2011

A comparative analysis of the security of internet banking in Australia:a customer perspective

Panida Subsorn
Suan Dusit Rajabhat University, Thailand

Sunsern Limwiriyakul
Edith Cowan University

A COMPARATIVE ANALYSIS OF THE SECURITY OF INTERNET BANKING IN AUSTRALIA: A CUSTOMER PERSPECTIVE

Panida Subsorn[1], Sunsern Limwiriyakul[2]
Suan Dusit Rajabhat University, Thailand[1],
School of Computer and Security Science,
Edith Cowan University, Western Australia[2]

slimwiri@our.ecu.edu.au

Abstract

Internet has its own inherent security issues in terms of confidentiality, integrity and privacy. The main impact of these kinds of issues is specifically on the banking industry as they have increased their Internet banking facilities in order to reduce costs and provide better services and banking convenience to their Internet banking customers. However, banking customers have not had a choice of Internet banking mainly due to the fact that they are already tied to whatever form of Internet banking that their current bank provides. This paper therefore examined Internet banking security systems in Australian banks by creating the proposed Internet banking security checklist which can benefit both existing and potential Internet banking customers to use as an Internet banking security guideline. Furthermore, the results uncovered were lack of Internet banking security in all the 16 selected Australian banks. These can impact its existing and potential customers' confidentiality in terms of using Internet banking. Better Internet banking security information, two-factor authentication and stronger encryption in use are some of the example recommendations. In addition, this study can be extended to cover more in-depth details which cover interviewing and auditing from a customer perspective, the design and format of the Internet banking website and mobile banking security.

Keywords

Australia, comparative analysis, customer perspective, Internet banking security

INTRODUCTION

With the advent of Internet technologies, the Internet has become a significant element in almost every business (Gunasekaran & Love, 1999; Karim et al., 2009). One of the most significant developments in this aspect is the banking industry (Hamid et al., 2007). The Internet has the capability to integrate and transform a traditional business to a model of electronic commerce (e-commerce) in providing banking alternatives and facilitating for the convenience to their Internet banking customers (Steinfield, 2002). In fact, most of the banks around the world have adjusted their business strategy to attain competitive benefits, reduce operational costs and enhance their performance by offering an Internet banking system to their Internet banking customers (Hutchison & Warren, 2003; the National Office for the Information Economy (NOIE) et al., 1999). Hence, the Internet banking customers have the option of accessing their bank accounts and making transactions anytime and anywhere (Gurau, 2002; Karim et al., 2009). However, the Internet banking systems have associated information security threats and risks which can be assessed as low, medium and high (Usonlinebiz, 2008). Privacy and security of Internet banking transactions and confidentiality of personal information are among the biggest concerns for both the banking industry and the Internet banking customers (Hutchison & Warren, 2001, 2003)

Adware, keylogger, malware, phishing, spyware, Trojans and viruses are the most common Internet banking security threats and risks (BankMuscat, 2009; Ekberg et al., 2007; RSA, 2010). Furthermore, there are some additional Internet banking security threats and risks that impact both the banks and the Internet banking customers. These include security awareness of the Internet banking customers and the banks, Internet banking customers' online behaviour, threats (both authentication and authorisation), exposure to new potential threats, Internet banking customers' trust of the Internet banking system, the mobile banking security problem, protection against man-in-the-middle attack and man-in-the-browser attack, identity and/or information theft sourced from social networking sites, healthcare and government portals using only a single-factor authentication (RSA, 2010). These factors have the potential to influence traditional baking customers from switching to the Internet banking. (Ekberg et al., 2007; Georg et al., 2009; RSA, 2010).

Therefore, the main purpose of this paper was to investigate the security of Internet banking systems of Australian banks by deploying a comparative analysis approach in generating a proposed Internet banking security checklist. This checklist could then be potentially used to evaluate their Internet banking security

systems based on the Internet banking information which is currently provided on the selected Australian banks' websites. As a result, the potential Internet banking customers can be provided with a security background and a notion of Internet banking security prior to choosing a bank to commence the Internet banking with. On the other hand, the existing customers can use this checklist to identify their own security weaknesses and better secure their Internet banking experience.

The rest of this paper is organised into four main sections: methodology, analysis and conclusions, recommendations and future works.

METHODOLOGY

This paper applied a qualitative research method by deploying a comparative analysis approach. This comparative analysis was conducted by examining the availability of Internet banking security features of the Australian banks.

