


“Internet banking fraud alertness in the banking sector: South Africa”

| | |
|--------------|---|
| AUTHORS | Shewangu Dzomira |
| ARTICLE INFO | Shewangu Dzomira (2017). Internet banking fraud alertness in the banking sector: South Africa. <i>Banks and Bank Systems</i> , 12(1-1), 143-151. doi: 10.21511/bbs.12(1-1).2017.07 |
| DOI | http://dx.doi.org/10.21511/bbs.12(1-1).2017.07 |
| RELEASED ON | Wednesday, 26 April 2017 |
| RECEIVED ON | Thursday, 23 February 2017 |
| ACCEPTED ON | Wednesday, 05 April 2017 |
| LICENSE |  This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License |
| JOURNAL | "Banks and Bank Systems" |
| ISSN PRINT | 1816-7403 |
| ISSN ONLINE | 1991-7074 |
| PUBLISHER | LLC “Consulting Publishing Company “Business Perspectives” |
| FOUNDER | LLC “Consulting Publishing Company “Business Perspectives” |



NUMBER OF REFERENCES

39



NUMBER OF FIGURES

4



NUMBER OF TABLES

4

© The author(s) 2024. This publication is an open access article.

Shewangu Dzomira (South Africa)

Internet banking fraud alertness in the banking sector: South Africa

Abstract

This paper analyzes internet banking fraud alertness to the general public by the South African banking institutions. The study is centered on routine activity theory, which is a criminology theory. A qualitative content analysis was used as the research technique for the interpretation of the text data from each bank's website through the systematic classification process of coding and identifying themes or patterns to provide an in-depth understanding of internet banking fraud alertness in the banking sector. A sample size of 13 out of 16 locally and foreign controlled retail banks in South Africa was used. The findings report that banks are not adequately providing internet fraud alertness information to the general public on their websites notwithstanding that most banks they do provide such information to log-in users and the use of that information is doubtful. This study suggests a need to augment internet banking fraud alertness information and passably inform internet banking users of the types of internet banking fraud perpetrated by internet fraudsters before they log-in for transacting. Considering the current and widespread quandary of internet banking fraud, the information of this paper is important for internet banking users to improve their aptitude in identifying fraudulent schemes and circumvent them, and for the banking institutions to invest more in the provision of internet banking fraud information to the general public.

Keywords: internet fraud, alertness, internet banking, e-commerce, cyber fraudster.

JEL Classification: G21, D18.

Received on: 23th of February, 2017.

Accepted on: 5th of April, 2017.

Introduction

The internet is a handy and an opportune means to get to a multitude audience exclusive of expend a lot of resources and is as well an intermediate employed by the banking sector to get to its customers instantaneously. According to Redelinghuis & Rensleigh (2010) South Africa has a well-developed and time-honored banking system which matches satisfactorily with those in many developed countries such as USA, but also sets South Africa apart from other emerging market countries like Brazil. Dlamini (2012) cited that the cybercrime that remains on top of the list of South Africa major cyber-attacks and threats include phishing, identity theft, monetary fraudulent attacks, key logging, malware, social engineering, spam, spyware and Trojan viruses (ISG Africa 2011). Kigerl (2012) undertook a study seeking to establish what variables envisage whether a nation is high in either spamming activity or phishing activity; it was found that wealthier nations with more internet users per capita had elevated cyber-crime activity.

According to Ladan (2003) with the speedy intensification of technology, the escalating exploitation of the internet and the expansion in information and communications technologies, business operations around the globe are more and more altering the manner they do business. A website, online message, or spam e-mail

can get to bulky numbers with very least amount of effort (Australian High Tech Crime Centre, 2010). While genuine websites, online messages and e-mails may be full of important information, and others make use of them as tools for perpetrating fraud. According to Cohen (2003) fraudsters have adopted the internet because of its amplified efficiency in easing the business processes of the illicit operations. The majority of people are swayed to do online business as e-commerce is progressively becoming more reliant on trust than brick and motor retail. Therefore as fraud increases the volume of e-commerce, transactions will be affected (Osford Ogis, 2012) and with the ever increasing of electronic market, fraud has become a crest barricade to e-commerce (Shouming & Bin, 2009).

Cybercrime and the hazard it crafts are rising in its reach, in concurrence with comparable expansion in information technology (Kigerl, 2012). According to Wang (2010) web service technology is perfect for system assimilation at the enterprise level, and for sustaining business-to-business integration and application-to-application electronic commerce (e-commerce) in the large disseminated internet and intranet environment together with the banking sector. The swift intensification of novel technologies brings into view advances in speeds and the aptitudes of wireless devices and networks, settles on continuous boost in customer prospects and forces e-commerce companies to concede customers, as their most chief asset (Stoica & Brote, 2012) nonetheless, as technologies advance so is internet fraudsters become more sophisticated. Internet fraud is escalating day after day with new ways for fraudulently extracting funds from corporations, businesses, and ordinary people emerging nearly hourly. The mounting utilization of on-line transactions and the invariable and sometimes ineffec-

© Shewangu Dzomira, 2017.

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

This is an Open Access article, distributed under the terms of the [Creative Commons Attribution-NonCommercial 4.0 International](#) license, which permits re-use, distribution, and reproduction, provided the materials aren't used for commercial purposes and the original work is properly cited.

tive alertness of both seller and buyer apparently lead to the conclusion that the cyber fraudsters seems to be one-step ahead at all times (Khin, 2009).

According to Dlamini & Modise (2012) better bandwidth and explosion of mobile phones with access to internet in South Africa entail enlarged access to internet by the South African population. Such colossal boost in right to use Internet amplifies vulnerabilities to cyber-crime and attacks. As a result education and awareness are consequently essential to guarantee that both financial consumers and businesses are alert of the substance of the internet fraud predicament and well-informed about its sprouting forms (OECD, 2008). Banking institutions for that reason have the duty to inform and educate their customers of impending threats and risks that may be allied with the use of internet and other digital banking alternatives (IBA, 2012). More so, according to Farmer (2013) awareness and education efforts by banking institutions can be attained via security links on the institution's website.

Against this background this paper seeks to analyze internet fraud banking fraud alertness to the general public in South African banking sector via their websites.

