International Journal of Computer (IJC)
ISSN 2307-4523 (Print & Online)

http://ijcjournal.org/

Cyber Security Challenges to Mobile Banking in SACCOs in Kenya

Nambiro Alice Wechuli[a*], Wabwoba Franklin[b], Wasike Jotham[c]

[a,b]*Department of Information Technology, Kibabii University, Bungoma, Kenya*
[c]*Department of Library Services, Kirinyaga University, Kerugoya, Kenya*
[a]*Email: alicenambiro@yahoo.com*
[b]*Email: fwabwoba@kibu.ac.ke*
[c]*Email: jothamwasike@gmail.com*

Abstract

Development of mobile technology has enabled mobile devices to be adopted in daily activities. Financial institutions are adopting mobile devices for banking purposes to enable their clients to bank from anywhere at any time. Although, the adoption of mobile technology enabled convenience to the users, it has brought about a great security challenge. This paper reviews the cyber security challenges to mobile banking and ways which SACCOs minimize the impact. Findings indicate that some mitigation strategies to cyber threats to mobile banking are in place though they seem not to address the major challenges.

Key words: Cyber-attack; Cybercrime; Cyber security challenges mitigation; Mobile banking; SACCO.

Sponsorship: We highly appreciate the National Commission for Science; Technology and Innovation; Kenya for the study financial sponsorship.

1. Introduction

Savings and Credit Cooperatives (SACCOs) are utilizing the opportunities offered by advances in ICTs to ensure their operations are user friendly, their products and services are competitive, and develop customer-centric strategies. The ubiquitous and universal access to information and services together with a possibility for a unique and personalized exchange of information provided by mobile services have an impact on consumers [1].

---

* Corresponding author.

While connectivity is indispensable for achieving such business success, SACCOs get exposed to a myriad of cyber-security challenges to mobile banking which when exploited lead to violation of Confidentiality, Integrity and Availability that erodes down the user perceived secure mobile banking service delivery.

According to [2], many financial institutions have incurred financial losses due to cybercrime leading to customers shunning away from mobile banking services as a result of eroded user perceived security in mobile banking services. According to [3], cyber security threats may cause significant loss of Confidentiality, Integrity and Availability. This may lead to the deprivation of public trust and organization image resulting in business loss because of disclosure of confidential client data such as credit card number to the public. [4] assert that the social engineering occurrence increased with reported losses in 2015 doubling from the year 2014 to $1 billion (KSh102 billion). The author further states that its impact is particularly disturbing in Kenya, which is globally attributed for its mobile phone penetration that is, eight in ten Kenyans own a cellphone, and popularity of mobile money platforms.

For the purpose of this paper, cyber security shall be considered to encompass a set of concepts which include confidentiality, integrity and availability of information. According to [5] confidentiality refers to the protection of sensitive or private information from unauthorized disclosure. Thus, ISO 27002:2005 introduced an important aspect of confidentiality that applies to mobile banking applications which is protecting information from intelligible interception [6] because some of the information required by the mobile banking device resides on the servers of the financial institution. Therefore, the transfer of that information from the financial institution's systems to the mobile device need to be addressed.

Integrity has been considered as the accuracy, completeness and validity of information [5]. According to [5] availability is defined as information that is accessible when required by the business process now and in the future. According to [7], cyber security is the collection of policies, security safeguards, risk management approaches, guidelines, technologies, actions and training that can be used to protect the organization and cyber environment together with the user's assets.

2. Cyber Security Challenges

Several organizations encounter the challenges brought about by cyber-attacks. According to [4], cybercriminals have sought to infiltrate organizations' databases by hacking into their networks. The author further states that a survey by audit firm PricewaterhouseCoopers found 33 per cent of firms had been affected by cybercrime in the last 24 months, and a third of them suffered significant financial impact. In addition, the Ministry of Information, Communication and Technology reported an increase in cyber-attacks by 100 per cent in 2014 over the year 2013 [4]. The cyber security challenges identified are as follows:

2.1 Inadequate Technical Skills

According to [8], insufficient technical skills, both at management and board levels are a challenge to secure mobile banking service provision in SACCOs in Kenya. According to [9], Computer Emergency Response Teams (CERTs) are valuable assets for performing the cyber security functions, but they are either lacking or in

nascent stages across Africa, Kenya included. The author further states that without the capable Computer Emergency Response Teams in place with the appropriate technical expertise to operate them, the African networks are more vulnerable to cyber threats, making the mobile money users vulnerable to attack and fraud.