Sample

In order to fulfil the purpose of this paper, 16 Australian banks including major, competitor and sub banks were selected as they were able to provide a good setting for the comparative analysis for the proposed Internet banking security checklist. Nevertheless, Bendigo Bank and Adelaide Bank Limited were separately analysed as they were using different security features on their Internet banking security systems prior to and after merging. The list of Australian banks used in the analysis is displayed below.

Table 1 List of Australian banks used in the analysis

Count	Banks	Headquarters
1	Adelaide Bank Limited	Bendigo
2	AMP Bank Limited	Sydney
3	Australia and New Zealand Banking Group Limited (ANZ)	Melbourne
4	Bank of Queensland Limited	Brisbane
5	Bank of South Australia (BankSA) (a division of the Westpac Banking Corporation)	Adelaide
6	Bank of Western Australia Limited (a subsidiary of CBA, trading as BankWest)	Perth
7	Bendigo Bank	Bendigo
8	Commonwealth Bank of Australia (CBA)	Sydney
9	Rural Bank Limited (a wholly owned subsidiary of Bendigo and Adelaide Bank Limited)	Adelaide
10	Macquarie Bank Limited	Sydney
11	Members Equity Bank Pty Limited	Melbourne
12	National Australia Bank Limited (NAB)	Melbourne
13	St.George Bank Limited (a division of the Westpac Banking Corporation)	Sydney
14	Suncorp-Metway Limited	Brisbane
15	UBank (a division of NAB)	Melbourne
16	Westpac Banking Corporation	Sydney

(Sources: Australian Prudential Regulation Authority (APRA), 2011, p. 1; the Australian Bankers Association (ABA), 2010, pp. 1-3)

Data collection

This paper utilised a secondary data source which was freely-and readily-available through the selected banks' websites in order to assess their Internet banking security features.

Furthermore, we created the proposed Internet banking security checklist for the purposes of evaluating the security features of the selected banks. The results and findings from the proposed Internet banking security checklist can provide external validity for other related sectors or organisations to best used as a guideline for improving their own performances on Internet banking security systems. The checklist is presented and explained in detail in the following sections.

The proposed Internet banking security checklist

There are six main security feature categories that banks provide and offer their Internet banking customers. These include (1) general online security and privacy information to the Internet banking customers; (2) Information technology (IT) assistance, monitoring and support; (3) software and system requirements and settings information; (4) bank site authentication technology; (5) user site authentication technology; and (6) Internet banking application security features. Details on each of these security feature category are explained below.

Section 1: General online security and privacy information to the Internet banking customers

This section covers general online security and privacy information as follows:

- Account aggregation or privacy and confidentiality;
- Losses compensation guarantee;
- Online/Internet security information; and
- Bank security mechanism system.

Account aggregation or privacy and confidentiality: This subsection investigates the current privacy and confidentiality policy which the banks provide to the Internet banking customers. The policy must comply with privacy laws and incorporate the National Privacy Principles in order to ensure the integrity of the Internet banking customers' confidential information. In terms of use and disclosure, the banks must also comply with any legal or regulatory obligations in their stipulation.

Losses compensation guarantee: This subsection examines with the banks current guarantee policy where the banks are obliged to cover any losses in case unauthorised transactions by someone other than the customer using customers' Internet banking accounts.

Online/Internet banking security information: This subsection inspects the Internet security information which is provided by the banks to their Internet banking customers. These cover important and related Internet banking security information such as threats, security guidelines and tips.

Bank security mechanism system: This subsection attempts to identify whether the banks provide information on their Internet banking security systems such as firewalls and intrusion detection systems (IDS) which have the capability to enhance privacy and confidentiality of the Internet banking customers.

Section 2: IT assistance, monitoring and support

This section consists of hotline and helpdesk service availability as well as Internet banking transaction monitoring by the banks.

Hotline/helpdesk service availability: This subsection checks the banks' websites in order to identify information related to an IT hotline or helpdesk support for the Internet banking customers. Ideally, the banks should provide several different modes of communication with the Internet banking customers. Telephony and secure email are some of the common communication methods.

Internet banking transaction monitoring by the banks: This subsection attempts to determine whether the banks provide their own dedicated teams for monitoring possible suspicion transactions on their Internet banking systems.

Section 3: Software and system requirements and settings information

This section is comprised of three parts as follows:

- Compatibility "best" with the popular Internet browsers;
- Internet banking user device system and browser setting requirement; and
- Free/paid security software/tool available to the Internet banking customers.

Compatibility "best" with the popular Internet browsers: This subsection identifies whether the banks' Internet banking systems are able to support or are compatible with the world's most popular Internet browsers such as Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and Apply Safari based on the information provided by the banks.