1. Literature review

User-customization is progressively more widespread in internet banking and commerce, while future speculation of wireless and internet banking benefits could generate more revenue to the banking services sector. Nevertheless, internet networks and electronic systems are experiencing attacks and threats from many areas. Information will be accessible on the classes of security and privacy threats, integrity threats, vulnerabilities, delay and denial threats that are being aimed at towards corporate, banking institution, and individual assets (Newman, 2006). An e-commerce centered society has demonstrated to be unavoidable and has been branded to be characterized with an assortment of other internet-related frauds allied with the use of ATM, Master-Card, Debit card, credit card and other medium for online transactions (Elufisan, 2012).

According to Felten et al. (1997) Web spoofing permits an attacker to craft "shadow copy" of the whole World Wide Web and accesses to the shadow Web are directed via the attacker's electronic gadget, permitting the attacker to screen all of the victim's activities including any passwords or account numbers the victim uses. The fraudster can also cause bogus data to be sent to Web servers in the victim's name, or to the victim in the name of any Web server. In concurrence to that Dinev (2006) alluded that counterfeit web sites hoodwink the innocent into exposing personal data, undermining all consumers'

trust in e-commerce, no matter how honest the genuine online business really is. Consequently, it is uncomplicated for cyber fraudsters to make their websites and messages appear authentic and plausible and sometimes tough for customers and investors to tell the dissimilarity between verity and fiction (Australian High Tech Crime Centre, 2010). In support to that Grazioli & Jarvenpaa (2000) carried a study that sheds light on consumers' susceptibility to attack by hackers posing as a legitimate site (phony website). The study observes consumer assessments of a real commercial web site and a fraudulent site that imitates it and the spurious site holds malicious manipulations calculated to augment trust in the site, reduced apparent risk, and eventually add to the probability that visitors would purchase from it.

Georgescu (2005) posits that social-engineering schemes use 'spoofed' e-mails to direct consumers to sham websites premeditated to swindle beneficiaries into revealing financial data, such as credit card numbers, account usernames, passwords and social security numbers and Perumal (2008) added that they pretense as a truthful entity in an electronic communication. Phishing endeavors have targeted bank customers and online payment services. Research has revealed that phishers may in principle be able to ascertain what relationship a potential victim and a bank has, and then forward a proper spoofed email to this victim. Moreover by commandeering brand names of banks, e-retailers and credit card companies, phishers habitually persuade recipients to act in response. In some occasions technical artifice schemes plant crime-ware onto PCs to nick identifications directly, frequently using Trojan, key-logger, malware, spyware and pharming crime-ware misdirects users to fraudulent sites or proxy servers, classically through DNS hijacking or poisoning (Georgescu, 2005; US-CERT, 2008; First Bank, 2014).

Perumal (2008) alluded that sometimes smishing and vishing techniques are used since not all phishing attacks need a fake website. Messages that allege to be from a bank tell customers to dial a phone number concerning problems with their bank accounts asking users to enter their account numbers and PIN. Voice phishing occasionally uses bogus caller-ID data to give the appearance that calls come from a trusted organization. According to York (2010) residents of Sanford, Maine, received phone calls that seemed to be from the Sanford Institution for Savings (SIS), a local bank, informing them that their accounts had been frozen, and they required to give full account information in order to maintain their accounts open. The calls were not from SIS, but were from cyber fraudsters looking for tricking people into giving their financial account details.

As identity theft persists to nurture as a crime and a social, financial and security worry, questions of liability turn out to be more essential (Deybach, 2007). Identity theft involves financial or other personal information stolen with the target of ascertaining another person's identity as the thief's own. Identity theft related fraud is more widespread and involves financial or other private information stolen, or completely invented, to make purchases or gain right of entry to financial accounts (Hinde, 2005). As more organizations offer greater online access for their customers, professional criminals are effectively using methods such as phishing and pharming to pilfer personal finances and carry out identity theft at a global level (Perumal, 2008; McGuire & Dowling, 2013). Furthermore, identity theft is augmented by the nature of up-to-the-minute transactions systems where in the modern economy, sellers are willing to tender goods and services to unfamiliar person in exchange for a pledge to pay, provided the promise is supported by data that connect the buyer to a specific account or credit history (Anderson et al., 2008).

Mass marketing frauds and consumer scams such as 419 (advance fee) fraud, romance scams, pyramid schemes, inheritance scams, charity, lottery and phishing scams are frequently used to prop up phony money-spinning investment schemes or to multiply forged information about a business (McGuire and Dowling, 2013). Numerous scams, including advance fee frauds, use spam to get to would-be victims. These messages come from persons who claim to want help moving a large sum of money out of their country and folks who take action to the messages often turn into victims of fraud and identity theft (Holt & Graves, 2007). Concurring to that Chang (2008) posits that advance fee fraud on the internet is a plague that rakes in hundreds of millions of dollars annually. The dawn of the internet and propagation of its exploitation makes it an eye-catching means for corresponding fraud, facilitating a global reach.

According to McGuire & Dowling (2013) Oxford Internet Survey 2013 reported that 19% of internet users in Britain had experienced phishing scam; Communications Market Report (Ofcom, 2012) survey results show that 28% of UK internet users had experienced spam emails and Cyber Security Survey (Eurobarometer, 2012) survey results in UK reveals that 52% of internet users experienced a scam email. Given the level at which South Africa is in terms of finance and banking technologies it cannot be spared from experiencing similar incidents.

2. Theoretical framework

This study is premised on routine activity theory. Cohen and Felson (1979) postulated the routine activity theory (criminology theory) centred on the supposition that the majority of criminal acts need junction in

space and time of probable offenders, fitting targets and the nonappearance of proficient guardians against crime. In addition Tewksbury & Mustaine (2010) further emphasised the hub of routine activity theory, as three essential locational rudiments that must be there for crime to transpire: existence of potential offenders (individuals seeking/able/willing to commit offenses), presence of fitting targets (individuals or property that is vulnerable or available), and a deficiency of capable and prepared guardians (a need of protection/supervision or individuals/devices capable to ward off a reprobate). In support to that Pratt et al (2010) cited that changes in lawful opportunity structures, such as technology can amplify the meeting of aggravated criminals and appropriate targets in the deficit of proficient protection. The Internet has principally altered consumer practices and has concurrently long-drawn-out opportunities for cyber-fraudsters to target online consumers. However, Yar (2005) argued that from his assessment which wrap ups that, even though a few of the theory's core concepts can certainly be functional to cyber-crime, there lingers imperative differences between 'virtual' and 'terrestrial' worlds that limit the theory's expediency. Notwithstanding, according to Miro (2014) the routine activity theory also advocates that changes in the structure of the models of daily activity (technology driven life) could elucidate the ascending in (internet banking fraud) crime. Therefore there is need for financial guardians (banking institutions) to expand their internet banking fraud alertness.

