INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Automated Real-time Detection of Vishing & Smishing Attempts on Social Messaging Applications

A Dissertation by

Mr. Dushan Dissanayake

W1930626 / 20220133

Supervised by

Mr. Sithira Hewaarachchi

Submitted in partial fulfillment of the requirements for the MSc in Cyber Security & Forensics degree at the University of Westminster.

July 2023

Abstract

The advent of sophisticated mobile technology has led to the ubiquitous presence of mobile devices in society. These portable and versatile gadgets have become essential items for individuals due to their convenience and capabilities. As technology continues to play a crucial role in modern societies, an increasing number of people rely on mobile devices for financial activities such as online transactions, e-commerce, and routine business operations. However, the growing popularity of mobile devices has also exposed users to a higher risk of falling victim to fraudulent attempts. Perpetrators have been exploiting mobile users by pretending to present authentic and legitimate requests and opportunities, leading to the divulgence of personal and sensitive information. Such fraudulent activities have surged significantly, affecting individuals of varying ages, education levels, and technological literacy. Moreover, malicious actors leverage advanced tactics to conceal their identities, making it challenging to prevent and counter these attacks. Among the prevalent but under-addressed issues are voice phishing (vishing) and SMS phishing (smishing). This study proposes a system to identify vishing and smishing attempts and warn users in advance. The system uses natural language processing and machine learning techniques to analyze the content of voice calls and SMS messages. The system is able to identify suspicious artifacts, such as keywords and phrases that are commonly used in phishing attacks, as well as the context of the content. The system was evaluated using a dataset of vishing and smishing calls and SMS messages. The results showed that the system was able to identify vishing and smishing attempts with a high accuracy. The proposed system can be used to protect users from vishing and smishing attacks. The system can be deployed on mobile devices as a simple application. The system can also be used to train users to identify vishing and smishing attempts.

Keywords: Cyber Security, Phishing, Data Leakage, Natural Language Processing, Machine Learning,