Internet banking user device system and browser setting requirement: This subsection looks at operating systems, browser settings and screen resolution requirements information which are provided by the banks for optimum usage.

Free/paid security software/tool available to the Internet banking customers: This subsection is concerned with determining whether the banks have provided an optional Internet security software or tool for their customers in order to minimise any potential risks to the Internet banking customers' personal computers.

Section 4: Bank site authentication technology

This section involves an identification of the bank authentication technology which is currently employed to cover types of secure sockets layer (SSL) encryption, digital certificate technology and certificate authority (CA). SSL encryption generates an encrypted link between the banks' web servers and the Internet banking customers' Internet browsers in order to provide private and secure communications between both the parties (Comodo, n.d.).

Section 5: User site authentication technology

This section is concerned with identifying authentication technology that the Internet banking customers interact with to authenticate with the banks. This user site authentication technology section consists of the followings:

- Two-factor authentication for logon and/or for transaction verification available;
- Logon requirements;
- Logon failure limitation;
- Logon user input type;
- Scramble an on-screen input keypad;
- Password restriction/requirement; and
- Transaction verification.

Two-factor authentication for logon and/or for transaction verification available: Two-factor authentication can be considered as a strong authentication mechanism (RSA, n.d.). Typically, two-factor authentication requires a combination of two identifiers for the verification of a transaction or an identity (VeriSign Authentication Services, n.d.-a). These two identifiers are physical and remembered identifiers (Bank of Queensland Limited, n.d.). The physical identifier can be a short message service (SMS) mobile number or a pin number or a generated security token. This subsection identifies whether there are any two-factor authentication mechanisms in use for logon as well as for transaction verification at the selected banks.

Logon requirements: This subsection identifies the Internet banking logon requirements of the banks. In general, Internet banking logon requirements may include two to three identifiers. The first identifier may be a bank/credit card number or a bank register/customer ID or an email address of the Internet banking customers. This first identifier information is known by both the banks and the Internet banking customers. On the other hand, the second identifier may be a remembered type identifier such as a password which is only created by the Internet banking customers. Some banks may include its logon requirements by incorporating with another remembered identifier such as a personal access code or a security number. This can enhance user site authentication security. Finally, the third identifier may be two-factor authentication mechanism as mentioned earlier.

Logon failure limitation: This subsection verifies a number of consecutive unsuccessful login attempts which is allowed by the banks before disabling or locking out the Internet banking customers' Internet banking accounts in order to protect against unauthorised access (Suncorp-Metway Limited, n.d.). This verification detail is based on information provided on the banks' websites.

Logon user input type: This subsection identifies a logon user input type of the banks' Internet banking systems. Typically, the logon user input type may require input information from a keyboard. Furthermore, other input type such as a keypad can be incorporated with a logon authentication system.

Scramble an on-screen input keypad: This subsection involves checking on a logon user input keypad to determine whether the keypad has a scramble feature which changes the keypad at every logon. This can protect the Internet banking customers against any potential keylogger attacks which record the customer's keystroke information (e.g. login ID and password) without their knowledge.

Password restriction/requirement: This subsection investigates the password restrictions and requirements on Internet banking accounts. For example, the password length, combination of numbers and letters, case sensitivity, use of special characters, different passwords to any previously used passwords and automatically checking of password strength when creating or changing passwords.

Transaction verification: This subsection determines whether the Internet banking customers may require any type of verification during the Internet banking transaction period particularly when dealing with external transactions. Examples of such verification methods may be SMSs, tokens or passwords.

Section 6: Internet banking application security features

This section audits the following categories of security features of the banks' Internet banking applications:

- Automatic timeout feature for inactivity;
- Limited default daily transfer amount to third party account/BPAY/international transactions;
- Logging information; and
- Session management.

Automatic timeout feature for inactivity: This subsection identifies a default automatic timeout setting limit which can automatically log the Internet banking customers off, as well as end the Internet banking session in case of no activity occurring on the Internet banking session for a preset period of time.

Limited default daily transfer amount to third party account/BPAY/international transactions: This subsection intends to find out a default daily transfer amount limitation when the Internet banking customers transfer money locally and globally.

Logging information: This subsection aims to discover whether the Internet banking system logging information is available to the Internet banking customers based on the information provided on the banks' websites. Typically, the logging information can include last login information attempted such as the date and time. In addition, activity logging information may be included. The Internet banking customers can utilise this information to ensure that their logon activities are normal and expected.

Session management: This subsection investigates the Internet banking session management which includes session tokens, page tokens technologies which are currently deployed at the selected banks based on the information which is provided on their websites. Furthermore, clearing information on Internet browser's cookies after the Internet banking customers logoff or shut down the Internet browser is also investigated.