3. Methodology

The sampling frame for this study was made up of 16 locally controlled and foreign controlled retail banks, on the list that contains the latest information available to the Bank Supervision Department of the South African Reserve Bank in terms of the provisions of the Banks Act, 1990. A sample size of 13 banks was used and the banks were randomly selected on the basis of website accessibility. A qualitative content analysis was used as the research method for the interpretation of the text data through the systematic classification process of coding and identifying themes or patterns (du Plooy-Cilliers, 2014) to provide an in-depth understanding of internet banking fraud alertness in the banking sector. The content on internet banking fraud alertness was retrieved from each bank's website. Coding process was done on the retrieved texts marking segments of data under category – fraud type and the codes were represented by different fraud types and the variables were represented by bank, case and location. The statistical analysis was done using frequencies, cluster analysis, similarity matrices, co-occurrences and crosstab matrix. Bar charts and dendrograms were used to further visualize the display of the results.

4. Data source

The list of the banks and their websites used as the sample size was retrieved from the Reserve Bank of South Africa's website <https://www.resbank.co.za/RegulationAndSupervision/BankSupervision/Pages/SouthAfricanRegisteredBanksAndRepresentativeOffices.aspx> (accessed on 15 October 2016). The relevant data (internet banking fraud alertness) for analysis was subsequently copied from each bank's website.

5. Findings and discussions

5.1. Internet banking fraud types. The coding frequencies list from Table 1 below shows internet banking fraud types in the codebook along with

their description and the category to which they belong. It was used to obtain statistics for each fraud type, and the number of cases, in which they are found. It was found out that scam had the highest code frequency of 7.9% (code count of 11) appearing in 7 banks. It reflects that scam awareness is the highest than others but however using case frequencies results it shows that phishing and identity theft (both with similar case frequency of 64.30% from 9 banks) are the most disclosed across the banking sector. Credit card, pharming and cash send fraud have the lowest fraud type awareness frequency of 0.70% each from single appearance in 1 bank (7.10%). For further visual display the bar chart below (Fig. 1) displays the relative frequencies of fraud types in an ascending order.

Table 1. Internet and digital banking fraud type's awareness frequencies

| Category | Code | Count | % Codes | Cases | % Cases |
|---------------------------|--------------------|-------|---------|-------|---------|
| Fraud type | Scam | 11 | 7.90% | 7 | 50.00% |
| Fraud type | Phishing | 10 | 7.20% | 9 | 64.30% |
| Fraud type | Identity theft | 10 | 7.20% | 9 | 64.30% |
| Fraud type | Card skimming | 8 | 5.80% | 6 | 42.90% |
| Fraud type | ATM | 7 | 5.00% | 7 | 50.00% |
| Fraud type | Spyware | 5 | 3.60% | 3 | 21.40% |
| Fraud type | Trojans/virus/worm | 4 | 2.90% | 3 | 21.40% |
| Fraud type | Spoofing | 3 | 2.20% | 3 | 21.40% |
| Fraud type\ Phishing type | Smishing | 3 | 2.20% | 3 | 21.40% |
| Fraud type\ Phishing type | Vishing | 3 | 2.20% | 3 | 21.40% |
| Fraud type | Keylogging | 3 | 2.20% | 3 | 21.40% |
| Fraud type | Spam email | 3 | 2.20% | 2 | 14.30% |
| Fraud type | Business fraud | 2 | 1.40% | 2 | 14.30% |
| Fraud type | Debit card | 2 | 1.40% | 2 | 14.30% |
| Fraud type | SIM card swapping | 2 | 1.40% | 2 | 14.30% |
| Fraud type | Credit card | 1 | 0.70% | 1 | 7.10% |
| Fraud type | Pharming | 1 | 0.70% | 1 | 7.10% |
| Fraud type | Cash send | 1 | 0.70% | 1 | 7.10% |

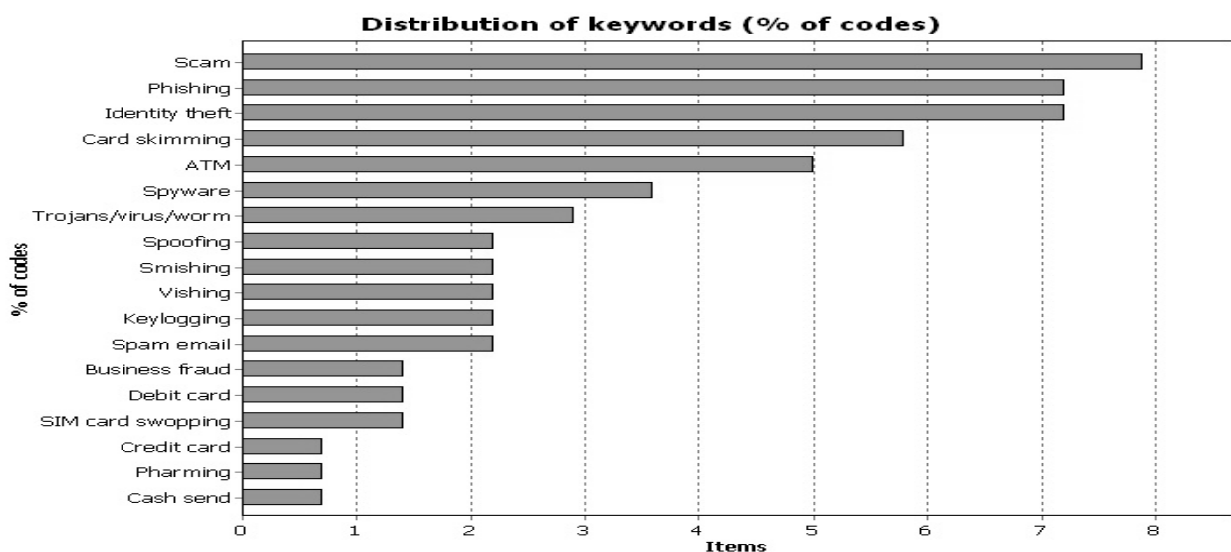


Fig. 1. Internet banking fraud type – bar chart

5.2. Internet banking fraud type alertness co-occurrence (similarity matrix and cluster analysis using similarity index). Using Ochiai's coefficient – this index is the binary form of the cosine measure which is represented by $SQRT(a^2/((a+b)(a+c)))$, where a represents cases where both items occur, and b and c represent cases, where one item is present but not the other one. From Table 2 below scam and identity theft alertness form a cluster with the highest co-efficient of 0.778 followed by two clusters, which are combinations of SIM card swapping and spoofing; and

