Use of Phishing Training to Improve Security Warning Compliance: Evidence from a Field Experiment

Weining Yang, Aiping Xiong, Jing Chen, Robert W. Proctor, Ninghui Li
Purdue University
• Problem: To protect users from entering information into an illegitimate website
• Domain traffic ranking as warning trigger
• Field Experiments
  o Pilot Study
  o Main Study
• Discussion
Problem

Phishing attacks keep growing and evolving

- Users
  - easily deceived
  - ignore browser-based cues
  - do not understand active phishing warnings

- Detection of phishing websites
  - blacklist-based methods
  - heuristic methods

- But not 100% accurate
Problem

- High false negative rate
  - Phishing sites often not up long
  - Renders blacklisting ineffective
  - Infrequently used sites, but mimicking frequently used sites
  - Mismatches easy for users to understand

- Conducted experiments based on conveying this information to users in warnings
Phishing sites visited infrequently, with more than 91% of them having a rank > 10,000

**Figure 1**: Cumulative density of reported phishing URLs in PhishTank based on traffic rankings
Active warning presented within a Chrome extension

- used traffic ranking as the criterion for phishing detection
- presented it as the reason why the warning was displayed in the warning interface.
Pilot Study: Warning

Domain name extracted to aid user’s decision about the website’s legitimacy

Figure 2: Warning Display
Pilot Study: Warning

Domain name extracted to aid user’s decision about the website’s legitimacy

Figure 3: Warning Display
Pilot Study: Method

6-week field experiment using the phishing warning Chrome extension for daily computer use:

- control group (no warning) and exp. group (warned when trying to type information on domains ranked greater than 10,000)
- participants required to fill out a survey on a web-site through a link in weekly email sent by us
- in week 6, links in the email were associated with newly registered “phishing” domain maintained by us, simulating phishing attacks
- At end, semi-structured interview
Pilot Study: Results

• No participants in experimental group chose “Close the page” or closed the tab
• However, only 1 of 6 provided correct passwords during the “phishing” week
• Wrong passwords observed mainly due to keying errors
• Tended to ignore the warning due to mainly the mandatory survey task and partly to the interface design
• About half the participants did not understand the meaning of phishing
Main Study

- a new phishing scenario that replicates a popular commercial website promotion requesting only a voluntary response
- a redesigned warning interface
- participants’ lack of knowledge of phishing taken into consideration
Figure 5: Email that spoofs an Amazon gift card
Figure 3: New Warning Interface.
**New Warning Interface**

*Figure 4: New Warning Interface after clicking on “Advanced”.*
Brief Phishing Training

• The definition of phishing was provided and a banking phishing email example was presented. Participants were also taught how to evaluate the legitimacy of a URL by identifying the domain name.

• In addition, participants were tested with a list of URLs that included both legitimate and fraudulent types, with feedback provided.
Table 1: Number of participants who visited our phishing page, entered information, and fell in the attack by group condition. Pwd stands for password.

<table>
<thead>
<tr>
<th>Training</th>
<th>Total</th>
<th>Identified Phishing Email</th>
<th>Visited Phishing Page</th>
<th>Identified Phishing Page</th>
<th>Warning</th>
<th>Total</th>
<th>Submit Form</th>
<th>Input Genuine Pwd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>30</td>
<td>4</td>
<td>24</td>
<td>4</td>
<td>Yes</td>
<td>12</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>2</td>
<td>27</td>
<td>0</td>
<td>No</td>
<td>8</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
<td>14</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>
Discussion

- Knowledge gained from the training enhances the effectiveness of phishing warnings
- The knowledge by itself was not sufficient to provide phishing protection
- Field experiment: time consuming vs. ecological validity