INVESTIGATING THE IDENTITY THEFT PREVENTION STRATEGIES IN M-COMMERCE

Dr Mahmood Hussain Shah[1], Mr Javed Ahmed[2] and Mr Zahoor Ahmed Soomro[2]
[1]*School of Strategy and leadership, Coventry University, Coventry, UK*
[2]*Lancashire Business School, University of Central Lancashire, Preston, UK*

ABSTRACT

Mobile commerce has provided extended business opportunities for online organisations and made it easier for customers to purchase products on-line from anywhere at any time. However, there are several risks associated with it, especially the identity theft. Online organisations commonly use electronic commerce approaches; however, these have some limitations in the m-commerce. This paper presents an evaluation of the approaches used in identity theft prevention and suggests guidelines to overcome the weaknesses in m-commerce. A case study approach, with semi-structured interviews was used as the data collection method. Thematic analysis method was adopted for the interpretation of the qualitative data. Themes and codes were created in relation to the processes, methods, approaches, activities and tools used for identity theft prevention. The results show that online organisations are using same approaches of identity theft prevention for all online business transactions, while m-commerce has some unique characteristics for which e-commerce arrangements are not effective. On the other hand, these arrangements are not evaluated for their effectiveness in m-commerce. This study suggests for the assessment of identity theft prevention system for effective functionality in m-commerce and forward guidelines for evaluation of the system in m-commerce. This study makes an important contribution by suggesting strategies for identity theft prevention in m-commerce.

KEYWORDS

Mobile Commerce, Identity Theft, Prevention Strategies, Mobile Security, Network Security

1. INTRODUCTION

Mobile commerce (m-commerce) has become a popular channel for consumers and online organisations. It allows the organisations to provide shopping facilities any time, at any location (Chong, Chan, & Ooi, 2012) thus, customers' get 24/7 shopping facilities. Such facility of online shopping is also espoused with many risks especially the identity theft (IDT). Currently, the online organisations are using various tools and technologies to prevent IDT in online transactions, yet they fail to control it. The major reason behind that failure is using electronic commerce (e-commerce) tools and techniques for all types of online transactions. Although mobile devices have unique characteristics such as touch screen, wireless network, limited bandwidth and memory space, wireless encryption, operating systems and limited processing power (Goyal, Pandey, & Batra, 2012; Nie & Hu, 2008), which may cause ineffectiveness of e-commerce arrangements.

In addition, these approaches have not been evaluated in m-commerce (Vidalis, Stafford, Angelopoulou, & Derby, 2014). To address the problems of IDT in m-commerce, this paper evaluates the approaches used by online organisations for prevention of IDT in m-commerce. The results show that the case organisation neither uses m-commerce specific systems, nor assesses the vulnerabilities of the systems to prevent IDT in m-commerce. The prevailing IDT system in the case organisation has been evaluated in m-commerce, the weaknesses are highlighted and suggestions are given to overcome these weaknesses. This paper makes an important contribution by suggesting approaches for IDT prevention in m-commerce.

2. BACKGROUND

M-commerce is growing rapidly and has become an important channel in online industry. In the UK, sales through mobile devices have increased by 186% in 2014(IMRG, 2014). Along with opportunities m-commerce also has many challenges especially the IDT. Customers' data security has a critical impact on m-commerce, as online retailers who do not secure their customers' data lose their customers (Wu & Wang, 2005). Surveys conducted in the USA and the UK on m-commerce challenges show that about 92% retailers are concerned with fraud risk (Kount, 2014) or are unable to manage identity frauds (Khan & Hunt, 2013).

The number of approaches and techniques are presented by various researchers for IDT prevention such as; network security (Al-Haj & Al-Shaer, 2011; Ray, 2013), internal and external data protection, encryption technology (AnnMcGee & Ralph, 2015; Peltier, 2013), customer education (Arachchilage & Love, 2014), threat and risk assessment (Beaumier, 2006), data access management and authentication systems (WenJie Wang, Yufei Yuan, & Archer, 2006). Although these all arrangements are made to prevent IDT yet the fraud is increasing (Khan & Hunt, 2013; Kount, 2014). The major cause of which may be the lack of evaluation of such systems in m-commerce. The online organisations use same e-commerce validation approaches for all types of transactions but these are not effective for m-commerce (Khan & Hunt 2013), so there is a need to investigate the arrangements for effective prevention of IDT in m-commerce (WenJie et al., 2006).

