ICIT 2015 The 7th International Conference on Information Technology
doi:10.15849/icit.2015.0070

A Review on Internet Banking Security and Privacy Issues in Oman

Elbek Musaev
Department of Management Information Systems
Dhofar University
Salalah, Sultanate of Oman

Muhammed Yousoof
Department of Management Information Systems
Dhofar University
Salalah, Sultanate of Oman

***Abstract*— Internet banking (IB) is not a new phenomenon anymore as more and more financial institutions worldwide jump onto this wagon as it creates win-win situation for all parties. There is no need to go to bank office to pay bills, check account balance and make funds transfer. Today banks with significant IB experience provide even more complicated online financial tools and services. Nonetheless, due to the fact that platform of IB is World Wide Web, security and privacy issues are of high concern. So banks in Oman, lacking technically advanced experience of other countries should provide more safe and secure IB services, as security issues in this vulnerable area do exist. This work studies security and safety problems and suggests theoretical and practical recommendations.**

Keywords*— *Internet banking; security; privacy; mobile banking

I. INTRODUCTION

Due to rapid development of interconnected online IT infrastructure financial institutions around the world urged to keep up with this development as many see the future of commerce and affairs done online. People can do banking operations sitting home, at work, or lying on their beds midnight as this can be done through computers or mobile devices. Internet Banking (IB) was defined as distantly performing financial transactions over internet with the help of bank's website [1]. Since banks provide internet-based services, they should have secure and reliable methods of authenticating their customers [2]. Therefore, banks have to better understand their customers, current adoption of IB and respond quickly to market developments by identifying reasons that impact customer perception of security and usability issues in IB [3].

We believe that many banks in Oman have security issues as there was a biggest ATM fraud heist in history of USD 45mln by hackers worldwide. The cash withdrawals were made through ATMs in 24 countries including the US, Germany, Japan, Russia, Romania, Egypt, Colombia, Britain, Sri Lanka and Canada. Hackers accessed Bank Muscat and Rakbank databases, removed withdrawal limits on prepaid debit cards and created access codes. Others loaded that data onto any expired plastic card with a magnetic stripe and distributed among themselves, thus stealing loads of money [4]. This case subsequently might have led to low use of IB in Oman, which can be seen in statistics discussed next.

As Oman is relatively new country that started providing essential provisions to keep up with the modern developments and needs to study from other technically advanced counterparts. According to Information Technology Authority – the institution responsible for implementing of Digital Oman Strategy – 67% of total population has used Internet in 2013, and only 8% of them used IB. This confirmed by additional statistics – a large majority, 85% of internet users have never bought or ordered anything online and only 8.3% conducted E-commerce activities within 3 months. In addition, when using E-government services, only 14% used online services or submitted online forms, the rest either downloaded online forms or just obtained information. Main reason for not using E-government services was no necessity (45%) or concerns about protection and security of personal data 44%) [21].

This leads to suggestion that one of major reasons to low usage of E-commerce and IB in Oman is fear of leakage of private data and security of services provided. Therefore this work in progress will be done in two stages: 1) survey bank customers and see if security issues lead to poor adoption of Internet and mobile banking and 2) find out IB security issues of three major banks in Oman through benchmarks of IB in South Korea and propose solutions. As people start slowly migrating from desktop computers to mobile tablets and smart phone devices, this study will examine both IB access from desktop and Mobile banking (MB) security issues, as well as mobile applications of studied banks will be thoroughly analyzed.

doi:10.15849/icit.2015.0070

II. INTERNET BANKING

There was a growing trend in the amount and attention given to IB adoption research that have increased over time and will supposedly remain as key area of studies in coming years [5] [18]. IB services give customers possibility most of traditional services without the need of going to bank offices saving time and money of both sides. For the past decade, IB usage has grown substantially and banks worldwide began to give this occurrence more attention and support[6]. Interestingly, another study argues that the "growth rate of those who adopt IB has not risen strongly as expected" [3] as there is little knowledge of true determinants of online banking adoption [7]. Technology acceptance model is used in this study to indentify if security and risk are having a good weight in adoption of IB and therefore can be accepted as major determinants.

In addition, as we see in everyday life that many people move from desktop and even laptop PCs to mobile equivalents like tablet PCs and smart phones. Thus, mobile banking being a subset of IB is likely to be used overwhelmingly and replace IB in the future due to convenience and ease of use of mobile devises [3] [8]. For this reason, large and commercial banks that always diversify their activities in constant search of additional benefits tend to quickly adopt mobile banking, offer more mobile financial services, security features and support more devices [9]. This research will try to identify any available online security issues and give practical recommendations to managers of bank institutions.