ANALYSIS

The analysis and results finding are summarised in Table 2 and the following discussions.

Table 2 A summary of the proposed Internet banking security checklist

Australian banks																	
		Major 4 banks				Competitor banks									Sub banks		
	Security feature categories	ANZ	CBA	NAB	Westpac	Adelaide	AMP	Queensland	BankWest	Bendigo	Rural	Macquarie	Members Equity	Suncorp-Metway	BankSA	St. George	UBank
1. General online security and privacy information to the Internet banking customers																	
1.1	**Account aggregation or privacy and confidentiality**																
1.1.1	Complied with the national privacy principles and privacy law	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1.2	**Losses compensation guarantee**																
1.2.1	100%	✓	✓	✓	✓	✓	✓	NI	✓	NI	NI	NI	NI	✓	✓	✓	✓
1.3	**Online/Internet banking security information**																
1.3.1	Threats: Hoax email, scam, phishing, spyware, virus and Trojan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	
1.3.2	Keylogger														✓	✓	
1.3.3	General online security guidelines	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
1.3.4	Security alert/up-to-date issue	✓					✓			✓	✓				✓	✓	
1.3.5	Provides password security tips	✓	✓		✓		✓	✓		✓	✓			✓	✓	✓	
1.4	**Bank security mechanism system**																
1.4.1	Antivirus protection														✓	✓	
1.4.2	Firewall(s)	✓	✓	✓			✓	✓	✓	✓	✓			✓	✓	✓	✓
1.4.3	IDS/alert system				✓			✓									
1.4.4	Other																
1.4.5	No information					✓						✓	✓				
2. IT assistance, monitoring and support																	
2.1	**Hotline/helpdesk service availability**																

2.1.1	24/7 customer contact centre by phone	✓	✓					✓	✓					✓	✓	✓	✓
2.1.2	Not 24/7 customer contact centre by phone			✓	✓	✓	✓			✓	✓	✓	✓				
2.1.3	Secured email	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	NI	✓	✓	✓	✓	✓
2.1.4	FAQ/online support form	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	
2.2	**Internet banking transaction monitoring by the banks**																
2.2.1	Provides dedicated team and technology for monitoring all transactions	✓	✓	✓	✓	NI	✓	✓	✓	✓	✓	NI	NI	✓	✓	✓	✓
3. Software and system requirements and settings information																	
3.1	**Compatibility "best" with the popular Internet browsers (based on the bank's information provided)**																
3.1.1	Chrome	✓	✓		✓				✓		✓			✓	✓	✓	
3.1.2	Firefox	✓	✓	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓	✓	✓
3.1.3	Internet Explorer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
3.1.4	Netscape			✓		✓	✓										
3.1.5	Opera					✓											
3.1.6	Safari	✓	✓	✓	✓	✓		✓	✓	✓	✓			✓	✓	✓	✓
3.1.7	No information											✓					
3.2	**Internet banking user device system and browser setting requirement**																
3.2.1	Operating system	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
3.2.2	Type of browser	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
3.2.3	Browser setting	✓	✓	✓	✓			✓	✓	✓							
3.2.4	Screen resolution	✓	✓			✓		✓	✓	✓				✓			
3.2.5	No information											✓					
3.3	**Free/paid security software/tool available to the Internet banking customers**																
3.3.1	Antivirus/anti-spyware	✓					✓		✓					✓			
3.3.2	Internet security suite	✓	✓		✓		✓		✓					✓			
3.3.3	Provides Internet links to security software vendor(s)							✓	✓	✓			✓	✓			
3.3.4	No information			✓		✓					✓	✓			✓	✓	✓
4. Bank site authentication technology																	
4.1	**Employed encryption and digital certificate technologies**																
4.1.1	SSL encryption	A	A	A	A	D	R	D	R	A	A	R	R	R	R	R	R

