

1-1-2010

# The Impact of Two-Factor Authentication Technology on the Adoption of Internet Banking

Joo Suk Han

*The University of Melbourne*

Sherah Kurnia

*The University of Melbourne, sherahk@unimelb.edu.au*

Fei Peng

*The University of Melbourne, feip@unimelb.edu.au*

---

## Recommended Citation

Han, Joo Suk; Kurnia, Sherah; and Peng, Fei, "The Impact of Two-Factor Authentication Technology on the Adoption of Internet Banking" (2010). *PACIS 2010 Proceedings*. Paper 146.  
<http://aisel.aisnet.org/pacis2010/146>

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 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact [elibrary@aisnet.org](mailto:elibrary@aisnet.org).

# THE IMPACT OF TWO-FACTOR AUTHENTICATION TECHNOLOGY ON THE ADOPTION OF INTERNET BANKING

Han, Joo Suk, Department of Information Systems, the University of Melbourne, 111 Barry Street, Parkville, Victoria, Australia.

Kurnia, Sherah, Department of Information Systems, the University of Melbourne, 111 Barry Street, Parkville, Victoria, Australia. sherahk@unimelb.edu.au

Peng, Fei , Department of Information Systems, the University of Melbourne, 111 Barry Street, Parkville, Victoria, Australia. feip@unimelb.edu.au

## Abstract

*The security risks of Internet banking have always been a concern to the service providers and users. There has been a global trend to adopt a multi-factor authentication scheme to increase the security of Internet banking. However, the introduction of two-factor authentication has not been well received. Particularly, there has been a conception that it creates barriers to Internet banking use because extra efforts are required to perform transactions online. This study explores the impact of the two-factor authentication on the adoption of Internet banking in Australia as perceived by the users, through a qualitative survey. The findings show that the two factor authentication does not affect most of the key factors affecting Internet banking adoption including ease-of-use and it helps reduce the perceived risks. However, it increases the security awareness and concern of the users and it somehow affects users' trust in using Internet banking.*

*Key Word: Two-Factor Authentication; Internet Banking; Security; Adoption*

# 1 INTRODUCTION

The wide-spread availability of Personal Computers and broadband has facilitated the adoption of the Internet and consequently the development of various online businesses in many countries. In Australia, a large variety of online services have been offered by businesses and government from simple informational services to online transactions and Internet banking. The Australian financial institutions, in particular, are among the most active adopters of the Internet technology, strongly encouraging their customers to utilise online banking services in order to achieve cost savings and tap into extra revenue streams (McCullagh and Caelli, 2005). Consequently, the Internet banking usage in Australia has steadily grown from 38% in 2001 to 52% in 2005 (DICTA, 2005). In addition, almost 70% of the Australian Internet users use Internet banking once a week or more (Nielsen 2007).

However, the security of Internet banking has always been a constant and significant concern to both the consumers and the providers (Schneier, 2005; Nilson et al 2005). As the traffic for Internet banking increases, the security risks become more prevalent. The attacks have become more sophisticated as the scale of online financial transactions grows (McCullagh and Caelli, 2005). Instead of targeting heavily invested bank's internal systems, the attackers are now targeting the end users' PCs, which are the weakest link in the online network, through various ways such as phishing, pharming, key-logger and Trojan horse attacks (Schneier, 2005). This is one of the main reasons why authentication, the process of verifying the identity of the users, has become one of the key issues for the Internet banking.

The traditional single-factor authentication is considered as "inadequate" to protect the transactions from criminal attacks such as account fraud and identity theft (FFIEC, 2005; Hong Kong Post 2007). A consensus regarding a more controlled protection over the security of online financial transactions has emerged and Australia has been following a global trend to adopt multi-factor authentication (Smith, 2006). For example, two of Australia's largest banks are now offering the Short Message Service (SMS) payment security service using mobile phones as a different channel for authentication while others provide password-generating tokens to their Internet banking customers.

However, despite its increased security assurance, the two-factor authentication techniques are not free from criticisms (Giesen 2006; Hoffman 2005). Schneier (2005) argues that two-factor authentication will not prevent all the attacks happening in remote authentication environments over the Internet. Moreover, although some two-factor authentication supporters argue that the customers would feel confident and secured if they have an extra layer of security, there is a conception that two-factor authentication will be a barrier for users to adopt Internet banking services because it will increase the amount of users' efforts to access their bank account and perform financial transactions (Matthews, 2006; Giesen 2006).

