South African Journal of Business Management
ISSN: (Online) 2078-5976, (Print) 2078-5585

The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention

Author:
Rachel Barker[1]

Affiliation:
[1]Department of Communication Science, School of Arts, College of Human Sciences, University of South Africa, Pretoria, South Africa

Corresponding author:
Rachel Barker,
barker@unisa.ac.za

Dates:
Received: 27 Jan. 2020
Accepted: 17 July 2020
Published: 14 Oct. 2020

How to cite this article:
Barker, R. (2020). The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention. *South African Journal of Business Management*, *51*(1), a1941. https://doi.org/10.4102/sajbm.v51i1.1941

Purpose: This study sets out to address the lack of studies to educate clients and create awareness on fraud prevention in this sector, specifically on e-banking fraud that falls into two main categories: phishing/vishing/Smishing and malware practices.

Design/methodology/approach: An interpretivist approach was used to analyse a real online website that is available to all users. The subject under study was the website of the South African Banking Risk Information Centre (SABRIC). The three concurrent cyclical flow of activity of the data analysis interactive model was utilised in the research. An abductive approach was used to report on the findings based on descriptions and interpretive comments relating it to and drawing on the theoretical thrusts identified. The research was conducted during the two time frames of 2017 and 2018.

Findings/results: It was found that SABRIC did use its website to communicate proactively with clients to create awareness and educate them on e-banking fraud prevention measures. A significant increase in proactive communication through various activities was evident when the 2017 and 2018 statistics were compared.

Practical implications: The main themes that emerged from the findings include the need for collaborative efforts, member training, intervention by government and law enforcement agencies and the importance of awareness of protective measures.

Originality/value: This study contributes to the limited body of knowledge and literature investigating the need for proactive communication through knowledge management typologies in emerging economic contexts to create awareness and educate clients on e-banking fraud prevention to address the intensification of cases in fraud.

Keywords: knowledge management; knowledge sharing; e-banking fraud prevention; fraudulent e-banking transactions; client relationships.

Introduction

> As banking fraud might ultimately affect customer relationship quality and customer loyalty, fraud prevention and its effective communication is an important topic for academic research. (Hoffman & Birnbrich, 2012, p. 390)

According to Mhamane and Lobo (2012), e-banking has become a prevalent mode for both online and internet-based transactions, resulting in intensification in cases of fraud associated with it. The results of a study conducted by Carminati, Caron, Maggi, Epifani and Zanero (2015, p. 176) highlighted the significant growth of e-banking fraud, fuelled by the underground economy of malware. According to them, internet banking fraud is difficult to detect because the fraudulent behaviour is dynamic, spread across different client profiles and are dispersed in large and highly imbalanced datasets (e.g. web logs, transaction logs, spending profiles). Jansen and Leukfeldt (2015) and Custers (2019) emphasised the need to educate people who have insufficient knowledge and skills regarding the safety and security of online banking, which makes it difficult for them to apply preventative measures to protect them. According to Miltonberger (2020), proactive communication on fraud prevention strategies may therefore enable the financial sector to enhance client relationships as it gives banks the opportunity to (re-)assure client trust in their services. They posit that proactive communication allows the financial sector to evoke a shared understanding of values between itself and its clients if they demonstrate their knowledge and competence regarding fraud prevention by communicating anti-fraud measures effectively, thereby creating a feeling of safety amongst clients (Rauyruen & Miller, 2007). This feeling of safety will arguably improve client relationship quality and loyalty, which are key success factors in the highly competitive retail banking industry (Alexander & Colgate, 2000). These results set the scene for this study to investigate the need for proactive communication and education of clients to create awareness on the prevention of fraudulent e-banking transactions through knowledge management (KM) and knowledge sharing within the emerging financial sector in a South African context. According to Jacobs and Maritz (2020), emerging economies differ from developed economies, specifically in terms of possible investors with greater profit earning opportunities, a much lower gross national income on a per capita basis, a greater reluctance towards accepting investment from other countries and the high degrees of exchange rate volatility. Most recent research focuses strongly on fraud detection measures and patents (Leite et al., 2018, p. 333; Pouwelse & Bruggink, 2016), with limited research conducted on fraud prevention. The purpose of this study is twofold: to propose a conceptual framework developed from a combination of different viewpoints to identify and discover different types of fraud and to examine how Africa's trusted financial crime risk information centre leveraging strategic partnerships used their website as one way for fraud prevention, by conveying information following fraudulent e-banking transactions to proactively manage and prevent clients to fall victims to these fraudulent actions.

The article is structured as follows. Firstly, a synopsis of the theoretical underpinning based on an extensive literature review is presented with specific focus on e-banking fraud, fraud prevention and client relationship building. Secondly, a theoretical framework is proposed. Thirdly, the methodology, data analysis and results are presented. Finally, a discussion of the main results based on the KM typologies that can be used to manage and control fraud prevention are described.

Key concepts

For application purposes, the key concepts of interest to this study are as follows:

E-banking fraud

E-banking fraud is one of the most profitable types of cybercrime today. According to Van der Meulen (2013, p. 713), 'the increased sophistication of attacks has complicated prevention and detection efforts, which in turn has allowed their success to proliferate'. Fraudulent e-banking transactions increase the financial burden on both service providers and clients, with the latter running increasing legal risks of being exposed to financial losses because of neglect. Jansen and Leukfeldt (2015, p. 31) stated the need to educate clients to avoid fraudulent schemes and emphasise that the move towards co-liability should not impede but enhance client relationship building. According to Andrews and Boyle (2008, p. 60), the main factors that affect client relations are the perceived risk, e-security, trustworthiness and privacy associated with transactions, especially in internet banking. The perceived risks emanating from cybercrime are equally as important in the world of growing digitisation, as clients face the risk of losing money through fraudulent transactions and misusing personal information (Drennan, Sullivan Mort, & Previte, 2006; Nataraj & Ashwani, 2018).

Fraud prevention

For the purpose of this study, 'fraud prevention describes the security measures to avoid unauthorised individuals from initiating transactions on an account for which they are not authorised' (Kovach & Ruggiero, 2011, p. 166) and includes education and training through proactive communication (Barker, 2018).

