PhishDuck: Capturing User Intention in an Email Client to Combat Phishing

Shao-Yu Wu
Carnegie Mellon University

Goals
- Protect users from phish
- Educate users about phish
- Minimal negative effects from habituation
- Minimal annoyance to users

Motivations
- Email clients only capture low-level actions, rather than the intention of the user.
- Knowing the users' intended destination could help block fake emails while allowing legitimate emails.

Concept
- Present interfaces to users if they click on suspicious emails, and help guide users towards making safe decisions

PhishDuck Warning Interface
- The PhishDuck warning interface is shown to the user if the link he clicks on is suspicious.
- Four options for the user to choose, each of which has corresponding UI for the further instruction

Interaction Flow
- Links are filtered with a whitelist
- If not on the whitelist, our system checks for brand names in the email
- If found, users are shown a warning interface, otherwise the redundancy interface.

PhishDuck Redundancy Interface
- The Redundancy interface is shown to the user if our system is not sure the legitimacy of the email after the user clicks on a link inside.

Result: Phishing Incidence Reduced

<table>
<thead>
<tr>
<th>Condition Name</th>
<th>Clicked</th>
<th>Visited a phishing site</th>
<th>Phished</th>
</tr>
</thead>
<tbody>
<tr>
<td>PhishDuck Warning with Redundancy</td>
<td>10(100%)</td>
<td>0(0%)</td>
<td>0(0%)</td>
</tr>
<tr>
<td>Redundancy</td>
<td>10(100%)</td>
<td>2(20%)</td>
<td>1(10%)</td>
</tr>
<tr>
<td>Thunderbird Phish Detector</td>
<td>10(100%)</td>
<td>7(70%)</td>
<td>7(70%)</td>
</tr>
</tbody>
</table>

* P < .01
** P < .05