“Financial consumer protection: internet banking fraud awareness by the banking sector”

AUTHORS	Shewangu Dzomira
ARTICLE INFO	Shewangu Dzomira (2016). Financial consumer protection: internet banking fraud awareness by the banking sector . *Banks and Bank Systems*, *11*(4-1), 127-134. doi:10.21511/bbs.11(4-1).2016.03
DOI	http://dx.doi.org/10.21511/bbs.11(4-1).2016.03
RELEASED ON	Thursday, 22 December 2016
JOURNAL	"Banks and Bank Systems"
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
0	0	0

Shewangu Dzomira (South Africa)

Financial consumer protection: internet banking fraud awareness by the banking sector

Abstract

This paper examines internet banking fraud awareness by the banking sector in Southern Africa as financial consumers' protection. The study is grounded on routine activity theory and criminology theory. A qualitative content analysis research technique was used for examination of the text content data through the consistent nomenclature process of coding and classifying themes or patterns to proffer a meticulous considerate of internet banking fraud awareness in the banking sector. The findings suggest that internet fraud awareness to the general public through website is very low by many Southern Africa banks. Most of the banks disclose less than half of the identified internet banking fraud awareness to the general public on their websites. Although some banks have internet fraud information on internet banking applications, however, the authentic efficacy of this information is tentative. This proposes that most of the financial customers engage internet banking transactions without sufficient awareness on potential internet threats and attacks. There is, consequently, high likelihood of financial consumers being internet banking fraud victims.

Keywords: internet fraud, internet banking, fraud awareness, financial consumer.
JEL Classification: G21, D18.

Introduction

As financial customers become more urbane, it becomes critical for the banks to consider the use of technology and awareness efforts to take action to their incessantly changing needs. The internet is getting hold of popularity as a delivery conduit in the banking sector and, at the same time, customer requests are shifting (Jayawardhena & Foley, 2000). The banks have to strengthen awareness programs to help customers to circumvent internet banking scams such as phishing, pharming, romance, and mobile scams such as smshing, sim-card swapping and vishing, that can lead to account usurping and other identity theft ways. With the fruition of electronic technologies, a more rapidly e-transaction has been made possible by the internet. It has been noted that internet fraud are increasing with the increase of e-transaction (Mahdi & Rezaul, 2012).

The surfacing of internet gives tremendous opportunity for proficient services and increases competitiveness to meet financial consumer demands via the formation of improved banking transaction course that reduces overall banking costs. Consequential enhanced performance from the espousal of internet services has hastily amplified with the introduction of World Wide Web. This convenience, however, may be offset to a certain degree by customers acuity of the risks allied with transacting in the wide-open cyber-world (Jih, Wong & Chang, 2009). Concurring to that (Alsheyyab & Singh, 2013) noted that lack of confidence has inhibited the embracing of internet banking services, as financial customers information is exposed to internet-fraudsters. Banking services principally engross the creation, processing, storage, and distribution of financial information. Most of these services can be expediently contained via internet-based information technologies.

In the recent decade, most scholars have been discussing the factors affecting the individual embracing of internet banking. The most noted influential factors affecting the internet banking usage include apparent usefulness and professed ease of use (Kesharwani & Tripathy, 2012). Fraud has evolved from being perpetrated by casual fraudsters to being committed by well thought-out crime and fraud rings that use classy ways to take over control of accounts and commit fraud. The problem is marked in the banking sector, where the compromises are more stylish than in other industries (Joyner, 2011). However, according to Abend, Peretti, Bach, Barry, Donahue et al. (2008), the banking sector need locked, resilient, and reliable systems to ensure flawless operations and maintain public confidence in monetary systems. Banking institutions are unceasingly beleaguered by cyber-fraudsters and others with malicious intent. (Dzomira, 2015) highlighted that the biggest challenge of the banking sector is to provide sufficient security and safety to customers' finances. Financial consumer awareness and information distribution concerning internet banking fraud seem to be the underpinning of these determinations.

Even though researches have been done surrounding internet banking fraud, the author found no research that specifically addressed internet banking fraud awareness to the general public in the Southern Africa banking sector through the website. In light of the above milieu, the paper aims to examine the coverage of internet banking fraud awareness by the Southern Africa's banking sector as financial consumer protection tool. The following sections of this paper outline the theoretical framework, literature review, methodology, findings and discussions, conclusion and implications and recommendations.