card skimming and phishing with co-efficient of 0.667 each. These clusters depict fraud types that tend to appear together and occur more often. At the end of the agglomeration is the combination of fraud types that are independent from one another or those that do not appear together (cash send, business fraud, spam email, smishing and pharming) with an average co-efficient of 0.1 on estimation. From Table 2 below 9 clusters have a co-efficient of 0.5 and above whilst 8 clusters have a co-efficient <0.5, which implies that there is moderate co-occurrence similarity.

Table 2. Internet banking fraud type – co-occurrence similarity matrix (Ochiai's coefficient)

| | ATM | Business fraud | Card skimming | Cash send | Credit card | Debit card | Identity theft | Keylogging | Pharming | Phishing | Scam | SIM card swapping | Smishing | Spam email | Spoofing | Spyware | Trojans/virus/worm | Vishing |
|--------------------|-------|----------------|---------------|-----------|-------------|------------|----------------|------------|----------|----------|-------|-------------------|----------|------------|----------|---------|--------------------|---------|
| ATM | 1 | 0 | 0.444 | 0 | 0 | 0.125 | 0.455 | 0.25 | 0.143 | 0.6 | 0.4 | 0.125 | 0.25 | 0.286 | 0.25 | 0.25 | 0.25 | 0.111 |
| Business fraud | 0 | 1 | 0.143 | 0.5 | 0.5 | 0.333 | 0.1 | 0 | 0 | 0.222 | 0.125 | 0 | 0 | 0 | 0 | 0.25 | 0.25 | 0.25 |
| Card skimming | 0.444 | 0.143 | 1 | 0.167 | 0 | 0 | 0.5 | 0.286 | 0.167 | 0.667 | 0.444 | 0.333 | 0.5 | 0.143 | 0.5 | 0.5 | 0.5 | 0.5 |
| Cash send | 0 | 0.5 | 0.167 | 1 | 0 | 0 | 0 | 0 | 0 | 0.111 | 0 | 0 | 0 | 0 | 0 | 0.333 | 0.333 | 0.333 |
| Credit card | 0 | 0.5 | 0 | 0 | 1 | 0.5 | 0.111 | 0 | 0 | 0.111 | 0.143 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Debit card | 0.125 | 0.333 | 0 | 0 | 0.5 | 1 | 0.1 | 0 | 0 | 0.222 | 0.125 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Identity theft | 0.455 | 0.1 | 0.5 | 0 | 0.111 | 0.1 | 1 | 0.333 | 0.111 | 0.636 | 0.778 | 0.222 | 0.333 | 0.1 | 0.333 | 0.2 | 0.2 | 0.2 |
| Keylogging | 0.25 | 0 | 0.286 | 0 | 0 | 0 | 0.333 | 1 | 0 | 0.333 | 0.429 | 0.667 | 0.2 | 0.25 | 0.5 | 0.2 | 0.2 | 0.2 |
| Pharming | 0.143 | 0 | 0.167 | 0 | 0 | 0 | 0.111 | 0 | 1 | 0.111 | 0.143 | 0 | 0.333 | 0 | 0.333 | 0.333 | 0 | 0.333 |
| Phishing | 0.6 | 0.222 | 0.667 | 0.111 | 0.111 | 0.222 | 0.636 | 0.333 | 0.111 | 1 | 0.6 | 0.222 | 0.333 | 0.1 | 0.333 | 0.333 | 0.333 | 0.333 |
| Scam | 0.4 | 0.125 | 0.444 | 0 | 0.143 | 0.125 | 0.778 | 0.429 | 0.143 | 0.6 | 1 | 0.286 | 0.25 | 0.125 | 0.429 | 0.25 | 0.25 | 0.25 |
| SIM card swapping | 0.125 | 0 | 0.333 | 0 | 0 | 0 | 0.222 | 0.667 | 0 | 0.222 | 0.286 | 1 | 0.25 | 0.333 | 0.667 | 0.25 | 0.25 | 0.25 |
| Smishing | 0.25 | 0 | 0.5 | 0 | 0 | 0 | 0.333 | 0.2 | 0.333 | 0.333 | 0.25 | 0.25 | 1 | 0 | 0.5 | 0.2 | 0 | 0.5 |
| Spam email | 0.286 | 0 | 0.143 | 0 | 0 | 0 | 0.1 | 0.25 | 0 | 0.1 | 0.125 | 0.333 | 0 | 1 | 0.25 | 0.25 | 0.25 | 0 |
| Spoofing | 0.25 | 0 | 0.5 | 0 | 0 | 0 | 0.333 | 0.5 | 0.333 | 0.333 | 0.429 | 0.667 | 0.5 | 0.25 | 1 | 0.5 | 0.2 | 0.5 |
| Spyware | 0.25 | 0.25 | 0.5 | 0.333 | 0 | 0 | 0.2 | 0.2 | 0.333 | 0.333 | 0.25 | 0.25 | 0.2 | 0.25 | 0.5 | 1 | 0.5 | 0.5 |
| Trojans/virus/worm | 0.25 | 0.25 | 0.5 | 0.333 | 0 | 0 | 0.2 | 0.2 | 0 | 0.333 | 0.25 | 0.25 | 0 | 0.25 | 0.2 | 0.5 | 1 | 0.2 |
| Vishing | 0.111 | 0.25 | 0.5 | 0.333 | 0 | 0 | 0.2 | 0.2 | 0.333 | 0.333 | 0.25 | 0.25 | 0.5 | 0 | 0.5 | 0.5 | 0.2 | 1 |

5.3. Internet banking fraud type alertness - similarity matrix by banks. Figure 2 below shows clustering performed on banks; the distance

matrix used for clustering consists of cosine coefficients computed on the relative frequency of the various fraud types alertness.