Client relationship building

The World Wide Web, specifically the internet, offers financial institutions the opportunity to build relationships with their clients and stakeholders. In addition, it can be used to disseminate information about a variety of topics, including fraud and to correct misinformation. Despite a growing sense that proactive communication on websites is important, research has found that website communication about fraud prevention is limited, especially in emerging economies. According to Greer and Moreland (2003), it is very important that websites should be used *in addition to* traditional media to communicate with employees and clients about fraud prevention and risk. Furthermore, empirical studies suggest that sustainable client relationships are characterised by mutual trust, satisfaction and commitment to addressing perceived risks (Lages, Lages, & Lages, 2005, pp. 1040–1048; Larghi, Lemus, Moguillansky, & Welschinger, 2015, p.18; Ng, Wang, Yap, Wood, & Krisnan, 2020).

Theoretical framework

The accelerated capacity of e-banking transactions and the internet can empower clients and counteract the threats posed by the increasingly fragmented media landscape. One way to counteract these threats is to engage with clients through proactive communication and KM by incorporating safety and security messages on the website. These messages should not only warn clients about prevalent fraudulent transactions but also reassure them. Authors like Gonzàlez-Herrero and Smith (2008, p. 145) point out that the internet either acts as a 'source of disinformation' based on rumours, hacking, copycat websites, web security breaks and all forms of cyberterrorism and cybercriminals or as a 'facilitator' or an agent that accelerates message dissemination and provides new knowledge. It is therefore argued that the KM theory, one of the most prominent theoretical approaches to the study of online communication, is one way of facilitating messages about fraud prevention. One of the key discourses of the KM paradigm is that embodied, tacit, implicit and narrative knowledge is important, as it is fundamental to all human awareness (Nonaka & Takeuchi, 1995). It allows for the transformation, sharing and processing of knowledge in four different forms: socialisation, externalisation, combination and internalisation (Barker, 2016; Nonaka & Takeuchi, 1995). The KM paradigm also presents a way to proactively manage and control the messages that are *acquired, transferred and assimilated* to ensure that knowledge is created, distributed and shared (Lee, Leong, Hew, & Ooi, 2013; Nonaka & Takeuchi, 1995).

A conceptual framework explains, either graphically or in narrative form, the key constructs and variables or factors that need to be studied and the presumed interrelationship between them (Miles, Huberman, & Salanda, 2013). This article uses the graphic conceptual framework proposed by Barker (2018, p. 81) to measure e-banking fraud prevention.

This conceptual framework focuses on fraud prevention and the three typologies of KM to communicate proactively with clients. In this context, *knowledge acquisition* refers to the provision of instructing information on the website to clients when a new fraudulent action has been identified and/or to remind them of existing methods used and procedures followed to commit cybercrime. It encompasses data gathering and mining, as well as knowledge construction based on the discovery of new knowledge. Three main types of messages should be constructed, namely messages that contain basic facts about fraud, messages with updated information and facts and messages that contain new information. These messages should tell clients what they can expect and how best to react to suspect events. Messages are usually sent via a security centre website and anti-fraud software pop-ups that warn clients when fraudsters access their accounts. Detailed links cover a broad spectrum of fraudulent transactions. *Knowledge transfer* is necessary and communication messages are continuously created and adjusted. Various messages and links enable real-time online interaction between banks and clients and share information to ensure the safety and security of online transactions. Examples of possible real-time fraudulent transactions should be given on various websites. Links should be used to transfer knowledge to the client. *Knowledge assimilation* should be substantiated through the control and management of messages before, during and after fraudulent actions by presenting methods and procedures to ensure safe e-banking transactions, providing informal and formal settings for interaction (e.g. hotlines and online links) and stating company practices to address fraud and the context in which it is managed and controlled. These are usually corroborated by linking clients to the security centre and using online fraud updates, media releases, campaigns, general security messages (formal or informal) and detailed methods, practices and procedures to address fraudulent actions proactively and reactively.

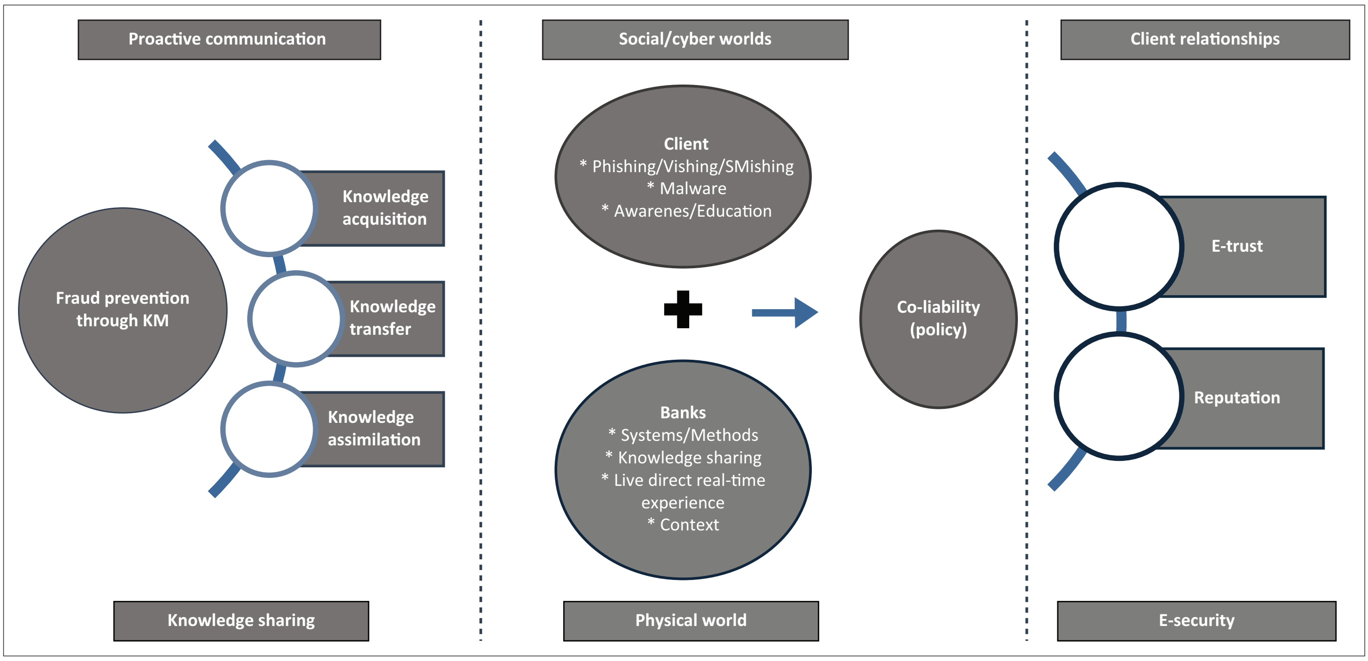
From this theoretical perspective, it is argued that the KM paradigm offers the opportunity to manage and control messages through knowledge sharing to educate clients and create awareness on e-banking fraud prevention. It is convenient to assess information through information and knowledge collection and knowledge donation and it is a significant antecedent to address reputational risks and innovation performance. Systems, methods, prompts, direct real-time experiences and so on can be used to educate and train clients and to create awareness to prevent third-party fraudulent transactions. It is further posited that such typologies should be used consistently and continuously to create awareness of fraudulent e-banking transactions in the social, cyber and physical worlds of both the client and the banks. Clients should be educated about and made aware of phishing/vishing/SMishing and malware-based fraudulent banking transactions and identify theft to prevent these crimes. This argument is indeed supported by various authors who indicated the need for the creation of awareness of fraudulent schemes and training in how to apply preventative measures. For example, according to Custers (2019, p. 71) this is 'critical in keeping online banking safe and secure'. Through constant prompts, clients should be made aware of existing and/or new fraudulent transactions and their coliability, which is crucial in the prevention of fraudulent e-banking transactions. The creation of e-security and e-trust will lead to sustainable client relationships and loyalty and maintain or enhance the reputation of the organisation.