Technologies with unlimited benefits have also some challenges if not deployed and evaluated properly (Phan & Vogel, 2010). The functionality of preventive technologies in fraud area is a critical issue and most of these technologies are not compatible with m-commerce transactions (Nie & Hu, 2008). As the prevention technologies are there to help mitigate the risks, but firms have to assure that these are being applied properly in the problem-solving domain (Phan & Vogel, 2010) . Lack of evaluation of prevention system in m-commerce is also a major obstacle to IDT (WenJie et al., 2006). For effective functionality, the IDT prevention systems should be assessed for their vulnerability (Soomro, Shah, & Ahmed, 2016; Vidalis et al., 2014), which will help to make the necessary changes to enhance their performance in m-commerce.

So it may be argued that having no prevention system is a failure, but having the system with improper implementation and lack of evaluation is same as having no system. Therefore, this study investigates the limitations of IDT prevention system and suggests guidelines to improve its effectiveness in m-commerce.

3. METHODOLOGY

Qualitative case study is helpful to investigate and evaluate the effectiveness of technology to understand what happened or how and why people are responding; and phenomena of people to the situations in natural settings related to technology (Kaplan & Maxwell, 2005; Yin 2014). Therefore, the case study approach was used to capture the opinions, perceptions, processes, knowledge and responses of people about the identity theft prevention in m-commerce.

For qualitative data collection case study approach was adopted and semi-structured interviews were conducted with seventeen representatives of an online retail firm based in the UK. The questionnaire was developed using existing literature. The questionnaire was categorised into various dimensions of IDT prevention such as information security, encryption, network security, and authentication system. Some additional questions were also asked where needed to grasp the in-depth information. The data was collected in the months of July and August 2015. The average time for each interview was about 40 minutes and recording was done with an audio recorder.

A variety of respondents were selected from various levels of management and a few operational staff for data collection. The respondents were fraud managers, IT security managers, top executives, a fraud analyst, a fraud advisor, fraud investigators and others concerned with the prevention of identity fraud. Consent for data collection was sought and an agreement of confidentiality was signed by the researcher and the company's management to comply with the ethical aspect of this research.

The qualitative data analysis software NVivo 10.0 was used to organise, code, group and analyse the data from interviews. Using the thematic analysis technique, the data were carefully analysed. Themes and codes were created according to approaches, activities and tools related to the parameters of identity fraud prevention. The findings and results of data analysis are discussed below.

4. RESULTS AND DISCUSSIONS

4.1 Identity Theft Prevention

Prevention is commonly used to stop fraud from occurring; it is a set of activities that help to stop identity fraud before being detected as suspicious or to create hindrances to committing IDT. The findings show that the organisation has implemented different measures for IDT prevention, mentioned as below.

4.2 Network and Information Security

The findings so far show that the organisation has implemented various approaches or measures at network and communication level to prevent IDT in m-commerce. These measures are firewall security, network threat vulnerability analysis, anti-virus system, network access security and encryption technology. These measures are investigated below in m-commerce.

4.2.1 Firewall and Database Security

Firewall is the important factor in network access and information security because it prevents the unauthorised access at the boundary of network and infrastructure. The firewall has to be in line with security policy (Al-Haj & Al-Shaer, 2011; Ray, 2013). The findings show that the organisation has contracted network security from a third party which provides security services for network communication, anti-virus, firewalls, IDS and data base security. Respondents (1 & 4) reported that: *"Third party manages our infrastructure and network…and they manage firewalls, antivirus, IDS and database security."*

The findings show that network security is constantly monitored and updated according to threats by third party and present a security matrix to the case organisation. In security policy of the organisation it is mentioned that firewall administrators have to get approval from the information security department. They document all the information about the rules and conditions that they implement on firewalls for further network security audit (Beaumier, 2006). As the organisation relies on third party for their network, firewall, and information security management, which may leave some weaknesses unfocused. Therefore, the organisation should consider the neutral organisation to evaluate effectiveness especially for IDT prevention.