4.1.2	Extended validation SSL certificates		✓		✓		✓	✓	✓					✓	✓	✓	✓
4.1.3	Signing CA	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
5. User site authentication technology																	
5.1	**Two-factor authentication for logon and/or for transaction verification available**																
5.1.1	Token device		✓		*			*		*	*			*			
5.1.2	SMS		✓	✓	✓												✓
5.1.3	Not in use	✓				✓	✓		✓			✓	✓		✓	✓	
5.2	**Logon requirement**																
5.2.1	Bank/credit cards number or bank register/customer ID or email address	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.2.2	Password	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
5.2.3	Other e.g. personal code or security number					✓		*					✓		✓	✓	
5.2.4	Two-factor authentication									*	*			*			
5.3	**Logon failure limitation**																
5.3.1	Max. (times)	3		3		3		3		3			3	3			3
5.3.2	In use but does not specific maximum number of failure allowed		✓						✓						✓	✓	
5.3.3	No information				✓		✓				✓	✓					
5.4	**Logon user input type**																
5.4.1	Keyboard	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
5.4.2	Keypad				✓	✓							✓				
5.5	**Scramble an on-screen input keypad**																
5.5.1	Customer ID	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.5.2	Password	NA	NA	NA		✓	NA	NA	NA	NA	NA	NA	✓	NA	NA	NA	NA
5.6	**Password restriction/requirement**																
5.6.1	Enforce good password practice	✓	✓	✓	✓	NA	✓	✓	✓	✓	✓	NI	NA	✓	✓	✓	✓
5.6.2	Password length (characters)	8-16	8-16	6-8	6	NI	6-15	8-20	6-10	8	8	NI	NI	6-8	6-12	6-12	NI
5.6.3	Combination of	✓	✓	✓	✓	N	✓	✓	✓	✓	✓	NI	N	*	✓	✓	✓

	numbers and letters					A							A				
5.6.4	Combination of upper and lower cases	*	✓	✓		NA	✓	✓	*			NI	NA	*	*	*	*
5.6.5	Special characters		*			NA		*				NI	NA				
5.6.6	Different passwords as compared to any of previous used passwords	NI	5	NI	1	NI	8	✓	NI	NI	NI	NI	NI	NI	NI	NI	NI
5.6.7	Automatically check password strength when creating or changing password	NI	✓	NI	NI	NI	✓	✓	NI	NI	NI	NI	NI	NI	NI	NI	NI
5.7	**Transaction verification**																
5.7.1	All transactions required token/SMS																
5.7.2	Some external transactions required token/SMS		✓	✓	✓			*		✓	✓			✓			✓
5.7.3	Other method e.g. password																
5.7.4	No information	✓				✓	✓		✓			✓	✓		✓	✓	
6. Internet banking application security features																	
6.1	**Automatic timeout feature for inactivity**																
6.1.1	Max. (mins)	15	15					10	15	10				10			20
6.1.2	In use but does not specify timeout length										✓				✓	✓	
6.1.3	No information			✓	✓	✓	✓					✓	✓				
6.2	**Limited default daily transfer amount to third party account/BPAY/international transactions**																
6.2.1	Less or up to $5,000 AUD		✓	✓			✓		✓	✓	✓			✓	✓	✓	
6.2.2	More than $5,000 AUD				✓								✓				✓
6.2.3	The default maximum daily limit transfer is vary depend on the type of the Internet banking customer	✓						✓	✓								

6.2.4	The maximum daily limit transfer may be increased with the approval by the banks		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	
6.2.5	No information					✓						✓					
6.3	**Logging information**																
6.3.1	Last login		✓							✓	✓			✓	✓	✓	
6.3.2	Activity log		✓							✓	✓			✓	✓	✓	
6.3.3	No information	✓		✓	✓	✓	✓	✓	✓			✓	✓				✓
6.4	**Session management**																
6.4.1	Session tokens						✓										
6.4.2	Page tokens						✓										
6.4.3	Clear session cookie information after logoff or shut down the Internet browser									✓							
6.4.4	No information	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓

✓	represents	yes	*	represents	optional
NA	represents	not applicable	NI	represents	no information
A	represents	AES 256-bit encryption	R	represents	RC4 128-bit encryption
D	represents	3DES-EDE-CBC 168-bit encryption	V	represents	VeriSign Authentication Services

Note:

Blue A is a wrong or not up-to-date information provided SSL encryption as 128-bit instead of 256-bit on the banks' websites.

Difficulty of finding some Internet banking security information

There was a level of difficulty to search for some related Internet banking security information on the websites of some of the selected banks. For example, in order to find out a password requirement from the AMP bank's website, the Internet banking customers have to visit "Terms and Conditions" page only (AMP Bank Limited, n.d.) as there was no link in the "Online Security" information section. In addition, using the AMP Bank's frequently asked questions (FAQ) and search engine also do not provide any required information.