Shewangu Dzomira, Research Associate, College of Economics & Management Sciences, University of South Africa, Pretoria, South Africa; Senior Lecturer, Department of Accounting, Great Zimbabwe University, Zimbabwe.

1. Theoretical framework

This study is grounded on routine activity theory as postulated by Cohen and Felson (1979). Routine activity theory is a criminology theory focused on the premise that generally criminal acts need convergence in space and time of likely offenders, suitable targets and the deficiency of proficient guardians against crime. Tewksbury & Mustaine (2010) emphasized the central part of routine activity theory as three indispensable locational rudiments that must exist for crime to happen, that is existence of budding delinquent (internet fraudster), incidence of apt targets (financial consumers), and nonexistence of capable and enthusiastic guardians (lack of protection by banks). The transformations in legitimate opportunity structures such as technology can increase the convergence of enthused reprobates and suitable targets in the dearth of capable protection (Pratt et al., 2010). The internet banking has principally changed consumer practices and has concurrently extended opportunities for internet fraudsters to mark internet banking consumers. In addition, Miro (2014) cited that the routine activity theory proposes that changes in the arrangement of the blueprint of daily technology motivated life could explain the rise in internet banking fraud. Consequently, there is great necessity for banking institutions which are the guardians of finance to spread out the internet banking fraud awareness to the general public.

2. Literature review

Internet and other electronic technologies have a grand potential for keeping on altering essentially the banking industry. The chance, which the internet banking services and technologies present to the banking sector in order to realize existing customer requirements and to draw new potential customers, are the motivating forces for banks in order to devise, develop and operate their own internet banking systems (Angelakopoulos & Mihiotis, 2011). Sophisticated internet banking fraud replicates the integrative abuse of resources in social, cyber and physical worlds. There is very limited information available to distinguish dynamic fraud from genuine customer behavior in such an extremely sparse and imbalanced data environment, which makes the instant and effective detection become more and more important and challenging (Wei, Li, Cao, Ou & Chen, 2013). Dzomira (2014), in a study concluded that challenges like lack of resources, inadequate cyber-crime laws and lack of knowledge through education and awareness affect the banking industry.

The internet banking system has grown hurriedly over the past years, and will continue to increase as financial institutions continue to encourage customers to do internet banking transactions such as money transfer, access information about the account or otherwise, as well as payment of monthly bills. It is during this moment internet criminals and fraudsters attempting to steal customer's personal information have hunted down the internet banking (Yazdanifard, Wanyusoff, Behora & Sade, 2012). As a result, consumer trust has been recognized as a critical component of the internet banking industry, as the factors that affect trust and its expansion vary from conventional banking services because of the vague nature of the cyber environment (Law, 2007).

In the contemporary environment, internet is the main tool for electronic business and the e-transactions are made faster by internet, as a result, internet fraud is increasing also (Mahdi et al., 2010). According to Jayawardhena & Foley (2000), internet banking renders location and time irrelevant, and sanctions customers with greater control of their accounts. However, internet, as a powerful worldwide tool for e-commerce, could be, to a great extent, insincere without the real validity of security, privacy, and the strong role of legislators against identity theft fraud (Ahmad, 2008) and educational awareness. The rapid augmentation of electronic commerce, and the corresponding desire on the part of consumers to feel secure when engaging in electronic commerce, has prompted various parties to develop mechanisms to reduce concerns about fraudulent misuse of information. It is uncertain, however, whether these mechanisms can actually reduce fraud in electronic commerce (Baker, 1999). Gavish (2003) added that fraud can be a major stumbling block for increasing the volume of internet commerce on the Web; it stirred research on trust building activities given the prevalence of fraudulent activities on the Web.

In a study, Grazioli & Jarvenpaa (2000) found out that consumers are vulnerable to attack by hackers posing as a legitimate site imitating the real commercial website. The counterfeit site contains malicious manipulations designed to increase trust in the site, decrease perceived risk, and ultimately increase the likelihood that consumers would transact from it. To that end, before banks shift their hub on to trust resources of consumer side, banks are advised to create clients' trust from internet banking side, such as situational normality and structural assurance (Yu & Asgarkhani, 2015). According to Chiemeke, Evwiekpaefe & Chete (2006), most of the banks execute extremely well in providing up-to date information. Conversely, they noted further improvements on security and provision of key ingredients of internet banking which includes confidentiality, effective communication integrity and availability, should be considered in order to satisfy customer's requirements.