Table 3. Internet banking fraud type – similarity matrix

| | BANK 1 | BANK 2 | BANK 3 | BANK 4 | BANK 5 | BANK 6 | BANK 7 | BANK 9 | BANK 10 | BANK 11 | BANK 12 | BANK 13 |
|---------|--------|--------|--------|--------|--------|--------|--------|--------|---------|---------|---------|---------|
| BANK 1 | 1 | 0.41 | 0.376 | 0.583 | 0.552 | 0.581 | 0.643 | 0.53 | 0.533 | 0.424 | 0.369 | 0.5 |
| BANK 2 | 0.41 | 1 | 0.46 | 0.446 | 0.608 | 0.696 | 0.514 | 0.775 | 0.671 | 0.57 | 0.843 | 0.621 |
| BANK 3 | 0.376 | 0.46 | 1 | 0.575 | 0.425 | 0.521 | 0.52 | 0.473 | 0.382 | 0.481 | 0.441 | 0.333 |
| BANK 4 | 0.583 | 0.446 | 0.575 | 1 | 0.55 | 0.694 | 0.447 | 0.573 | 0.658 | 0.552 | 0.421 | 0.425 |
| BANK 5 | 0.552 | 0.608 | 0.425 | 0.55 | 1 | 0.777 | 0.626 | 0.709 | 0.46 | 0.649 | 0.658 | 0.724 |
| BANK 6 | 0.581 | 0.696 | 0.521 | 0.694 | 0.777 | 1 | 0.603 | 0.752 | 0.544 | 0.55 | 0.588 | 0.686 |
| BANK 7 | 0.643 | 0.514 | 0.52 | 0.447 | 0.626 | 0.603 | 1 | 0.668 | 0.353 | 0.528 | 0.521 | 0.559 |
| BANK 9 | 0.53 | 0.775 | 0.473 | 0.573 | 0.709 | 0.752 | 0.668 | 1 | 0.701 | 0.858 | 0.901 | 0.662 |
| BANK 10 | 0.533 | 0.671 | 0.382 | 0.658 | 0.46 | 0.544 | 0.353 | 0.701 | 1 | 0.705 | 0.75 | 0.5 |
| BANK 11 | 0.424 | 0.57 | 0.481 | 0.552 | 0.649 | 0.55 | 0.528 | 0.858 | 0.705 | 1 | 0.88 | 0.674 |
| BANK 12 | 0.369 | 0.843 | 0.441 | 0.421 | 0.658 | 0.588 | 0.521 | 0.901 | 0.75 | 0.88 | 1 | 0.677 |
| BANK 13 | 0.5 | 0.621 | 0.333 | 0.425 | 0.724 | 0.686 | 0.559 | 0.662 | 0.5 | 0.674 | 0.677 | 1 |

The more similar two cases will be in terms of the distribution of codes, the higher will be this coefficient. From Figure 2 (tree graph) and Table 3 above, Bank 9 and Bank 12 have a cluster with the highest co-efficient of 0.901 followed by cluster of Bank 11 and Bank 12, and Bank 9 and Bank 11

with 0.88 and 0.858 co-efficient respectively. This means that the 3 banks have more similar fraud types awareness distribution on their website security centres or otherwise. The last cluster with the lowest co-efficient of 0.5 on average includes Banks 3, 13, 6, 5, 10 and 11.

Dendrogram

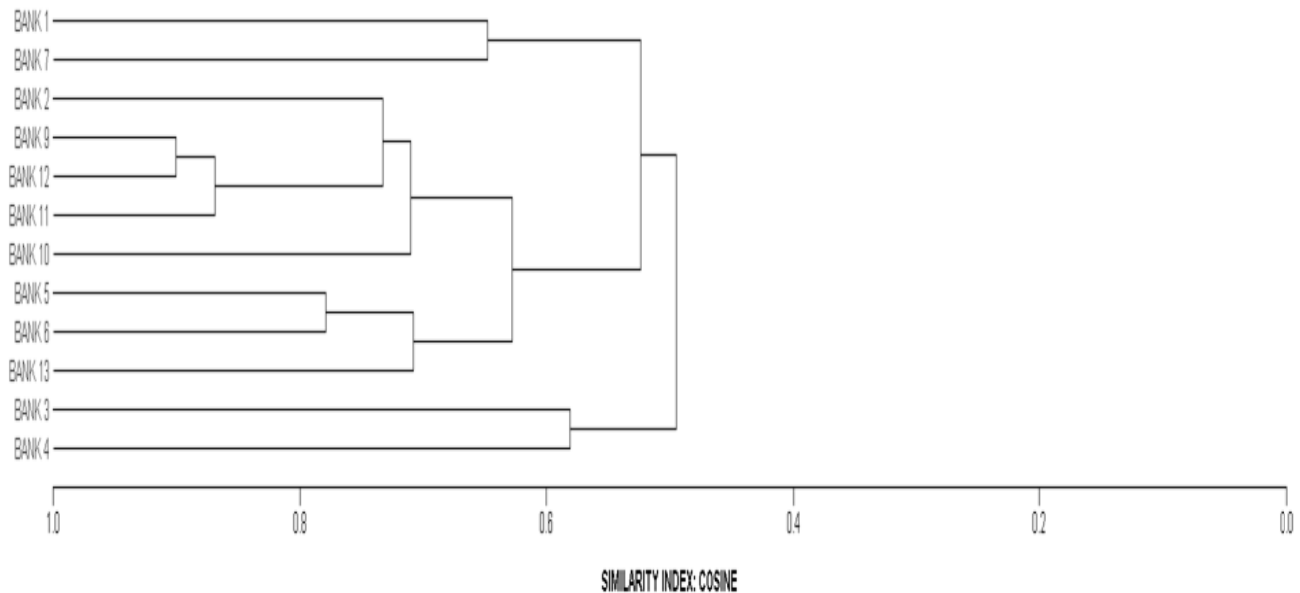


Fig. 2. Internet banking fraud type – similarity index

5.4. Internet banking fraud type alertness – crosstab matrix. The dialog box of Table 4 below explores the relationship between the fraud types

alertness distribution assigned to website documents and subgroups of cases defined by values of categorical variable.