III. METHODOLOGY

First part of research was conducted by surveying bank customers and find out if security is a major factor that causes slow usage and adoption of IB. Technology acceptance model (TAM) was used to identify whether insecurity in form of trust and risk influence the usage of IB, because it is one of the most influential theory models that predicts the adoption of any certain technology in Information Systems. TAM argues that perceived usefulness and perceived ease of use define an intention to use a system [5]. This work applies TAM with additional factors that describe security.

A. IB Security Issues

Perceived lack of security is "a perceived potential loss due to fraud or a hacker compromising the security of IB" [10]. So, IB threats can be accomplished through network attacks or through illegal access to the customer account by means of fabricated or faulty authentication [3]. For this reason, security and privacy threats are constantly increasing both in quantity and quality [11]. Thus, "online banking security is a primary concern", as banks supposedly provide all measures necessary to make customers believe that information is transmitted safely and securely [12]. Awareness of security has direct impact on trust and usage of IB and indirectly affects perceived ease of use [7], in other words security issues have significant effects on IB use [3] having negative causal relationship [10] [13]. To sum up, banks and financial institutions should build and enhance confidence and trust of their internet services and data transfer, as well as provide privacy and security protection, system reliability and financial quality information [14].

Thus we hypothesize that:

H1a: Trust has positive effect on the intention to use Internet banking.

H1b: Trust has positive effect on usefulness of Internet Banking

On the contrary, Lee et al. suggest that in South Korea few cases of customer fraud were reported due to good IB security infrastructure, but "serious potential problem now and in the future is leakage of private information" [15].

Nonetheless, other scholarly research supports ideas opposing security problems, e.g. security is not perceived as an obstacle or a major concern in mobile banking transactions [16]. It can be understood that people are ready to settle with less secure environment in favor of ease of use and convenience. Customers' IB use satisfaction drops if they have to memorize multiple pieces of credentials and use One-time password tokens provided by banks [7]. Therefore majority of people use simple, easy-to-remember, "convenient" passwords that can simply be guessed by people. SplashData provides such list of easily guessable, most frequently used passwords [17]. Thus people can trade-off encrypted, more secure Android phone to non-encrypted, as fully encrypted Android device, due to security, privacy concerns allows locking phone only with at least 6 character password, disabling pin, face, pattern and fingerprint unlocks. Thus it becomes very inconvenient to type passphrase every time to unlock a phone. Hence you can see many people use simple 4 digit PIN, pattern unlock, face unlock or by fingerprint. Latter two are biometric types of unlock and are a good research directions for future. Therefore usefulness and ease of use are critical factors in TAM:

H2a: Usefulness positively influences the intention to use Internet banking

H2b: Usefulness positively influences the ease of use of Internet Banking

H3: Ease of use has positive effect on intention to use Internet banking

Perceived risk is another major concern when customers connect remotely to bank servers and do various transactions. Thus it was found that perceived risk has considerable effect on intention to use [22] as risks are considered as important factors for frequent or non-frequent users [23].

H4: Perceived risk has negative effect on intention to use Internet Banking

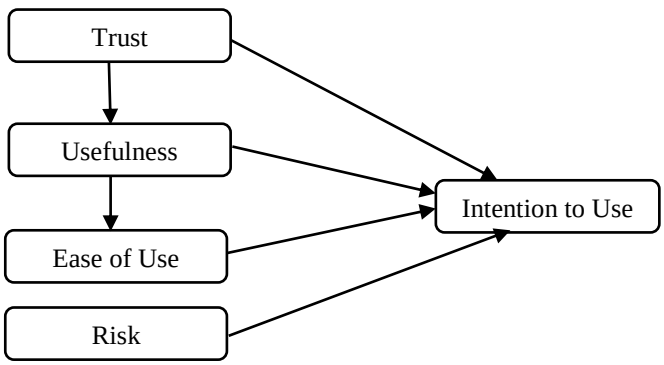

Fig.1 Hypothesized model

doi:10.15849/icit.2015.0070

B. Technical Analysis and Interview

Second part of the research will verify the online security of three big banks: Bank Muscat, Bank Dhofar and HSBC as a representative of foreign experience. The security of online banking application will be concentrated on three levels [12], security threats – measures approach and will further be extended from experience of South Korean banks. Security threats – measures approach includes several types of threats and measures – internal, external, human, non-human, accidental and intentional categories [19].