2.2 Lack of Awareness

Awareness is very important in realization of total cyber security. The mobile phones adoptions and applications like mobile money have enabled users with little prior experience with technology to own them. Users having limited digital literacy have a more likelihood to be unaware of cyber threats, which places themselves and the networks at greater risk [9]. The author further notes that lack of cyber awareness is a leading cause of infection across the globe.

2.3 Legislation

The Cooperative Societies (Amendment) Act of 2004 (Republic of Kenya, 2004a) is the legislation that guides the formation and management of cooperatives in Kenya [10]. This reinforced state regulation of the cooperatives movement through the office of the commissioner of cooperatives development. The legislation specifies the roles to be undertaken by the government which include: creation of the policy and legal framework for development of cooperatives, improvement of the growth and development of cooperatives by providing requisite services for the organization, the registration, the operation, the advancement and dissolution; and the development of partnerships with cooperatives through consultative processes which are focused on legislation policy and regulation. Because the cyber environment knows political boundaries, international cooperation on cyber security issues is necessary, but few African countries engage in cross border law enforcement efforts [11].

2.4 Low Prioritization

The cyber security state is hindered by the low prioritization from national leaders [12]. This is mostly attributed to the limited resources which must first be allocated to address the society's problems which are most fundamental. Thus, the low priority for cyber security in the face of some other pressing issues endangers vulnerable networks and their applications. This makes the organization least safe place for operating a sensitive application like mobile money.

2.5 Poor Technical Design

Technically expert adversary can take advantage of poor security design within mobile money apps or simply bypass poorly implemented encryption [13]. For example, a mobile application could track all the purchases made by the target illegally, then gives the adversary information about the target's strategies and physical location. Also, a mobile application can make random purchases on behalf of the target [9]. When performed in an inconspicuous fashion, such purchases would unlikely raise alarms in fraud detection systems.

2.6 Social Engineering Practices

Social Engineering is a process of deceiving people into giving away access or confidential information [14]. According to [11] define social engineering as a diverse and complex technique for gaining unauthorized access to confidential proprietary and personal information. According to [3], Social Engineering is a method of gathering information and performing attacks against Information and Information Systems.

Social engineering attacks are multifaceted and include physical, social and technical aspects, which are used in different stages of the actual attack. Social engineering tactics are used by criminals because it is easier to exploit a person's natural inclination to trust. According to [3], Social Engineering is considered as the greatest security threat for people and organizations.

Cyber-attacks on organizations have been rampant over the past years. Organizations are however getting smarter and putting in place systems to curb cyber-attacks, making it more difficult for hackers to gain access. Thus, the only fraudster's soft spot left is the human mind [4]. To gain access to an organization's sensitive information, such as client passwords or account details, the criminals have resorted to social engineering. Some of the techniques used include Phishing, Reverse social engineering, shoulder surfing, baiting and eavesdropping discussed as follows:

a) Phishing

Phishing is the process of enticing people into visiting fraudulent web sites and persuading them to enter their personal information on the same [15]. An e-mail or text message is sent by a phisher that appears to be coming from a legitimate bank, school, company or institution. According to [9], in phishing, the consumer receives an e-mail indicating that there is a problem with the account. The authors' further argue that instead of the e-mail to provide a fraudulent link to click on, it provides a customer service number that the client must call and is then prompted to log in using account numbers and passwords. Phishing attacks can also be conducted via email, phone calls, text messages and fax, as well as other methods of communication, including social media.