Table 4. Internet banking fraud type alertness – crosstab matrix

| | BANK 1 | BANK 2 | BANK 3 | BANK 4 | BANK 5 | BANK 6 | BANK 7 | BANK 9 | BANK 10 | BANK 11 | BANK 12 | BANK13 | Pearson's R | P value |
|--------------------|--------|--------|--------|--------|--------|--------|--------|--------|---------|---------|---------|--------|-------------|---------|
| Cash send | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | -0.459 | 0.133 |
| Spam email | 0.00% | 0.00% | 2.50% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | -0.279 | 0.379 |
| Spyware | 1.30% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 3.80% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | -0.189 | 0.557 |
| Business fraud | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | -0.163 | 0.612 |
| Pharming | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | -0.149 | 0.644 |
| ATM | 0.00% | 0.00% | 1.30% | 1.30% | 1.30% | 1.30% | 1.30% | 1.30% | 0.00% | 1.30% | 0.00% | 0.00% | -0.149 | 0.645 |
| Trojans/virus/worm | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 2.50% | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | -0.126 | 0.696 |
| Vishing | 1.30% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | -0.087 | 0.789 |
| Phishing | 2.50% | 0.00% | 0.00% | 1.30% | 1.30% | 1.30% | 1.30% | 1.30% | 1.30% | 1.30% | 0.00% | 1.30% | -0.084 | 0.795 |
| Card skimming | 1.30% | 0.00% | 0.00% | 0.00% | 1.30% | 1.30% | 3.80% | 1.30% | 0.00% | 0.00% | 0.00% | 1.30% | -0.008 | 0.979 |
| Debit card | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | 0.01 | 0.976 |
| Smishing | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.161 | 0.617 |
| Spoofing | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.211 | 0.511 |
| Credit card | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | 0.239 | 0.454 |
| SIM card swapping | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.355 | 0.257 |
| Keylogging | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 0.00% | 1.30% | 0.00% | 1.30% | 0.508 | 0.092 |
| Identity theft | 0.00% | 1.30% | 0.00% | 0.00% | 1.30% | 1.30% | 1.30% | 2.50% | 1.30% | 1.30% | 1.30% | 1.30% | 0.576 | 0.05 |
| Scam | 0.00% | 0.00% | 0.00% | 0.00% | 1.30% | 0.00% | 1.30% | 2.50% | 1.30% | 5.10% | 1.30% | 1.30% | 0.634 | 0.027 |

The table counts the total number of times a fraud type has been disclosed. It was found that scam has the highest frequency of 5.10% recorded in Bank 11. However, in terms of the distribution of the fraud types across all the banks, Bank 7 disclosed the highest

number of fraud type's awareness (11 types out of 17 types) and Banks 5 and 13 follow with 10 types out of 17 and 9 types out of 17 types respectively. However, Bank 2 has the least disclosure of fraud type awareness only disclosing one type of fraud (identity theft).

The findings also conclude that there is no statistically significant correlation between variables given that the P values are greater than 0.05 as shown in Table 4 above. This means fraud types do not significantly relate to banks. Only scam has a P value of 0.027, which is less than 0.05 and concludes that there is a statistically significant correlation between

scam and banks. Also Pearson's r is negative (negative correlation) for most of the variables. This means that as fraud types increases, the number of banks decreases and also the positive Pearson's r co-efficient are not closer to 1 and concludes that there is no stronger correlation (disclosure) of internet banking fraud and the banks.

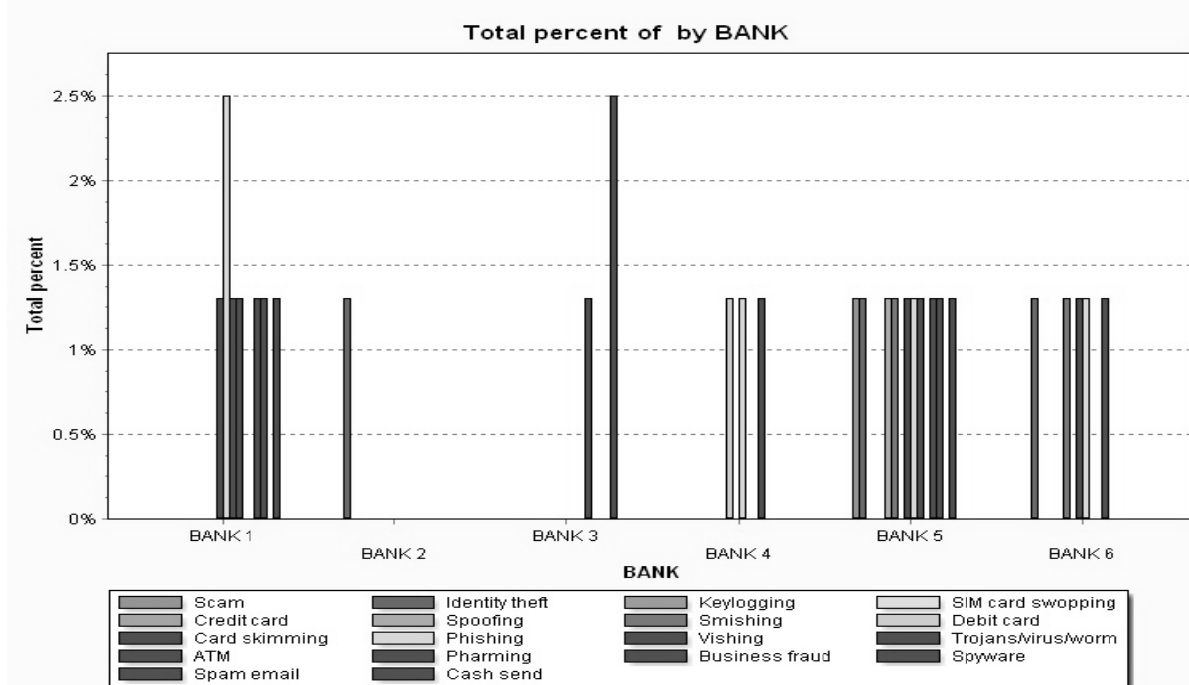


Fig. 3. Internet banking fraud type alertness – crosstab matrix (Banks 1-6)