At this stage, there is little understanding of the actual impact of introducing more complex security measures such as two-factor authentication. In particular, although the importance of authentication technologies has been widely recognised by industry white papers, government reports and numerous industry magazine journals, there is still a clear gap in regards to understanding the relationships between authentication technologies and adoption of Internet banking. Therefore, this research aims to investigate the impact of two-factor authentication on the key factors affecting Internet banking adoption, using Australia as the context of the study.

The question this research aims to answer is: How does two-factor authentication affect Internet banking adoption? In order to answer this question, this paper explores the following sub questions:

- What are the key factors that influence Internet banking adoption?
- What key factors are influenced by the introduction of two-factor authentication?

To answer the research questions, a literature review was first conducted to identify a number of key factors influencing the adoption of Internet banking. Then a qualitative survey involving 12 Internet banking users in Australia was conducted to explore the perceived impact of introducing a two-factor authentication technology on various factors affecting the adoption of Internet banking. The research findings indicate some influence of the introduction of two-factor authentication on the factors

influencing Internet banking adoption. The study further indicates that the introduction of two-factor authentication schemes should not reduce the Internet banking adoption, because two-factor authentication technologies in Australia appear not reduce the convenience and benefits of Internet banking

The outcome of this study provides a better understanding of how the two-factor authentication affects the Internet banking adoption. It also has the potential to assist financial institutions in establishing effective strategies regarding the introduction of this new security measure in order to maintain and promote the use of Internet Banking. Furthermore, the understanding obtained from this study can also be applied in other related areas such as electronic transactions for business-to-business and business-to-government environments. Thus, the research can provide a guideline for financial service providers offering online services in the introduction and implementation of two-factor authentication schemes.

## **2 LITERATURE REVIEW**

Two-factor authentication uses two factors for identity verification. Two-factor authentication has long been used in a certain banking product in offline environment. The most notable example is an ATM debit card which requires something a user knows, such a password, as well as something a user has, such as the physical card itself (Di Pietro et al 2005). FFIEC (2009) defines three major types of online authentication techniques that can be used as a second factor to verify Internet banking users' identity which are shared secrets, tokens and biometrics. Shared secrets can be defined as information elements that are shared by both the customer and the authenticating entity such as secret questions and answers. Tokens refer to the physical devices which can be used as a part of two or multi factor authentication system, which can include USB tokens and Smart Card. Finally, Biometrics technologies use a living person's physiological or physical characteristics to identify or authenticate the users identity.

In a climate where users are continually confronted with new online security risks, especially in the context of the Internet banking, it is critical to understand what factors can impact users' perceptions (Jin & Fei-Cheng, 2005). Then in this current study, we explore the impact of two-factor authentication on various factors affecting the adoption of Internet banking. Below, a number of key factors affecting Internet banking adoption and the underlying theories / literature are discussed.

### **Perceived Ease of Use and Perceived Usefulness**

Davis (1989) proposed in the TAM that there are two beliefs in determining the attitude and intention in adopting a new information technology, which are the use's perceived usefulness (PU) and the ease of use (PEOU). Davis (1989) defines PU as "the degree to which a person believes that using a particular system would enhance this or her job performance" while PEOU is defined as "the degree to which a person believes that using a particular system would be free of effort" (Davis, 1989, p.320).

In their research, Adams et al (1992) evaluated the relationship between ease of use, usefulness, and system usage. Through their empirical studies, validity testing and structural equation modelling the result suggests that both PU and PEU are important determinant of information technology use (Adams et al, 1992).

### **Relative Advantage, Compatibility and Complexity**

Rogers (1995) identified five major innovation attributes, which are relative advantage, compatibility, complexity, observability and trialability. However, only the first three factors are included in this study since observability and trialability are irrelevant attributes for Internet banking (Gerrard and Cunningham, 2005).

#### ***Relative Advantage***

Relative advantage is defined as "the degree to which an innovation is perceived as being better than its precursor" (Rogers, 1995). Economic benefits and convenience have been found to be the measures of relative advantage (Gerrard and Cunningham, 2005). Hence, it is reasonable to explain the adoption of innovation since the higher the economic benefits and convenience of the innovation, the more likely it will be adopted by the users (He et al, 2006).

