WALAILAK JOURNAL
http://wjst.wu.ac.th Information Technology

An Investigation of Internet Banking Security of Selected Licensed Banks in Vietnam

Panida SUBSORN[1] and Sunsern LIMWIRIYAKUL[2,*]

[1]*School of Information Technology, Suranaree University of Technology, Nakorn Ratchasima 30000, Thailand*
[2]*SECAU, Edith Cowan University, Joondalup 6027, Western Australia*

([*]Corresponding author's e-mail: s.limwiriyakul@ecu.edu.au)

Received: 23 December 2014, Revised: 5 June 2015, Accepted: 27 July 2015

Abstract

Currently, most Vietnamese banks provide internet banking services to customers. These services may include internet banking, online trading, and mobile banking. One critical aspect of internet banking is security. Confidentiality, integrity, and privacy are important elements for secure internet banking. This paper makes a comparative study of internet banking security features provided by the 22 selected licensed Vietnamese banks. The objective of the analysis was to improve the existing internet banking information security checklist (Version 1.05) and make it a more realistic and comprehensive international guideline. Results identified a lack of related internet banking security information on internet banking websites of all 22 selected licensed Vietnamese banks. Lack of security information by banks can impact negatively to the provision of confidentiality by the selected banks which may ultimately lead to a general reduction of trust from their current and potential internet banking customers.

Keywords: Customer perspective, internet banking information security checklist, internet banking security, personal internet banking, Vietnam

Introduction

Since economic renovation in 1986 in Vietnam (the promulgation of Doi Moi), over the past few decades Vietnam Gross Domestic Product (Vietnam GDP) has achieved steady success [1]. In terms of their banking system, Vietnam underwent a restructure. It opened up to foreign investment (joint venture) and allowed partial ownership by the private sector [2]. Furthermore, in 2011, Asia Focus stated that "Vietnam's banking sector is expected to have one of the highest growth rates in Asia during the next few years" [2]. Traditional banks systems in Vietnam required physical presence at the banks. As the banks provide their online service, features are offered based on the banks evaluation of security. This research is to offer banks an independent expert evaluation of their websites. In this regard, ScienceNetwork Western Australia (SNWA) has evaluated the checklist (1.0) and found the research to be valid in terms of authentication and encryption [3]. Vietnamese banks provide a wide range of banking services including traditional banking, telephone banking, internet banking, mobile banking as well as online trading in Vietnam. Vietnam's online banking systems are emerging and catching up to the rest of the world.

The country has a 4-tier banking system with (1) State-Owned Commercial Banks (SOCBs), (2) Joint Stock Commercial Banks (JSCBs), (3) Joint Venture Banks, and (4) Wholly Foreign-Owned Banks [2]. There were a total of 44 banks at the time of collection, 22 of which were selected as they offer internet banking technology to customers.

Internet banking technology provides customers with the advantages of flexibility and convenience which allows them to do their daily banking anytime without visiting the banks. These advantages can increase bank customer satisfaction [4]. Nevertheless, important factors such as threats, risks, and confidentiality concerns can reduce internet banking usage in both current and potential internet banking customers [5-10]. This is due to the fact that this issue impacts on the confidentiality, privacy, and integrity of internet banking customers [5-9,11,12].

The aim of this paper was to examine the security of internet banking facilities available to the internet banking customers of the 22 selected licensed Vietnamese banks through the use of the internet banking information security checklist (Version 1.06) criteria.

Furthermore, the internet banking information security checklist was developed after a gap in the security of online banking systems was identified. Since its inception, it has undergone a number of enhancements (Versions 1.01 to 1.06) in keeping with new developments in online banking usage trends. Historically, data sets were collected from the selected banks across several countries including Australia, Thailand, Hong Kong, Mainland China, and Vietnam. The details of the internet banking information security checklist have been modified or adapted to suit the data collected each time and is backward compatible. The current version (1.06) is therefore applicable to all previously collected data sets. However, it can also be used to audit other banks around the world. A list of selected countries and associated banks are displayed in **Table 1**.

Table 1 Checklist version development.

Version	Country	Type of Bank	Total selected banks
1.01 [5]	Australia	Major, corporate and sub banks	16
1.02 [6]	Thailand	Commercial	14
1.03 [7]	Australia	Foreign subsidiary banks	9
1.04 [9]	Hong Kong	Licensed	19
1.05 [8]	Mainland China	English support website	13
1.06	Vietnam	Stated-Owned and Commercial	22

The rest of the paper is organized into 3 main sections which are (1) materials and methods, (2) results and discussion, and (3) conclusion.

Materials and methods

The comparative analysis method was used to discover differences in internet banking security features between the 22 selected licensed Vietnamese banks. The results are presented in 2 main tables (1) **Table 5** A summary of the refined internet banking security checklist and (2) **Table 6** A summary comparison information between the 22 selected licensed Vietnamese banks.

Data sample and collection

There are a total of 46 3-tier banks in Vietnam [2], 22 of which were selected for this paper. These banks all provide internet banking facilities to their customers, whereas the remaining banks either do not provide the same, or support internet banking facilities in native Vietnamese only. Although Wholly-Owned Foreign Banks operate in Vietnam as well, they have been excluded from this investigation. The 22 selected licensed Vietnamese banks showed similarities in delivery of their banking websites including online or internet banking sections in English to their customers. In addition, data sources used in this analysis were collected solely from the websites of the selected banks. **Table 2** presents the list of these 22 selected licensed Vietnamese banks.

Table 2 The list of the 22 selected licensed Vietnamese banks.

Abbreviation	Bank name
ABBANK	An Binh Commercial Joint Stock Bank
BIDV	Joint Stock Commercial Bank for Investment and Development of Vietnam
DongA Bank	DongA Joint Stock Commercial Bank
Vietnam Eximbank	Vietnam Export Import Commercial Joint-Stock Bank
HDBank	Ho Chi Minh Development Joint Stock Commercial Bank
IVB	Indovina Bank Limited
LienVietPostBank	Lien Viet Post Joint Stock Commercial Bank
MDB	Mekong Development Joint Stock Commercial Bank
Maritime Bank	Vietnam Maritime Commercial Joint Stock Bank
OCB	Orient Commercial Joint Stock Bank
PG Bank	Petrolimex Group Commercial Joint Stock Bank
Sacombank	Saigon Thuong Tin Commercial Joint Stock Bank
SAIGONBANK	Saigon bank for Industry and Trade
SeABank	Southeast Asia Joint Stock Commercial Bank
SHB	Saigon - Hanoi Commercial Joint Stock Bank
Techcombank	Vietnam Technological and Commercial Joint Stock Bank
VIB	Vietnam International Commercial Joint Stock Bank
VID Public Bank	VID Public Bank
Vietcombank	Joint Stock Commercial Bank for Foreign Trade of Vietnam
VietinBank	Vietnam Joint Stock Commercial Bank for Industry and Trade
VPBank	Vietnam Prosperity Joint-Stock Commercial Bank
VRB	Vietnam - Russia Joint Venture Bank

All data relating to the internet banking websites of the 22 selected licensed Vietnamese banks were collected and analyzed during the period between March and July of 2014.

The refined internet banking information security checklist

Full details of the refinement of the internet banking information security checklist (Version 1.06) used in this analysis are presented in **Table 5**. The checklist has 6 main security feature categories, with a seventh for a multi-language support feature as a further item of comparison of the 22 selected licensed Vietnamese banks.

Data collection is based on product feature analysis of hardware or software offerings. As a refinement of the previous checklist from Versions 1.01 - 1.05, the categories of data collection were identified and expanded to reflect the dynamic nature of features on offer.

The following are some examples of the changing of the features of the checklists from Versions 1.02 - 1.06.

Version 1.02: (1) under sub-category internet banking application security features “notifications and alerts for login information” feature was added and (2) a languages category was added.

Version 1.03: (1) under sub-category user site authentication technology (password restriction/requirement) “cannot have 3 or more of the same characters in a row (e.g. aaa, 111)” and “cannot have 3 or more consecutive characters (e.g. abc, 123)” features were added and (2) under sub-category session management “cookie not in use” feature was removed.

Version 1.04: (1) under sub-category software and system requirements and settings information based on bank website information (free/paid security software/tool/information available to personal internet banking customers) “other services (e.g. automated tool, online security scanning)” feature was added, (2) under sub-category user site authentication technology (logon requirement) “bank/credit cards number or bank register/customer ID or email address” feature was separated into 2 features which are

bank/credit card/customer ID/email, and registered bank username (characters), and (3) under sub-category transaction verification for external or sensitive transaction (e.g. unregistered 3rd party account, BPAY) "others (e.g. USB key digital certificate)" feature was added.

