J. Patuakhali Sci. and Tech. Uni. 2018, 9 (1&2): 227-238 ISSN 1996-4501

INVESTIGATING FACTORS INFLUENCING THE ADOPTION OF INFORMATION SECURITY AWARENESS OF THE INDIVIDUAL USERS:AN EMPIRICAL STUDY IN BANGLADESH

Md. Tariqul Islam[1]

Abstract

Most of the countries of the world have established information security awareness programs due to the intensified need for improved information security and for ensuring the awareness of the people regarding the security risk. Users need to be aware of the information security to protect their system from unauthorized access. The aim of this paper was to investigate the factors influencing the adoption of information security awareness programs. The study was based on the data collected in two stages. At first, we obtained the constructs of the model through interviewing 20 IT professionals and then collected data by using structured questionnaire developed from the initial data. Through analyzing the data of 213 questionnaires by SmartPLS software, we found significant and positive relationship ($p<0.05$) of spam filtering, device password, and safety in social network, and negative but significant relationship of knowledge of cyber law with the adoption of information security awareness. However, we also found positive but insignificant relationship ($p>0.05$) of using antivirus and firewall with the adoption of information security awareness in Bangladesh.

KeyWords: Information system, Information security awareness, User adoption, Bangladesh.

Introduction

The practice of protecting information from unauthorized access, use, disclosure, and modification is called information security (Silic & Back, 2014). Ensuring authorized access to the content of digital media is a big challenge in this era of information. Only due to the illegal copying and sharing of digital media, the content owners are losing billions of dollars from their annual revenue (Kesselman & Kesselman, 2016). However, the global voice has been raised against these problems and digital rights managements systems have been introduced to address this(Han, Huang, Li, Ren, & Chen, 2016). But, end users have a significant role regarding the information security awareness (Hedström, Karlsson, & Kolkowska, 2013).

Educating the individual users regarding the inherent risks of the confidentiality, integrity, data, and how efficiently they can protect their system and data is called the information security awareness (B. Kim, 2014).The number of e-government service users in Bangladesh is increasing day by day. The concern of security measures has also increased with the pace of this growth. The government has taken many steps to ensure the security of the information system users (A. Islam & Tsuji, 2011).

The scenario of information security in the developed country is completely different than the developing countries. For example, the users of United States are taking advantage of the awareness of their citizens(Kunnathur, 2015).Russia and China is

[1] Assistant Professor, Department of Management Studies, Faculty of Business Administration and Management, Patuakhali Science and Technology University (PSTU), Patuakhali, Bangladesh.

the most spammed country followed by the Saudi Arabia (Alhussain & Drew, 2009).Despite the equal number of population, Italy has more than double the attacks that Thailand does. The root cause of it may be the higher number of internet users in Italy than Thailand (Phornphatcharaphong, 2011).

Information security awareness is very important for the individual user despite there is a paucity of empirical studies analyzing the factors influencing the adoption of information security awareness to the individual users of Bangladesh. Most of the previous studies focused on self-awareness before social networking (Hasan & Hussin, 2010), threats to information security (Whitman, 2003), mobile security in Bangladesh (M. A. Islam, Khan, Ramayah, & Hossain, 2011), perceived risk of information (Tsai & Yeh, 2010) , the relationship between information technology and information system (Latham, 2004). Thus, no or few study focused on the adoption of security awareness measures in Bangladesh. Our objective is to overcome this gap through identifying factors influencing the adoption of information security awareness in Bangladesh.

Status of information security in Bangladesh:

Ensuring people democracy, human rights, accountability, transparency, and justice through maximum use of technology is the core concept of digital Bangladesh. To fulfill these objectives, Bangladesh needs reliable physical and information communication technologies (ICTs)(Khalid & Pedersen, 2016). However, proper security is the global challenge now a days due to the increasing sophistication, frequency, and gravity of cyber threats(Jarmon, 2014). The technological infrastructure of Bangladesh was not up to the mark. That's why security system of Bangladesh was vulnerable. However, the government is trying their best to develop the infrastructure and has taken several initiatives. The raising of awareness and knowledge of the individual users as well as the development of the security guidelines are the prime initiatives taken by the government. To ensure further exploration activities, the government of Bangladesh is trying to develop international partnership and in some cases it has been already developed(Imran & Gregor, 2010).

