Paper title: Concept and development of a Facebook application to raise security and risk awareness regarding social engineering.

Topic: Education in IT Security

Iwan Gulenko, Technical University Munich

“IT Security for the Next Generation”
Use social networks against Social Engineering

Don’t accept friend requests from strangers.
1. Problem: Social Engineering
Not everyone behaves like Eugene Kaspersky.

Figure: Four phases of social engineering
(Source: Adapted from Siegel (2009, 8)).
1. Problem: Social Engineering
Not everyone behaves like Eugene Kaspersky.

853 it-professionals were asked: "Name most common source of social engineering threats" Dimensional Research (2011)

Guidelines for social media (security) lack hints regarding social engineering (Source: Our research)
2. Methods: Social against Social Engineering!
… using Aizen’s „Theory of planned behaviour“

“The large **majority** of the **existing literature** in the Information Systems field, such as many studies […] has **focused** most on investigating **attitude** […] “ (Bulgurcu/Cavusoglu/Benbasat (2010, 524))

→ What if we focus on the **social aspect**?

- Usual awareness training
- Using social networks
- Guidelines

Figure: Theory of Planned Behaviour (Source: In Adapted from (Ajzen 1991, 182))
3. Treatment: State of the Art…
…include other Facebook Apps and guidelines

- reclaimprivacy.org
  - Sets privacy settings.

- safeweb.norton.com
  - Scans wall for malicious links.

- defensio.com
  - Scans wall for malicious links.

- Facebook Guideline

---

<table>
<thead>
<tr>
<th>Problem</th>
<th>Methods</th>
<th>Treatment</th>
<th>Measurements</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Demo: Max M. works for a big company and uses Facebook…

1. Facebook privacy: “Public search” setting leads to **indexation** in search engines, **divulgation** of too much personal information.

   ![Google Search Screenshot]
   - User was clickjacked!
   - User ruins reputation of his company…

2. Clickjacking: Somebody tricked Max and **reputation** of his company is in danger.

3. **Identity theft**: An attacker befriended Max using the name of „Alexander“, who is a real friend of Max.
3. Treatment: Facebook App „Can You Be Googled?“

Users and their friends become “IT experts”.
They are less likely to become victims of social engineering.

1. Are Facebook privacy settings set correctly?
2. Detect Clickjacking.
3. Check what Google and "people search engines" know about the user.
4. Identity theft: Are there "double" friends in the friend list?

→ 1.-3. are applied to the user and also to the social circle of the user!
4. Measurement 1: Questionnaire
Qualitative analysis

The majority of users needed less than 10 minutes to use the app.

<table>
<thead>
<tr>
<th>How much time did you spent with the app?</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;5 Min</td>
<td>38.5%</td>
</tr>
<tr>
<td>5-10 Min</td>
<td>38.5%</td>
</tr>
<tr>
<td>&gt;10 Min</td>
<td>23.1%</td>
</tr>
</tbody>
</table>

The majority of users learned the idea behind Clickjacking, how privacy settings should be set etc. (multiple answers allowed) 😊

<table>
<thead>
<tr>
<th>What did you learn from app, blog and videos?</th>
</tr>
</thead>
<tbody>
<tr>
<td>What Clickjacking means.</td>
</tr>
<tr>
<td>How to protect my privacy better.</td>
</tr>
<tr>
<td>Why I should not trust Facebook applications.</td>
</tr>
</tbody>
</table>
4. Measurement 2: 117 users were tracked in a database...
...and at least 15 (~16%) changed their privacy settings in less than 10 minutes 😊