- *Security of customer information sent from PC or mobile device to web server.*

This includes the availability of secured website information of bank, namely IB section should be always be 128-bit and above secure socket layer (SSL) encrypted in order to remove man-in-the-middle external threats. However, such method is not proven to be completely secure as man-in-the-middle attack by hackers may lead to personal information and credentials leak [2] or people can use insecure ways of storing their login credentials on a piece of paper after forgetting passwords, login IDs, secret question – answers [19]. For this reason, if hackers use key logger software to gather information, website should include option of virtual input of data with the help of virtual keyboard. Study of two-factor authentication (2FA) of UK banks has also found that some websites do not hide passwords or pass-phrases [6]. In addition, from the personal experience of IB in South Korea, most of IB of Korean banks initially use additional software like anti-virus, anti-key logger, anti-screen capture, anti-malware installed obligatory before entering into IB section. After first installation, the next time you log in, these programs automatically run in the background to secure connection and transfer of any data from user PC to bank web server.

This method of installing additional software seem to have proven itself with time, as study of security of IB and financial private information in South Korea indicates that there were few cases of customer hacking fraud was reported [15].

- *Security of web server environment and customer information database.*

Real world example has shown that even banks and financial institutions pay great attention and invest heavily in security issues, all information systems have weaknesses that create opportunities for possible threats to the information housed in these systems [19]. As a result, Lee et al. suggest using central government regulated encrypted repository of all customer private information with the help of e-pin [15]. This means that after first registration in any bank, customer information is sent to the central repository and after authenticating user a unique password-protected e-pin number is issued. Next registration in bank will not require user to enter personal data again, but to enter the unique e-pin and the data will be retrieved by bank automatically and verified. This method will effectively eliminate perceived information system weaknesses and reduce possibility of external attacks.

- *Security measures to prevent unauthorized access to IB section.*

Two-factor authentication (2FA) has proven to be secure method customer verification requiring them to produce additional authentication [6] [11] together with their unique login ID and password like one time passcode (OTP) issued by OTP token or received by SMS to mobile device, phone call, card reader or a card with random numbers. Nonetheless, increased security could have negative effect on the IB system use [19] such are too many specific information, predefined security questions and answers that needed to be remembered by customers to verify their entry into IB section lead to decreased perceived usability [5] [6] [18] [19]. Moreover, 2FA schemes have conceptual vulnerabilities and not completely secure because OTPs can be intercepted [11].

Among other security measures are: session timeouts or auto-terminal/account logoff, automatic lockouts after a number of unsuccessful login tries, use of strong passwords [19].

Thus, security issues discussed above can be summarized as follows:

1. *Security of customer information sent from PC to web server.*
   a) Are online sessions secured at all times, i.e. are all web pages interacting with online banking 128(256) bit SSL encrypted (registration, login, fund transfer pages).
   b) Type passkey, passphrase, user ID by virtual keyboard (not physical keyboard).
   c) Entered characters hidden (e.g. asterisk *)
   d) Requirement of additional security software installed before registering or using online banking section (anti-virus, anti-spyware, anti-key logger, anti-screen capture).
2. *Security of web server environment and customer information database.*
   a) Is customer information saved in bank web server?
   b) Is customer information database securely protected?
3. *Security measures to prevent unauthorized access to online banking section.*
   a) Does bank use two-factor authentication (2FA)?
      - One time password token carried by customer
      - Card reader
      - A card with random numbers issued by bank
      - Mobile phone SMS authentication
      - Phone call
   b) Does bank use 2FA after login and for transactions?
   c) Does bank use 2FA only for transactions?
   d) Are there session timeouts after some time?
   e) Do automatic lockouts after 3 unsuccessful tries exist?
   f) Is creation of strong passwords suggested and assisted on web page?

IV. Results of Survey

The survey was conducted in Salalah, Oman from the sample of 200 respondents, returned results were 121 and after

doi:10.15849/icit.2015.0070

removing 14 unusable we had 107 filled survey papers at hand to analyze the model. 55% of respondents were females and 45% – males. 75% are at the age of between 20-29, 60% of respondents are Muscat bank users, 24% - Dhofar and few numbers of HSBC and National Bank of Oman. Largest share almost 70% were students.

The regression and correlation analysis was used to check the model and relationship of variables.

TABLE 1. CORRELATION RESULTS OF VARIABLES

	Intention to Use IB
Trust in IB	.914**
IB Usefulness	.747**
Ease of Use	.776**
Risk	.385**

** - Correlation is significant at the 0.01 level (2-tailed)

In addition, the correlations between trust, usefulness and ease of use are significant. Trust and usefulness - .741, usefulness and ease of use - .736. Other two correlations we didn't consider also have shown to be significant – trust and ease of use (.749) as well as risk and usefulness (.603). All correlations are significant at 10% level. Thus we can understand that it is paramount for that bank to gain trust of customers in order to introduce and encourage to use IB by providing safe and secure online services.