### ***Compatibility***

Compatibility refers to “the degree to which using an innovation is perceived as being consistent with the existing values, past experiences and the needs of potential adopters” (Rogers, 1995). For example, according to Black et al (2001), those who were comfortable with the Internet were more positive about Internet banking. In contrast, low levels of Internet usage and preference for using financial services over the counter resulted in the Turkish respondents viewing Internet banking as being far less compatible (Polatoglu and Ekin, 2001).

### ***Complexity***

Complexity refers to “the degree to which an innovation is perceived as difficult to understand and use” (Rogers, 1995). As performing financial transactions via the Internet requires a minimum level of technical experience and competence, Polatoglu and Ekin (2001) argues that well-educated people should find Internet banking less complex. Cheng et al (2006) imply that the complexity of an innovation has a negative effect on its rate of adoption.

### ***Users’ Security Awareness and Concerns***

According to Sathye (1999), security concerns is an important factor that is responsible for adoption of Internet banking, and in fact the empirical data on the research paper shows that it stands out as the highest reason for non-adoption of Internet banking. Internet is now an integral part of our lives, and as consumers become more adapt with online financial transactions, they are also becoming more concerned about the safety and security of Internet banking (Roxbury, 2005). Similarly, it is reasonable to make an assumption that recent hijacking attacks targeting Internet banking users’ account would have raised security awareness and concerns of the Internet banking users (Smith, 2005).

### ***Trust***

An empirical study of Internet banking adoption in Australia by Lichtenstein and Williamson (2006) suggest that the trust issue is often perceived by the Internet banking adopters. Kim and Prabhakar (2000) identified that there can be two different types of trust in the Internet banking environment, which are Initial Trust in E-Channel and Trust on Banks. Another study by Kim and Prabhakar (2004) discovered a significant relationship between initial trust in the electronic channel and the adoption of Internet banking. Gefen et al (2003) suggest that trust becomes an excellent predictor of technology adoption when the relationship between trust on the e-service providers and the use of a particular technology is placed in the context of TAM.

### ***Perceived Risks***

Risk is recognized as a common obstacle to adopting electronic commerce due to the lack of security and privacy protection over the Internet (Rhee and Riggins, 1997). Another potential factor influencing Internet banking adoption, therefore, is the extent to which Internet banking is perceived to be sufficiently safe, secure and reliable to use, which can be termed Perceived Risk (Walker and Johnson, 2006).

### ***Price/Cost***

Sathye (1999), suggest price/cost as another factor influencing Internet banking adoption, and identified two types of costs associated with Internet banking, which include the normal costs of Internet banking activities and the bank cost and charges. The importance of “Price Factor” in adoption and diffusion of innovation is also emphasised by Howard (1977).

## **3 RESEARCH METHODOLOGY**

For the purpose of this research, a qualitative survey of the Internet banking users in Australia was conducted to explore which Internet banking key adoption factors identified from the literature were influenced by the introduction of two-factor authentication. Face-to-face semi-structured interview was used allow an in-depth exploration on how the new authentication technologies affect the adoption of Internet banking (Neuman 2006). Most interview participants had some experiences in

using two-factor authentication methods, while for those who did not have any experience in using two-factor authentication technologies, a simple demonstration of two-factor authentication using the SMS security service provided by one of the major banks in Australia was offered to the participants.

A total of 12 interviews were conducted during the months of August and September. They consist of a combination of undergraduate and postgraduate students as well as full time and part time employees of various organisations. These participants cover various age groups which are considered the leading groups in technology adoption in Australia (ACMA 2007). Table 1 summarises the participants for this study. The locations were typically at the participants' residences in which Internet access was available to demonstrate one of the two-factor authentication technologies available in Australia. All interviews were recorded and brief notes were taken by the researcher for each interview.

Interview records were analysed to provide answers to the research questions. Open, axial and selective coding (Neuman, 2006) technique was used to uncover major and sub themes from qualitative data, to identify the relationships among those themes and to identify further supporting evidence for the identified themes.