4.2.2 Network Threat and Vulnerability Assessment

The security policy of the organisation explains that network security is randomly evaluated by a third party at least twice a year. Respondent (4) said: *"third party has to demonstrate to us the effectiveness of these systems but I don't know how they are evaluated."* This shows that third party is evaluating the effectiveness of the network and IT infrastructure against threats. However, the case organisation does not know what they are evaluating and how they are evaluating. Such information would help the organisation to identify the threats and verify the methods of evaluation and their effectiveness (Tsavli, Efraimidis, Katos, & Mitrou, 2015). Participants (1 & 4) have explained that the organisation relies on the security provided by third party and it is deemed to be fairly secure. Although the organisation has specific network security and access policy but methods of evaluation and vulnerability assessment are not clearly suggested. Therefore, the organisation should design such a policy which highlight the evaluation methods of network security and data access policy compliance (Soomro et al., 2016; Tsohou, Karyda, & Kokolakis, 2015).

4.2.3 Encryption (SSL, PKI, WPKI)

For encryption the findings show that the organisation is using a standard Secure Sockets Layer (SSL) kit to encrypt the data that comes from customers through an e-commerce website and other third parties. Respondent (3) explained that: *"No, I can't tell you that (how we secure the data transmission in mobile commerce). I can tell you that we have standard SSL and PKI in e-commerce."* This argument reveals that the organisation uses SSL and Public Key Infrastructure (PKI) for data encryption in e-commerce, but it is not clear that how are they securing data in m-commerce. While in m-commerce, normally at the gateway, the data is decoded from wireless transport layer security (WTLS) protocol to encode in SLL, creating the chances of IDT, because during that process the information is in plain text (Ray & Biswas, 2011).

The implementation of strong encryption, digital signatures and SSL for data security and authentication require more computational power and enough memory space while mobile devices have limited processing power and memory space (Goyal et al., 2012; Nie & Hu, 2008). SSL and digital certificates could be useful for data security at the network level but they could not contain any security features that provide protection against online IDT attacks at the application level where fraudsters can capture information in plain text before encryption (Ray & Biswas, 2011).

4.2.4 Information Communication Security

Information communication security would be considered as fundamental and the first step in online business (Peltier, 2013). In this regard, Respondent (4) expressed the possibility of the risk of IDT when credential data is transferred from the e-commerce website to the backend database servers. He stated: *"... data is encrypted by SSL but how do we get from the e-commerce website to the backend (server)? I don't know, but I do know it goes through the firewall so although our backend is protected I don't know whether it is encrypted or not but I think we cannot accept that to be the case on an insecure internet."*

This implies that the internal infrastructure and database servers are secure but the organisation has not evaluated the process of data transmission from an e-commerce website to the backend database servers because the organisation assumes that it would be encrypted and secure from threats of IDT. Therefore, it is suggested that the organisation should evaluate the data transmission flow not only from e-commerce website but also from mobile applications to the database servers (Beaumier, 2006). It may be concluded from discussion, that the organisation has strong network data protection at the internal level but there are some limitations in m-commerce at the customer level, mentioned in Table 1.

Table 1. Limitations and suggestions for network and information security measures

Measures	Limitations	Suggestions
Threat assessment	Third party is evaluating effectiveness but organisation does not know the process.	The organisation should analyse its methods of network security evaluation (Amori, 2008).
Firewall, database and network access	The organisation relies on security provided for firewalls, anti-virus, database and network access by third party and it is deemed to be fairly secure.	The organisation should ensure the security provided by third party according to their network security policy and analyse the firewall security through penetration testing and vulnerability test (Eisen, 2009).
Encryption	The organisation uses standard SSL and PKI which are not effective in m-commerce. The encryption key could be tempered by viru and malwares on the customer side.	The organisation should implement strong encryption such as point-to-point encryption of hardware; and should verify the encryption signature key during network authentication (AnnMcGee & Ralph, 2015).
Information flo security	The organisation does not evaluate the security of information flow from third party e-commerce platforms to the database.	The organisation should evaluate the in-depth data transmission flow not only from the e-commerce website but also from mobile applications to the database servers (Amori, 2008).

Table 1 shows that for preventing IDT, the organisation have implemented various network and information security measures. These measures are secure and implemented according to standards of e-commerce. The results show that the organisations are not giving proper attention to assessment and evaluation of these measures in m-commerce. Therefore, the organisations should examine the weakness and loopholes in network and information security process with respect to channels (Borum, Felker, Kern, Dennesen, & Feyes, 2015). The organisation should also ensure the security of data and information flow from business partners, third party contractors and customers (Borum et al., 2015; Tsavli et al., 2015).