Research methodology

The researcher followed an interpretivist approach, which required that information be seen as transient and understood only within context. The research was conducted in the natural setting of the subject under study and focused on unexplored processes (Babbie, 2007; Chambliss & Schutt, 2006); in other words, the focus was on a real online website that is available to all users. Based on the argument by Kim and Kuljis (2010) that:

> [*I*]nstead of investing a lot of time and energy in using more traditional methods for collecting data such as interviews, surveys and focus groups, a researcher may now be able to just download data from the Web without the need to engage with users. (p. 369)

This study focused on available web-based data only. Hence, the research culminated in an analysis of proactive communication on the website of the South African Banking Risk Information Centre (SABRIC) during two time frames (TF1: January 2017 to December 2017 and TF2: January 2018 to January 2019). The focus was on descriptive statistics on the prevention of fraudulent e-banking transactions and e-security, based on the identified and characterised theoretical typologies indicated in Figure 1. South African Banking Risk Information Centre, on behalf of the banking industry, cautions the public about banking crimes through proactive communication and knowledge sharing on their website. South African Banking Risk Information Centre is a non-profit foundation that has been established by the four major South African banks. It has 23 member banks and supports the South African banking industry in combating crime. South African Banking Risk



Source: Adapted from Barker, R. (2018). Knowledge management to prevent fraudulent e-banking transactions. *Communitas, 23*, 81. https://doi.org/10.18820/24150525/Comm.v23.5

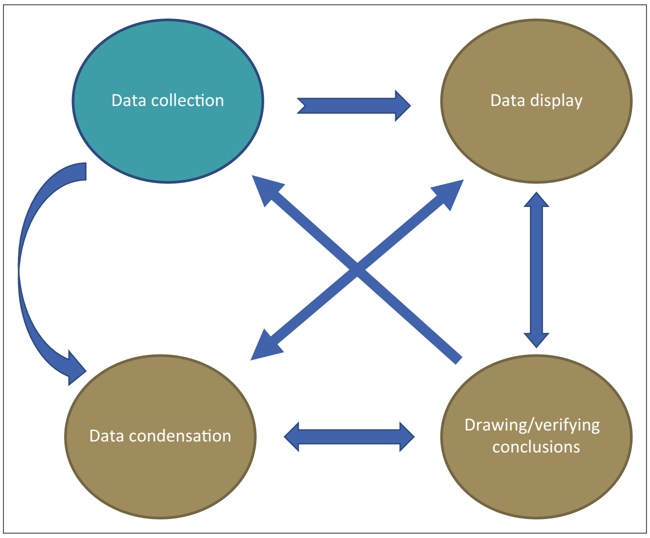
FIGURE 1: Conceptual framework for e-banking fraud prevention through knowledge management.

Information Centre's clients are South African banks and major Cash in Transit (CIT) companies, and its main responsibility is to detect, prevent and reduce organised crime in the banking industry. It coordinates interbank activities aimed at addressing organised bank-related financial crime, violent crime and cybercrime. It aims to create public awareness in order to enable banking clients to protect themselves against such crimes. It also acts as a nodal point between the banking industry and stakeholders in respect of issues relating to these crimes.

South African Banking Risk Information Centre was selected, as it represents most financial institutions in South Africa and was willing to participate in the research. In addition, information on proactive communication on the website was easily accessible and readily available, and the researcher was given permission to use information obtained through data mining. The research was guided by an in-depth analysis of a real-world dataset, which is 'paramount for our work (fraud analyse) and provides useful insights for future research' (Carminati et al., 2015, p. 177). The criteria were derived from a comprehensive literature review based on the conceptual framework and examined information used on the website to manage and control messages proactively through KM over two time frames. Messages sent before and after incidents of fraudulent e-banking transactions, and security measures that were communicated and put in place to prevent fraud, were investigated.

Data collection

For the purpose of this article, the four concurrent cyclical flows of activity in the data analysis interactive model, as proposed by Miles et al. (2013), were used in the website content analysis (see Figure 2).



Source: Miles, M.B., Huberman, A.M., & Saldana, J. (2013). *Qualitative data analysis: A methods sourcebook* (3rd edn). Los Angeles, CA: Sage

FIGURE 2: The four concurrent cyclical flows of activity in the data analysis interactive model.

Data collection investigated the use of proactive online communication aimed at controlling and managing awareness of fraudulent e-banking transactions. The data gathered included information on preventative measures posted on the SABRIC website during the specified time periods. Available and accessible pages with information about the prevention of fraudulent e-banking and/or e-security and the safety of online transactions were printed. Data condensation was carried out during the process of selecting, focusing, simplifying, abstracting and/or transforming selected website information in terms of the theoretical criteria and framework (Miles et al., 2013). Data display was used to organise, compress and assemble the information to enable the researcher to draw systematic and powerful conclusions. Conclusions were drawn and verified. The researcher noted patterns, explanations, casual flows and propositions, which were interwoven before, during and after data collection to make up the general domain called 'analyses'. The data displayed included all proactive communication such as media releases, videos, campaigns and safety measurements pertaining to fraudulent e-banking transactions.