Wong, Loh & Yap (2009) concluded that consumers' willingness to use internet banking chiefly depends on their perception of risk in transacting on

the internet and trust of the specific e-banking website. This suggests the need for banks to employ mechanisms to build trust for their specific e-banking website and, as well, banks should take measures to educate their customers and manage general consumer perceptions of the risks of transacting on the internet. Also Alsheyyab & Singh (2013) finds that trust is at the central pivot of an effective function internet banking system in Jordan. More so, a study by Pravettoni, Leotta, Lucchiari & Misuraca (2007) concluded that the website usability of e-banking services did not play a very important role for the user group, but, instead, institution-based trust such as the trust in the security policy of the Web merchant, customers, and the overall trust of the bank were the crucial factors in the adoption of e-banking. Therefore, banks should educate their customers and manage general consumers' discernment of the risks in transacting on the internet (Wong, Loh, Turner, Bak & Yap, 2009; Jih, Wong & Chang, 2009; Kesharwani & Tripathy, 2012).

Chang's (2008) interpretive findings suggest that scammers such as advance fee fraudsters employ specific methods that exploit the bounded rationality and automatic behavior of victims. Hence, the study suggested a need to inform internet users of the methods employed by advance fee fraudsters. Narayanan, Koo, Brian & Cozzarin (2012) concluded from a study that product characteristics and the education level of the head of the household critically affect consumer decision-making on internet transaction. In Greece, the moderately low internet bank usage, the non-familiarity with technologically advanced devices and problems regarding security and privacy were the main factors that have a negative influence on the embracing of e-banking services by customers (Angelakopoulos & Mihiotis, 2011). In addition, the analyses demonstrate that trust in the internet is particularly influenced by the security perceived by consumers regarding the handling of their private data (Carlos Flavián, Miguel Guinalíu, 2006). At the same time, card-not-present fraud losses are increasing at higher rate because of internet transaction, as there is no chance to use Chip and PIN, as well as card is not used face-to-face. Card-not-present fraud losses are growing in an un-protective and un-detective way through identity theft (Mahdi, Rezaul, & Rahman, 2010). All in all, as customers become more chic, it becomes essential for the banks to consider the use of technology and awareness efforts to respond to their continuously changing requirements.

3. Methodology

The total population for this study was made up of 67 commercial banks from randomly selected 5 SADC countries (South Africa, Zambia, Botswana, Zimbabwe and Namibia). A sample size of 13 banks was used and the banks were arbitrarily chosen on the basis of website ease of access and availability of the data. The sample size was calculated considering the precision of how closely the sample value relates to the population value and suggested 'equal precision' of 10% (Brink et al., 2013) and, in this study, 20% of the total population was used. A qualitative content analysis research technique was used for examination of the text content data through the consistent nomenclature process of coding and classifying themes or patterns (du Plooy-Cilliers, 2014) to proffer a meticulous considerate of internet fraud awareness in the banking sector. Information on internet banking fraud awareness was retrieved from each bank's website. Coding sequence was done on the retrieved scripts marking sections of data. The descriptive statistical analysis was done using frequencies, cluster analysis, similarity matrices, and crosstab matrix. To further visualize the staging of the outcomes, bar charts and dendrograms (tree graphs) were used.

4. Findings and discussions

The coding frequencies list from Table 1 below exhibits internet banking fraud awareness by all the 13 banks forming the sample size. The findings show that scam has the highest frequency of 8 counts out of total of 12 counts in 7 cases from a total sample size of 13 banks (53.80%). This is followed by malware/virus awareness which has a frequency of 6 counts from 6 cases out of 13 cases. Phishing, identity theft and spyware are identified with 5 cases each with a percentage of 38.50% for each bank. Pharming, smishing and spam awareness have 4 counts in each of the 4 banks with 30.80%. Key-logging and sim card swaping awareness have 3 counts in 3 cases. Ultimately, the least awareness from the sample size of 13 banks is on vishing and cash send fraud which has 2 and 1 counts, respectively.