4.3 Business Platform Security

The business platform is the channel through which sell and buy the products and services. In m-commerce, the business platform consists of the mobile device, mobile business application (apps) and wireless network for communication. The entities related to business platform security are discussed below.

4.3.1 Mobile App Security

The findings show that the organisation has a mobile application. it is developed by a third party and is managed by the e-commerce department. Most of the participants confirmed that more than 70% of orders are placed through mobile devices. Therefore, it is necessary to secure their mobile application from identity fraudsters who create threats to obtain their identity and credential information by exploiting mobile technology. In this regard, most of the respondents explained that the organisation has a mobile application but they do not know what security parameters are implemented for the prevention of IDT. For the effectiveness of mobile application, respondent (4) explained that: *"When the mobile app was produced we assessed the vulnerably point of view by the third party".*

The statement reveals that the organisation has evaluated the vulnerability by testing mobile applications once, at the time of its deployment. However, the literature suggests that m-commerce provides enough information and security through a mobile application that could be helpful to prevent theft in m-commerce. Because in m-commerce the online retail organisations are installing their applications direct to the customer's devices, it provides direct access rather than by clicking on URLs in e-commerce (Khan & Hunt, 2013). Therefore, it is suggested to the organisation that they enhance the security of their mobile application by adding extra security functionality such adding antivirus signature verification functionality, communicate through a virtual private network (VPN), and use an IMEI number for verification and authentication of customers. It is also suggested that the organisation should evaluate the effectiveness of their mobile application on a regular basis.

4.3.2 Anti-Phishing Technology

The organisation has purchased anti-phishing services from a third party which employs various means to provide end-to-end protection against phishing. These include monitoring and detection of phishing sites, real-time alerts and global network blocking, site shut down services, forensics and credential recovery and bait operations. Participant (4) said: *"Third party is monitoring fraud brands and shutting down phishing sites; on customer complaints sites about phishing again they respond to that and take those sites down."*

The findings show that anti-phishing measures are in place but only for the e-commerce platform. However, in m-commerce fraudsters could obtain credential information through other phishing methods such as mobile app, ad-jacking, SMshing (SMS phishing), Vishing (phishing thorough phone call), send URLs in emails, or installing malicious apps on a customer's device and through social media (Jakobsson & Myers, 2006). The findings also show that the organisation receives complaints from customers about phishing sites and third party responses to those complaints. This shows that the anti-phishing service is not as effective at detecting phishing URLs because customers are informing the organisation about illegitimate sites or fraudsters who are using other channels to trick the customer. In this regard, the organisation should consider monitoring and the detection of phishing mobile apps at mobile app store and employ extra measures to detect other methods of phishing. The limitations and suggestions are summarised in Table 2.

Table 2. Limitations and suggestions for business platform security measures

Measures	Limitations	Suggestions
Mobile applicatio security	The organisation A evaluated the vulnerability of mobile applications only once, at the time of its deployment.	The organisations should regularly evaluate the mobile apps concerning IDT prevention (Borum et al., 2015; Tsavli et al., 2015) and enhance its security by adding extra security functionality (Eisen, 2009).
Anti-phishing technology	The anti-phishing service is not effective to detect phishing URLs because receiving complains about illegitimate sites.	The organisation should implement continuous monitoring and a phishing detection system for mobile apps (Bose & Leung, 2007).

Table 2 shows that the organisation has implemented various prevention measures to secure business platform. These measures include internal anti-virus, anti-phishing technology, wireless (mobile) encryption. The measures were implemented for e-commerce and internal network security but mobile app which may increase the IDT risk at customer side. Therefore, it is suggested that the organisations should evaluate the vulnerabilities in m-commerce and enhance the security by adding extra features such as adding anti-virus in apps, VPN, SSL encryption and anti-phishing technology for mobile apps (Eisen, 2009).

