability of the existing password is defined as the exposure risk of passwords that can harm users of information systems, and measures vulnerabilities due to passwords recognized by users against existing character passwords [Peyravian and Zunic, 2000]. Generally speaking, the vulnerability is a perception of "how serious threats to personal information leakage threat me." If the user believes that the risks presented are irrelevant or insignificant, they do not affect information security awareness. However, if they think that vulnerability can be perceived and seriously harmed, the motivation to increase information security awareness is enhanced. Thus, these security vulnerabilities have a positive impact on information security behavior. Besides, Rogers [1983] assumed that the likelihood of occurrence and severity for the security problem would generate protective motivation and lead to protective behavior changes. Lee and Larsen [2009] also found that as smartphone users perceived vulnerabilities to threats more strongly, they increased their security attitudes by inducing strong protection motives. In the study of Heo and Ahn [2020], the awareness of security policies affects the information security behavior, and the perceived risk of information security has proven that there is a moderating effect between awareness of security policies and security behavior. In addition, Lee et al. [2015] verified that the individual's knowledge level affected his attitude toward information security. And the perceived security severity and the threat appraisal of the organization's employees have been verified to have a positive impact on the intention to follow security policy and thus have an impact on the security-related behavior [Kim and Song, 2011]. Therefore, we set the following hypotheses.

H5: The awareness of potential security problem has a positive effect on the security attitude toward the use of a biometric password.

H6: The security vulnerability of the existing password has a positive effect on the security attitude toward the use of a biometric password.

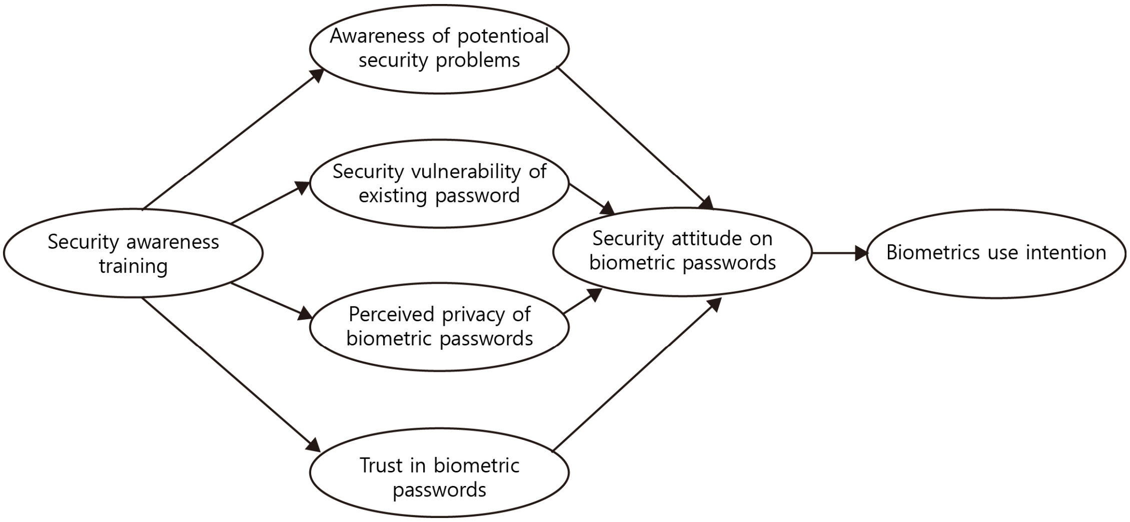
Perceived privacy often refers to "the level of individual control over information about oneself" and "the possibility of not using the information improperly" [Smith et al., 1996; Jarvenpaa and Todd, 1996]. Perceived privacy is defined as a perception that users'information will not be used elsewhere without his or her consent, and privacy is a situational concept that is changed by time, place, social and psychological factors [Jarvenpaa and Todd, 1996]. A study found that the positive relationship between privacy and behavioral intentions [Dinev and Hart, 2004]. James et al. [2006] studied the acceptability of biometric information devices in terms of perceived privacy. A study on privacy in online shopping found that consumers' perception of their personal information in online shopping affects their trust that influences purchase intention [Vijayasarathy, 2004; Flavian and Guinaliu, 2006]. Also, a study showing that perceived privacy affects the intention to use biometrics continuously through a trust [Lee and Kim, 2011]. Moreover, customers who are aware of these risks become more open to innovative methods of identification or verification, and personal privacy concerns significantly influence a customer's intention to use fingerprint technology [Kim and Bernhard, 2014]. Therefore, the following hypotheses were established based on previous studies.

H7: The perceived privacy of biometric passwords has a positive effect on the security attitude on a biometric password.
H8: The perceived privacy of the biometrics password has a positive effect on the trust in a biometric password.