Version 1.05: (1) under sub-category internet banking user device system and browser setting requirement "hardware device" feature was added, (2) under sub-category transaction verification for external or sensitive transaction (e.g. unregistered 3rd party account, BPAY) "password/extra password/reserved verification info./CAPTHCA" feature was added, and (3) under languages category "fully support other common language(s)" and "partly support other common language(s)" features were added.

Version 1.06: (1) under sub-category general online security and privacy information to the internet banking customers (losses compensation guarantee) "no responsibility" feature was added, (2) under sub-category transaction verification for external or sensitive transaction (e.g. unregistered 3rd party account, BPAY) email was added to the "password/extra password/reserved verification info./CAPTHCA", and (3) under sub-category limited default daily transfer amount to sensitive transaction (e.g. unregistered 3rd party and international accounts) "the default maximum daily transfer limit is variable dependent on the type of the internet banking customers" feature was added.

The 7 categories

The security features are classed into 6 main categories and one sub-category. The details of each category are described below.

Category 1: Provision of general online security and website privacy information to internet banking customers. It is divided into 4 sub-categories which are, account aggregation or privacy and confidentiality, losses compensation guarantee, online/internet banking security information, and bank security mechanism system information. The details are as follows:

1) Account aggregation or privacy and confidentiality

This sub-section examines the current privacy and confidentiality policy and its compliance with the privacy law and act as well as national privacy principles to ensure integrity of the internet banking customers' confidential information. It also covers the banks compliance with any legal or regulatory obligations in terms of use and disclosure;

2) Losses compensation guarantee

This sub-section inspects the banks' current guarantee policy and whether any compensation guarantee is provided by the banks. This is in relation to any losses caused by unauthorized access or misuse by unauthorized users other than the internet banking customers. It deals with the level and percentage of the compensation guarantees;

3) Online/internet banking security information

This sub-section identifies the amount and level of online/internet banking security information provided on websites by the banks to their internet banking customers. General online security guidelines, password security tips, internet banking threats, viruses and Trojans as well as security alerts/up-to-date issues are examples of this sub-section; and

4) Bank security mechanism system information

This sub-section is a discovery of information relating to website security mechanisms employed by banks to protect their websites and internet banking customers. Examples are the firewall system, the alert or intrusion detection system, the data encryption system and the patching system. Information such as this, serves to enhance privacy and confidentiality for both current and potential internet banking customers.

Category 2: IT assistance, monitoring, and support. It examines the IT assistance, monitoring, and support options available to the internet banking customers of each bank. The 2 sub-categories deal with the services provided by the banks for hotline/helpdesk service availability for personal internet banking customers and internet banking transaction monitoring by the banks. The details are as follows:

1) Hotline/helpdesk service availability for personal internet banking customers

This sub-category identifies the types of communication channels provided by the bank to internet banking customers. Examples are hotline service, secure email message box, Frequently Asked Questions (FAQ), online support form; and

2) Internet banking transaction monitoring by the banks

This sub-category determines whether the bank offers their own dedicated team and technology for monitoring all internet banking transactions particularly with respect to the detection of suspicion transactions.

Category 3: Software and system requirements and settings information based on the bank website information. It is comprised of 3 sub-categories as follows:

1) Compatibility "best" with the popular internet browsers

This sub-category examines whether the bank's website is compatible with or supports a wide range of the world's popular internet browsers such as Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, Netscape, Opera, and Safari;

2) Provision of information of internet banking user device system and internet browser setting requirements

This sub-category is concerned with information provided by the banks to their internet banking customers with regard to setting requirements for optimum usage of their internet banking system. These requirements relate to hardware device specifications, operating system, internet browser setting, screen resolution, including automatically or manual internet browser detection features; and

3) Free/paid security software/tool/information available to personal internet banking customers

This sub-category lists any free or paid security tools and/or information, web links provided by the banks to their internet banking customers in order to minimize any potential risks to customers' personal computers. The security tools are wide, ranging from simple anti-virus scanning to advanced personal firewall scanning tools. Other services such as automated scanning tools and security applet controls are also identified.

Category 4: Bank site authentication technology. This is concerned with the identification of current authentication technology used by the banks for internet banking customer verification. It is based on the level of Secure Sockets Layer (SSL) encryption employed by the banks such as 256-bit, 168-bit, and 128-bit SSL encryption types. It also covers Extended Validation (EV) SSL certificates and valid Certificate Authority (CA).

Category 5: User site authentication technology. This involves the identification of the technology used by the banks to authenticate current internet banking customers. It consists of the following 5 sub-categories:

1) Logon requirement

This sub-category details the logon requirements of the internet banking systems of the banks. Typically, internet banking logon requirements can include 2 or more identifiers. The first and second identifiers are what both the banks and their internet banking customers know or agree on, such as bank/credit card/customer Identification (ID)/email, and registered bank username and password/ Personal Identification Number (PIN)/security number. Other remembered type of logon identifiers such as additional password or secret question may also be incorporated into the logon requirements.

Furthermore, some banks may increase their security level by introduction of digital certificate related technologies into logon requirements. For example, using smart ID card, e-wallet with digital certificate embedded, e-banking code card or document certificate instead of typical bank or credit card number [13].

Other input verification methods like a Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) are also incorporated as part of logon requirement by some banks.

In addition, some banks have also included 2-factor authentication technology as an additional security layer, or have incorporated it into its internet banking logon requirement. Token and mobile phone with Short Message Service (SMS) capable devices are well-known examples of the 2-factor authentication technology;

2) Logon failure limitation

This sub-category details the logon failure limitation of internet banking based on information provided on the banks' websites. Monitoring of the number of sequentially unsuccessful login attempts allowed by the banks before lockout or disabling of internet banking accounts of customers is done;

3) Logon user input type

This sub-category identifies the internet banking system's logon user input type. Usually, the logon user input type requires input information from internet banking customer's keyboard. Some banks provide an alternative logon input type such as a virtual keyboard. The virtual keyboard is usually software based cryptography [14]. It may also include a scrambling feature. However, some banks incorporate a virtual keyboard with a traditional physical keyboard for internet banking logon;

4) Password restriction/requirement

This sub-category determines the password restrictions as well as requirements on internet banking accounts. Examples of restrictions and requirements are the password length, combination of numbers and letters, case sensitivity, use of special characters, different passwords as compared to any of 3 previously used ones, use of 2 or more consecutive identical characters, use of 3 or more consecutive characters, and automatic checking of password strength when creating or changing passwords. Enforcement of good password practice is also investigated in this category; and

5) Transaction verification for external or sensitive transaction (e.g. unregistered third party account, BPAY)

This sub-category investigates whether any type of verification methods are required when internet banking customers process their internet banking transactions, especially when dealing with external transactions such as BPAY. Typically tokens, SMS, Universal Serial Bus (USB) digital certificate with PIN, Public Key Infrastructure (PKI) token-CA, CAPTCHA, and passwords are some examples of verification methods.

Category 6: Internet banking application security features. The following 5 sub-categories of security features of the banks' internet banking applications are investigated at this point:

1) Automatic timeout feature for inactivity internet browser

This sub-category discovers the default automatic timeout setting limit for inactivity during the internet banking session;

2) Limited default daily transfer amount to sensitive transaction (e.g. unregistered third party and international accounts)

This sub-category discovers the default daily transfer amount limitation, when internet banking customers transfer money locally and globally. This sub-category also investigates whether the default daily transfer amount limit can be changed by the banks or by the internet banking customers.

3) Logging information and alert

This sub-category identifies logging and alert information provided by the banks' internet banking websites. Last login, activity log, or transaction history are some examples of logging information. With regard to alert features, some banks may provide this via email and/or messaging (SMS) technologies to internet banking customers.

4) Password policy management

This sub-category validates the frequency of the banks' password policy imposes changes to the internet banking customers login passwords such as enforcing a password change every 3 months.

5) Session management

This sub-category investigates the internet banking session management which includes the use of page or session tokens as well as use of cookies. This sub-category also investigates session management by the banks in relation to the use of cookies for other purposes unnecessary for internet banking. Examples are capturing Internet Protocol (IP) addresses, marketing, research, and statistics. In addition, this sub-category also investigates whether the banks provide automated feature to clear cookie information on internet browser after customer logoff or shut down of internet browser.

Category 7: Languages. This additional category examines whether the banks' websites provide full support for other common languages such as English.

The scoring technique

To provide a practical and comprehensive guideline, each main category was assigned a weight rating based on its importance according to current knowledge and best practice.

For example, Sub-category 5.3 Logon user input type has an assigned score of 10. The scoring details of each feature are based on the scoring format of **Table 3**. Dynamic scrambled virtual keypad was assigned the highest score (10) as compared to the other features. This is due to the fact that it offers better security than the other 2 (combination of virtual keypad and keyboard, and keyboard only) options. The dynamic scrambled virtual keypad is automatically generated with a scrambled key feature each time an internet banking customer accesses or opens the internet banking website's login page. Furthermore, the dynamic scrambled virtual keyboard may move on the screen during the login period. This moving technique will further enhance its security level against any potential information intercept or capture by spyware, malware software or autobot.