Table 1. Internet banking fraud awareness frequencies

Category	Code	Count	% codes	Cases	% cases
Awareness	Scam	8	16.00%	7	53.80%
Awareness	Malware/Virus	6	12.00%	6	46.20%
Awareness	Phishing	5	10.00%	5	38.50%
Awareness	Identity theft/fraud	5	10.00%	5	38.50%
Awareness	Spyware	5	10.00%	5	38.50%
Awareness	Pharming	4	8.00%	4	30.80%
Awareness	Smishing	4	8.00%	4	30.80%
Awareness	Spam	4	8.00%	4	30.80%
Awareness	Key logging	3	6.00%	3	23.10%
Awareness	Sim card swaping	3	6.00%	3	23.10%
Awareness	Vishing	2	4.00%	2	15.40%
Awareness	Cash send fraud	1	2.00%	1	7.70%

5. Internet banking fraud awareness - similarity matrix

Figure 1 below illustrates clustering presented on banks; the distance matrix used for clustering consists of cosine coefficients calculated on the comparative frequency of the assorted internet banking fraud awareness. The more analogous two cases will be in terms of the allotment of codes, the higher will be the coefficient. From the Dendrogram, Figure 1 and Table 3 below, banks STWZIM3 and BTSB1 have the highest cluster coefficient of 1 followed by STCHZ3 and STCZIM2 with a coefficient of 0.91. FBB2 and NBN2 banks have a similarity cluster coefficient of 0.89. The lowest similarity cluster coefficients are 0.14; 0.18 and 0.18 for banks NBN1 and FB2; and STBC3 and BCZ; and NBN2 and STBC3, respectively.

Table 2. Internet banking fraud awareness - similarity matrix

	BTSB1	FBB2	FBN1	NBN2	ABS1	FB2	STBC3	BCZ1	CVBZ2	STCHZ3	CBZIM1	STCZIM2	STWZIM3
BTSB1	1												
FBB2	0.37	1											
FBN1	0.54	0.84	1										
NBN2	0.4	0.89	0.77	1									
ABS1	0.72	0.4	0.59	0.28	1								
FB2	0.54	0.26	0.14	0.31	0.59	1							
STBC3	0.42	0.3	0.26	0.18	0.68	0.62	1						
BCZ1	0.7	0.63	0.77	0.7	0.5	0.31	0.18	1					
CVBZ2	0.7	0.37	0.31	0.4	0.72	0.77	0.66	0.4	1				
STCHZ3	0.34	0.7	0.56	0.58	0.32	0.2	0.56	0.58	0.34	1			
CBZIM1	0.54	0.45	0.31	0.54	0.59	0.66	0.62	0.31	0.77	0.38	1		
STCZIM2	0.37	0.56	0.45	0.63	0.21	0.26	0.5	0.63	0.37	0.91	0.45	1	
STWZIM3	1	0.37	0.54	0.4	0.72	0.54	0.42	0.7	0.7	0.34	0.54	0.37	1