Research Model and Hypotheses

There are some models regarding the adoption of technology among which frequently used models are the Theory of Planned Behavior (TPB) (Ajzen, 2002), Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 2004), Technology Acceptance Model (TAM) (Venkatesh, Morris, Davis, & Davis, 2003), Innovation Diffusion Theory (IDT)(Moore & Benbasat, 1996), Social Cognitive Theory (SCT) (Wood & Bandura, 1989), and most recently the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh, Thong, Chan, Hu, & Brown, 2011). All these theories indicate the factors that influence the adoption of using technology. However, depending on the objectives of a particular research, constructs of the

model may vary. After reviewing some theories appropriate for the adoption of technology, it was found that no particular model is sufficient enough to identify the adoption factors of information security awareness in Bangladesh and thus we developed a new model with the constructs found from the experienced IT professionals. We conducted an exploratory study to test our proposed hypothesis. The exploratory study found six factors which have significant influence towards the awareness of information security for a particular user. These exploratory findings have become the basis for the research model and we propose that as the research model for this study depicted in Figure 1.

Using antivirus for the device means closing some of the security leaks(Velasquez, 2010). Antivirus program usually scan the files that enter into the computer and thus system becomes more secured. A system is guided as the shield through the antivirus program which detects the infected files and deletes it on the spot(Cobb & Myers, 2009). on the other hand, if the users do not adopt the antivirus software, he can either gamble on the safety of the files or limit the access to the system. Information security awareness is thus crucial for the system users(Ngoqo & Flowerday, 2015). So, it can be hypothesized that:

H1: Use of antivirus has a positive influence towards information security awareness. Users who adopt spam filtering are more aware for information security than the non-users(Cormack, Smucker, & Clarke, 2011). It is the service through which user's inbox is made free from spamming. Adoption of spam filtering enhances the user efficiency (Sadan & Schwartz, 2012). Spamming is more annoying when one's e- mail is bombarded with unwanted e- mails. Storing virus in the user's computer is the main reason behind the spam attack. Thus, spam filtering is very crucial for maintaining the clean and spam- free inboxes (Deng, Xia, Fu, Zhou, & Xia, 2013). So, we can hypothesize that:

We propose device password as another antecedent of information security awareness. Password usually implies the authentication system as the testimony of the user identity to access in any system. Users may have developed password due to some reasons like logging into account, retrieving e- mail, accessing applications, databases, networks, websites, and reading the online newspaper (Camenisch, Lehmann, & Neven, 2015). Besides, it has become a common practice to hide the passwords as it is typed due to avoid the risk inherent with this. Users who protect personal information are more secured and aware of information security (Yang, Hung, & Lin, 2013). Therefore, it can be hypothesized that:

H2: Spam filtering is positively related towards the information security awareness.

