2015

Scientifically Defensible and Measurable Anti-Phishing Training

Josh Rymer
Virginia Commonwealth University

Chris Neville
Virginia Commonwealth University

Robert Hodges
Virginia Commonwealth University

Follow this and additional works at: http://scholarscompass.vcu.edu/capstone

Part of the Computer Engineering Commons

© The Author(s)

Downloaded from
http://scholarscompass.vcu.edu/capstone/8
Scientifically Defensible and Measurable Anti-Phishing Training

Team Members: Josh Rymer, Chris Neville, Robert Hodges
Faculty Advisor: Milos Manic
Sponsor: Idaho National Labs
Sponsor Advisor: David Manz PNNL, Miles McQueen INL

Introduction
• February 2015 Anthem Insurance cyber attack.
  - Over 80 million member’s information compromised.
• Phishing: to try to obtain financial or other confidential information from Internet users, typically by sending an email.
• Project focuses on how to quantify the likelihood a phishing email will succeed in tricking the user.
• Conducted a study.
  - Used the data from study to make a program to gauge relative effectiveness of a phishing email.
• This is one of the most pressing issues in security today; How to secure the human element.

Algorithm
• To determine the strength of a phishing email, the individual parts must be examined.
• Areas of email that are biggest indication of phishing:
  - Email’s from field.
  - Lexical contents.
  - Spelling and grammar.
  - Addressing the recipient.
  - Keywords.
• The frequency of these test criteria in an email will be used to calculate it’s potential threat.
• The scale we are using is a logarithmic scale from 1 to 10.
  - 1 is a very poor email, and 10 is a theoretically “perfect” phishing email.

Study
• Our project is based on the results of a study.
  - Conducted in the Spring Semester.
• Asked for consent to conduct our study from VCU students.
• Crafted fake phishing emails.
  - Highlighting certain traits of known phishing emails.
• These emails contained links to a site that was hosted on VCU School of Engineering servers.
  - Able to track site visits.
• Using this information we developed an algorithm that could determine approximately how dangerous a phishing email is.
  - Checking for various traits and commonalities.