Dendrogram

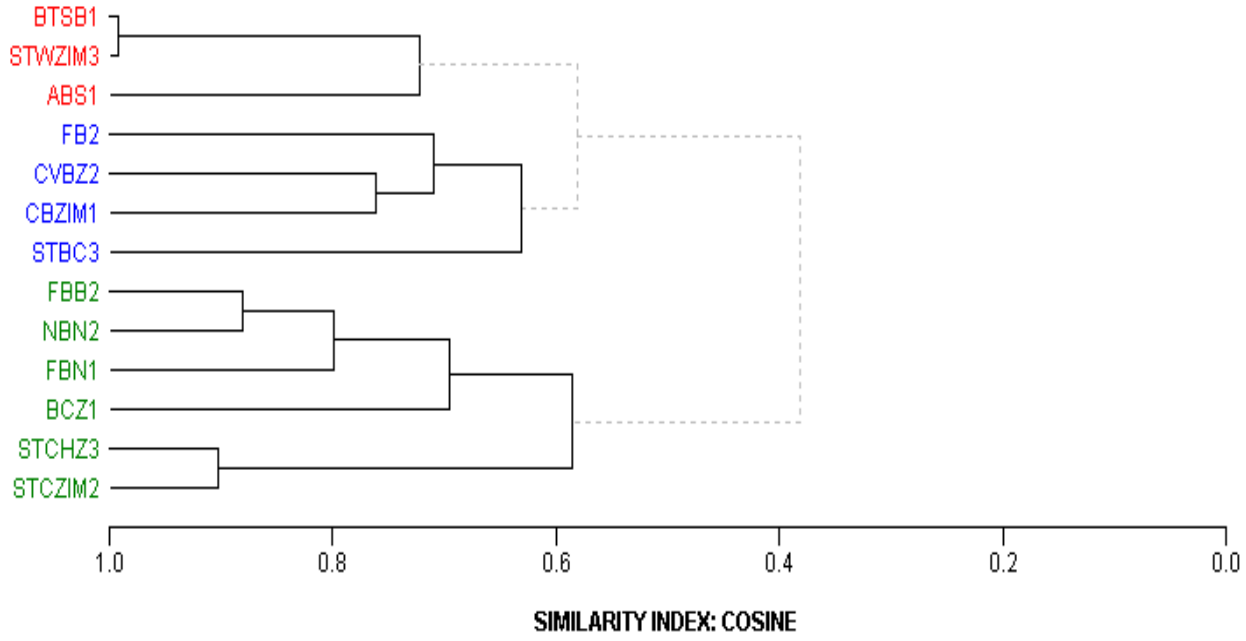

Fig. 1. Internet banking awareness similarity index

6. Internet banking fraud awareness crosstab matrix

The dialog box, Table 3 below, explores the connection between the internet fraud awareness distribution and subgroups of cases (banks). The table counts the total number of times internet fraud awareness has been disclosed by each bank from the sample size. The highest disclosure is displayed by STBC3 bank which has got 8 counts out of total of 12 (800%) followed by ABS1 bank which has got a frequency of 6 counts (600%). FBN1, FB2 and CBZZIM2 banks have a frequency of 5 each followed by STCHZ3 which has got a frequency of 4 counts (400%). STCZIM2 and FBB2 have frequency of 3 counts (300%) each. The least internet banking fraud awareness frequency

of 2 counts is displayed by the following banks each: BTSB1, NBN2, BCZ1, CVBZ2 AND STWZIM3. The Figure 2 below is a graphical display of the crosstab matrix to further visualize the findings.

In terms of correlation between the variables, the findings suggest that there is no statistically significant correlation between variables given that most p values are greater than 0.05, as shown in Table 3 below. This means increases or decreases in internet banking fraud awareness do not significantly relate to increases or decreases in cases. Only pharming and sim-card swaping have a p value less than 0.05 and that concludes that there is a statistically significant correlation between pharming and sim-card swapping, and cases. Also Pearson's r is negative (negative correlation) for most of the variables. This means that as internet banking fraud awareness increases in value, the cases decreases in value and also the positive Pearson's r co-efficient is not closer to 1 and concludes that there is no stronger correlation between the variables. This entails that internet fraud awareness by the Southern African banks is low, since there is no correlation (disclosure) of internet fraud awareness and the banking institutions.

Table 3. Internet banking fraud awareness - crosstab matrix

	BTSB1	FBB2	FBN1	NBN2	ABS1	FB2	STBC3	BCZ1	CVBZ2	STCHZ3	CBZIM1	STCZIM2	STWZIM3	Pearson's R	P value
Phishing	0.00%	0.00%	0.00%	0.00%	100.00%	100.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	0.00%	0.127	0.34
Pharming	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%	100.00%	100.00%	100.00%	0.00%	0.535	0.03
Scam	100.00%	0.00%	0.00%	0.00%	100.00%	100.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.124	0.344
Malware/ Virus	0.00%	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	-0.124	0.344
Key logging	0.00%	0.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	-0.293	0.166
Identity theft/fraud	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	100.00%	-0.211	0.244
Spyware	0.00%	100.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	-0.338	0.129
Cash send fraud	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	-0.077	0.401
Smishing	0.00%	0.00%	0.00%	0.00%	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%	0.045	0.443
Vishing	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	-0.057	0.427
Spam	0.00%	100.00%	100.00%	100.00%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%	-0.356	0.116
Sim card swaping	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%	100.00%	0.00%	0.00%	100.00%	0.00%	100.00%	0.00%	0.39	0.094