Table 3 Example assigned score to sub-category feature.

Sub-category feature	Threats	Potential risk	Assigned score
Dynamic scrambled virtual keypad with/without keyboard	Key-logger, spyware and malicious bots [15,16]	Lowest	10/10
Combination of virtual keypad and keyboard	Key-logger, spyware, malicious bots, click based screenshot capturing [15,16]	Low	8/10
Keyboard only	Key-logger, spyware , malicious bots, click based screenshot capturing [15,16]	Low/medium	7/10

Furthermore, each main category consists of sub-categories as well as their subsets. The total score of the combined categories is 200 points. The main Category 5 (user site authentication technology) was assigned the highest feasible score of 60 out of 200. This was due to the fact that the logon authentication feature was determined to be attack prone and therefore paramount in relation to a secure internet banking experience [17].

The scoring technique of all categories is detailed as follows:

Category 1 has 4 sub-categories. Each sub-category has a score value of 5 making a total of 20;

Category 2 has 2 sub-categories. Sub-categories 2.1 and 2.2 have a score value of 10 for a total of 20;

Category 3 has 3 sub-categories. Each sub-category was assigned a score value 5, which represents a total of 15;

Category 4 has a total score value of 35 for the employment of encryption and digital certificate technologies. This category is in turn comprised of 4 small sub-categories which are 256-bit SSL encryption, 128/168-bit SSL encryption, extended validation SSL certificates and signing CA.

Assignment of score values is based on the level of its security with regard to current trends. The sub-category 256-bit SSL encryption is assigned a score value of 20 whereas 128/168-bit SSL encryption was assigned a score value of 15. This is due to the fact that 256-bit SSL encryption has higher encryption bits in comparison to 128/168-bit SSL encryption. Extended validation SSL certificates and signing CA were each allocated a score value of 7.5;

Category 5 has a total score value of 60, which is the highest among the group. It has 5 sub-categories as described earlier. A score value of 15 is assigned to both logon requirement and transaction verification for external or sensitive transaction categories whereas the other 3 remaining categories (logon failure limitation, logon user input type, and password restriction/requirement) are assigned a score value of 10.

The reason that both logon requirement and transaction verification for external or sensitive transaction categories are allocated higher scores, is due to their high security impact to internet banking [17].

Category 6 consists of 5 sub-categories as described earlier. It has a total high score value of 50. With regard to internet banking security, this category is considered important as it covers aspects of internet banking application security features as mentioned above. Each sub-category is assigned a score value of 10; and

Category 7 has no score. It is only based on the features being offered or not. It consists of 3 sub-categories which are support for local language; full and partial support of other common languages.

More details of all categories are presented in **Table 5**.

Limitations

There were limitations to collecting internet banking website data of the 22 selected licensed Vietnamese banks. This was due to the fact that all data was obtained directly from the banks' websites (in English language) as a non-customer. Therefore, some internet banking security features such as logon failure limitations, password restriction/requirements, automatic timeout feature for internet browser inactivity could not be collected or audited. Furthermore, some existing internet banking security mechanisms not presented on the banks' websites but possibly in use, were not discovered. Antivirus and firewall systems normally widely used in corporations, particularly in the banking industry to protect against virus and hacker attacks were not determined. As a result, the average checklist score of the banks may result in lower than actual values.

Results and discussion

The coding technique used is described in **Table 4**, whereas **Table 5** displays and concludes the analysis and findings on internet banking security for the 22 selected licensed Vietnamese banks. **Table 6** displays a summary of comparative information between these selected banks. Further discussions of all the results and findings are also explained later.

Table 4 Coding technique.

Code	Represents
✓	Yes
*	Optional
A	AES 256-bit SSL encryption
C	Conditional
D	3DES-EDE-CBC 168-bit SSL encryption
E	English
G	GlobalSign Authentication CA
N	Entrust CA
R	RC4 128-bit SSL encryption
U	Russian language
V	VeriSign Authentication CA

Table 5 A summary of the refined internet banking information security checklist.

The refined internet banking information security checklist (Version 1.06)																									
		Vietnamese banks																							**Weights**
	Security feature categories	**ABBANK**	**BIDV**	**DongA Bank**	**Vietnam Eximbank**	**HDBank**	**IVB**	**LienVietPostBank**	**MDB**	**Maritime Bank**	**OCB**	**PG Bank**	**Sacombank**	**SAIGONBANK**	**SeABank**	**SHB**	**Techcombank**	**VIB**	**VID Public Bank**	**Vietcombank**	**VietinBank**	**VPBank**	**VRB**	
1. Provision of general online security and website privacy information to the internet banking customers (20 points)																									
1.1	Account aggregation or privacy and confidentiality																								5
1.1.1	Complied with the National Privacy Principles and the Privacy Act			✓	✓				✓				✓					✓				✓			5
1.1.2	No information	✓	✓			✓	✓	✓		✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓		0
1.2	Losses compensation guarantee																								5
1.2.1	100% or with condition				C				C									✓	C	C					5
1.2.2	No responsibility																								0
1.2.3	No information	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓				✓	✓	✓		0
1.3	Online/internet banking security information																								5
1.3.1	General online security guidelines								✓	✓	✓						✓	✓			✓				1
1.3.2	Provides password security tips				✓				✓	✓	✓		✓	✓			✓	✓							1
1.3.3	Threats: Hoax email, scam, phishing, spyware								✓	✓							✓								0.5
1.3.4	Trojan and virus/malicious programs								✓								✓	✓							0.5
1.3.5	Key loggers																✓								0.5
1.3.6	Security alert/up-to-date issue								✓																1
1.3.7	Others (e.g. mobile phone, wireless)								✓								✓	✓							0.5
1.3.8	No information	✓	✓	✓		✓	✓	✓				✓			✓	✓			✓	✓		✓	✓		0
1.4	Bank security mechanism system information																								5
1.4.1	Antivirus/phishing or security scanning protection software/system			✓	✓				✓								✓			✓					1.25
1.4.2	Firewall(s) filtering system								✓								✓								1.25
1.4.3	Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)/alert/monitoring system								✓																1.25
1.4.4	Others (e.g. Operation System (OS) patching, data encryption, password protected, physical security, regular audit and backup)								✓								✓								1.25
1.4.5	No information	✓	✓			✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓		0
2. IT assistance, monitoring, and support (20 points)																									
2.1	Hotline/helpdesk service availability for personal internet banking customers																								10
2.1.1	24/7 customer contact center by phone OR	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓		5
2.1.2	No 24/7 customer contact center by phone				✓						✓				✓										3
2.1.3	Secured email/message box OR	✓		✓	✓	✓			✓	✓						✓		✓				✓			3
2.1.4	Email	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓			1
2.1.5	Demo/FAQ/user guide /feedback/online support form		✓	✓	✓	✓		✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓		✓	✓		2
2.1.6	No information																								0
2.2	Internet banking transaction monitoring by the banks																								5
2.2.1	Provides dedicated team and technology for monitoring all transactions																								10
2.2.2	No information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		0
3. Software and system requirements and settings information based on the bank website information (15 points)																									
3.1	Compatibility “best” with the popular internet browsers																								5
3.1.1	Google Chrome		✓				✓		✓	✓	✓						✓					✓			1
3.1.2	Mozilla Firefox		✓		✓		✓		✓	✓	✓						✓		✓			✓			1
3.1.3	Microsoft Internet Explorer		✓		✓		✓		✓	✓	✓						✓		✓			✓			1
3.1.4	Netscape/Opera		✓								✓						✓								1
3.1.5	Safari										✓						✓								1
3.1.6	No information	✓		✓		✓		✓				✓	✓	✓	✓	✓		✓		✓	✓		✓		0
3.2	Provision of information of internet banking user device system and internet browser setting requirements																								5
3.2.1	Hardware device																								1
3.2.2	Operating system		✓						✓	✓															1
3.2.3	Type of browser and setting (e.g. cookie, java, certificate)						✓		✓								✓		✓						1
3.2.4	Screen resolution										✓											✓			1