Participant	Age Range	Status
1-3	18-25 years	Undergraduate student
4-6	26-35 years	Postgraduate student
7-8	26-35 years	Part time employee
9-10	36-45 years	Full time employee
11-12	Above 45 year	Full time employee

Table 1. The Participants

#### 4 STUDY FINDINGS

In this section, the impact of introducing two-factor authentication method to improve the security of the Internet banking on each of the key factors affecting Internet banking adoption is discussed. For brevity, related factors are grouped together in the discussion.

##### Perceived Ease of Use, Compatibility and Complexity

Due to the simple and user-friendly nature of the two-factor authentication approach that is currently being adopted, the interviewees demonstrated no significant change in the perceived ease of use of the Internet banking services. The adoption of commonly available devices such as mobile phones as the facilitator for the second factor authentication allowed the banks to take advantage of the consumers' existing familiarity with the token device and consequently minimise the initial learning required for operating such device. In addition, it also minimises the user's potential resistance to change by using a familiar device as the operating media, which would significantly reduce consumers' perception of the degree of change in operations, as revealed in the interview quote below:

*"If someone can read and type the numbers correctly then he is already skilful using it (SMS Security service), because I think I am (skilful)." (Participant 2)*

##### Perceived Usefulness and Relative Advantage

The interviews emphasised that the majority of the participants did not feel much difference in using Internet banking with and without a two-factor authentication technology. According to the comments from a number of the participants, the introduction of two-factor authentication does not create an observable impact on the usefulness and the relative advantage of Internet banking. All participants agree that Internet banking has been useful and has significant relative advantages, compared to the traditional physical banking practice. Furthermore, the current two-factor authentication technologies offered by some Australian banks are considered easy and convenient to use by the interview participants. The quote below reflect the above observation:

*"Well, I can still sit in front of my desk and do it (Internet banking). I don't really need to go somewhere else to do this two-factor thing. (Participant 11 )"*

However, some participants from the older age groups expressed a decrease in their perceived ease of use of Internet banking in a business environment. According to them, as the current two-factor

authentication technologies are designed only for individual users, therefore the technologies are difficult to use in some situations where there are more than one person responsible to manage a business account. As this research only focuses on the individual users, this issue was not explored further.

### **Trust**

Although some participants feel that the two-factor authentication increases their trust level towards the Internet banking, most participants still showed a significant level of distrust towards Internet banking regardless of the introduction of two-factor authentication method. The respondents' level of trust towards the banks is dependent upon their perception of bank's motivation behind the implementation of the two-factor authentication measure. For consumers who perceives banks' action as a proactive measure for improving Internet banking security, their trust level increases as reflected in the following quote:

*"...So it's even better because I feel much safer now." (Participant 11)*

On the other hand, there are also some participants, mostly from the younger age groups who regard the bank's adoption of two-factor authentication as a confirmation of Internet banking's inherent security issue and their reactive gesture to keep up with the industry trend. As a result, their trust level has actually decreased with the adoption of the two-factor authentication approach as shown in the following quote:

*"I still don't believe the banks, and I think they are doing it because everyone else is doing it." (Participant 3)*

### **Security Awareness and Concerns**

A positive effect of introducing two-factor authentication on security awareness and concerns was identified from the interview data. Security concerns of users were increased as the introduction of two-factor authentication measures emphasised the recent security risks and issues in Internet banking. It brought into users' attention the potential dangers involved in conducting Internet banking and consequently acted as an effective means for educating the users about the security issues of the Internet Banking. The interviewees also generally expressed their curiosity about the motivation of banks to adopt two-factor authentication schemes, which further raised the Internet banking security issues for the users who usually lack security awareness as demonstrated in the following quotes:

*"I knew that username and password can easily be leaked but I didn't know that the problem is that serious. That's why the banks are doing two-factor things, right?" (Participant 4)*

### **Perceived Risk**

As expected, the interview responses suggest a negative relationship between introduction of two-factor authentication and the perceived risk of using the Internet banking. Since most participants expect the new security measure to protect or prevent their bank accounts from the attacks in a certain level, the perceived risk of Internet banking decreases as two-factor authentication measures are introduced. This is reflected in the following quotes:

*"I still don't think this new technology can save me from all of those online attacks. But at the same time, I hope this two-factor technology can block those weak attacks." (Participant 12)*

*"Well, it's better than having nothing. I'm pretty sure it can protect my Internet banking." (Participant 5)*