4.4 Identity Verification and Validation (Authentication) System

The findings show that the organisation has a standard authentication system through account numbers and passwords. Other security measures and tools are used such as SSL, password protection, database security and customer data protection, but customer authentication is an important step in checking and verifying a genuine customer at the time of login or account access. Respondent (2) explained that: *"Just standard on the website, such as account number, login details, and password - obviously if you don't have these details then it would not allow you to log in but that's how fraudsters are obviously obtaining the credentials."*

The findings of the authentication process show that the organisation has a standard authentication system through account numbers and passwords. It also shows that fraudsters illegally obtain these credentials via hijacking the customers' accounts and placing online orders. Literature suggested biometric authentication such as fingerprinting, voice recognition, keystroke dynamics, facial recognition and eye retina recognition would enhance customer identification and non-repudiation of information security (Karnan, et al., 2011; Usman & Shah, 2013). However, WenJie, et al., (2006) illustrates that the biometric authentication system could be effective for authentication but it also contains some limitations such as once biometric information theft has taken place, it is difficult to recover. Concerning this, respondent (1) explained: *"We are looking at logins and the amount of time of people are using certain keys* [keystroke dynamics] *and we're able to identify patterns; as well as this we are researching photo recognition systems with a view to the future."*

This shows that the organisation has concern about authentication systems and they are researching the biometric system. M-commerce supports for biometric authentication because it contains a live camera, touch screen and built-in biometric technology such as fingerprinting, eye retina verification, palm verification and face recognition as well as voice recognition (Teh, Zhang, Teoh, & Chen, 2016). M-commerce also provides a unique international mobile equipment identity (IMEI) number and contact number that could be helpful in the identification of a customer by implementing multifactor authentication. This technology is now widely used in large banks to authenticate the customer through a mobile app (Gu & Peng, 2010). Using this method of authentication, the customer devices are registered alongside their accounts at the time of downloading the app. The organisation could utilise these technologies and methods in order to implement an effective authentication system. The strategical steps towards the effective prevention of IDT in m-commerce are highlighted below in figure 1.

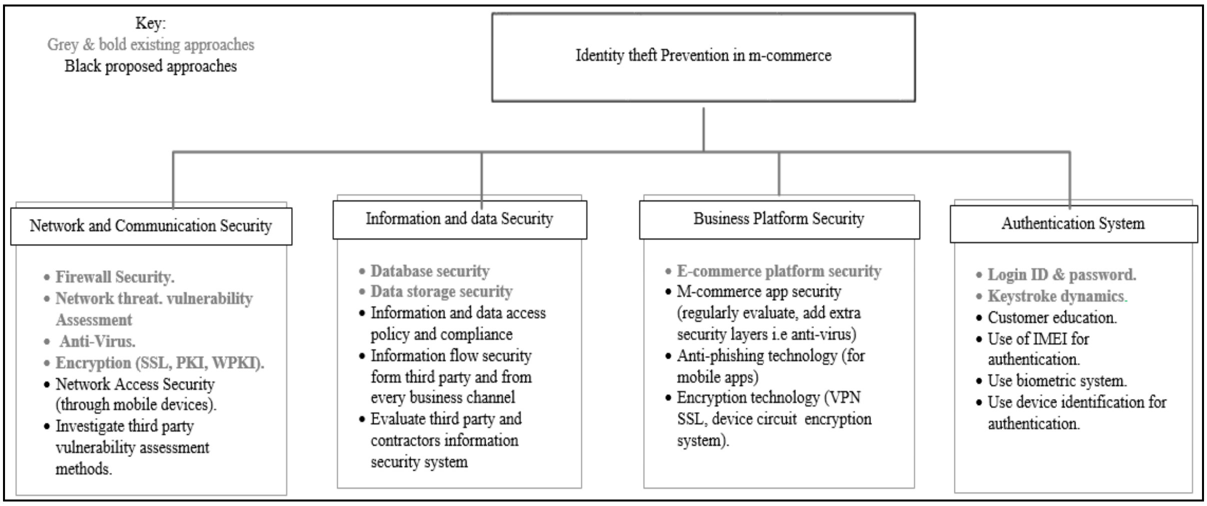
Key:
Grey & bold existing approaches
Black proposed approaches
Identity theft Prevention in m-commerce
Network and Communication Security
• Firewall Security.
• Network threat. vulnerability Assessment
• Anti-Virus.
• Encryption (SSL, PKI, WPKI).
• Network Access Security (through mobile devices).
• Investigate third party vulnerability assessment methods.
Information and data Security
• Database security
• Data storage security
• Information and data access policy and compliance
• Information flow security form third party and from every business channel
• Evaluate third party and contractors information security system
Business Platform Security
• E-commerce platform security
• M-commerce app security (regularly evaluate, add extra security layers i.e anti-virus)
• Anti-phishing technology (for mobile apps)
• Encryption technology (VPN SSL, device circuit encryption system).
Authentication System
• Login ID & password.
• Keystroke dynamics.
• Customer education.
• Use of IMEI for authentication.
• Use biometric system.
• Use device identification for authentication.