The refined internet banking information security checklist (Version 1.06)																									
	Security feature categories	Vietnamese banks																							Weights
		ABBANK	BIDV	DongA Bank	Vietnam Eximbank	HDBank	IVB	LienVietPostBank	MDB	Maritime Bank	OCB	PG Bank	Sacombank	SAIGONBANK	SeABank	SHB	Techcombank	VIB	VID Public Bank	Vietcombank	VietinBank	VPBank	VRB	
3.2.5	Browser automatic or manual test feature available																	✓						1
3.2.6	No information	✓		✓	✓	✓		✓				✓	✓	✓	✓	✓		✓		✓	✓		✓	0
3.3	Free/paid security software/tool/information available to personal internet banking customers																							5
3.3.1	Antivirus/anti-spyware/anti-phishing					✓																		1
3.3.2	Internet security suite OR					✓																		2
3.3.3	Provides internet information/links to security software vendor(s) (e.g. antivirus, personal firewall)								✓								✓							2
3.3.4	Other services (e.g. automated tool, online security scanning tool, security applet control)																							2
3.3.5	No service and/or information	✓	✓	✓	✓		✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	0
4. Bank site authentication technology (35 points)																									
4.1	Employed encryption and digital certificate technologies																							35
4.1.1	256-bit SSL encryption OR	A			A		A	A	A															20
4.1.2	128/168-bit SSL encryption		R	R		D				R	R	R	A	D	R	R	R	A	A	R	R	A	R	15
4.1.3	Extended validation SSL certificates	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓		✓	✓	✓	✓	7.5
4.1.4	Signing CA	G	G	V	V	V	V	V	V	V	G	V	V	V	V	V	V	G	N	V	V	V	V	7.5
4.1.5	No information																							0
5. User site authentication technology (60 points)																									
5.1	Logon requirement																							15
5.1.1	Bank/credit card/customer ID/email OR		✓	✓					✓				✓											2
5.1.2	Registered bank username (characters) OR	✓			✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	3
5.1.3	Smart ID card/e-wallet with digital certificate embedded/e-banking code card/document certificate																							4
5.1.4	Password/PIN/security number	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	3
5.1.5	Additional password or secret question OR																							3
5.1.6	Others (e.g. CAPTCHA)				✓		✓	✓		✓	✓	✓	✓		✓	✓			✓	✓		✓		2
5.1.7	One-Time Password (OTP): Two-factor authentication/dynamic password card/USB key digital certificate/SMS (min. 6 digit PINs)								✓					✓			✓	✓	*					5
5.1.8	No information																							0
5.2	Logon failure limitation																							10
5.2.1	Standard max. (3 times) OR			C	✓		✓		✓								✓		✓		✓			10
5.2.2	Max. more than 3 times OR																	5		5				8
5.2.3	In use but does not specific max. number of failure allowed																					✓		5
5.2.4	No information	✓	✓			✓		✓		✓	✓	✓	✓	✓	✓	✓							✓	0
5.3	Logon user input type																							10
5.3.1	Dynamic scrambled virtual keypad with/without keyboard OR		*	✓			*																	10
5.3.2	Combination of virtual keypad and keyboard OR				*					*	*	*	*				*		*		✓	*		8
5.3.3	Keyboard only	✓				✓		✓	✓					✓	✓	✓		✓		✓			✓	7
5.4	Password restriction/requirement																							10
5.4.1	Enforce good password practice													✓										2
5.4.2	Password/PIN length (min. 8 characters length)				6					4+				8			4-8		7-20	6-20				1
5.4.3	Numbers only OR																							0
5.4.4	Combination of numbers and letters				✓									✓			✓		✓	✓				1
5.4.5	Combination of upper and lower cases													✓			✓			✓				1
5.4.6	Special characters																			✓				1
5.4.7	Different passwords as compared to any of 3 previous used passwords													✓										1
5.4.8	No 2 or more consecutive identical characters (e.g. aa, 11)																							1
5.4.9	No 3 or more consecutive characters (e.g. abc, 123)																							1
5.4.10	Automatic password strength check on creation or change of password																							1

The refined internet banking information security checklist (Version 1.06)																									
	Security feature categories	Vietnamese banks																							Weights
		ABBANK	BIDV	DongA Bank	Vietnam Eximbank	HDBank	IVB	LienVietPostBank	MDB	Maritime Bank	OCB	PG Bank	Sacombank	SAIGONBANK	SeABank	SHB	Techcombank	VIB	VID Public Bank	Vietcombank	VietinBank	VPBank	VRB	
5.4.11	No information	✓	✓	✓		✓	✓	✓	✓		✓	✓	✓		✓	✓		✓			✓	✓	✓	0
5.5	Transaction verification for external or sensitive transaction (e.g. unregistered third party account, BPAY)																								15
5.5.1	OTP: Token device/dynamic password OR			✓	✓	✓				✓			✓	✓	✓		✓	✓	✓	✓		✓		15
5.5.2	OTP: SMS (no. of digit PINs) OR			✓	✓	✓	✓		✓	✓			✓	✓	✓	✓		✓	✓	✓	✓	✓		15
5.5.3	Others (e.g. USB key digital certificate with PIN, PKI token-CA) /passcode authentication card/ Europay, MasterCard and Visa (EMV) AND/OR				✓		✓																	15
5.5.4	Password/extra password/reserved verification info./CAPTCHA/email			✓		✓										✓			✓		✓	✓		10
5.5.5	No requirement																							0
5.5.6	No information	✓	✓					✓			✓	✓											✓	0
6. Internet banking application security features (50 points)																									
6.1	Automatic timeout feature for inactivity internet browser																								10
6.1.1	Max. (less than or equal 15 mins) OR								10	5								15						10
6.1.2	In use but does not specify timeout length																✓		✓					8
6.1.3	No information	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓				✓	✓	✓	✓	0
6.2	Limited default daily transfer amount to sensitive transaction (e.g. unregistered third party and international accounts)																								10
6.2.1	Less or up to Vietnamese Dong (VND) 100,000,000 (~ 4,600 US Dollar) OR						✓		✓	✓				*					✓	✓	✓	✓		5
6.2.2	More than VND 100,000,000			✓	✓												✓					C		4
6.2.3	The default maximum daily transfer limit may be increased with the approval by the banks								✓															2
6.2.4	The default maximum daily transfer limit may be decreased by an internet banking customer								✓	✓														2
6.2.5	The default maximum daily transfer limit is variable dependent on the type of the internet banking customers			✓			✓		✓						✓					✓		✓		1
6.2.6	No information	✓	✓			✓		✓			✓	✓	✓			✓		✓					✓	0
6.3	Logging information and alert																								10
6.3.1	Last login									✓														4
6.3.2	Activity log/transaction history				✓	✓	✓		✓	✓									✓	✓	✓	✓		3
6.3.3	Alert available via email and/or SMS			✓			✓			✓					✓				✓	✓				3
6.3.4	No information	✓	✓					✓			✓	✓	✓	✓		✓	✓	✓					✓	0
6.4	Password policy management																								10
6.4.1	Frequently enforce changing login password (no more than 6 months)																		✓					10
6.4.2	Frequently enforce changing login password (more than 6 months)																							7
6.4.3	No information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	0
6.5	Session management																								10
6.5.1	Use of page or session tokens OR																	✓						10
6.5.2	Use of cookie technology																✓			✓				7
6.5.3	Use of cookie for other purposes (e.g. capturing IP address, marketing, research and/or statistics)																							0
6.5.4	No information	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓		✓	✓	✓	0
7. Languages (no points)																									
7.1	Employed multi-languages																								
7.1.1	Support local language	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
7.1.2	Fully support of other common language(s) OR				E		E		E						E								E	
7.1.3	Partially support of other common language(s)	E	E	E		E		E		E	E	E	E	E		E	E	E	E	E	E	E	U	

Provision of general online security and website privacy information to the internet banking customers

In terms of privacy compliance with Vietnam legal regulations, only 6 (DongA Bank, Vietnam Eximbank, MDB, Sacombank, VIB, and VPBank) of the 22 selected licensed Vietnamese banks displayed information on their internet websites. The majority of the 22 selected licensed Vietnamese banks (17) did not provide any information in relation to liability for any claim, loss, or damage with regard to using internet banking services. Only one (VIB) of the 5 banks provided a 100 percent guarantee without conditions, to internet banking customers, whereas the 4 remaining banks provided guarantees with conditions. More details are found in **Table 5** in Sections 1.1 and 1.2.

The majority of these selected banks provided little to none of either online/internet banking security or bank security mechanism system information on websites apart from MDB and Techcombank. These 2 banks provided useful information on general internet security as well as their banking security mechanism system on their websites. **Table 5** Sections 1.3 and 1.4 list more details.

In addition, only 2 banks (Vietnam Eximbank and MDB) scored over 50 percent (10 marks) of overall score in terms of providing general online security and website privacy information to the internet banking customers. The majority of the remaining banks scored less than half or were scoreless. See **Table 6**, Category 1 for more details.

IT assistance, monitoring, and support

The majority of the banks (19) provided 24/7 customer contact center phone support, whereas the remaining 3 banks provided non 24 h telephony support to their internet banking customers. Several types of IT assistance and support such as demonstration (demo), FAQ, forum, email were provided by most banks. No information with regard to internet banking transaction monitoring, was provided by any of the selected banks. For more details see Sections 2.1 and 2.2 of **Table 5**.