The concept of trust is defined differently depending on the researcher's perspective or discipline. Rousseau et al. [1998] defined trust as "a psychological state that includes the willingness to accept risk possibilities based on positive expectations of other people's intentions or actions." Thus, trust in biometrics involves a belief that risk will be reduced, and the willingness to take risks for biometrics [Das and Teng, 1998]. Trust has been used in a variety of studies in the IS field, such as cohesiveness, attitudes, and intentions of knowledge sharing, and organizational value creation [Tamjidyamcholo et al., 2013]. There are also many studies on the positive relationship between trust in a biometric system and the behavioral intention to use biometric passwords [Ring and Van De Ven, 1994; Ngugi et al., 2011]. The security attitude refers to the degree to which the user positively evaluates the use of the security system [Bulgurcu et al., 2010]. Trust on biometrics authentication reflects credibility on security and privacy and affects the security attitude and intention to continuous use of biometrics due to the perceived usefulness [Lee and Kim, 2011; Soh et al., 2010]. Therefore, we set the following hypotheses based on previous studies.

H9: The trust of a biometric password has a positive effect on the security attitude on a biometric password.

The biometrics use intention is referred to the users' behavioral intention to use biometric passwords and measured it as opposed to using any alternate passwords [Bhattacherjee, 2001]. Bulgurcu et al. [2010] asserted that security attitudes and behavioral intentions are important cognitive processes before action. The positive attitude toward the security of smartphone and personal computer users positively influences the intention of security behavior, and the security attitude affects the positive influence of security behavior intention [Kim and Kim, 2014; Kim et al., 2016]. Besides, security attitudes positively influence the security behavior of internet users and the intention of security activities of using social networks [Park et al., 2012]. Anderson and Agarwal [2010] also argued that attitudes have a positive effect on the security behaviors of personal computers and the intentions of security activities on the Internet. Therefore, we set the following hypotheses based on these previous studies.


Awareness of potentioal security problems
Security vulnerability of existing password
Security awareness training
Security attitude on biometric passwords
Biometrics use intention
Perceived privacy of biometric passwords
Trust in biometric passwords

〈Figure 1〉 Research Model

H10: The security attitude toward biometric password has a positive effect on the intention to use a biometric password.

Based on the theoretical review, we propose a research model on the use of biometrics in the view of individuals'motivational protection factors such as security awareness, comprehension of the security vulnerability, perceived privacy and trust. 〈Figure 1〉 represents a proposed research model showing the relationship with relevant factors affect on the biometrics use intention.

3. Research Methodology

3.1 Measurement

A questionnaire survey was conducted for those who have used biometrics authentication passwords. Fingerprint passwords occupied about 70% that respondents have used followed by iris recognition and face recognition. They were asked about the extent of security awareness training, the level of awareness of potential security issues, vulnerabilities in existing passwords and the intention to use biometric authentication. A total of 1478 questionnaires was used in the final analysis excluding the incorrect or missing questionnaires. Since the surveys were collected mostly from university students, the ages of 20 to 25 were mostly occupied for 70% of the age distribution. By age, 1040 people in their 20s, 121 people in their 40s, 120 people in their 10s, 108 people in their 30s, and 67 people in their 50s. Women accounted for about 70 percent of the population of 1,035, far higher than men. This was because mainly a women's university where the survey was conducted. The limitations of the study were to explain if there were differences in gender-specific outcomes. This will be argued in the research limitation at the end.

The questionnaires were developed based on the previous researches on biometrics, and all the measurement items were measured with 7 points Likert scale. 〈Table 1〉 represents the items and sources of the questionnaires used in the research model.

〈Table 1〉 The Measurement Items of Variables

Variables	Survey Items	Source
Awareness of potential security problems	- Passwords can create security threats. - Passwords can expose you to security threats. - There is a possibility that a password could cause harm to a malicious attack.	Rogers [1983], Anderson and Agarwal [2010], Ifinedo [2012]
Security vulnerability of existing password	- The security of existing character passwords is highly vulnerable due to an unchanged. - Existing character passwords are vulnerable because of the possibility of using duplicate use in multiple sites. - The existing character password is highly vulnerable, depending on the length of the password. - Existing character passwords are vulnerable because of the possibility to create sensitive information.	Peyravian and Zunic [2000], Kim and Kang [2008]
Perceived privacy of biometric passwords	- My biometric information will not be used for other purposes without my approval. - My biometric information will not be used by others without my approval. - My personal information in the biometric authentication system will not be used for other purposes without my consent. - My personal information in the biometric authentication system will not be used by anyone without my consent.	Smith et al. [1996], Roca et al. [2006]
Trust in biometric passwords	- The biometric authentication password is reliable. - The biometric authentication password can be trusted as a user identification method. - Personal information of the biometric authentication password can be managed by a user-centered. - The reliability of the biometric authentication password is undoubtedly trustworthy. - Personal information of the biometric authentication password is managed by a reliable management system.	Vatanasombut et al. [2008], Roca et al. [2006]
Security attitude on biometric passwords	- A biometric password is necessary for security. - A biometric password is important for security. - It is wise to use a biometric password for security.	Davis [1989], Bulgurcu et al. [2010]
Security awareness training	- Schools/institutions often provide training for password security. - Schools/institutions often advertise on password security awareness. - The school/institution provides a strong policy on password security.	Limayem et al. [2004]
Biometrics use intention	- I will use a biometric authentication password. - I want to use a biometric authentication password. - For user identification, I would prefer the biometric authentification password. - If possible, I would like to use the biometric authentification password.	Bhattacherjee [2001], Lin et al. [2005]