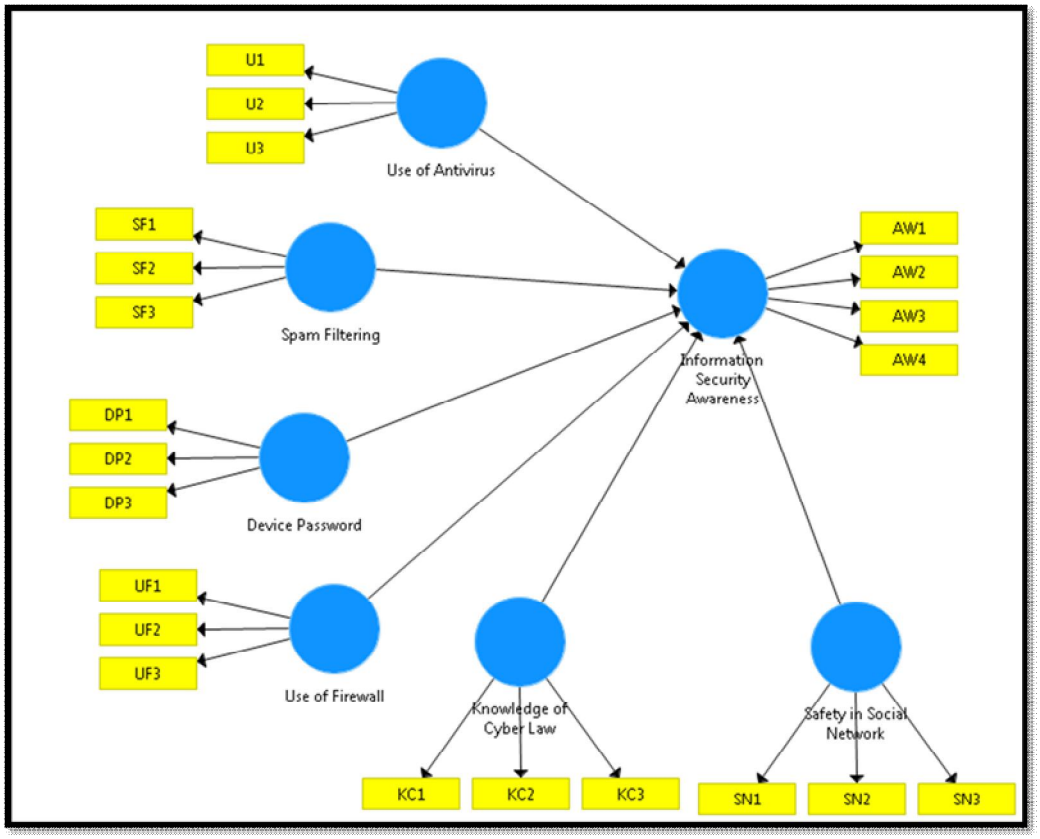

Figure 1. Research Model

H3: Device password has positive influence towards the information security awareness.

Firewall is a software which allows or blocks the information depending on the settings of the program coming from internet (Wilkinson *et al.*, 2011). Users who are connected to one server through router at the office or other location also have built-in firewall to secure the system. To be secured in using information system the default password should be changed during a time interval (Koo, Chang, & Wei, 2011). From the above literature, it can be hypothesized that:

H4: Use of firewall has positive influence towards the information security awareness.

Cyber terrorism is the most recent and frequent attack in this era of information technology. This is occurring through the use of cyber space by the hackers. Manipulating IP address of the computer and hacking personal information is the most renowned cybercrime in today's world (Schneier, 2011). Cyber risk is at the top of all the risk in international arena due to frequent attack and some failure in mitigating security which has adverse impact on the global economy. At present, the

voice has been raised from different parts of the world to have better cyber security strategies for protecting the rights of the users (Banday, Qadri, & Shah, 2009). For this entire phenomenon, it is assumed that cyber security has become an emergence issue in today's world. Thus, it can be hypothesized that:

H5: Knowledge of cyber law has positive influence towards the information security awareness.

Safety measures in social network are also assumed the vital factors that have influence towards the information security awareness. Personal information is available to the public in social network as it is relying on the connection and communication through using network. Hackers can use personal information for social engineering attack(Tankard, 2011). Moreover, it is also seen that one may reveal the password and other information to the trusted friend which can also pose serious problem for the security. The users, who are aware of the safety measures in social network, are more conscious for information security than the non-adopters (Wei, Bu, Guo, & Gollagher, 2014). Therefore, it can be assumed that:

H6: Safety measures in social network have positive influence towards the information security awareness.

Methodology

For exploring the potential factors affecting information security awareness for the individual users, at first we adopted an interview approach with the twenty experienced IT professionals. The identifying factors contributed to develop our proposed model. By getting the major constructs through interviewing the experienced professional, we developed a structured questionnaire for collecting the relevant data and measuring latent constructs in the research hypotheses. It seems that we adopted mixed method approach for the collection of data in order to strengthen the quality of the proposed model. In the structured questionnaire, there were some questions regarding the different constructs in the research model on a 5 point Likert scale starting from strongly disagree (1) to strongly agree (5). We distributed 250 questionnaires out of which 213 were returned and used for further analysis. SmartPLS 3.0 was used for data analysis and model confirmation in this research.