Phishing is defined by [16] to be an exploit that is generally defined as impersonating a trusted third party by a phisher in order to gain access to private information. In such case, the phisher sends an email that appears to come from a legitimate business or individual requesting verification of information and warning of terrible consequence if it is not provided. Usually, the email contains a link to a fraudulent web page that appears legitimate, sometimes with company logos and content and requests private information. The author further states an example which is spear phishing, in which the attacker initially gathers personal information about the target victim and uses it to tailor the phishing scheme, which increases the probability of success.

b) Reverse Social Engineering

Reverse social engineering is a sophisticated form in which the attacker creates a situation in which the unwitting victim believes that the attacker can help solve a problem. Social engineering consists of three major parts: sabotage, advertising and assisting [17]. The first step is sabotaging the company's computer system which can range anywhere from disconnecting someone from the company's network to sophisticated manipulation of the victim's software applications. The attacker then poses as a technical aide to fix a problem

that the attacker created or that does not exist. The attacker communicates his capability to help, such as through advertising or a phone call. Finally the victim invites the attacker to assist, which eventually allows the attacker to access to the desired information.

c) Shoulder Surfing

Secret information should be protected from sensitive and various applications by use of secured authentication system [18]. This is because the vulnerabilities of textual passwords such as short passwords are easy to remember [19], which makes them vulnerable for attackers to break. Shoulder surfing is stealthily looking over the shoulder of someone who enters security codes or passwords.

d) Baiting

This is an exploit that uses malware infected physical media such as CD-ROM, USB drives e.t.c to achieve an attack [16]. Looking legitimate, the Trojan horse relies on the curiosity or greed of the victim who finds and uses the device, enabling installation of the malware on the targeted organization's internal computer network. In order to increase the chances of success of such attacks, the perpetrators often try to develop a relationship with their future victims. According to [20], the most prevalent type of social attacks is performed by phone.

e) Eavesdropping

Eavesdropping is unauthorized information capturing for example usernames and passwords leading to compromise in the confidentiality [21]. Communication in a mobile device is over a wireless network. The confidentiality and integrity of the communication can be compromised by the means of eavesdropping, man in the middle attack or by spoofing because the communication goes over the air. When information is manipulated, it compromises the integrity of the data.

3. Approaches to Securing Mobile Banking Service Provision

In order to effectively defend against cyber-attacks, a multifaceted approach needs to be used. This can be achieved through physical security mechanisms, technical controls, security policy and education and training.

3.1 Access Control

Physical security must be properly implemented because many attacks succeed through gaining physical access [11]. Therefore, access control must be put in place to allow authenticated users to gain access and keep the rest off. According to [22], double passwords control can help a great deal in the war against physical insecurity. The double password control includes the log-in password and the transaction password. For the log-in password a mixture of numbers and letters needs to be used and this means confidentiality is ensured to a certain degree and this is limited to log in. The transaction password on the other hand is required when users need to transfer funds.

3.2 Technical Controls

Proper technical controls can help reduce the social engineering risks [11]. One of the technical controls that can be employed is the use of firewalls. According to [23], firewalls employ a combination of computer hardware and software that is designed to separate the Internet from the Internal Web servers, networks, computer systems and databases securely. Back-up and recovery is another technical control. An off-site back up is required for recovery from major failures to ensure continuity in business operations [22].

3.3 Security Policy

According to [11], security policy is the key and most important element of a good defense against social engineering because it can take out uncertainty which is what social engineering depends on. According to [22], in an organization, the written security policy document provides a very high-level description of the several controls the organization uses to protect information. Also, the strength of any system is not greater than its weakest link. Thus, protecting information that is confidential in an organization is a business and legal requirement. With financial resources justifiably limited, leaders are required to take policy actions that will increase the user trust without requiring exceptional monetary and other resource allocations [9]. This may take into consideration the information like licensing for mobile money services to include explicit rules for the collection and sharing of personal information. The existing security policy needs to be reviewed and updated at periodical intervals [22].

3.4 Education and Training

People's vulnerability to social engineering is described in terms of their awareness to the types of social engineering attacks [11]. Therefore, people need to be educated and trained constantly to be resistant to social engineering. Improved knowledge of threats is often cited as critical to enhance cyber security. Financial institutions try to educate their customers, in part through new channels of communication such as Twitter and YouTube, in addition to more frequent website updates. The financial institutions are required to educate their security personnel and their end-users on a continuous basis [22]. Nations are required to commission public awareness campaigns which are focused on cyber security and personal data [9].