3.2 Data Analysis

In this study, reliability, feasibility analysis, and path analysis were carried out using a statistical program SPSS 18 package and Amos 18 package, which is a structural equation program. First, Cronbach's Alpha coefficients were measured in reliability tests to determine whether internal consistency existed among the constructed questionnaire items. In general, if the value is 0.6 or more, it can be considered the construct is reliable

〈Table 2〉 The Internal Consistency and Convergent Validity

Construct	#item	Communality	Cronbach's Alpha	AVE
Awareness of potential security problems	1	0.841	0.918	0.792
	2	0.888		
	3	0.852		
Security vulnerability of existing password	1	0.664	0.845	0.577
	2	0.723		
	3	0.707		
	4	0.677		
Perceived privacy of biometric passwords	1	0.795	0.921	0.746
	2	0.81		
	3	0.825		
	4	0.816		
Trust in biometric passwords	1	0.724	0.902	0.648
	2	0.743		
	3	0.663		
	4	0.776		
	5	0.747		
Security attitude on biometric passwords	1	0.829	0.876	0.676
	2	0.848		
	3	0.747		
Security awareness training	1	0.908	0.899	0.824
	2	0.906		
Biometrics use intention	1	0.761	0.919	0.733
	2	0.803		
	3	0.837		
	4	0.826		

[Chae, 2001]. As shown in 〈Table 2〉, all the construct used in this study is shown 0.8 or above for Cronbach's alpha values, which indicates that internal consistency is highly reliable. Also, the communality analysis shows that all the reference values are above 0.6 satisfying threshold criteria in indicating that each item reflects the constructs well [Chang and Jung, 2015]. Convergent validity issatisfied by the average variance extraction value (AVE) of greater than 0.5 [Fornell and Larcker, 1981].

In this study, confirmatory factor analysis was carried out using Amos 18. The factor analysis using principal component analysis and varimax rotation indicates that the individual items used in this study are all reliable by showing the loading value greater than 0.7 and the cross-loading values for other items are less than the loading values of a correlated construct. The result is shown in 〈Appendix 1〉.

3.3 Hypothesis Testing

In order to verify the hypothesis, path analysis was performed with Amos' structural equation. The fit of the model is recommended over 0.8 for GFI, NFI, RFI, IFI, TLI, CFI, and RMSEA is less than 0.1 [Jin et al., 2012]. The fitness of this model is NFI = 0.920, RFI = 0.901, IFI = 0.929, TLI = 0.912, CFI = 0.929 and RMSEA = 0.070 representing the fitness of the research model is appropriate. The results of the hypothesis test are summarized in 〈Table 3〉, and the results are as follows. The hypothesis is accepted when C.R. (critical ratio) is greater than 1.96 with $p < 0.05$.The path analysis of this study shows that all hypothesis has been accepted except hypothesis 4 and 7, which are not satisfied with the threshold criterion. Hypothesis 3 and 5 are accepted with $p<0.05$, while hypotheses 1, 2, 6, 8, 9 and 10 are accepted with $p<0.001$.

First, security awareness training has a positive effect on the perceived possibility of a security problem, perception of security vulnerability of the existing password, and perceived privacy of biometrics. Thus, hypotheses 1, 2 and Hypothesis 3 were adopted. However, the result shows that security awareness training does not directly relate to the trust of the biometric password. Thus, the positive relationship between security awareness training and trust in a biometric password (Hypothesis 4) was rejected. Second, the awareness of the possibility of security problems and the recognition of the security vulnerability of existing passwords have a positive effect on the security attitude toward biometric passwords. Therefore, Hypothesis 5 and Hypothesis 6 are accepted. It can be seen that the more a user recognizes that a password is likely to cause harm due to a malicious attack or a risk of being exposed to a security threat, the more the user positively

〈Table 3〉 The Result of Hypothesis Test

Hypothesis	Model Path	Estimate	S.E.	C.R.	Result
H1	Security awareness training → Awareness of potential security problems	.166	.030	5.466	Supported***
H2	Security awareness training → Security vulnerability of existing password	.074	.022	3.374	Supported***
H3	Security awareness training → Perceived privacy of biometric passwords	.061	.025	2.446	Supported*
H4	Security awareness training → Trust in biometric passwords	.009	.017	.515	Not Supported
H5	Awareness of potential security problems → Security attitude on biometric passwords	.043	.017	2.537	Supported*
H6	Security vulnerability of existing password → Security attitude on biometric passwords	.232	.026	9.004	Supported***
H7	Perceived privacy of biometric passwords → Security attitude on biometric passwords	.023	.030	.766	Not Supported
H8	Perceived privacy of biometric passwords → rust in biometric passwords	.627	.023	26.920	Supported***
H9	Trust in biometric passwords → Security attitude on biometric passwords	.575	.037	15.459	Supported***
H10	Security attitude on biometric passwords → Biometrics use intention	.726	.030	24.170	Supported***

