Study Results:
Failure-Triggered Training Trumps Traditional Training

Sean Palka
Sean Palka
palka_sean@bah.com

Booz | Allen | Hamilton
delivering results that endure
Social Engineering Attacks Impact You and Your Organization by . . .

- Wasting fiscal resources
- Increasing costs
- Damaging reputations
- Causing clients to lose trust or go elsewhere
“Phishing attacks” target the weakest link in the information security chain — the individual end users. These attacks are really a people problem first and a technology problem second.
Our Study Sought to Determine if . . .

- **Interactive** phishing awareness training would
  - Be significantly more effective for learning transfer than both **placebo** and **static** page-turning training
  - Receive satisfactory reaction ratings and post-test scores
- **Failure-triggered training** would have a significant positive impact on learning transfer

Failure-triggered training: Unannounced blind exercises delivered in spaced intervals, combined with immediate tailored remedial training provided only to the users that “fail” the exercises.
After Initial Training, Groups Received Unannounced Attacks Over a 9-Month Period

Training
(pre-incident training completed by 3 study groups)

Unannounced Phishing Attacks
(conducted 3 separate, time-spaced exercises)

Post-Training Reaction Survey
(Kirkpatrick Evaluation Level 1 reaction data)

Training Post-Test
(Kirkpatrick Evaluation Level 2 learning data)

Failure-Triggered Training
(Kirkpatrick Evaluation Level 3 behavior data)
Control Group Received: Placebo Training

Control Group training did not address how to respond to phishing attacks.
Experimental Group 1 Received: Traditional Static Training

Experimental Group 1 training included phishing awareness content copied from a wiki.

Web-based attacks are categorized into the following classes:
- Fake Banner Advertising Attacks
- Man-in-the-Middle Attacks
- URL Obfuscation Attacks
- Cross Site Scripting (CSS or XSS) Attacks

victim into submitting their personal information. Once at the website, the attacker must continue to trick the victim into believing that personal information is required. The websites are often carbon copies of the real sites having similar fonts and images.
Experimental Group 2: Received Interactive Training

Experimental Group 2 training included “identifying suspicious item” activities to enable the practice of proper action responses.
<table>
<thead>
<tr>
<th></th>
<th>Overall Assessment</th>
<th>Delivery was engaging</th>
<th>I am better prepared to recognize phishing</th>
<th>I would recommend to others (Yes)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Group</strong> (N=114)</td>
<td>3.4</td>
<td>3.5</td>
<td>2.7</td>
<td>63%</td>
</tr>
<tr>
<td><strong>Wiki Group</strong> (N=88)</td>
<td>3.7</td>
<td>3.6</td>
<td><strong>4.1</strong></td>
<td>85%</td>
</tr>
<tr>
<td><strong>Interactive Group</strong> (N=114)</td>
<td><strong>3.8</strong></td>
<td><strong>4.1</strong></td>
<td>3.9</td>
<td>85%</td>
</tr>
</tbody>
</table>

Maximum score 5.0
Post-Tests Indicated Both Experimental Groups Knew How to Respond to Suspicious Emails

<table>
<thead>
<tr>
<th>Correct Response to: Who should be notified of suspicious emails</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wiki Group (N=88)</td>
</tr>
<tr>
<td>Interactive Group (N=114)</td>
</tr>
</tbody>
</table>
When simulated phishing attack are sent, the use of interactive training will result in

A. Significantly less incorrect responses compared to both the Control and Static groups

B. Significantly less incorrect responses than the Control Group only (no difference from the Static Group)

C. No difference in incorrect responses
Following training, we conducted unannounced simulated attacks. We expected to have significantly more incorrect actions from the Control Group than the Experimental Groups.
What We Discovered in Exercise 1 . . .

Based on the simulated attacks, we discovered no significant difference between training and no training!
What Do You Do When Training Fails (WTF)?
We Used Failure-Triggered Training

Failure-Triggered Training is like the “Secret Shoppers” used by the retail shopping industry.
Over the Next Six Months, Study Participants Received Three Exercises

- Participants were sent three different phishing emails on spaced intervals. Each user’s response/action was tracked.

- Interactive Training

- Correct Responses
  - User deletes the email (no responses are captured)
  - User reports the email through appropriate channels

- Incorrect Responses
  - User clicks an inappropriate link in the email
  - User directly responds to the email

- Failure-triggered training is delivered
- Response metrics aggregated using the STAR*Phish™ system
Study Results Show Incorrect Responses Decreased Significantly ($P < 0.05$) Between Each of the Exercises Over a Period of Months.
Study Results: The Number of Reports to CIRT (AKA - An Additional Correct Action) Increased with the Failure Triggered Training Approach

- Exercise 1:
  - Control: 0
  - Wiki: 1
  - Interactive: 1

- Exercise 2:
  - Control: 5
  - Wiki: 2
  - Interactive: 4

- Exercise 3:
  - Control: 10
  - Wiki: 7
  - Interactive: 6
Learning at the point of realization refers to the state when users are open to learning because relevance, knowledge gaps, and immediate needs are identified in an engaging/unexpected and concrete fashion.

The phishing training seems to have triggered a point of realization for the learners.
Spaced Learning Effect and Forgetting Curve

Knowledge Retention

Time after course completion

Typical Forgetting Curve

Forgetting Curve with Decreased Slope

Learning Event * Failure-Triggered Training Event

Adapted from sources: Herman Ebbinghaus, Research Institute of America
I learned about the CIRT team through the phishing training email sent out a couple months back. It really stuck with me, since I ‘failed the test.’

Quote from a study participant that correctly reported an external phishing attack to the Critical Incident Response Team (CIRT) highlights that learning at the point of realization may greatly influence the level of learning transfer.
Remember, Our Study Sought to Determine if . . .

- Interactive phishing awareness training would
  - Receive satisfactory reaction ratings and post-test scores
    - CONFIRMED
  - Be significantly more effective for learning transfer than both placebo and static page training
    - NOT CONFIRMED
- Failure-triggered training would have a significant positive impact on learning transfer
  - INDICATED
What We Learned Was . . .

- Traditional one-time, pre-incident training was ineffective
- Failure-triggered training resulted in a positive significant difference
- Reaction to an actual external phishing attack indicated knowledge transfer
- Multiple training elements may have to be present for successful learning transfer

Failure-triggered training: Unannounced blind exercises delivered in spaced intervals, combined with immediate tailored remedial training provided only to the users that “fail” the exercises.
Follow-On Questions and Next Steps

- How much impact does the email content have on the results?
- How important was the interactivity level of the failure-triggered training?
- Do users respond to emails and failure-triggered training differently on mobile devices?