Results and Discussion

Measurement Model

To assess the measurement model, we fully analyzed the proposed research model in this section. The reliability results of the measurement model are shown in table 1. The value of cronbach's alpha and composite reliability (CR) is above the threshold value of 0.70 which indicates that all the constructs used in our study contains internal reliability. Weevaluated convergent validity through average variance extracted (AVE) and item loading, both of which are above the threshold value of 0.50which indicates the convergent validity of this study. We assessed discriminant validity by examining the squared correlation between a pair of latent variables.

Table 1. Measurement model

Constructs	Items	Loadings	C.R	Cronbach's Alpha	AVE
Information Security Awareness	AW1 AW2 AW3 AW4	0.590 0.612 0.864 0.702	0.777	0.821	0.589
Use of Antivirus	U1 U 2 U 3	0.860 0.743 0.843	0.810	0.796	0.622
Spam Filtering	SF1 SF 2 SF 3	0.578 0.763 0.773	0.844	0.760	0.641
Device Password	DP1 DP 2 DP 3	0.573 0.712 0.786	0.735	0.902	0.784
Use of Firewall	UF1 UF2 UF3	0.516 0.856 0.554	0.750	0.819	0.502
Knowledge of Cyber Law	KC1 KC2 KC3	0.592 0.684 0.669	0.803	0.755	0.558
Safety in Social network	SN1 SN2 SN3	0.581 0.744 0.790	0.989	0.717	0.695

AVE= Average Variance Extracted, CR= Composite Reliability

Our study has discriminate validity as the diagonal elements of the matrix (represent the square roots of the AVE) are greater than the off- diagonal elements of the corresponding row and column. The results of the discriminant validity are depicted in table 2.

Table 2. Correlation matrix and square root of the AVE

	Device Password	Information Security Awareness	Knowledge of Cyber Law	Safety in Social network	Spam Filtering	Use of Antivirus	Use of Firewall
Device Password	**0.696**						
Information Security Awareness	0.236	**0.538**					
Knowledge of Cyber Law	-0.084	-0.119	**0.508**				

Table 2. Cont'd.

Safety in Social network	0.214	0.221	-0.068	**0.628**			
Spam Filtering	0.021	0.186	0.079	0.126	**0.664**		
Use of Antivirus	0.105	0.068	-0.055	-0.058	0.115	**0.650**	
Use of Firewall	-0.036	0.092	-0.126	0.136	-0.007	0.025	**0.634**

Structural Model

The results of the structural model are summarized in table 3 reflecting the relationship between device password (DP) and information security awareness (AW) (t= 4.959, β= 0.185, p< 0.05), knowledge of cyber law (KC) and information security awareness (AW) (t= 3.629, β= -0.036, p< 0.05), social network (SN) and information security awareness (AW) (t= 2.507, β= 0.133, p< 0.05), spam filtering (SF) and information security awareness (AW) (t= 2.005, β= 0.160, p< 0.05), use of antivirus (U) and information security awareness (AW) (t= 0.243, β= 0.019, p> 0.05), use of firewall (UF) and information security awareness (AW) (t= 0.448, β= 0.140, p> 0.05). Our results show that H1, H2, H3, and H4 are significant and accepted whereas H5 and H6 are found less significant and not supported in this study.

Table 3. Structural Model

Hypothesis	Path	(β)	t- statistics	Comments
H1	DP-> AW	**0.185**	4.959	Accepted
H2	KC ->AW	-0.036	**3.629**	Accepted
H3	SN -> AW	0.133	2.507	Accepted
H4	SF -> AW	0.160	2.005	Accepted
H5	U -> AW	0.019	0.243	Rejected
H6	UF -> AW	0.140	0.448	Rejected

Discussion

Most of the previous studies revealed the significance of information security awareness and its constructs despite the divergence of their findings. We considered use of antivirus, spam filtering, device password, use of firewall, knowledge of cyber law, and safety in social network as the antecedent of adopting information security awareness. Our results found significant influences of device password, knowledge of cyber law, social network, spam filtering, and use of antivirus on the adoption of security awareness. It supports four of the six hypotheses in which device password, knowledge of cyber law, safety measures in social network, and spam filtering

hypotheses are relevant with the adoption of information security awareness measures and consistent with the previous studies. Adopting device password spam filtering results in the awareness of information security adoption (A. Harris & P. Patten, 2014). User's awareness regarding information security is best guided with the device password (Da Veiga & Eloff, 2010). Safety measures in social networking are the outcome of information security awareness adoption (Mohamed & Ahmad, 2012). The users who are more caring about their safety in social network are better equipped with information security awareness(Shin, 2010). Knowledge of cyber law usually makes people aware regarding information security (Choo, 2011).