*$p < 0.05$, **$p < 0.01$, ***$p < 0.001$.

evaluates the use of the biometric password. Also, the more users perceived the weakness of the existing character password security method, the higher the degree of user's positive evaluation of the use of a biometric password. This can be interpreted that the user of the protected motivation to prevent it through the perception of security vulnerabilities and that the existing password security incident is likely to cause the formation of a positive attitude to a biometric password.

Third, the perceived privacy of biometrics is not positively influenced bythe security attitude toward biometrics, rejecting Hypothesis 7. The perceived privacy of biometrics is positively related to the trust of biometrics and the trust in biometrics has a positive effect on security attitudes toward biometrics. Thus, Hypothesis 8 and 9 are accepted. That is, as the user perceives that his or her personal information will not be used elsewhere without the consent of the user in the biometrics system, the reliability of the biometrics authentication system increases. And as the reliability of the biometrics system becomes higher, the attitude toward the use of a biometrics password is getting positive. Lastly, hypothesis 10 was accepted representing that the security attitude toward biometrics will have a positive effect on the intention to use biometrics. As the user represents a positive attitude for the biometrics password, the use of the biometrics increases. Therefore, the result shows that the rational behavior theory which explains the influence of security attitude on security activity intention can also be applied in the case of the biometrics field.

4. Discussion and Implication

As the digital environment becomes more commonplace, concerns about information security and privacy have increased and the introduction of biometric authentication technology has become commonplace. However, despite the recognition of convenient biometrics to replace the poor security of the commonly used ID password, many people still tend to be reluctant to use biometric passwords. Therefore, it is necessary to examine what factors increase the intention to use biometric authentication passwords and how to increase trust in biometric systems.

This study provides underlying factors and paths to increase the use of biometric authentications and suggest its use of intention in the view of protection motivational behavior. This study shows that security awareness training is essential to increase the intention of using biometric passwords with enhancing the level of comprehension for the security problem and the vulnerability of the existing passwords. First, the recognition of the security problem isa major factor affecting the security attitude and use intention of a biometric password. When a user recognizes that a security problem can occur due to a password, the user is motivated to protect it. As a result, a positive security attitude toward biometrics authentication is formed, which increases the intention to use the biometric authentication. Therefore, it is necessary to understand the importance of security protection and the possibility of security threats through security awareness training. Second, it is confirmed that the security vulnerability of existing passwords is the main factor affecting the intention to use biometrics. That is, the more the user recognizes that the existing password security is weak, the more positive the user will be using the biometric password. After all, it is necessary to recognize that the text password of the existing user authentication has a high risk of damaging the users' information such as information leakage.

Third, trust in biometrics is an important factor affecting the security attitude toward biometrics and intention to use biometric identification. We found from this study that trust in biometrics can be developed through the recognition of the privacy in biometrics that also can be established by security awareness training. That is, security awareness can increase the understanding of privacy issues on biometrics and thus enhance trust in biometrics. On the other hand, even if the user perceives that the personal information will not be used without the approval of the user in the biometric system, the intention to use the biometric password will not be enhanced unless it leads to overall trust in the biometric system. Because biometrics possess potential problems such as the fact that the biological information cannot be easily changed once it is leaked, it is important to increase the overall reliability and trust of the biometrics system. However, the results of this study show that security awareness training does not increase directly the overall trust in the biometric password use. Security awareness training only increases the understanding of privacy strength of biometric password that leads to the trust of the biometrics. That is, security awareness could provide the understanding that the biometrics can protect private information, and thus thereby enhancing the reliability of the biometrics and increasing the intention of use. In short, because security awareness is the first step in information security management [Chen et al., 2018], it is important that training and education for security awareness continue to be performed at all levels of users.