In order to determine the cumulative number of fraud-related messages posted by SABRIC on the website during TF1 and TF2, the researcher conducted post hoc analyses of the site contents. Included in the analyses were additions and deletions of individual company-generated messages (e.g. media releases from the expert). The material printed included fraudulent e-banking transaction pages and links to additional information (campaigns, media releases and videos). Internal validity was addressed by evaluating the website and the concepts under investigation consistently during both time frames. This study also addressed validity through generalisation; it used KM and proactive communication typologies (see Figure 1), which can also be used in comparative studies in future.

Data analysis

Data were analysed following an iterative process. The researcher used data coding to identify typologies of initial concepts and integrative concepts applicable to all the subjects under study and selective coding to categorise these into emergent themes. Bowen (2009) referred to the iterative process as the skimming (superficial examination), reading (thorough examination) and interpretation of websites. In line with the objectives of the study, the printed documents proved to be rich sources of data. The researcher, as a non-participative observer trying to understand the meaning transferred to the clients, also used 'lurking'. This means that the researcher visited the SABRIC website and forums, but never contributed. The focus was on the three components of KM and only on asynchronous communication (communication with people through a one-to-many approach at different times). Table 1 summarises the main message constructions and links pertaining to e-banking fraud prevention on the SABRIC website during the specified study period.

The most prominent emerging themes in the proactive communication were the following:

1. *Collaboration:* Leveraging of partnerships with banks, cash-in-transit companies, government, law enforcement agencies (South African Police Service), the National Cybersecurity Hub (by putting robust proactive measures in place to build cyber resilience and create awareness of cybercrimes), Centre for Research in Information and Cyber Security (videos) and mobile network operators.
2. *Training:* Employees (MOU with Kaspersky Lab, a global cybersecurity company, to support SABRIC members to enhance skilled capacity through specialised training to combat cybercrime and contribute to create cybersecurity resilience in South Africa) and youth (collaboration with StarSave to celebrate Global Money Week from 12 to 18 March 2018).
3. *Protective measures to educate and create awareness through proactive communication*: Warnings and tips via regular proactive messages to clients with real-time examples of all scams.
4. *Need for intervention*: Urging government and law enforcement authorities to put special interventions in place across the country.

TABLE 1: Content of the website: comparison between message construction in 2017 and 2018.

KM/KS	Message constructions on e-banking fraud prevention	TF1: 2017	TF2: 2018
Videos (cyber-crime)	**2017:** *Skelm* (cybercriminal) is watching – Empower yourself, ATM card fraud (in 3 of the 11 official languages, that is, English, Afrikaans and Zulu), Carrying cash safely. This is called phising, Phishing – don't get hooked, If it is too good to be true it is, Sarah adventures videos **2018:** 10 New SABRIC surveys on computer online shopping, card fraud, computer hygiene, mobile hygiene, mobile protection pointers – cybercrime, computer malware, card fraud, malware protection, online shopping, mobile banking (focuses on tips), computer hygiene (2018)	6	10
Campaigns	**2017/2018:** We need your help! Small favour, big return, Banking Industry launches protection of personal information campaign. Keep your money safe this Festive Season, SABRIC warns consumers to beware of phishing and malware	4	4
Media releases (some released more than once)	**2017:** SABRIC Report: Credit card fraud has risen by 1%, SABRIC lauds special meeting on cash-in-transit heists. Release on card fraud statistics 2017, SABRIC & Nelson Mandela University join forces in the fight against cybercrime, Money matters matter, Ponzi & Pyramid schemes, Ngcobo station attack. 2018: Protect your money this festive season – introduced 'Money Bomb' scam, Kaspersky Lab helps build skilled capacity with SABRIC, Digital banking crime statistics – emphasises the 'no-clicking' principle. Beware when carrying cash – two types of crime with examples ('spotters' following clients after cash withdrawal or following them to another spot), Contactless bank cards – assurance that no 'tap and go' cards have been exploited. Update your details at the bank – for you safety and the country's, SABRIC concerned by increase in card fraud, SAPS and SABRIC recommit to intensify fight against bank robberies. Don't be a victim of criminals this festive season. Beware of the change in banking details scam, SABRIC welcomes release of annual crime statistics, SABRIC commends SAPS for speedy arrest of criminals. Online shopping just got safer, be vigilant to avoid card skimming, tighten social media security settings to avoid social engineering, SABRIC urges, SABRIC warns consumers to beware of phishing and malware. Banking industry launches protection of personal information campaign. Industry pleased by decrease in associated robberies, SABRIC statement on the decrease in certain bank-related crimes – focus on cash-in-transit and related crimes, card fraud decreases, banking industry report, you could be sharing too much personal information on social media, Department of Home Affairs (DHA) online services – as part of on-going working relationship and in spirit of co-operation with SABRIC to combat fraud, SABRIC encourages bank consumers to take care of their cybersecurity – inspiration of campaign against 'skelms' (sinister rascals), Wise up and watch out for schemes and scams, SABRIC cautions women to be alert on dating sites and social media platforms – Women's Month, Get rich quickly – money schemes, Don't let criminals get their hands on your money, Safe banking over the festive season, ATM card swopping, OR Tambo heist, SABRIC release of card fraud stats, Cyber-intelligence research group – cyber-exposure index released	7	43
Stay Safe	**2017/2018:** Safe banking awareness (links to scams) – Security Centre	18	26

SABRIC, South African Banking Risk Information Centre; SAPS, South African Police Services; KM, knowledge management; KS, knowledge sharing; TF, time frame.

Figure 3 shows an increase in proactive knowledge-sharing activities aimed at the prevention of fraudulent banking transactions from TF1 to TF2.

The videos focused mainly on warnings about cybercrime, ATM card fraud, cash safety, schemes and scams, phishing or vishing and tips and pointers for protection. The campaigns not only tried to create awareness about a wide range of fraudulent activities, but also focused on the importance of protecting personal information (against identity theft), money safety, phishing and malware practices. The major increase in media releases can be attributed to the intensive campaigns launched during 2018. From the nine media releases postings on the website during TF1, the following types of messages were posted: safe banking (three), cybercrime/security (two), get-rich schemes (one), cash-in-transit heists (one) and statistics (two). The following main types of messages were included in the 43 press releases posted on the website during TF2: safe banking (17), cybercrime/security (4), get-rich-quick schemes (2), cash heists (7), collaboration with other stakeholders (7) and statistics (6). The results of knowledge-sharing use in e-banking fraud prevention are indicated in Figure 4, which compares the messages of TF1 with that of TF2 and indicates an increase in proactive KM activities.