Encryption and digital certificate

Nine out of 16 selected banks or 56 percent deployed extended validation SSL certificates. According to VeriSign Authentication Services (n.d.-b, p. 1), extended validation SSL certificate provides "high-security Internet browsers information to clearly identify a Web site organisational identity". Furthermore, six out of the16 selected banks or 37.5 percent use SSL certificate with 256-bit encryption whereas the other two banks use 168-bits and the remaining eight use 128 bit-encryptions. Upgrading to extended validation SSL certificate and 256-bit encryption can provide maximum security for bank site authentication as well as increase the potential new Internet banking customers' security confidentiality. In addition, in terms of CA, all of the selected banks have signed with a trustworthy public commercial VeriSign Authentication Services. Section 4 in Table 2 presents more details on encryption and digital certificates.

IT hotline/helpdesk support

Eight out of the 16 selected banks (50 percent) do not fully provide 24/7 IT helpdesk via telephone support regarding Internet banking system issues. However, all of the selected banks, except Macquarie Bank Limited provide online, FAQ and secured email supports. For example, the contactable times of NAB Internet banking telephone support service are available from 7 a.m. to 9 p.m. on Monday to Friday and 8 a.m. to 6 p.m. on Saturday and Sunday. Thus, by providing 24/7 IT helpdesk can increase convenience as well as confidentiality to banks' customers. See Section 2.1 in Table 2 for more details.

Logon user input type

All selected banks require a keyboard as their primary input type for inserting a user ID, a bank register ID, a bank card number or an email address. Only three (Adelaide, Members Equity and Westpac banks) out of these 16 selected banks use a keypad for a password input type. Out of these three banks, two banks utilise a scramble method on their keypad. This means that the keypad is changed every time the webpage is opened. This method can reduce the potential risks of the unauthorised keystroke recording. See Sections 5.4 and 5.5 in Table 2 for more details.

Password requirements/restrictions

No information regarding password restrictions were found in four (Adelaide, Macquarie, Members Equity and UBank banks) out of the 16 selected banks. Six of the remaining 12 selected banks required a minimum password length of six characters while the other six banks required a minimum password length of eight characters. In terms of best practices, the banks that required a minimum password length of six characters may be considered less secure as compared to eight characters. Particularly, Westpac Banking Corporation required only a six character password length. Furthermore, there were only two banks CBA and Queensland out of the 16 selected banks (12.5 percent) that allow their customers to use special characters as optional to be included into the customer password. This provides a stronger password as compared to using only combinations of just numbers, letters, lower and upper cases. In addition, there were only three out of the 16 selected banks that have a mechanism for automatically checking password strength when its customer creates or changes his or her password. This mechanism can assist banks' customers in order to create strong password. See Section 5.6 in Table 2 for more information.

Session management

AMP and Bendigo banks out of 16 selected banks are the only two banks that provide session management security information on their websites. For example AMP bank provides session tokens and page tokens whereas Bendigo bank provides session cookie information. By providing session management details this will enhance Internet banking security awareness as well as Internet banking usage confidentiality to its customers. See Section 6.4 in Table 2 for more information.

Similarity of Internet banking system

Based on simple information auditing on the selected banks' websites, there were similarities of the Internet banking systems between the Bendigo Bank and Rural Bank. This may be due to the fact that Rural Bank Limited is a subsidiary of Bendigo and Adelaide Bank Limited (Rural Bank Limited, 2010). Furthermore, BankSA and St. George Bank have similar Internet banking systems as they are divisions of Westpac Banking Corporation (St.George Bank Limited, n.d.). This explains the similarities in the Internet banking technology. This provides benefits in terms of reduced complexity of having to manage and maintain two different Internet banking systems. However, there may be a small potential risk to both the banks in case of one of its partner's Internet banking system was compromised which consequently exposes the other bank to infiltration.

Two-factor authentication

SMS mobile phone and/or token-generated pin techniques are used for the two-factor authentication system in half of the selected banks. These two-factor authentication systems are used for logon and/or transaction verification purposes by their Internet banking customers. Furthermore, seven out of these eight selected banks have made the two-factor authentication system compulsory for transaction section verification to their Internet banking customers. See Section 5.7 in Table 2 for more details. Only three out of the eight selected banks allow their Internet banking customers to use the two-factor authentication system for logon purpose as an option. See for further details in Section 5.2 in Table 2.

Websites information not up-to-date

There was no up-to-date Internet banking information found on some of the selected banks' websites. For example, incorrect information on SSL encryption technology, as well as four banks (ANZ, CBA, NAB and Bendigo) not providing up-to-date information. Three out of these four banks were from the major four banks group. These four banks provided information on their website which indicated that they were using SSL 128-

bit encryption. However, based on the auditing results these SSL encryption at all four banks were 256-bit. See more details on Section 4.1 in Table 2. These results can provide wrong indication to the Internet banking customers and can consequently influence the confidence and decision of the potential Internet banking customers to enlist as customers.