The results of this study also suggest both academic and practical implications to the educators and companies introducing and adopting biometrics passwords. Academically, this study extends existing research into security-related issues based on perceived usefulness, ease of use, or theories such as TAM. This study has found important variables and new pathways that affect the intention to use biometrics in addition to the perceived usefulness and perceived ease of use. The underlying factors such as security problems and understanding of biometric passwords could protect the security vulnerability in using digital devices. However, most students and users tend to have insufficient knowledge of the password procedure and principle. In this, security awareness is able to increase the awareness of security problems and understanding of biometric passwords as shown in this study. The educational programs or training for security awareness help users recognize that passwords can cause harm to a malicious attack or that they are vulnerable to security threats. It also enhances the information security awareness of the organization and the user's information management capability. Moreover, the password security awareness education helps the user to recognize the weakness of the existing character password security method and allows the user to recognize that the user's personal information in the biometric system will not be used elsewhere without the user's consent. However, according to the results of this study, it can be seen that the overall reliability of the user's biometrics system is not increased by security awareness training alone. The intention of the biometric authentification can be increased by the motivational factors such as the understanding of security problems, security vulnerabilities of existing passwords, and the privacy of biometric systems. Therefore, it is suggested that educators need to organize and develop educational programs for all levels of users regularly to aware security vulnerabilities that may result in serious problems. In sum, improving security awareness and understanding of the weakness of security can help users avoid information leaking and protect privacy. However, the programs for security awareness are still insufficient and lacking in many organizations and educational institutions [Furnell and Vasileiou, 2017]. Therefore, this study suggests that programs and training for security awareness should be undertaking regularly in not only educational institutions but organizations that deal with data and information. Also, it is necessary to motivate information security through education on password selection and understanding of its importance and usage.

As to the practical implications, security awareness is encouraged due to the following concerns. First, The use of digital devices is becoming commonplace and security incidents are becoming frequent, and security is the critical issue to be considered especially for organizations where all the data and information are keen for their success. Companies are responsible for the damage done to their customers might causeany loss and leaking of data, which in the future could result in impact on their trust in their services. Thus, security awareness training should put in place with a great consideration that couldprevent tremendous organizational loss and financial damage caused by any security threat. With that, this study suggests enhancing the human side of information security such as understanding the vulnerability of security and password techniques. As the evidence form previous research showing that the effective security awareness program can be the strongest protective methods for security threats [Abawajy, 2014], organizations should put security awareness programs in place to enhance user awareness vulnerabilities. Second, companies have the advantage of being able to conduct objective and real-time management of users. When using character ciphers, users are likely to share a single ID and password as needed. For example, acquaintances can share a paid service with a single ID. This has a direct adverse effect on the profit of the company, and the company cannot manage the information of the user properly. Recently, all information of users is stored and utilized as big data. If the company cannot manage the information of the user properly, the records of the users stored and utilized by the company can be mismatched and misidentified, which causes substantial loss and financial damage. Moreover, the solution to the problem of how to store biometric information securely will be a major challenge to increase the use of biometrics, the next generation of cryptography. Therefore, this study promotes the use of biometrics in corporations and organizations, and it should be accompanied by an understanding of proper security awareness and biometrics passwords. Continuous security education suggests that it is an important prerequisite to increase the use of biometric passwords and to solve the security problems that may arise in the organization.

5. Conclusion and Limitation

As information technology becomes more utilized and various important information is being used through networks and digital devices, concerns and strengthening of personal protection and security have become important. Even though biometrics technology cannot easily change the physical and behavioral characteristics of the body once it is leaked, and it can be a problem of privacy invasion in using the information on the user's body part, the use of biometrics authentication is increasingly widespread as it ensures superior security. However, people are still likely to avoid using biometrics authentication in reality. In order to put a light on why people are afraid of using biometrics, this study has empirically verified the major factors influencing the intention to use biometrics in the context of biometric authentication technology. And this study reveals the new paths of variables affecting security attitude and intention to use biometrics by suggesting the importance of security awareness training and emphasizing the importance of security enhancement using biometrics. The security awareness training will be able to play an important role in increasing the use of biometric passwords and thus the educators and policy-makers should take it for consideration in developing the curricular for security issues. In conclusion, in order to protect information and data of companies and organizations as well as their own personal information in recent digital environment, rather than considering the application of technical security devices first, security education should be given top priority to raise awareness of security problems and vulnerabilities and to improve understanding of authentication and biometrics.

Although this study suggests important implications for the attitude and intention of using biometrics technology, it has the following limitations. In this study, the most common group in the demographic distribution is fingerprint cipher in the type of biometric cipher, female in sex, and 20 in the age group. However, we could not compare the main variables and path differences for each group. Therefore, in future research, it is necessary to investigate further comparisons of key variables and paths that affect the intention to use biometrics by gender, age, and type of biometrics.

References

〔1〕 Abawajy, J., "User preference of cyber-security awareness delivery methods", *Behavior & Information Technology*, Vol. 33, No. 3, 2014, pp. 237-248.

〔2〕 Albrechtse, E. and J. Hovden, "Improving information security awareness and behavior through dialogue, participation and collective reflection", *An Intervention Study, Computers and Security*, Vol. 29, No. 4, 2010, pp. 432-445.

〔3〕 An, J. S., "Biometric authentication for banknotes ... Will it settled as a new trend?". Available at http://www.segye.com/newsView/20160202004025 (Downloaded 03 Feb. 2016).

〔4〕 Anderson, C. L. and R. Agarwal, "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions", *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 613-643.