4. Conclusion

Realizing user perceived secure mobile banking free from cyber-attacks is a dream for financial institutions in general and SACCOs in particular. Literature reviewed presents several challenges to mobile banking service provision which need to be addressed to secure the confidence for clients using the service. Several attempts have been put in place to mitigate the challenges encountered in effective provision of user perceived secure mobile banking. However, they have not address all the challenges encountered. A major omission observed in the cyber threats mitigation strategies is the lack of a dedicated financial plan in order to achieve all the identified strategies. This begs for the need for a user perceived mobile banking cyber security framework to address the gaps identified.

References

[1] Watson, R., Leyland, P.P., & George, Z. U-Commerce: Expanding the universe of marketing. Journal of the Academy of Marketing Science, 30(4), 333-347, (2002).

[2] 2015 industry drill-down report. Financial services, (2015).

[3] Chitrey A., Singh D., Bag M. and Singh V. A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. International Journal of Information & Network Security (IJINS), 1(2), (2012).

[4] Omondi, D. How fraudsters are sneaking into your mobile phone to steal private information. The Standard Newspaper, (2016 February 8th).

[5] ISACA, (2012). ISACA ® Glossary of Terms. Available at: https://www.isaca.org/glossary.

[6] Paans, R. Part 6D Introduction Code of Practise for Information Security Code ISO 27002:2005. Post Graduate IT Audit opleiding Vrije Universiteit. (2010).

[7] Nambiro, A. W., Muchiri, G. M. and Matoke, N. Survey of Cyber Security Frameworks. International Journal of Technology in Computer Science & Engineering, 1(2), 33-39 ISSN 2349-1582, (2014). Available online at http://www.ijtcse.com

[8] SACCO Briefs. Managers and Board Members: Implications of the SACCO Societies Act and Regulations, (2011).

[9] Harris, A., Goodman, S. and Traynor P. Privacy and Security Concerns Associated with Mobile Money Applications in Africa. Washington Journal of Law, Technology & Arts, 8 (3), (2013).

[10] Mumanyi, E. A. L. Challenges and opportunities facing SACCOs in the current devolved system of government of Kenya: A case study of Mombasa County. International Journal of Social Sciences and Entrepreneurship, 1 (9), 288-314, (2014).

[11] Janczewsk L. J. and Fu L. Social Engineering-Based Attacks: Model and New Zealand Perspective. Proceedings of the International Multiconference on Computer Science and Information Technology pp. 847–853, (2010).

[12] Blackburn, J.and Waters, G. Optimizing Australia's Response to the Cyber Challenge. Kokoda Foundation. (2011).

[13] Fried, I., (2012). At Defcon, Hackers Show How to Hack Your Android Phone Encryption, ALL THINGS D, http://allthingsd.com/ 20120728/at-defcon-hackers-show-how-to-bypass-android-encryption/.

[14] Hasan M., Prajapati N. and Vohara S. Case study on social engineering techniques for persuasion. International journal on applications of graph theory in wireless ad hoc networks and sensor networks, 2 (2), (2010)

[15] Purkait S. Phishing counter measures and their effectiveness – literature review. Journal of Information Management & Computer Security, 20 (5), (2012)

[16] Greitzer F. L., Strozer J. R., Cohen S., Moore A. P., Mundie D. and Cowley J., (2014). Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. 2014 IEEE Security and Privacy Workshops.

[17] Nelson R. (2008). Methods of Hacking: Social Engineering. online. Available at: http://www.isr.umd.edu/gemstone/infosec/ver2/ papers/socialeng.html, last accessed on 2013-07-04.

[18] Thorawade M.B. and Patil S.M. Authentication Scheme Resistant to Shoulder Surfing Attack Using Image Retrieval. International Journal of Knowledge Engineering, 3 (2), (2012).

[19] Adams A. and Sasse M.A. Communications of the ACM, 42, 41-46, (1999)

[20] Granger, S. Social Engineering Fundamentals, Part I: Hacker Tactics. SecurityFocus, (2001).

[21] Schmidt, A.D. Detection of Smartphone Malware. Technischen Universitat Berlin, (2011).

[22] Jassal R., K. and Sehgal R., K. Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example. IOSR Journal of Computer Engineering, 13 (1) pp 114-121, (2013).

[23] Mannan M. and van Oorschot P.C. Security and Usability: The Gap in Real-World Online Banking. New Security Paradigms Workshop, (2007).