CONCLUSION, RECOMMENDATIONS AND FUTURE WORKS

The results of the proposed Internet banking security checklist uncovered several interesting issues. All of the Australian banks have generally provided a standard Internet banking security system with some optional security services to their Internet banking customers. However, these selected banks should enforce a mandatory two-factor authentication system for a logon as well as for transaction verification (Ekberg et al., 2007; Federal Deposit Insurance Corporation (FDIC), 2004; Georg et al., 2009; Hines, 2006; MidSouth Bank, n.d.; Reavley, 2005; RSA, 2010).

Furthermore, a good and effective security policy employed by the banks and legislation instituted by local or state governments should be in use and enforced in order to improve security in Internet banking systems (Georg et al., 2009; Karim et al., 2009; Victoria Teachers Credit Union, n.d.). Two-factor/multi-factor authentication systems, transaction verification, 256-bit encryption with extended validation SSL certificate, auto logout feature, suspicious activity monitoring, last login time display, account lockout and audit trails are some of examples of a good and effective security policy that could be legislated for.

Additionally, the banks should provide better authentication and/or transaction processes/mechanisms as new and improved technological security measures such as Internet fraud protection (Ekberg et al., 2007; Grimes, 2006; Karim et al., 2009).

Moreover, the banks can coordinate with the local and state government agencies such as Australian Taxation Office (ATO) to build up the confidentiality for online payment systems and enhance performance and better Internet banking security services such as personal information theft protection, personal financial information theft protection, identity fraud protection and online crime protection (RSA, 2010).

The banks who currently employ a 128-bit encryption SSL should consider upgrading to a 256-bit encryption method. Furthermore, upgrading from standard validation to extended validation SSL certificate should also be considered. These two upgrades can provide better confidentiality to both existing and potential Internet banking customers (VeriSign Authentication Services, n.d.-b).

In addition, the banks must be vigilant of new threats/risks such as phishing via SMS/text message ("SMiShing"), phishing over the phone ("Vishing"), SSL–evading Trojans (Ekberg et al., 2007; RSA, 2010). Furthermore, the banks should be cognisant of customers' demands, opinions, concerns, mistrusts and/or expectations such as their transaction activities monitoring, online and mobile threats concerns and strong security methods for online activities, by conducting a survey and offering rewards for customer feedback (Ekberg et al., 2007; Georg et al., 2009; RSA, 2010). The feedback from these surveys may be used to build up the confidentiality of both existing and potential Internet banking customers. The banks must also properly educate and encourage their Internet banking customers to gain awareness on Internet banking security threats/risks (Bishop, 2005; Georg et al., 2009; RSA, 2010). The banks should also offer a useful link to download and or update antivirus and Internet security software and firewall protections as well (Hines, 2006).

In the future, the banks may consider deploying biological authentication through biological detection tools to protect their Internet banking systems against the attackers such as finger and hand geometry, retinal scan, iris scan, fingerprint recognition, face recognition, voice recognition, keystroke recognition, handwriting recognition (Bishop, 2005; NewScientist, 2006). Alternatively, the banks may also offer insurance for losses compensation due to any potential Internet banking security threats/risks which may occur by inexperienced Internet banking customers or lack of their knowledge and/or awareness (Georg et al., 2009).

Finally, the usefulness of this paper can be enhanced by conducting an in-depth Internet banking customer interview and audit particularly on the design and structure of the Internet banking website and mobile banking security. These interview and audit can provide benefits to both existing and potential Internet banking customers.

REFERENCES

AMP Bank Limited. (n.d.). BankNet and BankPhone terms &conditions. Retrieved April, 2011, from https://secure.ampbanking.com/au/TermsConditions

Australian Prudential Regulation Authority (APRA). (2011). Australian-owned Banks Retrieved April, 2011, from http://www.apra.gov.au/adi/adilist.cfm#AOBC

Bank of Queensland Limited. (n.d.). Using the BOQ security token. Retrieved April, 2011, from http://www.boq.com.au/online_enhancedIB_security_token.htm

BankMuscat. (2009). Internet banking security threats. Retrieved April, 2011, from http://www.bankmuscat.com/en-us/ConsumerBanking/bankingchannels/internetbanking/Pages/InternetBankingSecurityThreats.aspx

Bishop, M. (2005). Introduction to computer security. USA: Prentice Hall

Comodo. (n.d.). What is SSL (Secure Sockets Layer)? Retrieved April, 2011, from http://www.whichssl.com/what_is_ssl.html