Overall, 15 of the 22 selected licensed Vietnamese banks scored poorly (below 10 marks or 50 percent). All of the banks scored nil in relation to information provision about dedicated team and technology for monitoring all transactions of their internet banking customers on websites. **Table 6**, Category 2 lists more details.

Software and system requirements and settings information based on the bank website information

Nine of the 22 selected licensed Vietnamese banks provided some information about software and system requirements on their websites whereas the remaining banks provided none. In terms of free/paid security software/tool/information available to personal internet banking customers, only 3 (HDBank, MDB, and Techcombank) banks provided such tools (antivirus or personal firewall) or internet links for them to its internet banking customers. See Sections 3.1, 3.2, and 3.3 of **Table 5** for more details. Furthermore, only one (Techcombank) of the 22 selected licensed Vietnamese banks scored more than half (50 percent) whereas more than half of the selected banks (12) achieved any score at all. See scoring details in **Table 6**, Category 3.

Bank site authentication technology

Five (ABBANK, Vietnam Eximbank, IVB, LienVietPostBank, and MDB) of the 22 selected licensed Vietnamese banks employed 256-bit SSL encryption (currently highest SSL encryption) [18,19], whereas the remaining 17 banks employed 128-bit SSL encryption. With regard to extended validation SSL certificate, the majority of the banks deployed the technology apart from 3 (Maritime Bank, Techcombank, and VID Public Bank) which deployed standard SSL certificate. More details are shown in Section 4.1 of **Table 5**.

The overall majority of the 22 selected licensed Vietnamese banks performed well in this section. Five of the 22 selected licensed Vietnamese banks scored full marks or 100 percent whereas 14 of the remaining banks scored 33 or 94 percent. **Table 6**, Category 4 presents the overall scores.

User site authentication technology

In terms of login, the majority (18) of the 22 selected licensed Vietnamese banks required their internet banking customers to use a registered login account or ID instead of a standard bank account number. More than half (12) of the 22 selected licensed Vietnamese banks required CAPTCHA as an additional security field to both login ID and password. Furthermore, 5 out of the 22 selected licensed Vietnamese banks also required a One-Time Password (OTP) for website login. For example, Techcombank provided an OTP security token device (Rivest, Shamir, Adleman (RSA) algorithm) for their internet banking customers. The customer was required to login with a login ID and password as a first step. Next, a 6 digits number from the registered OTP security token device (provided by the banks) has to be entered to continue. Alternatively, the SAIGONBANK provided either SMS or a security token device to the internet banking customers. Section 5.1 of **Table 5**, provides overall login details of all the 22 selected licensed Vietnamese banks.

With regard to login failure limitation, 6 of the 22 selected licensed Vietnamese banks provided information on their websites as to the maximum login failure limit of 3 attempts. Two of the remaining banks allowed the login failure limit to 5 times. The majority of the banks provided no login failure limitation information on their websites. See Section 5.2 of **Table 5** for more details.

In relation to logon user input type, only 3 of the 22 selected licensed Vietnamese banks utilized a scrambled virtual keyboard feature for internet banking. Only for one (DongA Bank) of the 3 banks deployed this feature as a compulsory requirement whereas the other 2 banks (BIDV and IVB) allowed their internet banking customers to choose between a scrambled virtual keyboard and a typical keyboard. Section 5.3 of **Table 5** elaborates on this.

In terms of password restriction/requirement, only 6 of the 22 selected licensed Vietnamese banks displayed a password length requirement on their websites. Only one (SAIGONBANK) of the 6 banks required a set minimum password length of 8 characters [20]. The remaining 5 banks had a set minimum length of less than the 8 characters. Five (Vietnam Eximbank, Maritime Bank, Techcombank, VID Public Bank, and Vietcombank) of the 6 banks also required their internet banking customers to use a combination of numbers and letters as well as lower and upper cases for their passwords. Furthermore, the remaining 16 banks did not display any information with regard to password restriction as well as requirement. See **Table 5**, Section 5.4 for more details.

In response to transaction verification for external or sensitive transactions, the majority (16) of the 22 selected licensed Vietnamese banks required the use of OTP (either SMS or security token device) via an external process for these transactions. Six of the 16 banks also provided basic transaction verification as an option for their internet banking customers, in other words, using passwords or CAPTCHA instead of OTP. Section 5.5 of **Table 5** displays more details.

Additionally, 15 of the 22 selected licensed Vietnamese banks scored 50 percent or more. Eight of the 15 selected licensed Vietnamese banks scored 40 or above out of 60 marks. Both Techcombank and VID Public Bank scored group highest as 46 and 47 (76 and 78 percent), respectively. **Table 6**, Category 5 lists more details.

Internet banking application security features

Seventeen of the 22 selected licensed Vietnamese banks did not display any information related to an automatic timeout feature for internet browser inactivity. Three (MDB, Maritime Bank, and VIB) of the remaining 5 banks stated that their internet banking systems had this feature. These limits were set to 10, 5, and 15 min respectively. The remaining 2 banks did not provide the timeout feature limit. See Section 6.1, **Table 5** for more details.

In terms of limited default daily transfer amount for sensitive transactions, 10 of the 22 selected licensed Vietnamese banks did not display website information such as non-registered third party accounts, BPAY, and international transactions. Section 6.2 of **Table 5** elaborates on this.

With regard to logging information and alerts, half of the 22 selected licensed Vietnamese banks did not provide any such information on their websites. Six of the remaining 11 banks provided an alert feature via SMS to their internet banking customers. **Table 5**, Section 6.3 lists more details.

In relation to password policy management, only one (VID Public Bank) of the 22 selected licensed Vietnamese banks provided this website information. See Section 6.4 of **Table 5** for more details.

Only 3 (Techcombank, VIB, and Vietcombank) of the 22 selected licensed Vietnamese banks displayed session management information on their websites. The majority of the remaining banks did not provide any such session management information. Section 6.4 of **Table 5** provides more details.

In addition, only MDB and VID Public Bank scored over 50 percent (25 marks) which are 27 and 29 respectively. The majority of the selected banks scored below 10 marks. See Category 6 of **Table 6** for more details.

Languages

All of the 22 selected licensed Vietnamese banks provided their internet banking information in Vietnamese. Five (Vietnam Eximbank, IVB, MDB, SeABank, and VRB) provided full support for English on their websites. VRB also provided partial support for Russian. The remaining 17 banks' websites provided only partial support for English.

Table 6 A summary comparison information between the 22 selected licensed Vietnamese banks.

Banks	Categories							
	1	**2**	**3**	**4**	**5**	**6**	**Total**	**%**
	20	**20**	**15**	**35**	**60**	**50**	**200**	**100**
	marks	**marks**	**marks**	**marks**	**marks**	**marks**	**marks**	
ABBANK	0	8	0	35	13	0	56	26.7
BIDV	0	8	5	33	15	0	61	29.0
DongA Bank	6.25	10	0	33	40	8	97.25	46.3
Vietnam Eximbank	12.25	8	2	35	42	7	106.25	50.6
HDBank	0	10	3	33	28	3	77	36.7
IVB	0	6	4	35	43	12	100	47.6
LienVietPostBank	0	8	0	35	15	0	58	27.6
MDB	19.5	10	7	35	42	23	136.5	65.0
Maritime Bank	2.5	10	4	25.5	31	27	100	47.6
OCB	2	6	6	33	16	0	63	30
PG Bank	0	6	0	33	16	0	55	26.2
Sacombank	6	8	0	33	30	0	77	36.7
SAIGONBANK	1	8	0	33	39	5	86	41
SeABank	0	4	0	33	30	4	71	33.8
SHB	0	10	0	33	30	0	73	34.8
Techcombank	7.75	8	8	25.5	46	19	114.25	54.4
VIB	13	10	0	33	41	20	117	55.7
VID Public Bank	5	8	3	25.5	47	29	117.5	56
Vietcombank	6.25	8	0	33	41	19	107.25	51.1
VietinBank	1	6	0	33	39	8	87	41.4
VPBank	5	10	4	33	38	9	99	47.1
VRB	0	7	0	33	13	0	53	22.5

Discussion

Six of the 22 selected licensed Vietnamese banks scored above 50 percent whereas, the majority of the remaining banks performed poorly in the provision of internet banking and security related information generally in Categories 1, 3, 5, and 6, and particularly in Sub-categories 1.1, 1.2, 1.3, 1.4, 3.2, 3.3, 5.2, 5.4, 6.1, 6.4, and 6.5. On the contrary, VID Public Bank and VIB achieved the highest scores amongst the 22 selected licensed Vietnamese banks. See **Table 6** for more details.