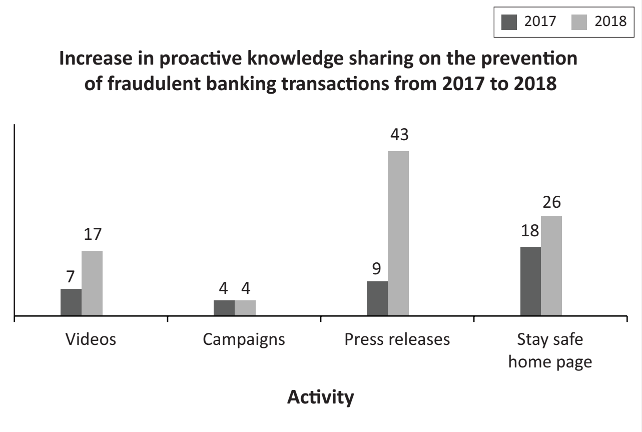


FIGURE 3: Knowledge sharing for e-banking fraud prevention during each time frame.

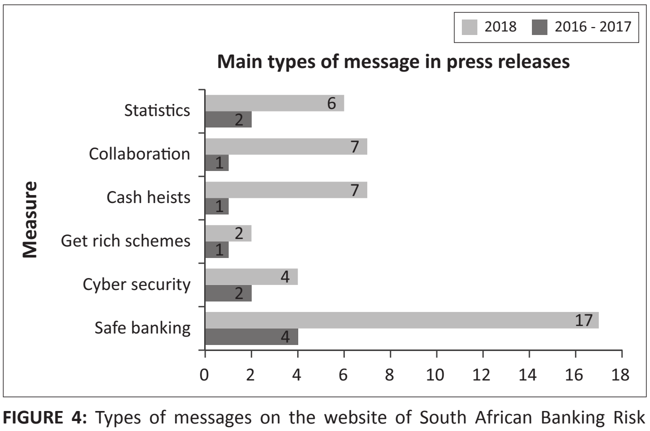


FIGURE 4: Types of messages on the website of South African Banking Risk Information Centre during each time frame.

Figure 4 clearly shows that there was a greater increase in preventative measures to ensure safe e-banking during TF2 than TF1. The measures focused specifically on keeping money safe, cybercrime and security. Clients were warned about identity theft, the use of social media and dating sites (i.e. to keep personal information safe) and about cash-in-transit heists. For example, a message from the CEO of SABRIC (2018) during TF2 read as follows:

> Criminals will use these techniques in the hope of tricking recipients into disclosing their personal information on bogus online platforms or on spoofed websites. And all it takes is a few duped individuals to make phishing a profitable business for cybercriminals. (The South African Banking Risk Information Centre [SABRIC], 2019)

On the Stay Safe webpage, each scam is identified and each link directs users to detailed information about these scams and safety tips during both time frames, with an increase from 18 links in TF1 to 26 links in TF2.

Table 2 presents the research results in terms of the three KM typologies that ensure that proactive communication through knowledge sharing takes place during both time frames.

Ethical consideration

The SOP for exempting non-health, negligible and low-risk research ethics applications from full REC (College of Human Sciences at the University of South Africa) review at departmental level (Communication Science) is supportive of the sections mentioned in the SOP on risk assessment. Ethical clearance number 2018-CHS-0027.

Findings and critical analysis of results

The statistics of TF1 (as on 04 July 2018) are indicated in the media release 'Beware when carrying cash' (SABRIC, 2018). According to these statistics, there was a 33% decrease in incidents of banking crime from January to June 2018 (478 incidents) when compared with the same period in 2017 (709 incidents). Banking client cash losses from January to June 2018 amounted to just over R21 million, which represents a decrease of 5% when compared with the same period in 2017. This is a significant improvement, as there was 4% increase in incidents from 2016 to 2017. In a press release on 17 September 2018 entitled 'SABRIC welcomes release of annual crime statistics', the Centre indicated that there had been increases in bank robberies, bank burglaries and CIT robberies. The good news, however, an 11% decrease was reported in ATM attacks compared with the previous year. This decrease indicated the fight against ATM attacks was bearing fruit. On 31 October 2018, the following statistics were released in a media release entitled 'Digital banking crime statistics':

> The South African Banking Risk Information Centre (SABRIC) is pleased to be releasing its inaugural digital banking crime statistics. We are all too aware that the advent of digital technology

TABLE 2: Data analysis based on knowledge management typologies.

Typology	Components/criteria	Variables/results
Knowledge acquisition	**Technical** (website): 1. data gathering and mining 2. knowledge construction	Detailed information about banking scams and fraudster statistics. All third-party frauds have visual links and each cover a broad spectrum of fraud and safety measures. Messages constructed based on existing data and fraudulent transactions. Information not yet prevalent (about cryptocurrency fraud and SMishing) but included in a new media release.
Knowledge transfer	**Proactive organisational communication** (messages): 1. create 2. direct real-time interactions 3. sharing of information	Communication through the creation and sharing of detailed messages through direct real-time interactions on homepage. Detailed information on each of the scams, modus operandi, tips on how to prevent them, general safety guidelines, what to do if fraud happened, dos and don'ts, telephone numbers to report incidents, tips on how to use a pin and password correctly, security measures for PCs and mobile apps, how to recognise a scam and deal with it, symptoms of possible spams and hacking, and general safe banking awareness (focusing on the prevalent modus operandi of each scam, social engineering tactics to trick victims to disclose sensitive information and passwords). Sharing information about and examples of fraudulent activities and direct real-time interactions.
Knowledge assimilation	**Human** (client): 1. methods/procedures to link clients 2. informal/formal setting for interaction 3. company practices to address crises 4. context	Homepage includes warning about fraudulent transactions. Prominent and visual links to all scams. Media and press releases. Partners. Stay Safe webpage (updated details on each fraudulent banking action and latest scams). Contact details. General security messages in informal and formal settings. Detailed methods, practices and procedures provided to clients to ensure security in informal and formal settings. Clear indication of practices to address fraudulent online transactions both proactively and reactively. Clear contextualisation of messages.

