Phishing Susceptibility: An Investigation Into Human Information Processing of Spear-Phishing

Aiping Xiong¹, Huanyi Ge², Jeremiah Blocki², Ninghui Li², Robert W. Proctor¹
¹Department of Psychological Sciences, ²Department of Computer Science

Background

Phishing
• Unique campaign increased 29% in Q3 2017 compared to Q3 2016 (APWG, 2018)
• 91% spear phishing in enterprise and organization (GreatHorn, 2017)

Phishing Emails Detection and Prevention
• Microsoft office 365 missed about 9.3% emails containing spam, phishing, and malware (Cyren, 2017)
• Purdue Cisco quarantine
  • filtered most false positives
  • 27 false negatives (spear-phishing emails) received in my Purdue inbox since 07/2017

Research Questions:
1. How do Purdue undergraduates process spear-phishing emails and determine whether to respond to them?
2. How does a Cisco quarantine email influence their subsequent decisions?

Online Study

• Email Management
Instructed to read 10 emails (2 spear-phishing, 8 legitimate) and take actions as they would normally do

• 2 × 2 Mixed Design

Research Questions:
1. How do Purdue undergraduates process spear-phishing emails and determine whether to respond to them?
2. How does a Cisco quarantine email influence their subsequent decisions?

Results

• Action Selection Results of Spear-Phishing Emails
  w Cisco Quarantine (238)

<table>
<thead>
<tr>
<th></th>
<th>w/ Cisco Quarantine (238)</th>
<th>w/o Cisco Quarantine (226)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Archive</td>
<td>Reply</td>
</tr>
<tr>
<td>sp_2 unknown</td>
<td>51%</td>
<td>16%</td>
</tr>
<tr>
<td>sp_1 known</td>
<td>47%</td>
<td>13%</td>
</tr>
</tbody>
</table>

• Enter Information on Phishing Webpages

Percentage of Enter Input:
- Both 12.4%
- Once 5.8%
- None 11.2%

• Phishing Awareness Results

Q1: Participants’ responses to spear-phishing emails and phishing webpages varied as a function whether the campaign was known or unknown, indicating a response bias and a lack of knowledge of how to identify phishing scams.

Q2: The presence of a Cisco quarantine email showed an impact on participants awareness of phishing but minimal effect on participants’ responses to spear-phishing emails and phishing webpages.

Reference: