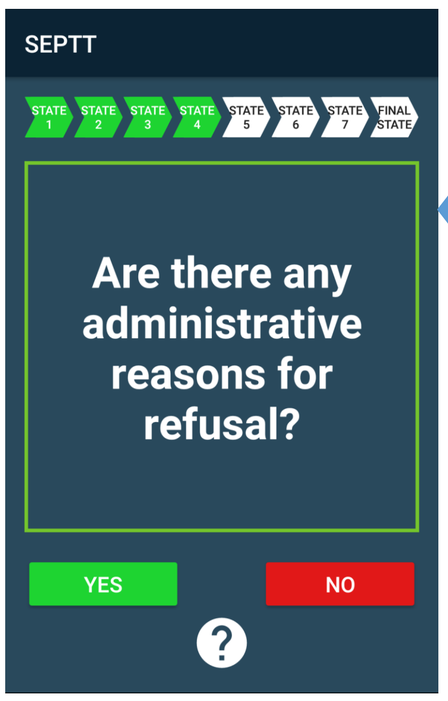
# Social Engineering Prevention Training Tool

## Overview

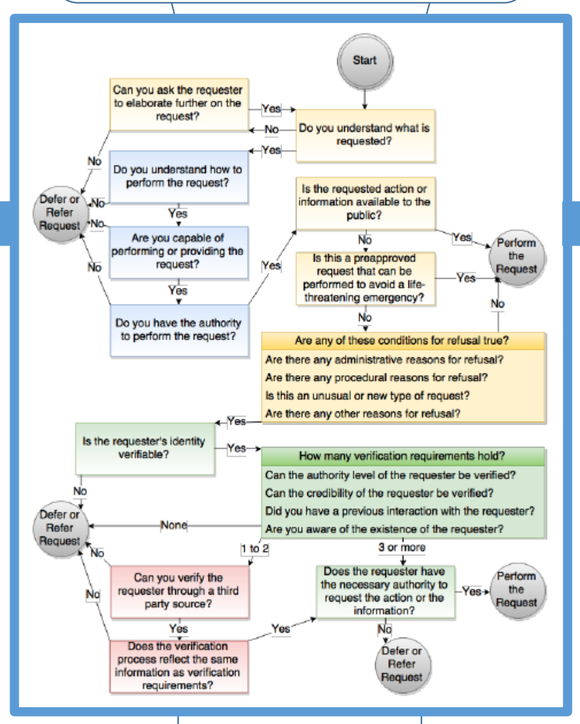
Social engineering refers to the various techniques that are used to obtain information through the exploitation of human vulnerability. This project aimed at developing and testing a Social Engineering Protection Training Tool, to determine if it was effective at preventing different possible types of social engineering attacks. The underlying model that the tool uses is the Social Engineering Attack Detection Model version 2 (SEADMv2), which was implemented as an Android application and a web application.

## Android Application

- Developed for general public use.
- Intended to prevent social engineering attacks that target individuals.
- Tested on 20 subjects.



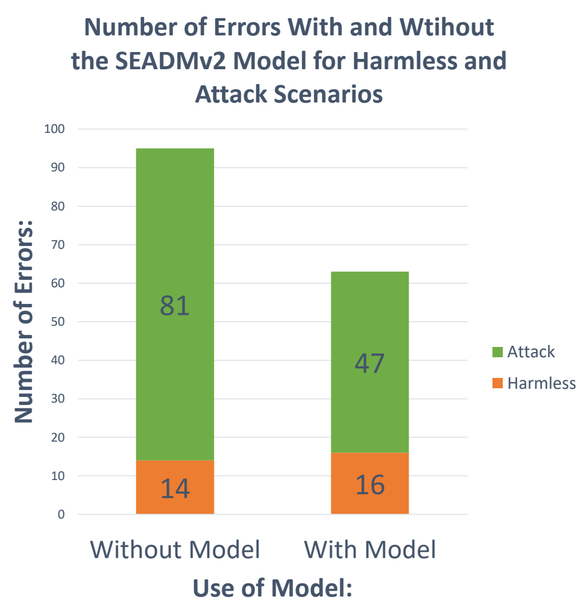

## SEADMv2



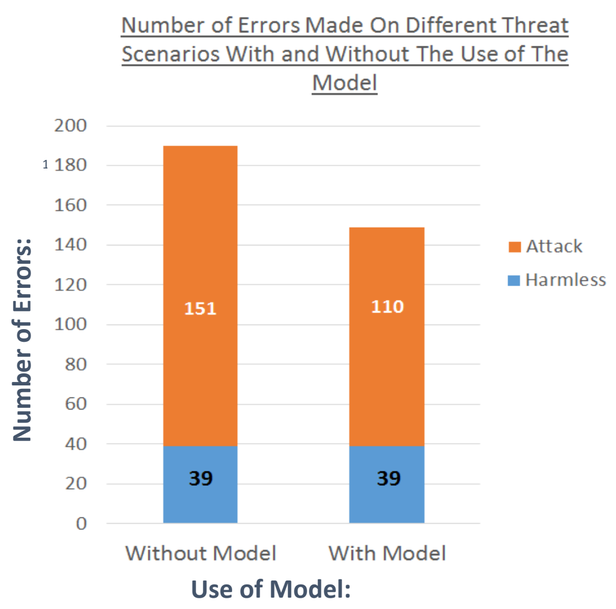

## Web Application


- Developed for a corporate environment.
- Intended to prevent social engineering attacks that target companies.
- Tested on 45 subjects.

## Overall Results




## Overall Results




## Conclusions

Both implementations of the SEADMv2 produced similar results.

- **Both applications significantly reduced the number of scenarios in which subjects fell victim to social engineering attacks. (Tool works for attack scenarios)**
- **Both applications did not significantly reduce the number of scenarios in which harmless requests were satisfied by subjects. (Tool doesn't have an effect on harmless scenarios)**


**University of Cape Town**
Department of Computer Science
Private Bag X3, Rondebosch, 7701
Email: dept@cs.uct.ac.za
Tel: +27 21 650 2663

**Team Members**
Saleem Manjoo
Michael Pepper
Marcel Teixeira

**Supervisors**
Prof. Tommie Meyer
Francois Mouton