> has seen the exploitation of digital platforms by criminals. In 2017, 13 438 incidents across banking apps, online banking and mobile banking cost the industry more than R250 000 000 in gross losses. While incidents from January to August 2018 already show a 64% increase, we are pleased that the increase in gross losses is just 7% when compared to the same period in 2017. When comparing January to August 2017 to the same period in 2018, mobile banking incidents showed an increase of more than 100%, with gross losses of R23 593 631, while online banking incidents showed an increase of 44% with gross losses of R89 368 722. For the same period, banking app incidents increased by 20%, with gross losses of R70 156 364. SIM swops saw 4040 incidents from January to August 2017, and 8254 incidents from January to August 2018, an increase of 104%. (SABRIC, 2018:1)

A critical analysis of the results of the proactive communication and knowledge sharing on the SABRIC website revealed that the content of the website closely applied the three KM typologies identified in the literature review. It is posited that proactive communication through KM can contribute to the management and control of messages aimed at preventing fraudulent e-banking transactions. It can lead to enhanced e-trust, loyalty and e-security, strengthen the positive reputation of institutions and safeguard client relationships. A summary of the main results in terms of the three typologies follows: Knowledge acquisition was facilitated by providing clients with information via the website. Clients were told how they could keep their money safe. They were warned that there was an increase in types of fraud and during TF2 more links were created to sites that contained detailed information about different banking scams and fraudster statistics. Warning messages included visual links to each type of fraud, safety measures, accurate information and existing data on fraudulent transactions. Clients were advised on how to take proactive action based on data gathering, data mining and knowledge construction.

Three main types of message that were based on data mining and knowledge construction were identified. The first type of message contained basic facts about fraudulent e-banking transactions; the second contained updated information and facts and the third provided new information. The messages were aimed at preparing clients for possible fraudulent acts, told clients what they could expect and advised them how to react to such acts. The Stay Safe webpage with detailed visual links was launched to cover the broad spectrum and context of fraudulent e-banking transactions. It was apparent that knowledge transfer took place. Communication messages were created and then adjusted after the immediate impact of the fraudulent e-banking transaction had worn off. Various messages were posted, and clients were linked to websites that facilitated direct, real-time interactions so that they could share and receive information about the safe and secure use of online banking services. Each link took users to examples of possible real-time fraudulent transactions and explained these transactions, the modus operandi of criminals, what the scam entailed and how clients could prevent or address it. Numerous safety tips were also included, such as the warning not to click on links or icons in unsolicited emails or SMSs. This warning was followed by the caution that cybercriminals used fear tactics to target clients because clients were the weakest link. However, SABRIC assured clients that it managed the cybersecurity of banks proactively through social engineering and that banks deployed robust mitigation strategies to protect their clients. Most of the SABRIC media releases included examples of possible fraudulent actions and how they should be managed by clients.

The website facilitated knowledge assimilation by controlling and managing the messages sent before, during and after fraudulent e-banking transactions during both time frames. This was evidenced by the following: The homepage included warnings about fraudulent transactions; provided prominent visual links to scams; gave clients access to press releases and news; contained details about partners; allowed easy access to the main link to the Stay Safe webpage (where the latest details about each fraudulent banking action and the latest scams appeared); contained contact details; included general security messages in informal and formal settings; gave detailed information about the methods, practices and procedures that would ensure the safety and security of clients in informal and formal settings and gave a clear indication of practices to address both proactive and reactive fraudulent e-banking transactions with a clear contextualisation of messages. In addition to these, the website also provided links to informal and formal settings for interaction (e.g. Facebook and Twitter, although these were not included this study). It provided information about company practices to address fraud and about the context in which fraud is managed and controlled. This was corroborated by linking clients to Stay Safe and general security messages. The security messages included both formal messages like media releases and informal messages like video messages that would be understood by both highly literate and less literate clients. Detailed information was given about methods, practices and procedures to address fraud proactively and reactively. There was a notable increase in media releases during campaign periods in TF2, especially September 2018.

The analysis indicated that SABRIC definitely complied with all accounts and that most of the criteria of each typology of the KM paradigm were met. Messages were proactively controlled and managed, and clients were reassured that online transactions were safe and secure to build trust and client relationships. For each of the KM typologies, experts initiated messages to react, warn and update clients (proactively and reactively), and these messages included real-time examples and information about the modus operandi of fraudulent emails, SMSs and scams. Messages were sent out immediately after incidents of fraudulent e-banking transactions had come to light (whether through asynchronous media such as media releases, links and emails or synchronous media like Facebook and Twitter). They were factual and informed clients about the security and safety measures applied by the bank involved. This was in line with the argument in the literature that initial responses to fraudulent e-banking transactions should be quick, consistent, open, sympathetic and informative to create awareness and educate clients about e-security and to safeguard client relationships using the three KM typologies that would ensure knowledge sharing.

The main link to the Stay Safe webpage was (and still is) visually prominent and easily accessible on the homepage. As indicated before, links to Stay Safe increased from 18 main links (to each of the fraudulent e-banking scams and activities) in TF1 to 26 main links in TF2. The main aim of Stay Safe was to show clients how they could keep their money safe. Although the SABRIC website did not provide a link to information about the fraudulent e-banking transaction scam known as SMishing, there were links to press releases that mentioned the scam. For example, one press release (SABRIC, 2018) stated:

> SABRIC would like to remind bank clients to always be on the lookout for Phishing, Vishing and SMishing scams … (and) to make conscious decision to institute good habits to avoid becoming victims … (p. 1)

There were also no direct references to cryptocurrencies, but warnings about the 419 scam ('if it sounds too good to be true, it is') could also be applicable to them. As there are such a vast number of these scams, research is ongoing.

Based on the findings, it is argued that the website messages were organised according to the main types identified in Table 1 and if correlated with the typologies in Table 2, there are overlaps. This supports the argument that KM can be used as a theoretical starting point to manage and control different types of proactive communication messages to create awareness, educate clients and share knowledge and information in order to prevent fraudulent e-banking transactions, enhance e-security and safeguard client relationships.

In general, the homepage of the SABRIC website not only communicated immediately and proactively with users via the Stay Safe links to information about the scams during each time frame, but also provided a direct link to the Who We Are webpage, where users could obtain information about SABRIC's staff, vision, values and mission statement. This webpage emphasised that crime should be viewed as a shared responsibility and a collective priority for clients and public–private partners, which could be regarded as a first step towards (co-)liability. There were also links to a media and news webpage (press releases, campaigns, downloads and videos); and to our partners, namely the four major banks who had founded SABRIC and the 23 other financial partners. Lastly, there was a link to the Careers webpage, which advertised vacant positions at SABRIC itself.