<table>
<thead>
<tr>
<th>No</th>
<th>Process of starting application</th>
<th>Instant change</th>
<th>Sum of mins</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>True, 1.9 days, True, 5.03 days, True, 2.62 minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>False, True, 7.6 minutes, True, 19.56 days</td>
<td>✓</td>
<td>7.6</td>
</tr>
<tr>
<td>3</td>
<td>False, True, 19.37 minutes, True, 4.02 hours</td>
<td>✓</td>
<td>19.37</td>
</tr>
<tr>
<td>4</td>
<td>False, True, 29.42 minutes</td>
<td>✓</td>
<td>29.42</td>
</tr>
<tr>
<td>5</td>
<td>False, True, 11.6 minutes</td>
<td>✓</td>
<td>11.6</td>
</tr>
<tr>
<td>6</td>
<td>False, False, 58.0 seconds, True, 8.84 days</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>False, False, 2.13 minutes, True, 10.85 minutes, True, 1.35 minutes</td>
<td>✓</td>
<td>12.98</td>
</tr>
<tr>
<td>8</td>
<td>False, True, 5.77 minutes</td>
<td>✓</td>
<td>5.77</td>
</tr>
<tr>
<td>9</td>
<td>False, True, 13.12 minutes</td>
<td>✓</td>
<td>13.12</td>
</tr>
<tr>
<td>10</td>
<td>False, False, 19.0 seconds, True, 7.57 minutes</td>
<td>✓</td>
<td>7.886.7</td>
</tr>
<tr>
<td>11</td>
<td>False, True, 1.67 minutes, True, 1.95 minutes, True, 3.1 minutes, True, 14.07 minutes, True, 46.0 seconds, True, 6.57 minutes, True, 44.0 seconds, True, 2.7 minutes, True, 1.17 hours, True, 1.4 minutes</td>
<td>✓</td>
<td>1.67</td>
</tr>
<tr>
<td>12</td>
<td>False, True, 51.0 seconds</td>
<td>✓</td>
<td>0.85</td>
</tr>
<tr>
<td>13</td>
<td>False, True, 2.94 days</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>False, False, 2.05 minutes, True, 6.72 minutes, True, 0.0 seconds</td>
<td>✓</td>
<td>8.77</td>
</tr>
<tr>
<td>15</td>
<td>False, False, 18.0 seconds, False, 6.05 minutes, True, 1.18 minutes, True, 72.94 days, True, 0.0 seconds, True, 5.75 days, True, 0.0 seconds</td>
<td>✓</td>
<td>7.53</td>
</tr>
</tbody>
</table>

**Mean**: 10.54

**Standard deviation**: 7.48

Results of the measurement of the ‘Can You Be Googled?’ Facebook application.
5. Conclusion: Main findings and future work

**Main findings:** Means to beat Social Engineering with Social Networks:

1. **Guidelines** for social media (security) **lack** hints regarding **social engineering**.
2. 16% became „**IT experts“**.
3. The app spread **viral**y because the **social circle** of the users was included.

**Future work:** Hit ‘em where it hurts!

- Does it work on other social networks?
- Can we get better than 16% (better design!)?
- How to improve the app (there are performance issues, if the user has >150 friends)?

**Try it yourself:** 😊

- **App**: apps.facebook.com/can_you_be_googled
- **Blog**: www.clickjacked.org
- **Awareness-Videos**: www.youtube.com/user/clickjackedorg
1. Deactivate "public Search" in Facebook: A 😊-smile next to your name means, that you have opted-out of Facebook’s search engines feature. If there is a 😐-smile next to your name your profile can be found through search engines. Unless you need to be found in Google you should disable this option.

Google Hits:
Research profiles from Constance Mussa to Tuya Myagmardorj in ...

Profile with 9 Likes,
1 x Spam?

Found double friends in your friendlist, are you a victim of Identity theft?

Alexandem Testusername
This is how your profile looks to most people on Facebook. Show
Backup slides
In case the internet lets us down.

1. Deactivate "public Search" in Facebook: A 😊-smile next to your name means, that you have opted-out of facebook's search engines feature. If there is a 😞-smile next to your name your profile can be found through search engines. Unless you need to be found in Google you should disable this option: