Training, Awareness, and Incentives

A presentation by
Dr. Justin Albrechtsen

Cyber Security Through a Behavioral Lens II Workshop
October 24-25, 2011
Why this topic?

■ Problem
  – Users often make it difficult to keep information secure online and on networks

■ Potential Solution
  – Get users to improve their cyber security posture
    ■ Training
      ● The teaching and acquisition of knowledge and skills
    ■ Awareness
      ● The conscious application of the knowledge and skills taught during training
    ■ Incentives
      ● Factors that motivate a particular course of action
Example

■ Problem
  – Users click on spear-phishing emails exposing network data

■ Solution
  – Get users to quit clicking on spear-phishing emails
    ■ Training
      ● Users are taught and acquire knowledge about how to recognize spear-phishing emails via embedded training in emails in their actual email accounts
    ■ Awareness
      ● Users consciously apply this knowledge while checking email every day
    ■ Incentives
      ● Provide users an incentive (such as a recognition from management) every time they recognize a potential spear-phishing emails
3 Actions of Memory

- **Encoding**
  - Getting information into memory
    - Reading the training page

- **Storage**
  - Keeping information in memory
    - Remembering the information on the training page during the time between emails

- **Retrieval**
  - Getting information out of memory
    - Getting the information out of memory when the next spear-phishing email is received
Stages of Memory

■ **Short-term Memory (STM)**
  – Memories are initially stored into STM
  – Capacity = Between five and nine meaningful items
  – Duration = 20 seconds without rehearsal

■ **Long-term Memory (LTM)**
  – Memories are later encoded into LTM
  – Capacity = essentially limitless
  – Duration = essentially limitless

■ **Rehearsal**
  – The conscious repetition of information in order to encode it from STM to LTM
Basic Model of Memory

Information ➔ Encoding ➔ Short-term memory ➔ Encoding ➔ Long-term memory

Retrieval
Training and Awareness Questions

- Are participants reading and concentrating on the training in order to encode it properly?

- Is the training organized in a way that will facilitate storing the information?

- How can we help users to better remember information?
Yerkes-Dodson Law

- Optimal arousal
- Optimal performance
- Impaired performance because of strong anxiety
- Increasing attention and interest

Performance

Arousal

Strong

Strong

Weak

Weak

Low

Low

High

High
<table>
<thead>
<tr>
<th>Arroyo</th>
<th>Foulke</th>
<th>Millar</th>
<th>Ramirez</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bellhorn</td>
<td>Kim</td>
<td>Mirabelli</td>
<td>Schilling</td>
</tr>
<tr>
<td>Cabrera</td>
<td>Lowe</td>
<td>Mueller</td>
<td>Timlin</td>
</tr>
<tr>
<td>Damon</td>
<td>Martínez</td>
<td>Nixon</td>
<td>Varitek</td>
</tr>
<tr>
<td>Embree</td>
<td>Mientkiewicz</td>
<td>Ortiz</td>
<td>Wakefield</td>
</tr>
</tbody>
</table>
Serial Position Effect

![Graph showing the serial position effect](image)

- Words recalled (%)
- Position in sequence
- Primacy, intermediate, Recency
Basic Model of Memory

Information → Encoding → Short-term memory → Encoding → Long-term memory

Retrieval
Ways to Improve Memory

- **Acoustic encoding**
  - Catch phrases and lyrics
  - Example – “If the glove doesn’t fit, you must acquit”

- **Self reference effect**
  - Relating the information to yourself
  - Example – 2004 Boston Red Sox players
Ways to Improve Memory

■ Chunking
  – The organization of information into meaningful units
  – Example – Acronyms
    ■ FAMOUS
      ● French-American Mid-Ocean Undersea Study

■ Imagery
  – People remember images better than words
  – Example – people can remember more than 2,000 pictures with 90% accuracy
Review

■ Successful training
  – Allows information to be encoded into long term memory
    ■ Basic model of memory
  – Gets users into an appropriate state of arousal
    ■ Yerkes-Dodson law
  – Presents information in an order that enhances memory
    ■ Serial Position effect
  – Gets the user’s attention
    ■ Acoustic encoding
    ■ Self reference effect
    ■ Chunking
    ■ Imagery
Incentives

Factors that motivate a particular course of action

Third piece of potential solution

- Get users to quit clicking on spear-phishing emails

Training

- Users are taught and acquire knowledge about how to recognize spear-phishing emails via embedded training in emails in their actual email accounts

Awareness

- Users consciously apply this knowledge while checking email every day

Incentives

- Provide users an incentive (such as a recognition from management) every time they recognize a potential spear-phishing emails
Incentives Questions

- What incentives do people find motivating?

- What incentives are realistic for your organization?

- Is it better to give incentives constantly or sporadically?

- Is reinforcement or punishment more effective at changing behavior?

- Are incentives a sustainable model?
**Behavioral Psychology**

Studies behavior without reference to mental processes

- Organisms can be conditioned (trained) to do anything
- Organisms have little or no choice
- Organisms do not play as strong a role in learning

**Cognitive Psychology**

Studies the mental processes behind behavior

- Feeling, emotions, and thoughts affect how people respond to conditioning
- People have choices
- People play a strong role in learning
Behaviorism

- **Law of effect**
  - Rewarded behavior is more likely to reoccur
  - Punished behavior is less likely to reoccur

- **Conditioning**
  - Process of associative learning (training)
  - Example – Parent trains child by requiring a timeout every time the child misbehaves

- **Reinforcement**
  - *Increases* the frequency of a behavior

- **Punishment**
  - *Decreases* the frequency of a behavior
Types of Reinforcement

■ Continuous reinforcement
  – Reinforcing the desired response every time
  – Every time user catches a spear-phishing email they receive incentive
  – Best when first beginning to condition a behavior

■ Intermittent reinforcement
  – Reinforcing a response only part of the time
  – User must catch spear-phishing email several times before receiving incentive
  – Most resistance to extinction
Motivation vs. Practicality

■ Incentives
  – Factors that motivate a particular course of action

■ Incentives that are perceived as most motivating
  – Expensive
  – Difficult to attain

■ Incentives that are perceived as most practical
  – Cheap
  – Easy to attain

■ Incentives that are both motivating and practical
  – Praise
  – Items that are already available (free parking)
  – Lotteries
Individual vs. Group Reinforcement vs. Punishment

- Individual reinforcement
  - Rewarding the individual for individual behavior

- Individual punishment
  - Penalizing the individual for individual behavior

- Group reinforcement
  - Rewarding the group for individual behavior

- Group punishment
  - Penalizing the group for individual behavior
Types of Motivation

■ Extrinsic motivation
  – A desire to perform a behavior due to promised rewards or threats of punishment
  – Example – performing positive cyber security behaviors because user wants to receive the incentive

■ Intrinsic motivation
  – A desire to perform a behavior for its own sake
  – Example – performing positive cyber security behaviors because user wants to keep information safe online

■ Which type of motivation is more sustainable?
Review

- Successful incentives

  - Motivate a particular course of action
  - Are practical
  - Begin as continuous reinforcement but progress toward intermittent reinforcement
  - Encourage intrinsic motivation
Study 2:
Understanding Incentivization for Good Security Behavior
Incentivization Study: The Problem

■ Research
  – No empirical research on incentives for good cyber behavior

■ Motivation
  – We don’t really know how to encourage users to do the right thing.

■ Practicality
  – What is the best use of organization security spending on incentives?
Incentivization Study: Experimental Design

- Recruit participants to assess the “Cyber Security Scorecard”

- Experimental Manipulation
  - Informed Consent and Pre-Questionnaire
  - Random Assignment to Incentive Condition

  - Control Group:
    1. Users given no incentive

  - Experimental Groups:
    1. Public Recognition
    2. Time off
    3. Lottery for Parking Spots
    4. Lottery Big Ticket Item
    5. Small Ticket Item
    6. Pick your own Incentive from above
Incentivization Study: Experimental Design

- Provide Awareness of Good and Bad Cyber Posture
  - Three positive behaviors
    - Patch compliance, Patch RT, reporting suspicious activity
  - Three negative behaviors
    - Accessing blocked, uncategorized, and file-sharing sites
- Pre-test vs. post-test
  - Monitor users for 30 days before and after manipulation
- Post-questionnaire and debriefing
Incentivization Study: Challenges/Limitations

■ Generalizability:
  – Did we pick the right incentives?
  – Could other organizations give these incentives?
  – Could other organizations monitor these behaviors?

■ One Institution Sample after Institution Approvals
  – Only one organization would be used for the study

■ Snap Shot in Time vs. Longitudinal
  – Difficult to determine how long behavioral influence effects last if they are only measured at one point in time
  – Longitudinal research is expensive and time-consuming (i.e., 1-year +).