In the light of knowledge obtained about the indicators of encryption or secure online transaction systems, it is argued that SABRIC has a strong reputation and a positive image. The centre offered factual information about e-security and safeguarding practices on its website. Its messages varied from a general description of a scam to details on how to prevent becoming a statistic. Most of the information was contained in the press releases, thus offering multiple connections from dual locations on the website. Furthermore, there were visual links to different Stay Safe webpages, which contained detailed information about possible schemes and how clients could avoid them. It is contended that SABRIC was consistently proactive during both time frames, used frequent informative messages, included factual information and knowledge-sharing messages to assist clients, provided contact details and reassured clients continuously that online transactions were safe and secure. The vision, values and mission of SABRIC clearly indicated its commitment to crime prevention through proactive communication and the move towards shared responsibility and (co-)liability. This is in line with Bowen's (2009) argument that the image of an organisation is usually linked to its mission, and it is the mission of the centre to reduce financial crime. South African Banking Risk Information Centre used the Stay Safe webpage for proactive communication and knowledge sharing aimed at reassuring clients, informing them of e-security measures and warning them about fraudulent e-banking transactions. The centre used KM as a change agent. It assured clients that if they used the information available via its links, they would be safeguarded and their e-security (e-trust and loyalty) would be enhanced. In this way it safeguarded its client relationships and its reputation as a risk reliever. Its messages could influence perceptions of risks and e-security positively, as its agents were regarded as experts in the field who could provide reliable and valid information about encryption or insecure e-banking transactions. South African Banking Risk Information Centre maintained the same basic website format and frequently updated its messages and links.

Although the move towards (co-)liability seems to be imminent, it is suggested that a clear policy is needed to apply the principles of (co-)liability consistently and transparently. However, because SABRIC sent new messages about the long-lasting effects of fraudulent e-banking transactions and the vast number of new scams, it can be argued that it used reactive communication in the most acute phase of fraud, that is, right after scams had come to light (Gonzàlez-Herrero & Smith, 2008, p. 151).

Conclusion and implications

The findings of the study provide insight into the importance of proactive communication to educate clients and create awareness about the prevention of e-banking security to ensure continued and positive client relationships. The results confirm that the biggest advantage of using KM in research into fraudulent e-banking transactions is the amount of information and knowledge available to verify the need for proactive communication, education and knowledge sharing that would benefit clients and the banking industry. The research revealed a few unexpected considerations. For example, it showed that the accessibility and use of the internet hold advantages and disadvantages for banks and their clients. South African Banking Risk Information Centre (on behalf of the financial industry) also regards communication with clients as crucial to ensure that they have up-to-date information about fraudulent transactions. It is also important that clients should actually take ownership of the knowledge shared by SABRIC and realise that transparency, proposed strategies and policies will become a reality and will affect their lives. The study examined proactive communication and knowledge sharing via KM to control messages about fraudulent e-banking transactions. Although KM may result in the construction of opposing viewpoints, it is argued that this tendency was ameliorated by promoting recognition of the scams to alleviate concerns about the safe and secure use of online transactions. The main contributions of the study are threefold to deal with the scarcity of research in this field: (1) an in-depth analysis of the website of a real-world online data set in the banking sector through a theoretical framework for e-banking fraud prevention, (2) an evaluation of the SABRIC website content during two time frames, which sets the scene for further research and deployment to other large financial institutions and (3) it revealed the need for fraud prevention strategies and policy (including planning strategies, incentives, action plans, code of conduct website, involvement of other role-players like government, to name a few). Although it is realised that some level of fraud will always remain, it is posited that it can be minimised through a holistic approach to data security. This study confirms the results of a previous study conducted by Hoffman and Birnbrich (2016), who emphasised the need for a more comprehensive understanding of the importance of fraud prevention through the creation of client awareness, understanding and knowledge about fraud and the measures banks take to prevent it, which has substantial potential to improve relationships with retail bank clients and to enhance these relationships and add value to the bank by triggering re-buying and cross-buying. Recognising this potential of effective fraud prevention is important for the financial sector to rethink their current strategies in fighting fraud and proactively communicating it to establish high-quality client relationships, ensuring they are well-informed, knowledgeable and value relationship quality.

The next step is to develop a KM strategy that SABRIC can use to address perceived risks and safeguard client relationships and the centre's good reputation by addressing the role of government, industry, academics and non-governmental organisations in the prevention of banking fraud. The need for government intervention is underlined by Nataraj and Ashwani (2018) who said:

> [*V*]arious measures initiated by government to deal with banking-sector challenges and how an attempt is made to adapt regulatory measures from global best practices could help the banking sector to become more robust, efficient and effective in preventing all fraudulent transactions and enhancing the quality of its assets. (p. 484)

The two main issues that need to be addressed will be to: (1) formally and specifically, identify e-banking fraud as a serious issue and (2) create an enterprise-wide e-banking fraud prevention plan. Hence, it is recommended that quantitative research be conducted to obtain more account and a deeper understanding of the effect of message control and management on perceived risk. Rahman and Anwar (2014, p. 102) emphasised this need for intensive holistic research by stating the following: 'All the components of deterrence, prevention, detection, mitigation, analysis, policy, investigation and prosecution must be simultaneously implemented in order to effectively prevent and detect fraud within banks'.

Acknowledgements

Competing interests

The author declares that no competing interest exists.

Author's contributions

I declare that I am the sole author of this research article.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability statement

Data sharing is not applicable to this article as no new data were created or analysed in this study.

Disclaimer

The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any affiliated agency of the authors.

References

Alexander, N., & Colgate, M. (2000). Retail financial services: Transaction to relationship marketing. *European Journal of Marketing, 34*(8), 938–953. https://doi.org/10.1108/03090560010331432

Andrews, L., & Boyle, M.V. (2008). Consumer's accounts of perceived risk online and the influence of communication sources. *Qualitative Market Research: An International Journal, 11*(1), 59–75. https://doi.org/10.1108/13522750810845559

Babbie, E. (2007). *The practice of social research* (11th edn). Belmont, CA: Thomson Wadsworth.

Barker, R. (2016). Knowledge management as change agent to ensure the sustainability of emerging knowledge organisations. In S. Moffett & B. Galbraith (Eds.), *Proceedings of the 17th European Conference on Knowledge Management*, 01–02 September 2016, Belfast, (pp. 45–53).