〔5〕 Bhattacherjee, A., "Understanding Information Systems Continuance: An Expectation-Confirmation Model", *MIS Quarterly*, Vol. 25, 2001, pp. 351-371.

〔6〕 Bulgurcu, B., H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information security Awareness", *MIS Quarterly*, Vol. 34, No. 3. 2010, pp. 523-548.

〔7〕 Chae, S. I., *Social Science Investigation Methodology*, Hakhyeonsa, Seoul, Korea. 2001.

〔8〕 Chang, H. S. and D. H. Jung, "A study on the Relationship between Cyberloafing Characteristic and Cognitive Dissonance", *Journal of The Korea Society of Computer and Information*, Vol. 20, No. 9, 2015, pp. 73-80.

〔9〕 Chang, M. H. and D. Y. Kang, "Factors Affecting the Information Security Awareness and Perceived Information Security Risk of Employees of Port Companies", *Journal of Navigation and Port Research*, Vol. 36, No. 3, 2012, pp. 261-271.

〔10〕 Chen, X., L. Chen, and D. Wu, "Factors That Influence Employees' Security Policy Compliance: An Awareness-Motivation- Capability Perspective", *Journal of Computer Information Systems*, Vol. 58, No. 4, 2018, pp. 312-324

〔11〕 Coventry, L., A. De Angeli, and G. Johnson, "Usability and Biometric Verification at the ATM Interface", *SIGCHI Conference on Human Factors in Computing Systems*, 2003, pp. 153-160.

〔12〕 Das, T. K. and B. Teng, "Between Trust and Control: Developing Confidence in Partner Cooperation in Alliance", *Academy of Management Review*, Vol. 23, No. 3, 1998, pp. 491-512.

〔13〕 Davis, D., "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology", *MIS Quarterly*, Vol. 13, No. 3, 1989, pp. 319-340.

〔14〕 Dinev, T. and P. Hart, "Internet Privacy Concern and their Antecedents-Measurement Validity and a Regression Model", *Behavior and Information Technology*, Vol. 23, No. 6, 2004, pp. 413-422.

〔15〕 Eminagaoglu, M., E. Ucar, and S. Eren, "The positive outcomes of information security awareness training in companies: A case study", *Information Security Technical Report*, Vol. 4, 2010, pp. 1-7.

〔16〕 Flavian, C. and M. Guinaliu, "Consumer Trust, Perceived Security and Privacy Policy: Three Basic Elements of Loyalty to a Web Site", *Industrial Management and Data Systems*, Vol. 106, No. 4, 2006, pp. 601-620.

〔17〕 Fornell, C. and D. F. Larcker, "Evaluating Structural Equation Models with Unobservable Variables and Measurement Error", *Journal of Marketing Research*, Vol. 18, No. 1, 1981, pp. 39-50.

〔18〕 Furnell, S. and I. Vasileiou, "Security education and awareness: Just let them burn?", *Network Security*, Dec. 2017, pp. 5-9.

〔19〕 Heo, J. and S. J. Ahn, "Effects of Biased Awareness of Security Policies on Security Compliance Behavior", *The Journal of Korean Association of Computer Education*, Vol. 23, No. 1, 2020, pp. 63-75.

〔20〕 Ifinedo, P., "Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory", *Computers and Security*, Vol. 31, No. 1, 2012, pp. 83-95.

〔21〕 James, T., T. Pirim, K., Boswell, B. Reithel, and R. Barkhi, "Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model", *Journal of Organizational and End User Computing*, Vol. 18, No. 3, 2006, pp. 1-24.

〔22〕 Jarvenpaa, S. L. and P. Todd, "Consumer Reactions to Electronic Shopping on the World Wide Web", *International Journal of Electronic Commerce*, Vol. 1, No. 2, 1996, pp. 59-88.

〔23〕 Jemal, A., "User preference of cyber security awareness delivery methods", *Behaviour & Information Technology*, Vol. 33, No. 3, 2014, pp. 237-248.

〔24〕 Jin, S. H., D. G. Lee, and S. J. Lee. "The Influence of Technostress and Antismart on Smartphones", *Journal of Digital Convergence*, Vol. 10, No. 10, 2012, pp. 187-195.

〔25〕 Johnston, A. C. and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study", *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 549-566.

〔26〕 Kang, D. Y. and M. H. Chang, "An Analysis of Compliance with Information Security Policy Effects on Information Security Ability and Behavior: Focused on Workers of Shipping and Port Organization", *Journal of Korea Port Economic Association*, Vol. 30, No. 1, 2014, pp. 97-118.

〔27〕 Kim, B. R., J. W. Lee, and B. S. Kim, "Effect of Information Security Training and Services on Employees' Compliance to Security Policies", *Informatization Policy*, Vol. 25, No. 1, 2018, pp. 99-114.