The provision of significant details about internet banking and security related information as well as improved related internet banking technologies to cover all categories (1 - 7) is strongly recommended. It can increase security awareness and confidentiality to both current and potential internet banking customers. Furthermore, it also translates to improved internet banking security features to both the banks and their internet banking customers.

The following are overall guideline recommendations based on all 7 categories derived from the refined internet banking information security checklist (Version 1.06).

Category 1

Internet banking information such as general online security, privacy, liability, and bank security mechanism system can influence and increase internet banking security knowledge, confidentiality, and trust to current internet banking customers. Furthermore, it may also attract new or potential internet banking customers.

In addition, the banks can provide other extra treatment services to internet banking customers. For example, losses compensation guarantee (not caused by the internet banking customers) should be included without limitation to the amount of the relevant transaction, the amount of the direct loss, or actual damage. Instead it should include time and effort spent by the customer to recover the loss. Offering such extra services may increase confidence and security assurance to both current and potential internet banking customers.

Category 2

Apart from providing typical email, demo, FAQ, user guide, and online support forum, the provision of secured email or secured message would be an excellent feature for internet banking customers. The facility provides a channel for secure communication between banks and internet banking customers, where all data (messages) transfers occur across secure communication (Hypertext Transfer Protocol Secure: HTTPS) between the customer's internet browser and the bank's internet banking server [21].

Other services such as 24/7 hotline or helpdesk is strongly recommended due to the fact that the banks' internet customers can contact and speak to bank staff directly as needed at any time. This service will enhance banks' internet banking security level and increase confidentiality, confidence and security assurance to internet banking customers, particularly during logon or money transfers to third parties.

Category 3

It is strongly recommended that the banks have their internet banking system provide compatibility to several popular and well-known internet browsers such as Mozilla Firefox, Google Chrome, Microsoft Internet Explorer (IE), Safari, Netscape, and Opera. The systems should also include usage of various internet browser versions such as IE Versions 8, 9, and 10. This compatibility feature allows the flexibility of using internet banking customers preferred internet browsers.

Furthermore, the provision of information relating to internet banking user device system and internet browser setting requirement is also strongly recommended. The information can provide flexibility to the banks' internet banking customers for correct user system setup. Provision of this type of information is in the banks' best interest as it may reduce calls for assistance in user system setup by internet banking customers.

Another strong recommendation is that the banks provide information or external links related to various internet security software or tools, such as internet security suite, antivirus/spyware software together with potential security risks on their internet banking websites. It would be better if the banks

can provide free or paid (at special price) internet security software to their internet banking customers. This service can be a joint venture between the banks and the internet security software vendors. It will benefit the banks, the internet security software vendors, and ultimately the internet banking customers.

Additionally, the inclusion of an internet banking security automated tool or security control tool to the internet banking system can enhance the security level to both banks and internet banking customers. For example, China Merchants Bank (CMB) provides a free anti-phishing security tool to its internet banking customers to prevent email and web phishing attacks [22]. This additional feature may work alongside any internet security suite or personal firewall.

Category 4

In terms of bank site authentication technology, both strong 128-bit and 256-bit SSL encryptions should be supported by the banks for establishing a secure connection between banks' systems and customers' internet browsers for internet banking during transactions. This allows encrypted data transfer between the customers' computers and banks' internet banking systems. Moreover, 256-bit SSL encryption is the highest commercially available standard in the world [18,19]. Supporting both 128-bit and 256-bit SSL encryptions may provide compatibility to various internet browsers. This is due to the fact that either 128-bit or 256-bit SSL encryption is used depending on the encryption capabilities of the internet banking sites (the servers) and the customer's internet browsers [23].

A further recommendation is the inclusion of an extended validation SSL certificate to banks' authentication systems. It provides "high-security internet browsers information to clearly identify a web site organizational identity" [24]. Finally, a well-known and trustworthy public commercial CA service is recommended.

Category 5

In relation to logon requirements (Section 5.1 in **Table 5**), it is strongly recommended that the banks set their logon requirements to at least 3 remember identifiers, and 2 verifications such as CAPTCHA and 2-factor authentication (minimum 6 digits and with PIN protection).

First remember identifier: login name should be what both the banks and their internet banking customers agree on such as appropriate registered bank usernames. The registered bank usernames should contain upper and lower cases as well as numbers. Ideally, they should have an appropriate length such as 10 or more characters (longer is better). To avoid lengthy usernames, the banks can set a length requirement such as between 10 to 15 characters. In general, this provides better security as compared to usage of a bankcard/credit number or customers' email addresses. This is due to the fact that such information (bankcard or customers' email addresses) can be spoofed or obtained with or without the customers' knowledge.

Second remember identifier: usually a password, PIN, or security number with an appropriate length range such as 10 or more characters. Further details of password restriction/requirement are described in the password restriction/requirement sub-category (Section 5.4 in **Table 5**).

Third remember identifier: An additional password or secret question should be combined into logon requirements. This method provides a second level of security check to just typical username and password logon requirements.

CAPTCHA verification: it is also strongly recommended as additional security to the logon requirement for internet banking. The objective of this verification method is "to render automated attacks against authenticated sessions ineffective" [14]. The legitimate internet banking customer is required to enter or "input information conveyed as scrambled images which are difficult for automated robots to process and recognize" [14]. Not only does the CAPTCHA method provide an extra level of security, it is also considered cost effective when compared to typically 2-factor authentication such as an SMS or a security token device.

Two-factor authentication (security token device or SMS) verification: this technology is strongly recommended to incorporate into the logon requirement. In comparison to typical login username and password input verification type, 2-factor authentication technology provides better security and is considered as a strong authentication mechanism [25]. It uses a combination of 2 identifiers which are

physical and remembered identifiers [26]. Both the combinations of the 2 identifiers are required for logon to internet banking [27]. The physical identifier is something provided by the banks to their internet banking customers such as a security token device. This security token device is used for generating OTP and displayed to the internet banking customers for a short period of time. The internet banking customers must enter OTP to the internet banking systems to be authenticated [17]. The use of this type of authentication technology is an extra cost to the banks as they have to provide security token devices to their internet banking customers. This extra cost is sometimes charged to the internet banking customers [28].

For further security operation on a security token device, HSBC Bank Australia provides a security token device with PIN protection to the internet banking customers. A security code generated by a security token device is required for logon to the bank's internet banking website as well as to conduct any internet banking transactions. HSBC's internet banking customers must enter the PIN in order to enable or activate the security token device first. Then, the security token device must be used to generate a security number or code by pressing a required button on the security token device [29]. Thus, this logon activation PIN feature provides an extra security layer to internet banking customers particularly in the case of a lost security token device.

Some banks use mobile phones as an alternate display device instead of a security token device. Typically, this authentication mechanism is used as a second or additional layer for logon [30]. Successful logon using this mechanism involves 2 steps. The first step is the internet banking customer's successful logon to the bank's internet banking system using their credentials (e.g. username and password). The second step occurs when the bank generates a OTP and sends it through SMS in a text form to the internet banking customer's registered mobile phones. The internet banking customers are then required to enter the received OTP to the banks' logon websites within a limited period of time. This technique prevents the traditional Man-in-the-middle (MITM) replay attack. However, OTP via SMS does not protect against shoulder-surfing attack [31]. Furthermore, this authentication mechanism also provides an alternative to the banks as they do not need to provide security token devices to their internet banking customers. However, the internet banking customers must have their own mobile phones with the SMS feature. The provision of this technology is an extra cost to potential internet banking customers who do not use mobile phones in their normal day to day lives.

Typically, OTP is made up of 6 to 8 digits decimal numbers in length and is only valid for a set period of response time [32]. For example, UBank provides a unique 6 digit decimal numbers OTP via SMS [33]. It allows the banks to choose different set response times to provide to their internet banking customers such as 10 min, 5 min, 60 s, and 30 s. The response time for 30 s means that the security token device will generate a new security number or code every 30 s [34]. Longer response times can increase potential exposure to internet banking security attacks by unauthorized users before it is used by the internet banking customers [35]. Usually, the length of the response time of the security token device is 60 s [36]. In addition, a longer response time means a longer wait time for the internet banking customers to receive the next OTP security code as they must wait until the last successful OTP finishes it's time cycle first. This can impact on internet banking usability for the internet banking customers [35].

Other verification technology such as digital certificate and smart ID card are other options which can be incorporated into the logon requirement. However, they can be difficult to implement as it relies on the internet banking customers to install the system (hardware/software) on their laptops or computers prior to access to the internet banking websites. However, this type of technology may be challenging for inexperienced computer users in particular.