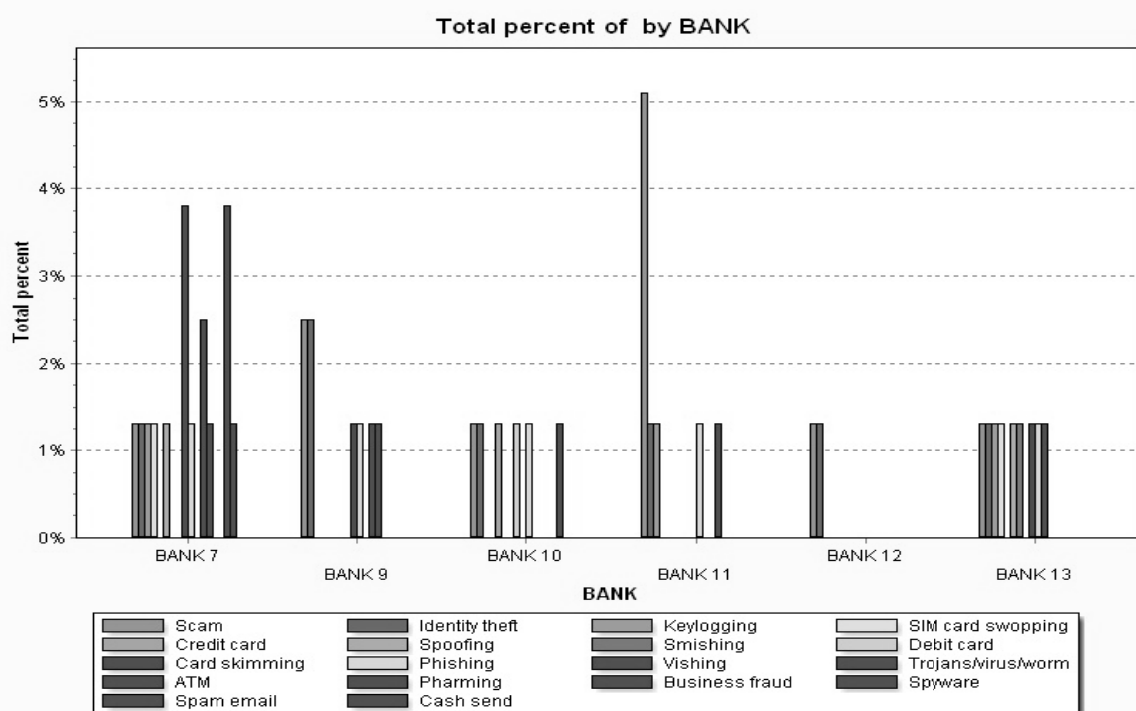


Fig. 4. Internet banking fraud type alertness – crosstab matrix (Banks 7-13)

This means that the disclosure of internet banking fraud alertness is low in many South African banks as is shown by the findings above. Most of the banks disclosed less than half of the cited in-

ternet banking fraud types as alertness on their websites. This suggests that most of the customers engage internet banking without sufficient alertness on potential cyber threats and attacks al-

though it can be argued that much of the internet fraud information is disclosed to log-in users. However, its usability is doubtful given that most of the internet banking customers do not have time to go through the log-in awareness. There is consequently high probability of being fatalities of internet banking fraud.

Regardless of the dissimilarity in type of methodology, the results of this paper correspond with Banking Fraud Survey carried by Deloitte (2015) in India, the results propose that there is lack of customer awareness as far as internet fraud is concerned. Moreover, the results from Nelson Mandela Bay study by Grobler et al. (2011) are consistency with this paper's findings which suggest that people in that area needed to be educated and informed about cyber security as they were naive of internet and digital technologies, and risks connected by using them. Moreover, this paper's findings are alike to Redelinghuis & Rensleigh (2010)'s study results on 'Customer perceptions on Internet banking information protection' in South Africa, which suggest that in numerous cases, the information is exhibited, when a client logs onto an Internet banking site to perform Internet banking transactions. The real efficacy of this information is hesitant. Banking institutions should educate and inform their clients passably, and the banks' clientele must also make use of the various opportunities given to them to broaden their knowledge with regard to Internet banking.

Conclusion and implications

Routine activity theory is inimitable among theories of criminology in that it seeks out to explicate shifting internet banking fraud persecution risks among

individuals and the responsibility of criminal location in the occurrence of criminal events perpetrated online. At the hub of routine activity theory is the thought that crimes can only crop up, when three fundamentals of a situation are in existence: cyber fraudsters or internet fraudsters, internet users, mostly bank customers who are the target, and incompetent, indisposed, or missing custodians (letdown by the banking institutions to bring up to date customers about internet fraud). When these three situational rudiments come jointly in place and time, the likelihood of internet banking fraud event happening is considerably augmented mostly in the absence of awareness.

While there is pleasure of the accessible information on internet banking fraud to the public on South African banks' websites, this study proposes a need to amplify the information and inform internet users of the types of internet banking fraud perpetrated by internet fraudsters. Internet banking fraud alertness is an imperative area to focus on for banking institutions and should relentlessly capitalize in it. Internet banking fraud material should be fluently retrievable and communicated in a mode that makes logic to the assorted clientele base, particularly within South Africa with its hodgepodge of humanities and vernaculars. Also, to curtail internet fraud risk allied with internet banking activities conducted both domestically and cross-border, banks should make plenty disclosure and awareness of internet fraud information on their web sites to the broad-spectrum public and take proper measures to guarantee observance to customer privacy necessities pertinent in the jurisdictions, to which the bank is providing internet banking services.

