NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

FACULTY OF APPLIED SCIENCES

COMPUTER SCIENCE DEPARTMENT

An evaluation of the effectiveness of Mobile Banking System Security Strategies at Zimbabwean Commercial Banks

Student Name : Moyo Thabiso

Student ID : N012 5104P

Supervisor : Mr. S. Ngwenya

Co-Supervisor: Mr. K. Sibanda

This dissertation is submitted to the National University of Science and Technology, Computer Science Department, in partial fulfilment of the requirements for the Master of Science Degree in Information Systems.

August 2013

Abstract

Short Message Service (SMS) is considered a globally accepted wireless service initially adopted and developed for use in the Global System for Mobile communications (GSM). It enables transmission of alphanumeric messages between mobile subscribers and external systems. However questions about data confidentiality, user authentication and data integrity arise. Internet and mobile technologies are increasingly being adopted and utilised in the banking industry. Mobile banking is a system that allows customers of a financial institution to conduct financial transactions through a mobile device such as a mobile phone or personal digital assistant .In as much as mobile banking is improvement in terms of technology; it raises concerns for customers about the security and privacy of their information. The increasing popularity of mobile banking has attracted the attention of both legitimate and illegitimate banking practices, thereby, exposing customers to criminal activities, fraud, thefts and various other threats of similar nature. The major concern is whether mobile banking system security measures that have been deployed are effective. It is critical to deliver a secure mobile banking system to avoid the risk of negative effects which include clients accounts being tampered with, phishing or identity theft. This research therefore evaluated the effectiveness of the security strategies in use in Zimbabwe commercial banks. To achieve this a representative sample of 7 bank system administrators and 3 Virtual System Administrators from telecommunications providers were interviewed and asked to complete questionnaires which were analysed using Statistical Package for Social Sciences(SPSS). From the analysis, it was discovered that the majority of banks are using between two and five mobile banking security strategies. The strategies included passwords, firewalls, encryption, PIN codes and secure socket layers. It was therefore concluded that Zimbabwean banks are effective in offering secure mobile banking services. Suggested mitigation strategies for improvement of the security strategies being employed are the use of one time passwords, the use of hardware security modules and the carrying out of risk analyses periodically to ascertain if measures in place are still effective.