In relation to sub-category logon failure limitation (Section 5.2 in **Table 5**), this verification method is used to protect against unauthorized access [37]. It is strongly recommended to set the standard number of logon failure limit to the maximum of 3 attempts similar to the maximum number of logon failures of Automated Teller Machine (ATM) cards. After the maximum (3 times) failed logon attempts has been reached, the internet banking system lockout feature should be enforced. The authorized customers are then required to contact the banks immediately or within a reasonable period of time in order to reactivate their internet banking accounts.

With regard to sub-category logon user input type (Section 5.3 in **Table 5**), it is strongly recommended that the banks provide a virtual keyboard with a scrambling feature as logon user input type, rather than the typical keyboard to their internet banking customers. The scrambling feature changes positions of the contents such as numbers and/or characters on the virtual keyboard. This scrambling method can reduce spelling errors or mistyping compared to traditional physical keyboards. It also provides better security for protection against keylogger attacks that capture information typed on the internet banking customers' keyboards (e.g. usernames and passwords) without their knowledge [14].

In terms of password restriction or requirement sub-category (Section 5.4 in **Table 5**), it is strongly recommended that the banks provide related information on their websites. The websites should automatically enforce or detect that all requirements and restrictions are met, as well as feature a real time display of level of password strength during customer password creation or change. The following are the password requirement recommendations:

1) Minimum password length of 10 characters or more;
2) A combination of numbers and letters;
3) A combination of upper case and lower case characters;
4) Must contain a minimum of one special character or symbol (e.g. !, @);
5) A new password must be different to any of 3 previously used passwords;
6) The use of 3 or more consecutive identical characters (eg. aaa) should be disallowed; and
7) The use of 3 or more consecutive characters (eg. 123, abc) should be disallowed.

It is strongly recommended to have a transaction verification method for external or sensitive transactions such as OTP technology (security token device or SMS). However, CAPTCHA and extra password would be other more cost effective alternatives. Newly emergent CAPTCHA technology developed by Google called "reCAPTCHA" could be an alternative, especially for the banks. According to [38], reCAPTCHA "uses an advanced risk analysis engine and adaptive CAPTCHAs to keep automated software from engaging in abusive activities" on the website. Users of this internet technology need only to click on the "I'm not a robot" option, rather than type in typical CAPTCHA text which may sometimes be difficult to read. This feature can therefore provide significant convenience to the banks' internet banking customers during verification procedures. The use of transaction verification can mitigate potential authentication security threats to the internet banking customers [17].

Category 6

In relation to the automatic timeout feature for internet browser inactivity sub-category (Section 6.1 in **Table 5**), it is recommended to set the maximum inactivity period to 15 min by default. In our opinion, this inactivity time length is considered reasonable as it provides sufficient time for the internet banking customers to do other things simultaneously. A longer inactivity period can cause potential risks from unauthorized access to the customers' internet banking accounts in case of non-attendance. This default automatic timeout feature can automatically logoff the internet banking customers from the banks' internet banking systems and thereby reduce potential risks of unauthorized access particularly when the internet banking customers forget to logout [5,6]. It is also recommended that information on the automatic timeout feature for internet browser inactivity be displayed. The display of this information can increase internet banking security awareness to both current and potential internet banking customers. Moreover, it can also increase usability to both groups. In addition, there should be a warning message or pop-up screen (including sound) reminder prior to the end of the 15 min inactivity period. This may provide the internet banking customers the option to continue or end their sessions.

With regard to the limited default daily transfer amount to sensitive transactions sub-category (Section 6.2 in **Table 5**), it is recommended that the internet banking system should provide both flexibility and better security to internet banking customers. Flexibility means that the banks allow the internet banking customers to decrease the default daily transfer amount limit by themselves over the internet without directly contacting the banks. On the other hand, in order to increase the default daily transfer amount limitation, the internet banking customers have to contact or get an approval from their banks first by providing identity verification checks. This technique can mitigate the potential risk of losing larger amounts of money per transaction in case of unauthorized usage, thereby increasing the

security of the internet banking system. In addition, the level of limited default daily transfer amount should be based on the type of internet banking customer's account types such as personal, business, and investment. Some accounts may have higher limited default daily transfer amounts. For example, a business account may have higher limited amount than a typical personal account.

In terms of the logging information and alerts sub-category (Section 6.3 in **Table 5**), it is strongly recommended that last login and activity log/transaction history details should be incorporated into the internet banking system. The last login information can include date and time details, whereas the activity log or transaction history can log past customer activity information. The activity log/transaction history details feature allows the internet banking customers to retrieve their internet banking activities which can be viewed on the screen, printed, or downloaded in a spreadsheet format. A longer length of transaction activity history period such as 12 months, and an alert feature available via email and/or SMS to internet banking customers is also recommended. By providing logging information and alert features, internet banking customers can utilize such information in order to make sure that their logon activities are normal and expected. It also enhances the security of the internet banking system [9].

With relation to the password policy management sub-category (Section 6.4 in **Table 5**), it is recommended to regularly enforce password policy management for a particular period of time, such as every 3-6 months to internet banking customers. Changing online passwords regularly provides better security against password attacks [39].

With regard to the session management sub-category (Section 6.5 in **Table 5**) when cookie technology for the collection of information about the internet banking customers is used, it is recommended that the purpose and type of information collected be explicitly stated, for example, allocate a bank identification number to the customer internet browser, determine if customers have previously visited the bank's website [40]. The collection of too much and unnecessary information may create a potential risk to a cross-site scripting attack [41]. Additionally, the provision of an automated feature to clear cookie information on internet browser after the internet banking customers' logoff or close of internet browser (session end) is strongly recommended. This technique ensures that all the cookies used during the private browsing session can be cleaned out. It therefore serves to reduce the ability of potential unauthorized persons to track the cookie history on the internet banking customers' browsers.

Category 7

In terms of the languages sub-category, providing full support for a local language is compulsory. Full support of least one universal international language such as English is strongly recommended. This may allow local and foreign speakers to be able to access, receive, and conduct business through understanding of more details on the internet banking website. Thus, this may reduce the potential of misunderstanding as well as increase confidentiality and online banking security awareness to both current and potential internet banking customers.

Conclusions

The recommendations within the refined internet banking information security checklist have been developed over the past few years from Version 1.01 (2011) to Version 1.06 (2014). The data collections were from the banks in several countries including Australia (25), Mainland China (13), Hong Kong (19), and Thailand (12). The total number of the selected licensed banks including Vietnam (22) was 91 from a selection of both private (local and foreign) and public banking entities.

The application of the refined internet banking information security checklist recommendations (Version 1.06) to the 22 selected licensed Vietnamese banks may standardize usability and information security of the respective internet banking systems. If the internet banking checklist is made available to banks and their customers it may be more useful in evaluating their web systems for the features and may enhance the confidentiality and security awareness of the banks' current and potential internet banking customers.

Mobile internet users who use smartphones for internet banking may also benefit. The banks can use and adapt the checklist recommendations (Version 1.06) to cover additional mobile internet banking facilities such as the provision of information about mobile phone security, provision of security scanning applications, or links to well-known antivirus providers. Furthermore, the security related information could be displayed in easily read mobile phone format.

In addition, the banks could establish a solid standard process in dealing with registration of their internet and mobile banking customers. Customer documentation should be scanned, encrypted and kept in the secure central environment such as the banks' head offices. Documentation such as drivers' licenses or national ID cards must contain photo identification. It should only allow access across the bank's computer network to all senior staff or branch managers for further reference and usages. The scanned document (photo identification) can be used to ensure against attempts by unauthorized persons to open an internet or mobile banking account at a branch other than the originating one.

The refined internet banking information security checklist (Version 1.06) can be used as a guideline by any bank to raise the security awareness, confidence and confidentially of current or potential internet banking customers in using internet banking. However, it may be adapted as a checklist for auditing any similar services in other organizations apart from the banking industry by a typical novice or expert IT personal in both public and private sectors. For instance, it can be adapted to validate online payment systems in local or state government sectors such as in Western Australia, where online rate payment services were provided over HTTPS with standard SSL certificate [42-44]. These services can be enhanced by upgrading the use of extended validation SSL certificate instead. See Section 4.1.3 in **Table 5** for more details. Another example is the Western Australia State Government public tender website. This website is used to support the tendering process of Western Australia Government contracts. It is a requirement for interested bidders to be registered prior to any tender application. Both username and password are required for login over HTTPS (standard SSL certificate) [45]. The application of extended validation SSL certificate as well as the cost effective validation CAPTCHA may increase the security level for logon at the website.

Education programs in schools or universities may also gain an advantage from the refined checklist. Both education related staff or students may apply and adapt the checklist to their daily life activities or future related careers, respectively. For instance, related IT staff may adapt the refined checklist to audit their organizations' internal internet/intranet web systems for further improvement. Students may learn security lessons from the refined checklist to extend their knowledge beyond textbooks or classrooms. Consequently, the refined checklist may raise the security awareness of both staff and students while conducting online shopping or internet trading.