Ekberg, P., et al. (2007). Online banking access system: Principles behind choices and further development, seen from a managerial perspective. Retrieved April, 2011, from http://www.essays.se/essay/6974685cb6/

Federal Deposit Insurance Corporation (FDIC). (2004). Putting an end to account-hijacking identity theft. Retrieved April, 2011, from www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf

Georg, L., et al. (2009). The value of information security to European banking. Retrieved April, 2011, from www.personal.lse.ac.uk/LIEBENAU/BankingSecurityDETECOM.doc

Grimes, R. A. (2006). E-commerce in crisis: When SSL isn't safe. Retrieved April, 2011, from http://www.infoworld.com/d/security-central/e-commerce-in-crisis-when-ssl-isnt-safe-127

Gunasekaran, A., & Love, P. (1999). Current and future directions of multimedia technology in business. International Journal of Information Management, 19(2), 105-120.

Gurau, C. (2002). Online banking in transition economies: The implementation and development of online banking systems. International Journal of Bank Marketing, 20(6), 285-296.

Hamid, M. R. A., et al. (2007). A comparative analysis of Internet banking in Malaysia and Thailand. Journal of Internet Business(4), 1-19.

Hines, M. (2006). Banks to serve as virus firewalls. Retrieved April, 2011, from http://www.eweek.com/c/a/Web-Services-Web-20-and-SOA/Banks-to-Serve-as-Virus-Firewalls/

Hutchinson, D., & Warren, M. (2001). A framework of security authentication for internet banking. Paper presented at the International We-B Conference (2nd), Perth.

Hutchinson, D., & Warren, M. (2003). Security for Internet banking: A framework. Logistics Information Management, 16(1), 64 -73.

Karim, Z., et al. (2009). Towards secure information systems in online banking. Paper presented at the International Conference for Internet Technology and Secured Transactions, 2009 (ICITST 2009), London

MidSouth Bank. (n.d.). Enhanced security for online banking. Retrieved April, 2011, from https://www.midsouthbank.com/onlinebanking/.../ MFASecurityCommunication.pdf

NewScientist. (2006). Keep your fingers out of my accounts. Retrieved April, 2011, from http://www.newscientist.com/article/mg19225745.600-keep-your-fingers-out-of-my-accounts.html

Reavley, N. (2005). Secure online banking. Card Technology Today, 17(10), 12-13.

RSA. (2010). RSA 2010 global online consumer security survey. Retrieved April, 2011, from www.rsa.com/.../consumer/.../10665_CSV_WP_1209_Global.pdf

RSA. (n.d.). Two-factor authentication. Retrieved April, 2011, from http://www.rsa.com/glossary/default.asp?id=1056

Rural Bank Limited. (2010). Rural Bank to become wholly owned subsidiary of Bendigo and Adelaide Bank. Retrieved April, 2011, from http://ruralbank.com.au/about-us/news/2010/article/964

St.George Bank Limited. (n.d.). About us. Retrieved April, 2011, from http://www.stgeorge.com.au/about-stgeorge/overview/about-us

Steinfield, C. (2002). Understanding click and mortar e-commerce approaches: A conceptual framework and research agenda. Journal of Interactive Advertising, 2(2), 1-10.

Suncorp-Metway Limited. (n.d.). Automatic lock-out. Retrieved April, 2011, from http://www.suncorpbank.com.au/security/how-we-protect-you

the Australian Bankers Association (ABA). (2010). ABA members. Retrieved April, 2011, from http://www.bankers.asn.au/Members/default.aspx

the National Office for the Information Economy (NOIE), et al. (1999). Banking on the Internet: A Guide to Personal Internet Banking Services. Retrieved April, 2011, from http://www.archive.dcita.gov.au/1999/08/banking

Usonlinebiz. (2008). Types of Internet banking and security threats Retrieved April, 2011, from http://www.usonlinebiz.com/article/Types-of-Internet-Banking-and-Security-Threats.php

VeriSign Authentication Services. (n.d.-a). Two-factor authentication. Retrieved April, 2011, from http://www.verisign.com/authentication/two-factor-authentication/index.html

VeriSign Authentication Services. (n.d.-b). FAQ: Extended validation SSL. Retrieved April, 2011, from http://www.verisign.com.au/ssl/ssl-information-center/extended-validation-ssl-certificates/?

Victoria Teachers Credit Union. (n.d.). Internet banking security. Retrieved April, 2011, from www.victeach.com.au/.../Internet%20Banking%20Security-8887a5b5-89b9- 4eba-a059-a24beacf5a66-0.pdf