〔28〕 Kim, J. K. and D. Y. Kang, "A Study on the Factors Affecting the Information Systems Security Effectiveness of Password", *Asia Pacific Journal of Information System*, Vol. 18, No. 4, 2008, pp. 1-26.

〔29〕 Kim, J. K. and J. H. Kim, "An Empirical Study on Security Behavioral Intention of Individual Users: Comparison between Personal Computers and Smartphones", *The Journal of Internet Electronic Commerce Research*, Vol. 14, No. 6, 2014, pp. 45-69.

〔30〕 Kim, J. K., J. Y. Kim, and Q. Li, "A Study on Factors Affecting Smartphone User's Security Behavior Intention", *The Journal of Internet Electronic Commerce Research*, Vol. 16, No. 6, 2016, pp. 115-136.

〔31〕 Kim, J. S. and B. Bernhard, "Factors influencing hotel customers' intention to use a fingerprint system", *Journal of Hospitality and Tourism Technology*, Vol. 5, No. 2, 2014, pp. 98-125.

〔32〕 Kim, S. H. and Y. M. Song, "An Empirical Study on Motivational Factors Influencing Information Security Policy Compliance and Security Behavior of End-Users (Employees) in Organizations", *The e-Business Studies*, Vol. 12, No. 3, 2011, pp. 327-349.

〔33〕 Korea Consumer Agency, Mobile Payment Service Status Survey, 2016.

〔34〕 Lee, B. Y. and M. Y. Kim, "Factors affecting the Continuance Usage Intention of Biometric Technology: Comparing Dark Scenario with Bright Scenario", *The Journal of Society for e-Business Studies*, Vol. 16, No. 3, 2011, pp. 1-22.

〔35〕 Lee, C. S. and Y. H. Kim, "An Analysis of Relationship between Industry Security Education and Capability: Case Centric on Insider Leakage", *The Journal of Society for e-Business Studies*, Vol. 20, No. 2, 2015, pp. 27-36.

〔36〕 Lee, K. E., J. Y. Kim, J. S. Hyun, and C. J. Park, "The Effects of Information Security Vaccine User's Construal Level and Message Type on the Information Security Behavior", *The Journal of Korean Association of Computer Education*, Vol. 18, No. 6, 2015, pp. 33-42.

〔37〕 Lee, S. K. and M. S. Chae, "An Study on the Factors that Motivate The Compliance of the Organizational Security Policy", *Korean Journal of Business Administration*, Vol. 27, No. 6, 2014, pp. 927-953.

〔38〕 Lee, Y. and K. R. Larsen, "Threat or coping appraisal: determinants of SMB executives' decision to adopt antimalware software", *European Journal of Information Systems*, Vol. 18, No. 2, 2009, pp. 177-187.

[39] Liang, H. and Y. Xue, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective", *Journal of the Association for Information Systems*, Vol. 11, No. 7, 2009, pp. 394-413.

[40] Limayem, M., M. Khalifa, and W. W. Chin, "Factors Motivating Software Privacy: A Longitudinal Study", *IEEE Transactions on Engineering Management*, Vol. 51, No. 4, 2004, pp. 414-425.

[41] Lin, C. S., S. Wu, and R. J. Tsai, "Integrating Perceived Playfulness into Expectation-Confirmation Model for Web Portal", *Information and Management*, Vol. 43, No. 5, 2005, pp. 683-693.

[42] Moody, J., "Public Perceptions of Biometric Devices: The Effect of Misinformation on Acceptance and Use", *Journal of Issues in Informing Science and Information Technology*, Vol. 1, 2004, pp. 753-761.

[43] Ngugi, B., A. Kamis, and M. Tremaine, "Intention to Use Biometric Systems", *e-Service Journal*, Vol. 7, No. 3, 2011, pp. 20-46.

[44] Park, K. A., D. Y. Lee, and C. M. Koo, "An Empirical Study about Internet and Social Network Security Behavior of End User", *Journal of Information Systems*, Vol. 21, No. 4, 2012, pp. 1-29.

[45] Peyravian, M. and N. Zunic, "Methods for Protecting Password Transmission", *Computers & Security*, Vol. 19, No. 5, 2000, pp. 466-469.

[46] Ring, P. S. and A. H. Van De Ven, "Developing Processes of Cooperative Inter-organizational Relationships", *Academy of Management Review*, Vol. 19, 1994, pp. 90-118.

[47] Roca, J. C., C. M. Chiu, and F. J. Martinez. "Understanding E-learning Continuance Intention: An Extension of the Technology Acceptance Model", *Human-Computer Studies*, Vol. 64, No. 8, 2006, pp. 683-696.

[48] Rogers, R. W., *In Social Psychophysiology: A Sourcebook. Cacioppo*, J. T. & Petty, R. E. (Eds.). Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protected Motivation. New York: The Guilford Press, 1983.

[49] Rosa, R. H., A. S. Patrick, and A. Ozok, "Perception and Acceptance of Fingerprint Biometric Technology", *Symposium On Usable Privacy Security(SOUPS)*, 2007.