## **5 DISCUSSION AND CONCLUSION**

The main purpose of this research is to investigate how the introduction of two-factor authentication technologies affects the adoption of Internet banking by assessing its impact on the key adoption factors. The findings show that the use of two-factor authentication technologies does not actually affect the ease of use, compatibility and complexity of using Internet banking in a negative way, as anecdotal evidence suggests. With the presence of a two-factor authentication scheme, Internet banking is still convenient to use as perceived by the study participants. However, the introduction of

stronger authentication systems to an online environment has been considered undesirable by many online service providers, mainly because it leads to a more complicated user access control and inconvenience. In particular, as convenience has been recognised as the major advantage of using online services by numerous research, the industry experts have expressed their concerns of introducing “inconvenient” two-factor authentication measures despite of its ability to improve the Internet banking security. The findings from this research thus clearly show little or no connection between convenience and two-factor authentication methods in Australia. The two-factor authentication methods currently available in Australia involve very simple processes so that the convenience aspect of using Internet banking can still be maintained at a preferable level.

Likewise, the introduction of a two-factor authentication scheme is not expected to impair the usefulness and relative advantage offered by Internet banking. Most interview participants observed little differences in respect to the usefulness and relative advantages of Internet banking with the introduction of two-factor authentication scheme and, hence, it is expected not to affect the adoption of Internet banking.

This study further suggests that the introduction of two-factor authentication technologies by the Australian banks reduced the perceived risks associated with Internet banking. Although the introduction of the new technologies may increase the users’ security awareness, most interview participants shared a common perception that the two-factor authentication schemes can reduce the associated risks by protecting their bank accounts from the online attacks.

In addition to the increase in users’ security awareness and concern, our study also indicates that the impact of introducing two-factor authentication schemes on users’ trust of using Internet banking varies. This implies that banks and other financial institutions offering online services need to devise a strategy carefully in introducing a two-factor authentication technology. They must ensure that they will not impair the trust of Internet banking users with the introduction of two-factor authentication schemes which is intended to further protect users.

To the best of our knowledge, this study is the first study to explore how the introduction of two-factor authentication influences the adoption of Internet banking, particularly in Australia. As the importance of online authentication measures has been raised by the financial industry, this research provides a valuable guideline for future studies and for the banking and financial institutions in their effort to better address the security concerns with online services.

Despite the contributions provided by this research, some limitations are also acknowledged which can potentially be addressed in the future studies. One of the limitations of this research is because the empirical study was conducted only with a limited number of current Internet banking users. Considering the fact that the Internet has become an integral part of people’s lives in developed countries like Australia, it was difficult to find non-adopters of Internet banking, particularly in Australia. Therefore, future studies that consider the perception of non-adopters of Internet banking with a larger sample size, possibly in other countries, would complement the findings of this study. Another limitation is that this study does not consider other factors related to the institution and the social system in which individual users are related to. Thus, considering the individual user’s relationship with the financial institution as well as the influence of the social norms in a similar study would further enrich the understanding of how two-factor authentication would affect the adoption of Internet banking.

## **References:**

- ACMA, 2007, "Telecommunications Today: Consumers attitudes to take-up and use," Australian Communications and Media Authority, The Australian Government.
- Adams, D.A., Nelson, R., Todd, P.A., 1992, Perceived Usefulness, Ease of Use, and Usage of Information Technology: A Replication, *MIS Quarterly*, June 1992, pp. 227-247.
- Black, N. J, Locket, A., Winklhofer, H. and Ennew, C. 2001, The adoption of Internet financial services: a qualitative study, *International Journal of Retail & Distribution Management*, Vol 29, No 8, pp 390-398
- Cheng, T.C.E, Lam, D.Y.C, Yeung, A.C.L (2006) Adoption of Internet banking: An empirical study in Hong Kong, *Decision Support Systems*, Vol 42, No 3, December 2006, Pages 1558-1572