Acknowledgements

We would like to extend our sincerest thanks and appreciation to Dr. Yunous Vagh for providing us with essential advice to complete this paper.

References

[1] D Son, N Que, P Dieu, T Trang and M Beresford. Policy reform and the transformation of Vietnamese agriculture, Available at: ftp://ftp.fao.org/docrep/fao/009/ag089e/ag089e04.pdf, accessed October 2014.

[2] A Ho and R Baxter. Banking reform in Vietnam, Available at: http://www.frbsf.org/banking-supervision/publications/asia-focus/2011/june/banking-reform-vietnam/june-banking-reform-in-vietnam.pdf, accessed October 2014.

[3] N White. Study finds online banking security shortfalls, Available at: http://sciencewa.net.au/topics/technology-a-innovation/item/1021-study-finds-online-banking-security-shortfalls/1021-study-finds-online-banking-security-shortfalls, accessed May 2015.

[4] C Yiua, K Grant and D Edgar. Factors affecting the adoption of internet banking in Hong Kong-Implications for the banking sector. *Int. J. Inform. Manag.* 2007; **27**, 336-51.

[5] P Subsorn and S Limwiriyakul. A comparative analysis of the security of internet banking in Australia: A customer perspective. *In*: Proceedings of the 2nd International Cyber Resilience Conference. Perth, Western Australia, 2011.
[6] P Subsorn and S Limwiriyakul. A comparative analysis of internet banking security in Thailand: A customer perspective. *Procedia Eng.* 2012; **32**, 260-72.
[7] P Subsorn and S Limwiriyakul. An analysis of internet banking security of foreign subsidiary banks in Australia: A customer perspective. *Int. J. Comput. Sci. Issues* 2012; **9**, 8-16.
[8] P Subsorn and S Limwiriyakul. A case study of internet banking security of Mainland Chinese Banks: A customer perspective. *In*: Proceedings of the 4th International Conference on Computational Intelligence, Communication Systems and Networks 2012. Phuket, Thailand, 2012.
[9] S Limwiriyakul and P Subsorn. A customer perspective investigation on internet banking security of licensed banks in Hong Kong. *In*: Proceedings of the International Conference on Security and Management 2012. Las Vegas, USA, 2012.
[10] Usonlinebiz. Types of Internet banking and security threats, Available at: http://www.usonlinebiz.com/article/Types-of-Internet-Banking-and-Security-Threats.php, accessed April 2011.
[11] D Hutchinson and M Warren. A framework of security authentication for internet banking. *In*: Proceedings of the International We-B Conference 2001. Perth, Australia, 2001.
[12] D Hutchinson and M Warren. Security for Internet banking: A framework. *Logist. Inform. Manag.* 2003; **16**, 64-73.
[13] Dah Sing Bank. How can I login Dah Sing E-Banking service? Available at: http://www.dahsing.com/en/html/other_services/ebanking/faq_ds_login.html, accessed October, 2014.
[14] L Peotta, M Holtz, B David, F Deus and RT Sousa. A formal classification of internet banking attacks and vulnerabilities. *Int. J. Comput. Sci. Inform. Tech.* 2011; **3**, 186-97.
[15] M Agarwal, M Mehra, R Pawar and D Shah. Secure authentication using dynamic virtual keyboard layout. *In*: Proceedings of the International Conference and Workshop on Emerging Trends in Technology 2011. Mumbai, India, 2011.
[16] S Rajarajan, K Maheswari, R Hemapriya and S Sriharilakshmi. Shoulder surfing resistant virtual keyboard for internet banking. *World Appl. Sci. J.* 2014; **31**, 1297-304.
[17] Federal Financial Institutions Examination Council (FFIEC). Authentication in an Internet banking environment, Available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf, accessed October 2014.
[18] VeriSign Incoporation. The Latest advancements in SSL technology, Available at: http://www.verisign.com/static/042485.pdf, accessed October 2014.
[19] National Security Agency. Suite B cryptography, Available at: https://www.nsa.gov/ia/programs/suiteb_cryptography, accessed October 2014.
[20] The Open Web Application Security Project (OWASP). Password length and complexity, Available at: https://www.owasp.org/index.php/Password_length_%26_complexity, accessed October 2014.
[21] Comodo CA Limited. What is HTTPS? Available at: https://www.instantssl.com/ssl-certificate-products/https.html, accessed October 2014.
[22] China Merchants Bank (CMB). All in One Net: Personal Internet Banking General Edition, Available at: https://pbsz.ebank.cmbchina.com/CmbBank_GenShell/UI/GenShellPC_EN/Login/Login.aspx#, accessed October 2014.
[23] DigiCert. Behind the scenes of SSL cryptography, Available at: https://www.digicert.com/ssl-cryptography.htm, accessed October 2014.
[24] VeriSign Authentication Services. FAQ: Extended validation SSL, Available at: http://www.verisign.com.au/ssl/ssl-informationcenter/extended-validation-ssl-certificates/? accessed April 2011.
[25] RSA, The Security Division of EMC. Two-factor authentication, Available at: http://www.rsa.com/glossary/default.asp?id=1056, accessed April 2011.

[26] Bank of Queensland Limited. Using the BOQ security token, Available at: http://www.boq.com.au/online_enhancedIB_security_token.htm, accessed October 2014.
[27] VeriSign Authentication Services. Two-factor authentication, Available at: http://www.verisign.com/authentication/two-factor-authentication/index.html, accessed April 2011.
[28] Suncorp-Metway Limited. Internet banking security tokens: How do I order / activate a security token?, Available at: http://www.suncorpbank.com.au/about/ways-to-bank/internet-banking/security-tokens#_accordion-tiles-2, accessed October 2014.
[29] The Hongkong and Shanghai Banking Corporation (HSBC) Bank Australia Limited. We're serious about online banking security, Available at: http://www.hsbc.com.au/1/2/osd, accessed October 2014.
[30] Bendigo Bank. Security tokens, Available at: http://www.bendigobank.com.au/public/personal/ways-to-bank/online-banking-old/security-tokens?fb_keyword=security+tokens, accessed October 2014.
[31] F Cheng. A secure mobile OTP Token. *In*: Proceedings of the 3rd International Conference, Mobilware 2010. Chicago, USA, 2010, p. 3-16.
[32] JD Aussel. Smart cards and digital identity, Available at: http://www.telenor.com/wp-content/uploads/2012/05/T07_3-4.pdf, accessed October 2014.
[33] UBank. What we do to protect you, Available at: https://www.ubank.com.au/security, accessed October 2014.
[34] C Marinakis and N Karanikolas. Strengthening the security of E-banking transactions. *In*: Proceedings of the 11th Panhellenic Conference in Informatics 2007. Patras, Greece, 2007.
[35] D M'Raihi, S Machani, M Pei and J Rydell. TOTP: Time-based one-time password algorithm, Available at: http://www.hjp.at/doc/rfc/rfc6238.html, accessed October 2014.
[36] JC Liou and S Bhashyam. A Feasible and Cost Effective Two-Factor Authentication for Online Transactions. *In*: Proceedings of the 2nd International Conference on Software Engineering and Data Mining. Chengdu, China, 2010.
[37] Suncorp-Metway Limited. How we protect your money online: Automatic lock-out, Available at: http://www.suncorpbank.com.au/security/how-we-protect-your-money-online, accessed October 2014.
[38] Global Organization Of Oriented Group Language Of Earth (Google). The reCAPTCHA advantage: What is reCAPTCHA?, Available at: https://www.google.com/recaptcha/intro/ index.html#the-recaptcha-advantage, accessed October 2014.
[39] S Gaw and E Felten. Password Management Strategies for Online Accounts. *In*: Proceedings of the Symposium on Usable Privacy and Security 2006. Pittsburgh, USA, 2006.
[40] The Bank of Western Australia Limited (BankWest). Website terms of use, Available at: http://www.bankwest.com.au/terms-conditions/website-terms-of-use, accessed October 2014.
[41] The Open Web Application Security Project (OWASP). Cross-site Scripting (XSS), Available at: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS), accessed October 2014.
[42] City of Perth. Payment types, Available at: https://eservices.perth.wa.gov.au/ePathway/Production/Web/Payments/PaymentTypes.aspx, accessed October 2014.
[43] City of Joondalup. Rates, Available at: https://www.joondalup.wa.gov.au/Live/PayOnline/Rates.aspx, accessed October 2014.
[44] City of Melville. Payments, Available at: https://services.melvillecity.com.au/ePathway/Production/Web/Payments/PaymentEntry.aspx? accessed October 2014.
[45] Tenders WA. Welcome to tenders WA, Available at: https://www.tenders.wa.gov.au/watenders/index.do, accessed October 2014.