UNG

Annual Research Conference

Kevin Lin

Abstract

The purpose of this poster is to examine social engineering regarding how people interact with it. Specifically, the poster will go over the Social Engineering Toolkit that is available on Kali Linux to showcase how phishing emails can be created, how they are used to trick people, and how they can be spotted. There phishing emails will also be disguised with different methods such as hiding the sender information, sending the user to legitimate websites afterwards, etc. There will be a survey given out to people including different versions of emails (some will be normal emails while some will be phishing emails), and the responses will be recorded. The survey will present the different emails and will allow people to select which emails select which emails seemed normal, increasing the likelihood of them being clicked on. The data will go over information such as what kind of phishing emails are most effective, how often people fall for phishing emails, and so on. The data will be concluded with information about how phishing emails use social engineering to gather information from people without them realizing what has happened.

Key words: *Social engineering, phishing, emails, keyloggers, passwords, security, cyber security, social engineering toolkit, websites, computer science*