By testing the model by the analysis of variance we can understand that independent variables have good weight in explaining the model and intention to use IB.

TABLE 2. STATISTICAL INDICATORS OF THE MODEL

R	**R^2**	**St.Err**	**Mean.**	**Chronbach**	**Sig.**
.932	.869	.876	85.4	.902	.000

TABLE 3. HYPOTHESES TEST RESULTS

	Mean	**St.dev.**	**Sig.**	**Hypothesis**
H1a	4.03	2.06	.000	Accept
H1b	4.52	1.97	.004	Accept
H2a	4.58	1.91	.000	Accept
H2b	4.56	1.64	.000	Accept
H3	4.06	2.02	.000	Accept
H4	4.07	1.75	.003	Accept

Sig. level <0.05

Results have shown that all of the hypotheses are accepted at various significant levels.

V. DISCUSSION AND IMPLICATIONS

The analysis has shown the expected results of trust, usefulness, ease of use and risk having various degrees of influence on the intention to use IB.

Any research has limitations, as current work was based on student survey and in Salalah. The study of respondents in Muscat will certainly show different results as they live closer to Dubai, world trade hub and may use IB more often than those who live in Salalah. This is due to the fact that most people prefer traveling to Dubai directly and do their shopping there. Creating e-commerce presence between Dubai and Omani shoppers would greatly help reduce traveling costs and time. Thus by using more e-commerce people would use IB more and other forms like MB.

As the chosen variables not completely determine the intention to use IB, more research should be conducted in order to find all determinants of the model implemented in this work.

As to implications to practitioners, banks should develop trust of customer perceptions in use of new technologies and review security features of website and mobile applications. They are advised to pay attention to make the use of services easy and useful by explaining and showing that customers can save time by doing non-cash services. Risk from losing money by possible attack of hackers was supported weakly which means that customers care mostly about trust and ease of use, together with usefulness.

Second part of the work will be conducted later in order to get whole picture of bank security issues in Oman, however we can derive following by looking into some features:

Security of customer information sent from PC to web server.

Study showed that one of reviewed bank website login page is secure and encrypted and has virtual keyboard input, but when after navigating to bank registration page, web page vulnerability was detected by internet browser indicating that data is not completely secure and can be intercepted by external human factor that could intentionally steal required information. Thus, private data is not secured and after stealing that information, hackers have better chances to access IB web section with little or no efforts [19].

If one compares this case with website of South Korean banks, it can be seen that when entering to IB section, website forces to install additional software like anti-virus, anti-malware, anti-key logger and anti-screen capture. This ensures that private data and credentials are secure when transmitting data from user PC to web server. Therefore we can conclude that there were not many online cases of money fraud in South Korea [15].

Detailed study will be conducted later with the interviews of bank representatives and analysis of the websites and mobile applications of related banks.

Security of web server environment and customer information database.

Security of bank web server environment is not completely secure and even high tech South Korea banks were often hacked by international cyber crime groups, however there was no case in Korea like with Oman. There are two possible solutions for Omani banks to possibly prevent breach of web

doi:10.15849/icit.2015.0070

servers. Firstly, all banks should carry out independent audit of their information systems by network security analysts or hackers [19]. Secondly, as it was suggested earlier, use of centralized repository of population of Oman in one place with the help of e-pins [15] for the reason that inter-institution networks are more protected and secured and it is easier to protect one system effectively, than trying to secure many places at once.

Security measures to prevent unauthorized access to online banking section.

All of the banks reviewed use 2FA security features with HSBC providing physical secure keys. Other banks use SMS based 2FA. However, these banks use 2FA for money transaction only, and not for login sessions. Although banks in South Korea also use 2FA for transactions only their IB environment is more secure that those of Oman. For other security features like session timeouts and lockouts all banks met the requirement. However, they do not give customers feedback to check whether passwords are strong or not, but only mention about use of strong passwords.

Many studies suggest use of biometrics [6] [2] as a solution to complicated process of memorization of specific data and 2FA replacement. Among the suggestion is voice recognition [9], hand eye scan and fingerprint [2]. Saleh suggests using RFID to authenticate customers in order to improve IB security and improve trust [12]. Thus scholarship research could give more attention to research novel ways of authenticating IB customers.

REFERENCES

[1] G. Shao, "The diffusion of online banking:research trends from 1998 to 2006, Journal of Internet Banking and Commerce, vol. 12, No. 2, August 2007, pp. 1-13.

[2] F. Amtul, "E-Banking security issues – is there a solution in biometrics?", Journal of Internet Banking and Commerce, vol. 16, No. 2, August 2011, p.1.

[3] H.S. Yoon and L. Occena, "Impats of customers' perceptions on internet banking use with a smart phone", Journal of Computer Information Systems, vol. 54, No. 3, Spring 2014, pp. 1-9.

[4] B. Thomas, "9 arrested for $45mn bank muscat, rakbank prepaid card fraud", http://www.muscatdaily.com/Archive/Oman/9-arrested-for-45mn-bank-muscat-Rakbank-prepaid-card-fraud-290x, (Accessed in February 2015), May 2013.

[5] P. Hanafizadeh, B.W. keating and H.R. Khedmatgozar, "A systematic review of Internet banking adoption", Telematics and Informatics, Vol. 31, No. 3, April 2014, pp. 492-510.

[6] K. Krol, E. De Cristofaro and A. Sasse, "They brought in the horrible key ring thing!" Analysing the usability of two-factor authentification in UK online banking", Cornell University Library, arXiv:1501.04434, unpublished

[7] M.S. Alnsour and K. Al-Hyari, "Internet banking and Jordanian corporate customers: Issues of security and trust", Journal of Internet Banking and Commerce, vol. 16, No. 1, April 2011, p.1.

[8] R. Weber and A. Darbellay, "Legal issues in mobile banking", Journal of Banking Regulation, vol. 11, No. 2, 2010, pp. 129-145.

[9] H. Lee, Y. Zhang and K.L. Chen, "An investigation of features and security in mobile banking strategy", Journal of International Technology and Information Management, vol. 22, No. 4, October 2013, pp. 23-46.

[10] M. Lee, "Factors influencing the adoption of Internet banking: An integration of TAM and TPB with perceived risk and perceived benefit", Electronic Commerce Research and Applications, vol. 8, No. 3, May-June 2009, pp. 130-141,.

[11] A. Dmitrienko, C. Liebchen, C. Rossow and A.-R. Sadeghi, "Security analysis of mobile two-factor authentication schemes", Intel® Technology Journal, vol. 18, No. 24, 2014, pp. 138-161.

[12] Z. Saleh, "Improving security of onilne banking using RFID", Academy of Banking Studies Journal, vol. 10, No. 2, July-December 2011, pp. 1-8.

[13] C. Kim, M. Mirusmonov and I. Lee, "An empirical examination of factors influencing the intention to use mobile payment", Computers in Human Behavior, vol. 26, No.3, May 2010, pp. 310-322.

[14] J-P.L. Mangin et al., "The moderating role of risk, security and trust appliet to the TAM model in the offer of banking financial services in Canada", Journal of Internet Banking and Commerce, vol. 19, No. 2, August 2014, pp. 1-21.

[15] J.H. Lee, W.G. Lim and J.I. Lim, "A study of the security of Internet banking and financial private information in South Korea", Mathematical and Computer Modeling, vol. 58, No. 1-2, July 2013, pp. 117-131.

[16] T. Laukkanen, "Internet vs mobile banking: comparing customer value perceptions", Business Process Management Journal, vol. 13, No. 6, 2007, pp. 788-797.

[17] "Password" unseated by "123456" on SplashData's annual "Worst Passwords" list" retrieved from http://splashdata.com/press/worstpasswords2013.htm, (accessed in February 2015).

[18] H.M. Sabi, "Research trends in the diffusion of Internet banking in developing countries", Journal of Internet Banking and Commerce, vol. 19, No. 2, August 2014, pp. 1-31.

[19] A. French, "A case study on E-Banking security – When security becomes too sophisticated for the user to access their information", Journal of Internet Banking and Commerce, vol. 17, No. 2, August 2012, pp. 1-14.

[20] F. Sidi et al., "Measuring computer security awareness on Internet banking and shopping for Internet users", Journal of Theoretical and Applied Infromation Technology, vol. 53, No. 2, July 2013, pp. 210-216.

[21] "Survey on access to, and use of ICT by households and individuals in Oman 2013", retreived from http://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=97, (accessed in January 2015)

[22] A. Kesharwani, S.B. Singh, "The impact of trust and perceived risk on internet banking adoption in India: An extension of technology acceptance model", International Journal of Bank Marketing, Vol. 30, No. 4, 2012, pp. 303–322.

[23] C. Chen, "Perceived risk, usage frequency of mobile banking services", Managing Service Quality, Vol. 23, No. 5, 2013, pp. 410-436.