- Davis, F., 1989, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly*, 13(3), pp.319-340.
- Di Pietro, R., Me, G., Strangio, M.A., 2005, A Two-Factor Mobile Authentication Scheme for Secure Financial Transactions, Proceeding of the International conference on Mobile Business (ICMB'05), DICTA (Department of Information Communication Technology and Art), 2005, The Current State of Play, DICTA, Canberra, Australia, viewed at: <http://www.dicta.gov.au>, last accessed May 2007.
- FFIEC (Federal financial Institutions Examination Council), 2009, Authentication in an Internet Banking Environment, viewed at <http://www.ffiec.gov>, last accessed June 2008.
- Galliers, R.D., 1991, Choosing Information Systems Research Approaches, in H-E NNoen, H.K Klein, and R.A. Hirschheim (eds.), *Information Systems Research: Contemporary Approaches and Emergent Traditions*, Proc. IFIP TC8/WG8.2 Working Conference, Dec 1990, North-Holland.
- Gefen, D., Karahanna, E., Straub, E.W., 2003, Trust and TAM in Online Shopping: An Integrated Model, *MIS Quarterly*, Vol. 27, No. 1, March 2003, pp. 51-90.
- Gerrard, P. and Cunningham, J.B., 2005, The service quality of e-banks: an exploratory study, *International Journal of Financial Services Management*, Vol 1, No 1, pp 102-117.
- Giesen, L., 2006, A different Mousetrap needed for later Online Bill Pay Adopters, *Banking Strategies*, Chicago, Mar/Apr 2006, Vol. 82, No. 2, pp. 30.
- Hoffman, K.E., 2005, What lengths will customers go to protect their online account? *Banking Strategies*, Chicago, Nov/Dec 2005, Vol. 81, No. 6, pp. 62.
- Hong Kong Post, 2007, Hong Kong Post e-Cert - From Secured to Re-assured The Solution to Online Trading, <http://www.hongkongpost.gov.hk/about/intro/index.html>, last accessed: July 2009.
- Howard, J. 1977, *Consumer Behavior: Application of Theory*, McGraw-Hill Book Co., New York, NY.
- Jin, N. and Fei-Cheng, M., 2005, Network Security Risks in Online Banking, Proceedings of Networking and Mobile Computing, 2005 International Conference, vol. 2, 23-26 Sept. 2005, pp. 1229 – 1234.
- Kim, K., and Prabhakar, B., 2004, Initial trust and the adoption of B2C e-commerce: The case of Internet banking. *SIGMIS Database*, Vol. 35, No 2, June, pp. 50-64.
- Matthews, M., 2006, Where next for account aggregation? *International Journal of Bank Marketing*, , 24/2, pp. 133-138.
- Neuman, W.L., 2006, *Social Research Methods: Qualitative and Quantitative Approaches*, Sixth Eds, Pearson, USA.
- Nielson Australia, 2007, Aussie consumers choose Internet banking over ATM, phone and branch, 2007, Sydney, <http://au.nielsen.com/news/20070426.shtml>, last accessed June 2009.
- Nilson, M., Adams, A., Herd, S., 2005, 'Building Security and Trust in Online Banking', in *CHI '05 Extended Abstracts on Human Factors in Computing Systems*, Portland, USA, 02-07 April 2005, ACM Press, New York, pp. 1701-1704.
- Polatoglu, V.N and Ekin, S., 2001, An empirical investigation of the Turkish consumers' acceptance of Internet banking services, *International Journal of Bank Marketing*, Vol 19, No 4, pp 156-165.
- Rogers, E.M., 1995, *The Diffusion of Innovations*, 4<sup>th</sup> ed., the Free Press, New York, NY.
- Roxbury, R., 2005, Internet Banks Lose Consumer Confidence, *Hoosier Banker*, Sep 2005, Vol. 89, No. 9, Banking Information Source, pp. 22.
- Sathye Milind, 1999, Adoption of Internet Banking by Australian consumers: an empirical investigation, *International Journal of Bank Marketing*, 17/7, pp. 424-334.
- Schneier, B., 2005, Two-Factor Authentication: Too Little, Too Late, *Communications of the ACM*, vol. 48, No. 4, April 2005.
- Smith, P., 2006, Defence doubled, *Managing Information Strategies*, viewed at <http://www.misweb.com>, last accessed: 13 Oct 2008.
- Suh, B. and Han, I., 2002, Effect of trust on customer acceptance of Internet Banking, *Electronic Commerce Research and Applications*, 1, pp. 247-263.
- Walker, R.H. and Johnson, L.W., 2006, Why consumers use and do not use technology-enabled services, *Journal of Service Marketing*, 20/2, pp. 125-135.
- Wilson, C., 2002, the Great Authentication Debate, *Community Banker*, March 2002.