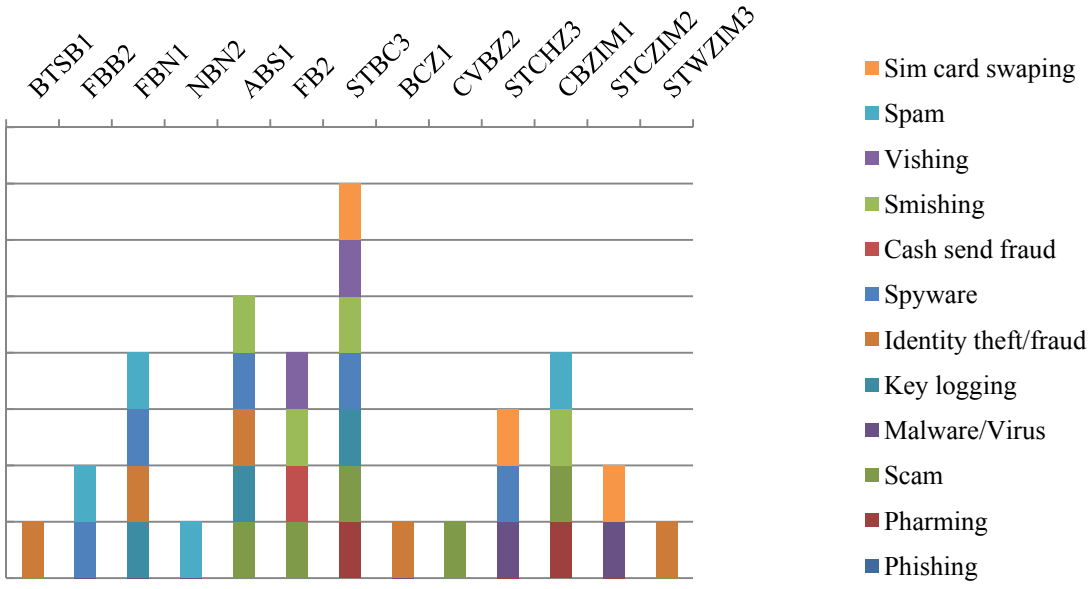

Fig. 2. Internet banking fraud awareness – bar display

The findings of this paper concur with banking fraud survey carried by Deloitte's (2015) findings in India which propose that there is lack of customer awareness in respect of internet fraud. Also, this study's findings are similar to Redelinghuis & Rensleigh's (2010) study on 'Customer perceptions on internet banking information protection' in South Africa. Their study conclusion suggests that, in many cases, the information is displayed when a client logs onto an internet banking site to perform internet banking transactions. The actual effectiveness of this information is uncertain. Financial institutions should educate and inform their clients adequately, but the bank's clientele must also make use of the various opportunities given to them to broaden their knowledge with regard to internet banking.

However, the findings of this study conflicts with the results from Federal Deposit Insurance Corporation (2004)'s study in US that financial institutions communicate directly with consumers to make them more aware of internet banking fraud such as identity theft fraud and phishing attacks. FDIC staff reviewed the Web sites of several of the nation's largest banks and found that banks are displaying the explanation of protections provided and not provided for online activities and alternative risk mechanisms. Correspondingly, Hutchings and Hayes (2009) found that the websites of Australia's four main banks, namely, the Commonwealth Bank of Australia, the National Australia Bank, Westpac and ANZ, were perused to identify how they advised their clients online about phishing attacks. All of these banking websites cautioned against accessing internet banking facilities from a link within an email.

Conclusion

This study concludes that internet banking fraud awareness disclosure is very low by many Southern African banks, as it is reflected by the findings above. Most of the banks disclosed less than half of the cited internet banking fraud awareness on their websites. This proposes that most of the financial customers engage internet banking transactions without sufficient awareness on potential internet threats and attacks. There is, consequently, high likelihood of being internet banking fraud victims.

Although there is positive reception of the accessible information on internet banking fraud awareness on Southern Africa banks' websites, this study proposes a call for increasing the awareness information and update financial consumers of internet banking fraud perpetrated by internetfraudsters. Internet banking fraud awareness is an imperative area to concentrate on for banking institutions and should unremittingly capitalize in it. The advent of the internet and proliferation of its use recently makes it an attractive medium for communicating the fraud, enabling a worldwide reach. Furthermore, to minimize internet banking fraud allied with internet activities conducted within the Southern Africa region, banks should make ample disclosure and awareness of internet fraud information on their websites and take correct measures to ensure adherence to customer privacy requirements applicable in the jurisdictions to which the bank is providing internet banking services. The expansion of internet and mobile banking requires newfangled recognition of customers' values for building long-term organization-customer relationships in the internet era.