References

1. Anderson, K. B., Durbin, E., & Salinger, M. A. (2008). Identity Theft. *Journal of Economic Perspectives*, 22(2), 171-192.
2. Australian High Tech Crime Centre. (2010). Internet fraud and scams. *SEC Webpage*. Retrieved from <http://www.sec.gov/investor/pubs/cyberfraud.htm>
3. Chang, J. J. S. (2008). An analysis of advance fee fraud on the internet. *Journal of Financial Crime*, 15(1), 71-81.
4. Cohen, F. (2003). Internet fraud: Mythical online scams. *Computer Fraud and Security*, 4, 19.
5. Deloitte. (2015). India Banking Fraud Survey, Edition II, April 2015. *Deloitte Touche Tohmatsu India Private Limited*. Retrieved from www.deloitte.com/in
6. Deybach, G. (2007). Identity Theft and Employer Liability. *Risk Management*, 54, 14. Retrieved from <http://proquest.umi.com.library.capella.edu/pqdweb?did=1195022681&Fmt=7&clientId=62763&RQT=309&VName=PQD>
7. Dlamini, Z., & Modise, M. (2012). Cyber security awareness initiatives in South Africa: a synergy approach. In *7th International Conference on Information Warfare and Security*. Academic Conferences International. Retrieved from <http://hdl.handle.net/10204/5941>.
8. Dinev, T. (2006). Why spoofing is serious internet fraud. *Communications of the ACM*, 49(10), 76-82.
9. Elufisan, T. O. (2012). Combating Cyber-Fraud in a Cashless Economy: The Role (Relevance) of Biometric System. *SSRN Electronic Journal*. Retrieved from <http://ssrn.com/paper=2037816>
10. Farmer, R. (2003). FFIEC Supplemental Guidance to Authentication in an Internet Banking Environment. *Whitepaper, FIS Enterprise Governance, Risk and Compliance (EGRC) Solutions*. Retrieved from www.fisglobal.com/egrc
11. Felten, E. et al. (1997). Web spoofing: An internet con game. *Software World*, 28(2), 1-9. Retrieved from <http://www.csl.sri.com/~ddean/papers/spoofing.pdf>

12. First Bank. (2014). Internet Banking Awareness and Education Program. *Retail/Consumer awareness program* Retrieved from <https://www.sterbank.com/resources/internet-banking-awareness-and-education-program-retailconsumer-and-businesscommercial-clients/>
13. Georgescu, M. (2005). Some Issues about Risk Management for E-Banking. Retrieved from <http://ssrn.com/abstract=903419>
14. 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*, 30(4), 395-410.
15. Grobler, M., Flowerday, S., von Solms, R., and Venter, H. (2011). Cyber Awareness Initiatives in South Africa: A National Perspective. *Proceedings of Southern African Cyber Security Awareness Workshop (SACSAW) 2011*. Gaborone, Botswana 12 May 2011.
16. Hinde, S. (2005). Identity theft & fraud. *Computer Fraud and Security*, 6, 18-20.
17. Holt, T. & Graves, D. C. (2007). A qualitative analysis of advance fee fraud e-mail schemes. *International Journal of Cyber Criminology*, 1(1), 1-13. Retrieved from <http://www.cybercrimejournal.com/thomas&danielleijcc.htm>
18. Indiana Bankers Association. (2012). Electronic Fraud Awareness Advisory. *Fraud Awareness Task Force February, 2012*, 1-5.
19. Kigerl, A. (2012). Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review*, 30(4), 470-486.
20. Khin, E. (2009). Employing Artificial Intelligence to Minimize Internet Fraud. *International Journal of Cyber Society and Education*, 2(1), 61-72. Retrieved from <http://www.academic-journals.org/ojs2/index.php/IJCSE/article/viewFile/753/17>
21. Ladan, M. (2003). An overview of e-commerce technologies and challenges. *ACS/IEEE International Conference on Computer Systems and Applications*, 2003. Book of Abstracts.
22. Lawrence E. (1979). Cohen and Marcus Felson, *American Sociological Review*, 44(4), (Aug., 1979), 588-608. Published by: American Sociological Association Article Stable. Retrieved from: <http://www.jstor.org/stable/2094589>
23. McGuire, M., and Dowling, S. (2013). Cyber-crime: A review of the evidence Research Report 75, Chapter 2: Cyber-enabled crimes-fraud and theft. *Home Office*, 1-27.
24. Miró, F. (2014). Routine activity theory. *The Encyclopedia of Theoretical Criminology*, 1-7.
25. Newman, R. C. (2006). Cybercrime, Identity Theft, and Fraud: Practicing Safe Internet - Network Security Threats and Vulnerabilities. In *Proceedings of the 3rd annual conference on Information security curriculum development (InfoSec2006)*, 68-78. Retrieved from <http://dl.acm.org/citation.cfm?id=1231064>
26. OECD. (2008). OECD Policy Guidance on Online Identity Theft. *OECD Ministerial Meeting on the Future on Internet Economy. Seoul, Korea, 17-18 June, 2008. Korea Communications Commission*.
27. Osford Ogis. (2012). Impact of Fraud on E-Commerce: Proposed new Technologies to Combat Internet Fraud. *Interdisciplinary Journal of Contemporary Research in Business*, 4(3), 634-640.
28. Perumal, S. A. (2008). Impact of Cyber Crime on Virtual Banking. *SSRN Electronic Journal*. Retrieved from <http://ssrn.com/paper=1289190>
29. 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), 267-296.
30. Redelinghuis, A., & Rensleigh, C. (2010). Customer perceptions on Internet banking information protection. *SA Journal of Information Management*, 12(1), Art. #444, 6. DOI: 10.4102/sajim.v12i1.444
31. Schuckers, S. A. C. (2002). Spoofing and Anti-Spoofing Measures. *Information Security Technical Report*, 7(4), 56-62.
32. Shouming, C., & Bin, Z. (2009). How to cope with fraud of trusted third party in E-commerce: An analysis based on evolutionary game theory. In *2009 WASE International Conference on Information Engineering, ICIE 2009*, 61-64.
33. Stoica, E., & Brote, V. (2012). New Technologies Shaping the E-Commerce Environment. *Revista Economică*, Supplement, 379-385.
34. South African Reserve Bank. (2015). South African Registered Banks and Representative Offices. Retrieved from <https://www.resbank.co.za/RegulationAndSupervision/BankSupervision/Pages/SouthAfricanRegisteredBanksAndRepresentativeOffices.aspx> (15 April 2015).
35. 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*, 187-193.
36. US-CERT. (2008). Banking Securely Online. Produced 2006 by US-CERT, a government organization. Updated 2008.
37. Wang, X. H. (2010). The security technologies of web services for e-commerce. In *2010 International Conference on E-Product E-Service and E-Entertainment, ICEEE2010*.
38. Yar, M. (2005). The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407-427.
39. York, D. (2010). Identity, Spoofing, and Vishing. In *Seven Deadliest Unified Communications Attacks*. Syngress, 117-136. Retrieved from <http://www.sciencedirect.com/science/article/B6MBK-4YSJV3B-3/2/95fe21f7f36982cc0c5465c543e3d9a6>