Barker, R. (2018). Knowledge management to prevent fraudulent e-banking transactions. *Communitas, 23*, 71–86. https://doi.org/10.18820/24150525/Comm.v23.5

Bowen, G.A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. *Computers and Security, 53*, 175–186. https://doi.org/10.1016/j.cose.2015.04.002

Chambliss, D.F., & Schutt, R.K. (2006). *Making sense of the social world: Methods of investigation*. Thousands Oaks, CA: Sage.

Custers, B.H.M. (2019). Banking malware and the laundering of its profits. *The Netherlands European Journal of Criminology, 16*(6), 728–745. https://doi.org/10.1177/1477370818788007

Drennan, J., Sullivan Mort, G., & Previte, J. (2006). Privacy, risk perception and expert online behaviour: An exploratory study of household end-users. *Journal of Organisational and End User Computing, 18*(1), 1–21. https://doi.org/10.4018/joeuc.2006010101

Gonzàlez-Herrero, A., & Smith, S. (2008). Crisis communications management on the web: How Internet-based technologies are changing the way public relations professionals handle business crises. *Journal of Contingencies and Crisis Managment, 16*(3), 143–153. https://doi.org/10.1111/j.1468-5973.2008.00543.x

Greer, C.F., & Moreland, K.D. (2003). United Airlines' and American Airlines' online crisis communication following the September 11 terrorist attacks. *Public Relations Review, 29*(4), 427–441. https://doi.org/10.1016/j.pubrev.2003.08.005

Hoffman, A.O.I., & Birnbrich, C. (2016). The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking, *International Journal of Bank Marketing, 30*(5), 390–407. https://doi.org/10.1108/02652321211247435

Jacobs, M., & Maritz, R. (2020). Dynamic strategy: Investigating the ambidexterity–performance relationship. *South African Journal of Business Management, 51*(1), a1643. https://doi.org/10.4102/sajbm.v51i1.1643

Jansen, J., & Leukfeldt, R. (2015). How people help fraudsters steal their money: An analysis of 600 online banking fraud cases. *Workshop on socio-technical aspects in security and trust*, 13 July 2015. Verona: IEEE Xplore. https://doi.org/10.1109/STAST.2015.12

Kim, I., & Kuljis, J. (2010). Applying content analysis to web-based content people and interactivity. *Journal of Computing and Information Technology, 18*(4), 369–375. https://doi.org/10.2498/cit.1001924

Kovach, S., & Ruggiero, W.V. (2011). Online banking fraud detection based on local and global behaviour. *ICDS 2011: The Fifth International Conference on Digital Society*, 23–28 February 2011. Gosier, Guadeloupe, France: IARIA, (pp. 166–170).

Lages, C., Lages, C.R., & Lages, L.F. (2005). The RELQUAL scale: A measure of relationship quality in export market ventures. *Journal of Business Research, 58*(8), 1040–1048. https://doi.org/10.1016/j.jbusres.2004.03.001

Larghi, S.B., Lemus, M., Moguillansky, M., & Welschinger, N. (2015). Digital and social inequalities: A qualitative assessment of the impact of the connecting equality program on Argentinean youth. *The Electronic Journal of Information Systems in developing countries, 69*(1), 1–20. https://doi.org/10.1002/j.1681-4835.2015.tb00496.x

Lee, V., Leong, L., Hew, T., & Ooi, K. (2013). Knowledge management: A key determinant in advancing technological innovation? *Journal of Knowledge Management, 17*(6), 848–872. https://doi.org/10.1108/JKM-08-2013-0315

Leite, R.A., Gschwandtner, R., Miksch, S., Kriglstein, S., Pohl, M., Gstrein, E., & Kuntner, J. (2018). EVA: Visual analytics to identify fraudulent events. *IEEE Transcations on Visualization and Computer Graphics, 24*(1), 330–339. https://doi.org/10.1109/TVCG.2017.2744758

Miles, M.B., Huberman, A.M., & Salanda, J. (2013). *Qualitative data analysis: A methods sourcebook* (3rd edn). Los Angeles, CA: Sage.

Miltonberger, T. (2020). *Fraud detection and analysis system* (US8280833B2). Guardian Analytics Inc. https://patentimages.storage.googleapis.com/41/55/44/bbeb25a90b1bb8/US8280833.pdf

Mhamane, S.S., & Lobo, L.M.R.J. (2012). Internet banking fraud detection using HMM. *Third international conference on computing, communication and networking technologies, banking*, 26–28 July 2012. Coinbatore, India: IEEE Xplore.

Nataraj, G., & Ashwani, D. (2018). Banking sector regulation in India: Overview, challenges and way forward. *Indian Journal of Public Administration, 64*(3), 473–486. https://doi.org/10.1177/0019556118783065

Ng, K.H., Wang, C., Yap, J.B.H., Wood, L.C., & Krisnan, S. (2020). Project management body of knowledge for motion picture production in a fast-developing economy. *South African Journal of Business Management, 51*(1), a1458. https://doi.org/10.4102/sajbm.v51i1.1458

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation.* New York, NY: Oxford University Press.

Pouwelse, J., & Bruggink, D. (2016). Reducing card-not-present fraud using pre-approved transactions. *Journal of Payments Strategy & Systems, 10*(1), 50–63.

Rahman, R.A., & Anwar, I.S.K. (2014). Effectiveness of fraud prevention and detection techniques in Malaysian Islamic banks. *Procedia: Social and Behavioural Science, 145*, 97–102. https://doi.org/10.1016/j.sbspro.2014.06.015

Rauyruen, P., & Miller, K.E. (2007). Relationship quality as a predictor of B2B customer loyalty. *Conference Proceedings*: *Journal of Business Research, 60*(1), 21–31.

Sathy, M. (1999). Adoption of internet banking by Australian consumers: An empirical investigation. *International Journal of Bank Marketing, 17*(7), 324–325. https://doi.org/10.1108/02652329910305689

The South African Banking Risk Information Centre (SABRIC). (2018). *Digital banking crime statistics*, viewed 02 February 2018, from: https://sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/

Van der Meulen, M.S. (2013). You've been warned: Consumer liability in internet banking fraud. *Computer Law & Security Review, 29*(5), 713–718. https://doi.org/10.1016/j.clsr.2013.09.007

Yousafzai, S.Y., Pallister, J.G., & Foxall, G.R. (2003). A proposed model of e-trust for electronic banking. *Technovation, 23*(11), 847–860. https://doi.org/10.1016/S0166-4972(03)00130-5