Figure 1. The strategy for identity theft prevention in m-commerce

The Figure 1 represents the suggested methods and approaches for IDT prevention. As the above findings show that organisation are more focusing on technological methods (anti-virus, encryption technology, firewall security, data security, login ID and password, keystroke dynamics and platform security etc.) to prevent the IDT. However, literature also suggests additional preventive steps that would be helpful in IDT prevention in m-commerce. These steps include; enhancing skills, knowledge and training to employees that they could evaluate and improve the performance of tools (Borum et al., 2015; Tsavli et al., 2015). The existing measures are also included on account of their effectiveness and usability in m-commerce.

So far, this study finds that the online organisations are using the e-commerce approaches for IDT prevention in m-commerce, which is a major obstacle towards its effectiveness. On the other hand, such prevention systems are not evaluated for their vulnerabilities in m-commerce. So this study suggests proper alignment of IDT prevention system with m-commerce characteristics and also forwards guidelines to assess and improve the effectiveness of IDT prevention approaches in m-commerce.

However, these measures are not sufficient to prevent IDT. So with the help of literature additional approached are highlighted to overcome the existing gaps in prevention of IDT through mobile devices. In addition to the adoption of these tools and approaches this research also suggest regular evaluation of these tools and approached to identify the limitations and enhance their performance in m-commerce. Application of suggested tools and approaches will help the online organisations to prevent IDT and related fraud losses and enhance customers' trust.

5. CONCLUSIONS

An investigation of the IDT prevention measures in m-commerce has been presented. The results show that the online organisations are using e-commerce approaches to prevent IDT in m-commerce. Although, these approaches have some controls on IDT in general but have some limitations. Firstly, these approaches are developed for e-commerce, so are not effective in m-commerce. M-commerce has unique characteristics, which cannot be addressed through e-commerce approaches. Secondly, these measures do not specifically address the challenges related to IDT in mobile devices. This study suggests that measures implemented in IDT prevention should be capable of addressing challenges in m-commerce. So there is a need to establish specialised measures capable of counterfeiting the IDT in m-commerce.

The results also show that the online organisations do not evaluate the measures used for IDT in m-commerce. Implementing measures without knowing their effectiveness is a greater risk. So this study suggests that the online organisations should systematically evaluate their IDT prevention measures in m-commerce. Thus, the research makes a significant contribution by highlighting the limitations of existing IDT prevention approaches in m-commerce. The study also suggests the guidelines for the effectiveness of existing approaches in IDT prevention which will help the online organisations to manage the vulnerabilities of their systems.

This study has some limitations, since research was conducted in the UK retail industry. However, other countries have different concepts, methods and approaches for IDT prevention. This research suggests future studies using data from other developed and developing countries to explore issues and remedies.

REFERENCES

Al-Haj, S., & Al-Shaer, E. (2011). Measuring firewall security. *4th Symposium on Configuration Analytics and Automation (SAFECONFIG)*, Arlington, VA. pp. 1-4. doi:10.1109/SafeConfig.2011.6111669

Amori, G. (2008). Preventing and responding to medical identity theft. *Journal of Healthcare Risk Management,* Vol. 28, No 2, pp. 33-42. doi:10.1002/jhrm.5600280206

Ann McGee, J., & Ralph Byington, J. (2015). Corporate identity theft: A growing risk. *Journal of Corporate Accounting & Finance,* Vol. 26, No 5, pp. 37-40. doi:10.1002/jcaf.22061

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior,* Vol. 38, No 0, pp. 304-312. doi:http://dx.doi.org/10.1016/j.chb.2014.05.046

Beaumier, C. M. (2006). Multifactor authentication: A blow to identity theft? *Bank Accounting & Finance* (08943958), Vol. 19, No 2, pp. 33-37.

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security*, Vol. 23, No. 3, pp. 317-332.

Bose, I., & Leung, A. C. M. (2007). Unveiling the mask of phishing: Threats, preventive measures, and responsibilities. *Communications of the Association for Information Systems,* Vol.19, No. 1, pp. 544-566.

Chong, A. Y., Chan, F. T., & Ooi, K. (2012). Predicting consumer decisions to adopt mobile commerce: Cross country empirical examination between china and malaysia. *Decision Support Systems*, Vol. 53. No 1, pp. 34-43.