Routine activity theory is incomparable among theories of criminology in that it seeks to explain varying internet banking fraud victimization risks among financial consumers and the role of fraudster spot in the occurrence of fraud events perpetrated on the internet. At the core of routine activity theory is the idea that fraudsters can only crop up when three bare bones of a circumstance are at hand: internet fraudsters, financial consumers who are the target and loath financial wardens (collapse by the banking institutions to enlighten customers about internet banking fraud). When these three situational fundamentals come jointly in place and time, the possibility of internet banking fraud incidents tiring is drastically amplified mostly in the dearth of awareness.

Implications and recommendations

This study proposes a policy by banking regulators or overseers in each of the Southern Africa jurisdictions for increasing the internet fraud awareness information and update financial consumers of internet banking fraud perpetrated by internet-fraudsters. This information must be exposed to the general public on the website of each banking institution not only to provide such information, when a customer has logged in on the internet application to transact. This would make internet banking fraud stuff readily retrievable and communicated in a mode that makes sense to the diverse financial customers.

More so, banking regulators in Southern Africa must enact regulations that make banking institutions to take correct measures to ensure adherence to customer privacy requirements applicable in the jurisdictions to which the bank is providing internet banking services.

The banking regulators also should make policies towards the prioritization of internet fraud risk on the risk registers. The banking institutions, therefore, should prioritize internet fraud risk aspects on organization's risk register so as to stand competitive advantage in the current technologically advanced era.