However, our findings revealed that use of antivirus and firewall has insignificant influence on the adoption of information security awareness. The reason behind this can be the lack of awareness regarding the use of antivirus and firewall in Bangladesh. Most of the users do not consider this and try to use the system without antivirus and password in Bangladesh (Noble & Corner, 2007). Thus, the users of Bangladesh are not secure enough to use their system. Use of antivirus and firewall are least significant influencing the adoption of information security awareness in Bangladesh.

Conclusions, Limitations and Future Studies

The aim of this study was to find out the factors that has impact on the adoption of security awareness in Bangladesh. We found device password, knowledge of cyber law, safety measures in social network and spam filtering are significantly influencing to the adoption of security awareness measures in Bangladesh. On the other hand, use of antivirus and firewall has insignificant influence towards the adoption of information security awareness in Bangladesh.The results of our study were based on the particular user (student) of Bangladesh, attempts to generalize these results for the overall users of Bangladesh which is also the major limitations of our study. Future research can be done through extending the other users of Bangladesh to have more concrete results.

Implications of the Research

Our study contributes to find out the adoption factors of information security awareness in Bangladesh. As our study found device password, knowledge of cyber law, safety measures in social network and spam filtering factors as the significant antecedents for the awareness of information security in Bangladesh, the model could also be applied for the other developing countries of the world.

References

A. Harris, M., & P. Patten, K. (2014). Mobile device security considerations for small-and medium-sized enterprise business mobility. *Information Management & Computer Security, **22*** (1), 97-114.

Ajzen, I. (2002). Constructing a TPB questionnaire: Conceptual and methodological considerations.

Ajzen, I., & Fishbein, M. (2004). Questions raised by a reasoned action approach: comment on Ogden (2003).

Alhussain, T., & Drew, S. (2009). *Towards user acceptance of biometric technology in E-Government: A survey study in the Kingdom of Saudi Arabia.* Paper presented at the Conference on e-Business, e-Services and e-Society.

B. Kim, E. (2014). Recommendations for information security awareness training for college students. *Information Management and Computer Security, **22*** (1), 115-126.

Banday, M. T., Qadri, J. A., & Shah, N. A. (2009). Study of Botnets and their threats to Internet Security.

Camenisch, J. L., Lehmann, A., and Neven, G. (2015). Password-based authentication: Google Patents.

Choo, K. K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers & Security, **30*** (8), 719-731.

Cobb, C., & Myers, A. (2009). Antivirus technology. *Computer Security Handbook, Sixth Edition*, 41.41-41.14.

Cormack, G. V., Smucker, M. D., & Clarke, C. L. (2011). Efficient and effective spam filtering and re-ranking for large web datasets. *Information retrieval, 14* (5), 441-465.

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. *Computers & Security, 29* (2), 196-207.

Deng, J., Xia, H., Fu, Y., Zhou, J., & Xia, Q. (2013). Intelligent spam filtering for massive short message stream. *COMPEL-The international Journal for Computation and Mathematics in Electrical and Electronic Engineering, 32*(2), 586-596.

Han, Z., Huang, S., Li, H., Ren, N., & Chen, J. (2016). Risk assessment of digital library information security: a case study. *The Electronic Library, 34* (3).

Hasan, M. R., and Hussin, H. (2010). *Self awareness before social networking: Exploring the user behaviour and information security vulnerability in Malaysia*. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M), 2010 International Conference on.

Hedström, K., Karlsson, F., and Kolkowska, E. (2013). Social action theory for understanding information security non-compliance in hospitals: The importance of user rationale. *Information Management & Computer Security, **21*** (4), 266-287.

Imran, A., & Gregor, S. (2010). Uncovering the Hidden issues in e-Government adoption in a least Developed Country: the Case of Bangladesh. *Journal of Global Information Management (JGIM), **18*** (2), 30-56.

