Reducing Cyber Security Threats: Training computer users to detect spear-phishing emails attacks

Dr. Deanna D. Caputo
Lead Behavioral Psychologist

Changing Behavior in the Workplace Panel

National Initiative for Cybersecurity Education (NICE) Conference

Wednesday, September 21, 2011

This material is based upon work supported by I3P Contract Award Number 5-36423-5730, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

MITRE

I3P Institute for Information Infrastructure Protection

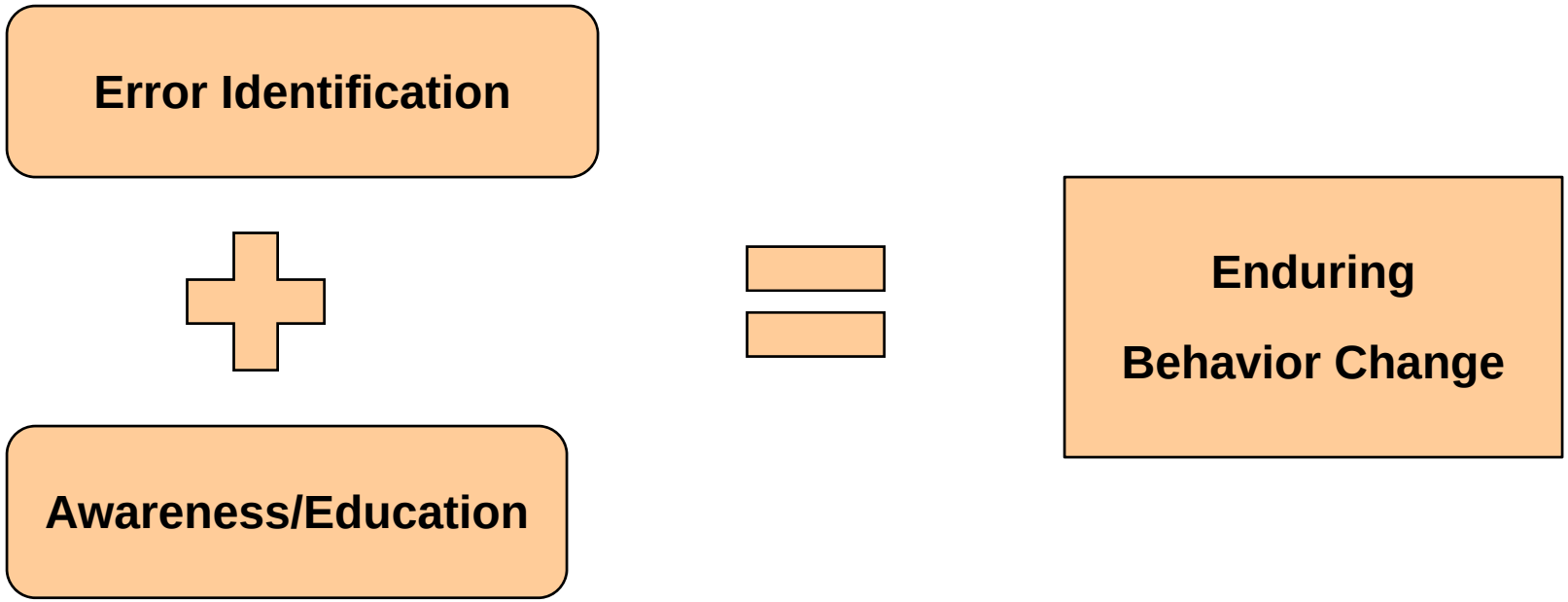
The Problem

- **Spear-phishing** is a *targeted* form of email phishing!
  - Someone plausible (employer, colleague, association, etc)
  - Seemingly legitimate topic
  - Urgency of a response
  - “Just click on link or open attachment”
- **Why do people click?**
  - No red flags, Curiosity, Haste, Illusion of invulnerability
  - “It’s security’s problem” Mentality
- **What do we want users to do?**
  - Think before clicking
  - Know what to do instead of clicking
  - Report if they click

Symantec's "Unlucky 13" Security Trends of 2010…
#2 Social engineering as the primary attack vector

Research Methodology

- **Embedded Email Training**



- **Real-time Feedback during regular daily email activity**
- **Encoding of solution with the problem**
- **Statistically Significant Reduction in Errors**

Hypothesis

If users are provided with training *immediately following* an error in judgment, then they will be less likely to make the same error when presented with a similar judgment.

Experimental Design

- **Participants:** Stratified Random Sampling 1300 employees from a medium-sized corporation in Washington D.C.
- **Control Group:**
  1. Users with annual InfoSec training
- **Experimental Groups:**
  2. Users provided with **gain–framed** and **individually** focused embedded email training to reduce clicking on links provided in emails. **(G&I)**
  3. Users provided with **loss–framed** and **individually** focused embedded email training to reduce clicking on links provided in emails. (**L&I)**
  4. Users provided with **gain–framed** and **other** focused embedded email training to reduce clicking on links provided in emails. **(G&O)**
  5. Users provided with **loss–framed** and **other** focused embedded email training to reduce clicking on links provided in emails. **(L&O)**

Procedure

- **Opt-Out Consent Email**
- **Spear-phishing emails sent to participants (3 Trials, 7 mos.):**
  - **Systematically modifying legitimate emails from each organization to contain 5 issues**
    - Abnormal “from” field
    - Typos, Improper Grammar, or Odd Spacing
    - Motivation to take immediate action
    - Links do not match status bar when mouse is hovered over
    - Intuition – overall feeling that something isn’t right
- **Participant reacts to email**
  - Clicks on link, Deletes, Forwards, Replies, Purges
  - Contacts Help Desk / Security
- **Training page is viewed by participant if he/she clicks on the link in the email**

Challenges and Limitations

- **Balanced Spear-Phishing Emails—**It is imperative that the spear-phishing emails are equal in effectiveness across trials
- **Snapshot in Time vs. Longitudinal—**It is difficult to determine how long behavioral influence effects last if they are only measured across a short time window
- **One Institution Sample—**Only employees from one company included in sample
- **Slightly Over-Educated Sample—**The company's employees tend to be more highly educated
- **Cannot Measure Reading of Training—**We will not be able to know for sure if participants read the one-page embedded training or simply closed the browser

Impact

Human Firewall is Essential

Changing Human Behavior is Difficult

- **Offering an empirically tested recommendation, a methodological approach, and an embedded training tool that will be well-documented and available for public or private sector use**
- **Government and Industry can apply experimental methodology and principles to other concerning behaviors**
  - Facebook links and files
  - Scareware
  - Malicious Pop-ups

It only takes one click to cause severe damage to systems and reduce National confidence in information security!

Thank you for your time!

QUESTIONS?

IRB and Management Issues

- Consent: None, Opt-In, Opt Out…
- Data Control: Ethical Issues
- Deception: Ever okay?
- Stakeholders: Everyone Wants to Know
- ACT: Internal vs. External Emails