References

1. Abend, V., Peretti, B., Bach, A., Barry, K. & Donahue, D. (2008). Cyber Security for the Banking and Finance Sector, *Homeland Security*, pp. 1-17.
2. Angelakopoulos, G. & Mihiotis, A. (2011). E-banking: Challenges and opportunities in the Greek banking sector, *Electronic Commerce Research*, Volume 11, Issue 3, pp. 297-319.
3. Ahmad, W. (2008). *Is credit card fraud a real crime? Does it really cripple the E-commerce sector of E-business?* Proceedings - International Conference on Management of e-Commerce and e-Government, ICMeCG, pp. 364-370.
4. Alsheyyab, M.M.A. & Singh, D. (2013). Effect of trust on E-banking user's satisfaction: A review.*Research Journal of Applied Sciences, Engineering and Technology*, Volume 5, Issue 4, pp. 1397-1406.
5. Baker, C.R. (1999). An analysis of fraud on the Internet, *Internet Research*, Volume 9, Issue 5, pp. 348-360.
6. Brink, H., Walt, C., Rensburg, G. (2012). *Fundamentals of Research Methodology for Healthcare Professionals*. Juta & Company, South Africa.
7. Chiemeke, S.C., Evwiekpaefe, A.E. & Chete, F.O. (2006). The Adoption of Internet Banking in Nigeria: An Empirical Investigation, *Journal of Internet Banking & Commerce*, Volume 11, Issue 3, p. 4.
8. Chang, J.J.S. (2008). An analysis of advance fee fraud on the internet, *Journal of Financial Crime*, Volume 15, Issue 1, pp. 71-81.
9. Cohen, L.E. & Felson, M. (1979). Social Change and Crime Rate Trends: ARoutine Activity Approach, *American Sociological Review*, Vol. 44, No. 4, pp. 588-608. Published by: American Sociological Association Article Stable URL: http://www.jstor.org/stable/2094589.
10. Deloitte. (2015). India Banking Fraud Survey, Edition II, April 2015. *Deloitte Touche Tohmatsu India Private Limited*. Available at: www.deloitte.com/in.
11. Dzomira, S. (2015). Online and Electronic Fraud Prevention & Safety Tips Cognizance in South African Banks. *The Scientific Journal for Theory and Practice of Socio-economic Development*, 4 (8).
12. Dzomira, S. (2014). Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe, *Risk Governance and Control: Financial Markets and Institutions*, Volume 4, Issue 2, pp. 16-26.
13. Du-Plooy-Cilliers, F., Davis, C. & Bezuidenhout, R. (2014). *Research Matters*. Juta & Company, South Africa.
14. Federal Deposit Insurance Corporation. (2004). *Putting an End to Account-Hijacking Identity Theft. Division of Supervision and Consumer Protection*, Technology Supervision Branch.
15. Flavián, C. & Guinalíu, M. (2006). Consumer trust, perceived security and privacy policy, *Industrial Management & Data Systems*, Volume 106, Issue 5, pp. 601-620.
16. Gavish, B. (2003). Trust and Fraud on the Internet, *Informatica (Ljubljana)*, Volume 27, Issue 4, pp. 377-383.
17. Grazioli, S. & Jarvenpaa, S.L. (2000). Perils of Internet fraud: An empirical investigation of deception and trust with experienced Internet consumers. IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans, Volume 30, Issue 4, pp. 395-410.
18. Jayawardhena, C & Foley, P. (2000). Changes in the banking sector – the case of Internet banking in the UK, *Internet Research*, Volume 10, Issue 1, pp. 19-31.
19. Joyner, E. (2011). *Detecting and preventing fraud in financial institutions*, SAS Global Forum 2011, Issue: July 2007, pp. 1-16.
20. Kesharwani, A. & Tripathy, T. (2012). Dimensionality of Perceived Risk and Its Impact on Internet Banking Adoption: An Empirical Investigation, *Services Marketing Quarterly*, Volume 33, Issue 2, pp. 177-193.
21. Law, K. (2007). *Impact of Perceived Security on Consumer Trust in Online Banking*. Thesis.
22. Mahdi, M.D.H., Rezaul, K.M. & Rahman, M.A. (2010). *Credit fraud detection in the banking sector in UK: A focus on e-business.* 4th International Conference on Digital Society, ICDS 2010, Includes CYBERLAWS 2010: The 1st International Conference on Technical and Legal Aspects of the e-Society, pp. 232-237.
23. Mahdi, M.D.H. & Rezaul, K.M. (2012). Detecting credit fraud in E-Business system: An information security perspective on the banking sector in UK. Strategic and Practical Approaches for Information Security Governance: Technologies and Applied Solutions, pp. 346-368.
24. Miró, F. (2014). Routine activity theory, *The Encyclopedia of Theoretical Criminology*, pp. 1-7.
25. Narayanan, M., Koo, B. & Cozzarin, B.P. (2012). Fear of fraud and Internet purchasing, *Applied Economics Letters*, Volume 19, pp. 1615-1619.
26. Pratt, T.C., Holtfreter, K. & Reisig, M.D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory, *Journal of Research in Crime and Delinquency*, 47 (3), pp. 267-296.
27. Pravettoni, G., Leotta, S.N., Lucchiari, C. & Misuraca, R. (2007). Usability and trust in e-banking, *Psychological Reports*, Volume 101, Issue 3, Pt 2, pp. 1118-1124.
28. Redelinghuis, A. & Rensleigh, C. (2010). Customer perceptions on Internet banking information protection, *SA Journal of Information Management*, 12 (1), Art. #444, 6 p. DOI: 10.4102/sajim.v12i1.444.
29. Tewksbury, R.A and Mustaine, E.E. (2010). Encyclopedia of Criminological Theory: Cohen, Lawrence E., and Marcus K. Felson: Routine Activity Theory, In Contributors: Francis T. Cullen & Pamela Wilcox (Eds.), *Encyclopedia of Criminological Theory*. pp. 187-193.
30. Wong, D.H., Loh, C. & Yap, K.B. (2009). To Trust or Not to Trust: The Consumer's Dilemma with E-banking, *Journal of Internet Business*, pp. 1-28.

31. Wen-Jang Jih, W-J., Wong, S-Y. & Chang, T-B. (2005). Effects of Perceived Risks on Adoption of Internet Banking Services: An Empirical Investigation in Taiwan, *International Journal of E-Business Research*, Volume 1, Issue 1, pp. 70-72.
32. Wong, D.H., Loh, C., Turner, B., Bak, R. & Yap, K.B. (2009). Risky business: Perceived risk, trust and the use of e-banking. *Australian New Zealand Marketing Academy ANZMAC*, pp. 1-8.
33. Wei, W., Li, J., Cao, L., Ou, Y. & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. *World Wide Web*, Volume 16, Issue 4, pp. 449-475.
34. Yazdanifard, R., Wanyusoff, W.F., Behora, A.C. & Sade, A.B. (2011). Electronic banking fraud; The need to enhance security and customer trust in online banking, *Advances in Information Sciences and Service Sciences*, Volume 3, Issue 10, pp. 505-509.
35. Yu, C. & Asgarkhani, M. (2015). An investigation of trust in e-banking Evidence from Taiwan and New Zealand empirical studies, *Management Research Review*, Volume 38, Issue 12, pp. 1267-1284.