Islam, A., & Tsuji, K. (2011). Bridging digital divide in Bangladesh: study on community information centers. *The Electronic Library, **29*** (4), 506-522.

Islam, M. A., Khan, M. A., Ramayah, T., & Hossain, M. M. (2011). The adoption of mobile commerce service among employed mobile phone users in Bangladesh: self-efficacy as a moderator. *International Business Research, **4*** (2), 80.

Jarmon, J. A. (2014). *The new era in US national security: an introduction to emerging threats and challenges*: Rowman & Littlefield.

Kesselman, M., & Kesselman, M. (2016). 2016 Consumer Electronics Show, Las Vegas: Virtual 3D Cameras and More. *Library Hi Tech News, 33* (3).

Khalid, M. S., & Pedersen, M. J. L. (2016). Digital exclusion in higher education contexts: A systematic literature review. *Procedia-Social and Behavioral Sciences.*

Koo, T.-M., Chang, H.-C., & Wei, G.-Q. (2011). *Construction P2P firewall HTTP-Botnet defense mechanism.* Paper presented at the Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on.

Kunnathur, A. S. (2015). Information security in supply chains: a management control perspective. *Information & Computer Security, **23*** (5), 476-496.

Latham, R. (2004). *Bombs and bandwidth: The emerging relationship between information technology and security*: Manas Publications.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. *Computers in Human Behavior, **28*** (6), 2366-2375.

Moore, G. C., & Benbasat, I. (1996). Integrating diffusion of innovations and theory of reasoned action models to predict utilization of information technology by end-users *Diffusion and adoption of information technology* (pp. 132-146): Springer.

Ngoqo, B., & Flowerday, S. V. (2015). Exploring the relationship between student mobile information security awareness and behavioural intent. *Information & Computer Security, **23*** (4), 406-420.

Noble, B. D., & Corner, M. D. (2007). Method and system to maintain application data secure and authentication token for use therein: Google Patents.

Phornphatcharaphong, W. (2011). *Information Technology Phenomenon in Thailand.* Paper presented at the International Joint Conference on Advances in Signal Processing and Information Technology.

Sadan, Z., & Schwartz, D. G. (2012). Social network analysis for cluster-based IP spam reputation. *Information Management & Computer Security, **20*** (4), 281-295.

Schneier, B. (2011). *Secrets and lies: digital security in a networked world*: John Wiley & Sons.

Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers, **22*** (5), 428-438.

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security, **22*** (3), 279-308.

Tankard, C. (2011). Advanced persistent threats and how to monitor and deter them. *Network security, 2011*(8), 16-19.

Tsai, Y. C., & Yeh, J. C. (2010). Perceived risk of information security and privacy in online shopping: A study of environmentally sustainable products. *African Journal of Business Management, **4*** (18), 4057.

Velasquez, D. (2010). *E-Government and Public Access Computers in Public Libraries*. Emerald Group Publishing Limited.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS quarterly*, 425-478.

Venkatesh, V., Thong, J. Y., Chan, F. K., Hu, P. J. H., & Brown, S. A. (2011). Extending the two stage information systems continuance model: Incorporating UTAUT predictors and the role of context. *Information Systems Journal, **21*** (6), 527-555.

Wei, J., Bu, B., Guo, X., & Gollagher, M. (2014). The process of crisis information dissemination: impacts of the strength of ties in social networks. *Kybernetes, **43*** (2), 178-191.

Whitman, M. E. (2003). Enemy at the gate: threats to information security. *Communications of the ACM, **46*** (8), 91-95.

Wilkinson, J., Batke, B. A., Hall, K. H., Jasper, T. J., Kalan, M. D., & Vitrano, J. B. (2011). Distributed learn mode for configuring a firewall, security authority, intrusion detection/prevention devices, and the like: Google Patents.

Wood, R., & Bandura, A. (1989). Social cognitive theory of organizational management. *Academy of Management Review, **14*** (3), 361-384.

Yang, C., Hung, J.-l., & Lin, Z. (2013). An analysis view on password patterns of Chinese internet users. *Nankai Business Review International, **4*** (1), 66-77.