

Detecting Social Engineering Attacks Using Semantic Language Analysis

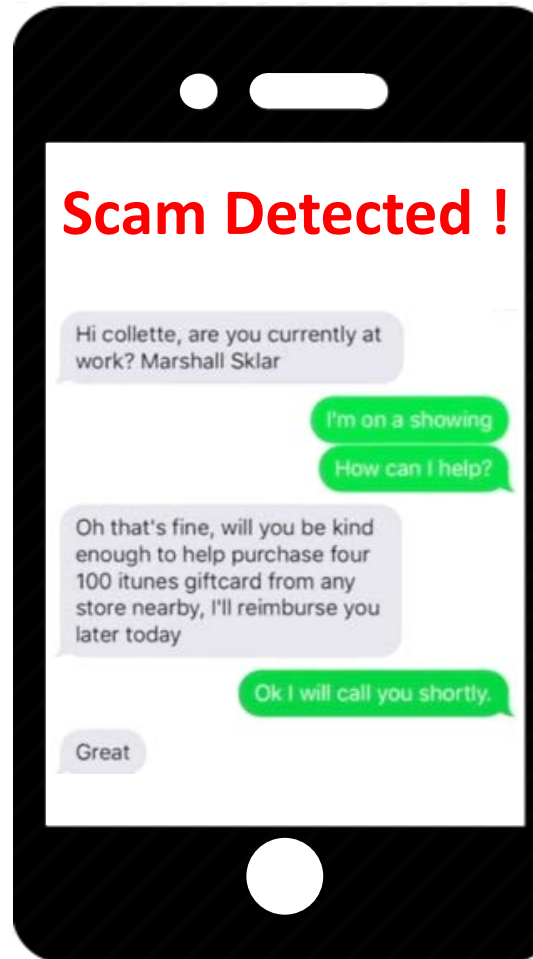


Challenge:

- Detecting **conversational social engineering attacks** in real-time
 - Phone, text, in-person
- Generate a corpus of realistic telephone-based attacks

Solution:

- Use **Natural Language Understanding** to infer malicious intent
- Detection approach based on **question-answering**
- Performing user study on effectiveness of scams



Scientific Impact:

- **Detection of conversational (non-email) attacks**
- **Corpus of realistic telephone-based attacks** is needed to support research in conversational attacks

Broader Impact:

- Telephone scams are rampant and currently not preventable
- It is common for people to ignore phone calls
- Social engineering detection can make phones usable again
- Phone app for detection is possible with speech-to-text technology
- User study trains students to resist scams

Award # 1813858
University of California Irvine
Professor Ian G. Harris
harris@ics.uci.edu