Dorminey, J., Fleming, A. S., Kranacher, M., & Riley Jr., R. A. (2012). The evolution of fraud theory. *Issues in Accounting Education*, Vol. 27, No. 2, pp. 555-579. doi:10.2308/iace-50131

Eisen, O. (2009). In-session phishing and knowing your enemy. *Network Security*, 2009, No. 3, pp. 8-11. doi:http://dx.doi.org/10.1016/S1353-4858(09)70027-3

Goyal, V., Pandey, U., & Batra, S. (2012). Mobile banking in india: Practices, challenges and security issues. *International Journal of Advanced Trends in Computer Science and Engineering*, Vol, 1, No. 2, pp. 55-66.

Gu, G., & Peng, G. (2010). The survey of GSM wireless communication system. *International Conference on Computer and Information Application (ICCIA)* Tianjin, pp. 121-124.

IMRG. (2014). IMRG capgemini e-retail sales index. Retrieved from http://www.imrg.org

Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: Understanding the increasing problem of electronic identity theft,* John Wiley & Sons, Hoboken, New Jersey.

Kaplan, B., & Maxwell, J. A. (2005). *Qualitative research methods for evaluating computer information systems.* Evaluating the organizational impact of healthcare information systems (pp. 30-55) Springer New York.

Karnan, M., Akila, M., & Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*, Vol.11 No.2, pp. 1565-1573.

Khan, A., & Hunt, J. (2013). The turning point: Optimise acceptance, maximise profits *(CyberSources 2013 UK eCommerce fraud report)*. (Business report). UK: CyberSource UK.

Kount. (2014). Mobile payments & fraud survey: 2014 report. Retrieved from http://www.kount.com/campaigns/mobile-survey-report-2014

Nie, J., & Hu, X. (2008). Mobile banking information security and protection methods. *International Conference on Computer Science and Software Engineering*, Wuhan, Hubei, Vol.3, pp. 587-590.

Peltier, T. R. (2013). Information security fundamentals CRC Press.

Phan, D. D., & Vogel, D. R. (2010). A model of customer relationship management and business intelligence systems for catalogue and online retailers. *Information & Management*, Vol. 47, No.2, pp. 69-77.

Ray, L. L. (2013). A matrix model for designing and implementing multi-firewall environments. *International Journal of Information Security Science,* Vol.2, No4, pp. 119-128.

Ray, S., & Biswas, G. P. (2011). Design of mobile-PKI for using mobile phones in various applications. *International Conference on (ReTIS) Recent Trends in Information Systems*, pp. 297-302. doi:10.1109/ReTIS.2011.6146885

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management,* Vol.36, No2, pp. 215-225. doi:http://dx.doi.org/10.1016/j.ijinfomgt.2015.11.009

Teh, P. S., Zhang, N., Teoh, A. B. J., & Chen, K. (2016). A survey on touch dynamics authentication in mobile devices. *Computers & Security*, Vol.59, pp. 210-235. doi:http://dx.doi.org/10.1016/j.cose.2016.03.003

Tsavli, M., Efraimidis, P. S., Katos, V., & Mitrou, L. (2015). Reengineering the user: Privacy concerns about personal data on smartphones. *Information & Computer Security*, Vol.23, No.4, pp. 394-405.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, Vol.52, pp. 128-141. doi:http://dx.doi.org/10.1016/j.cose.2015.04.006

Usman, A. K., & Shah, M. H. (2013). Critical success factors for preventing e-banking fraud. *Journal of Internet Banking & Commerce*, Vol.18, No.2, pp. 1-15.

Vidalis, S., Stafford, U., Angelopoulou, O., & Derby, U. (2014). Assessing identity theft in the internet of things. *IT CoNvergence PRActice* (INPRA), Vpl.2, No1, pp. 14-20.

WenJie Wang, Yufei Yuan, & Archer, N. (2006). A contextual framework for combating identity theft. *Security & Privacy, IEEE*, Vol.4, No.2, pp. 30-38. doi:10.1109/MSP.2006.31

Wu, J., & Wang, S. (2005). What drives mobile commerce?: An empirical evaluation of the revised technology acceptance model. *Information & Management*, Vol.42, No5, pp. 719-729.

Yin, R. K. (2014). *Case study research: Design and methods* (5th ed.). London: SAGE Publications, Incorporated.