[50] Rousseau, D. M., S. G. Sitkin, R. S. Butt, and C. Camerer, "Not So Different After All: A Cross-Discipline View of Trust", *Academy of Management Review*, Vol. 23, No. 3, 1998, pp. 393-404.

[51] Shaw, R. S., C. C. Chen, A. Harris, and H. J. Huang, "The impact of information richness on information security awareness training effectiveness", *Computers & Education*, Vol. 52, 2009, pp. 92-100.

[52] Smith, H., S. Milberg, and S. Berke, "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly*, Vol. 20, 1996, pp. 167-196.

[53] Soh, K. L., W. P. Wongand, and K. L. Chan, "Adoption of Biometric Technology in Online Applications", *International Journal of Business and Management Science*, Vol. 3, No. 2, 2010, pp. 121-146.

[54] Tamjidyamcholo, A., M. S. B. Baba, H. Tamjid, and R. Gholipour, "Information security: Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity and shared-language", *Computers & Education*, Vol. 68, 2013, pp. 223-232.

[55] Vance, A., M. Siponen, and S. Pahnila,

"Motivation IS Security Compliance: Insights From Habit and Protection Motivation Theory", *Information and Management*, Vol. 49, 2012, pp. 190-198.

〔56〕 Vatanasombut, B. M., A. C. Igbaria, and W. Stylianou, "Information Systems Continuance Intention of Web-based Applications Customers: The Case of Online Banking", *Information and Management*, Vol. 45, No. 7, 2008, pp. 419-428.

〔57〕 Vijayasarathy, L. R., "Predicting Consumer Intentions to Use On-line Shopping: The Case for an Augmented Technology Acceptance Model", *Information and Management*, Vol. 41, No. 6, 2004, pp. 747-762.

〔58〕 Yim, M. S., "Why Security Awareness Education is not Effective?", *Journal of Digital Convergence*, Vol. 12, No. 2, 2014, pp. 27-37.

〔59〕 Yu, J. W., Replace your secret number... Is there any problem with the introduction of biometric authentication in the financial sector?. Available at http://www.enewstoday.co.kr/news/articleView.html?idxno=690695 (Download 03 Feb. 2017).

〔60〕 Yun, J. B., "A Study on the Short Term Curriculum for Strengthening Information Security Capability in Public Sector", *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 26, No. 3, 2016, pp. 769-776.

〈Appendix 1〉 The Result of Factor Analysis

Construct		Factor						
		1	2	3	4	5	6	7
Awareness of potential security problems	1	.016	.037	.002	.224	.886	.051	.038
	2	.028	.030	-.018	.281	.893	.074	.067
	3	.008	.023	.000	.274	.877	.053	.071
Security vulnerability of existing password	1	.090	.082	.181	.733	.269	.083	.002
	2	.071	.086	.018	.794	.207	.193	-.012
	3	.104	.112	-.009	.805	.178	.052	.045
	4	.119	.106	.112	.777	.166	.076	.043
Perceived privacy of biometric passwords	1	.322	.150	.802	.123	-.006	.101	.008
	2	.309	.150	.814	.060	.008	.159	-.021
	3	.275	.132	.847	.056	.015	.093	.044
	4	.228	.145	.850	.070	-.023	.103	.068
Trust in biometric passwords	1	.690	.320	.296	.112	.032	.212	-.001
	2	.711	.309	.264	.103	.071	.235	-.034
	3	.717	.161	.272	.110	.051	.187	.012
	4	.802	.218	.263	.087	-.010	.076	.056
	5	.786	.171	.270	.107	-.031	.102	.072
Security attitude on biometric passwords	1	.183	.288	.131	.146	.070	.818	-.015
	2	.195	.280	.141	.180	.095	.817	-.055
	3	.318	.326	.214	.129	.057	.688	.006
Security awareness training	1	.029	-.002	.025	.053	.080	-.023	.947
	2	.044	-.011	.049	.013	.066	-.023	.947
Biometrics use intention	1	.274	.781	.122	.129	.018	.208	-.015
	2	.187	.829	.149	.111	.050	.208	.012
	3	.230	.850	.146	.117	.006	.162	.005
	4	.235	.827	.161	.076	.043	.231	-.017

Author Profile

Seungmin Jung

Seungmin Jung is an assistant professor of the department of Store Management, Soongeui Women's College. Her work has been published in Management & Information Systems Review, Journal of the Korea Academia-Industrial cooperation Society, and Journal of CEO and Management Studies. Her current primary research areas include system and information security, acceptance of new technology, and e-business.

Joo Yeon Park

Dr. Joo Y. Park is currently a Lecturer in the discipline of information technology, mathematics and statistics at Murdoch University, Western Australia. Her work has been published in the number of peer-review journals including Knowledge Management Research & Practice, Sustainability and Information & Management. Her research interests include management information systems, system security and digital entrepreneurship.