Do Users Attend to Highlighted Domains in Identifying Phishing Webpages?

Aiping Xiong¹, Weining Yang², Robert W. Proctor¹, Ninghui Li²

¹Department of Psychological Sciences, ²Department of Computer Science

Eye-Tracking Experiment

A laboratory Experiment
- 32 participants
- 2 groups of 6 frequently target phishing webpages (one set legitimate and the other fraudulent) based on a 5 point scale
- 2 phases: 1st phase AnyCue
  2nd phase AddressBar
- Domain highlighted (DH) or not (DNH) varied between-subjects

Research Questions:
1. Will users naturally attend to the address bar?
2. Will users use the domain name to judge the website’s legitimacy?
3. Can users recognize the legitimate domain names?

Results

Legitimate

<table>
<thead>
<tr>
<th></th>
<th>AnyCue</th>
<th>AddressBar</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>DNH</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
</tbody>
</table>

Fraudulent

<table>
<thead>
<tr>
<th></th>
<th>AnyCue</th>
<th>AddressBar</th>
</tr>
</thead>
<tbody>
<tr>
<td>DH</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
<tr>
<td>DNH</td>
<td>![Image]</td>
<td>![Image]</td>
</tr>
</tbody>
</table>

Safety Decision

Q1: Yes.
- Naturally, participants attended to the address bar but in a much less extent if compared to visual cues such as login and logos.

Q2 & Q3: No.
- Although fixations were longer and concentrated on the highlighted domains for the fraudulent webpages, the non-significant differences between DH and DNH conditions revealed that participants did not mainly rely on the domain name for the legitimacy decision.
- Consequently, it suggests a lack of knowledge of the legitimate domain names for the participants.