Abstract

Voice phishing (vishing) is a type of phishing attack where social engineers manipulate individuals during phone conversation into divulging sensitive information. Mobile users are target to most criminals, through mobile phone, users are able to carry out all bank services like cash withdraw, transfer and deposit, mobile phones offer payment services and through mobile phone, one is able to process loans. Social engineers prefer this form of attack because they can easily complicate the call routes, making it had for the investigator to locate them. Research shows most of this attacks are never reported to the relevant authorities because most victim blame themselves for their naivety. Unlike email phishing, which is classified, as tradition way of attack mobile phone vishing is a modern way of attack, less research exist on this area. This study proposed a practical model, which can be used by mobile phone users to detect social engineering attacks. The model seeks to assist user's to quickly and effectively identify if the caller is manipulating them in divulging sensitive information. The study employed a cross sectional survey research design. The sample size was comprised of 20 respondents, who were selected using random sampling. Data was collected using a structured questionnaire for mobile phone users and interview guide for the key informants in Kenya. Qualitative data was analyzed using content analysis while quantitative data was analyzed by use of SPSS using both descriptive. The study findings revealed that the main contributing factors in vishing attacks are psychological factors, technical factors and information sensitivity. Based on this three main factor a model was developed to aid mobile uses in detection of vishing attacks.