NoPhish App Evaluation: Lab and Retention Study

Gamze Canova, Melanie Volkamer, Clemens Bergmann and Benjamin Reinheimer
I. Introduction

- Importance for self-reliance
  ➔ Game-based education app (NoPhish) 🎮

- Evaluation 📚
  - Lab Study
  - Retention Study (5 months later)
  - N=19 (m=6, f=13)
  - Age: 20 to 36
II. Game Design

Level 3
Introduction

⚠️ New Attack
If the area between "http://" and the third slash "/" is an IP address, then the IP address is the Who-Section. **Do not enter any data here!**

In the following an example web address which has an IP address as Who-Section:

http://107.181.19.77/secure-login

Level 7
Exercise

Correct: 0 / 20
Level Score: 0

Is the following web address trustworthy?

✅ Trustworthy ✗ Phishing

www.ebay.online-auction.com/myebe

Start Exercise
II. Game Design

- Awareness Part
- Gaming Part: 8 Levels
  - Level 1: structure of a URL
  - Level 2: subdomain trick with very obvious domain name
  - Level 5: subdomain trick with trustworthy/related names
  - Level 7: trick where a character of the domain name is substituted
  - Level 8: trick where the host/brand name appears in the path part of the URL
III. Lab Study

(1) Informed Consent
(2) Website-Survey Before
(3) Play NoPhish
(4) Website-Survey After
(5) General-Survey After
(6) Certificates and Debriefing
Hypothesis 1:
After playing NoPhish, the participants give significantly more correct answers whether or not a website is a phishing website.

Wilcoxon signed-rank test
p-value < 0.001
Hypothesis 2: After playing NoPhish, the participants primarily base their decision whether or not a website is a phishing website significantly more often on the URL.

Wilcoxon signed-rank test p-value < 0.001
Hypothesis 3: After playing NoPhish, the participants primarily base their decision whether or not a website is a phishing website significantly more often on the domain of a URL.

Wilcoxon signed-rank test p-value < 0.001
III. Lab Study – Further Findings

- Confidence - 5 Likert Scale

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>21% with Median of 5 (very certain)</td>
<td>79% with a Median of 5</td>
</tr>
</tbody>
</table>

- Participant opinions – 5 Likert Scale

<table>
<thead>
<tr>
<th>NoPhish helped me identify phishing websites in the future</th>
<th>The text was easy to understand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median of 5</td>
<td>Median of 5</td>
</tr>
</tbody>
</table>
IV. Retention Study

(1) Phishing Survey
- The 24 examples from the lab study
- 10 new examples (5 phishing & 5 legitimate)
- Confidence about their answers

(2) General Questions
- „Did you receive a phishing email in the last few months?“
- „Do you think NoPhish helped you identify phishing attacks?“
Hypothesis 5 – Lab Study Before vs. Retention
In the retention study the participants give significantly more correct answers when deciding whether a website is a phishing website or not than before playing NoPhish.

Wilcoxon signed-rank test
p-value < 0.001
Hypothesis 6 – Lab Study After vs. Retention

In the retention study the participants do not give significantly fewer correct answers when deciding whether a website is a phishing website or not than directly after playing NoPhish.

Wilcoxon signed-rank test
p-value of 0.005
IV. Retention Study

Further Findings

(1) 58% participants detected a phishing attack

(2) 90% => App (very) important for phishing attack detection
V. Discussion

a. Hypothesis

- (H6) Website-survey after vs. retention

<table>
<thead>
<tr>
<th>Average After</th>
<th>Average Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>90,70%</td>
<td>81,89%</td>
</tr>
</tbody>
</table>

- Regression towards the mean
- Exponential nature of forgetting
V. Discussion

b. Individual URLs/Levels

1) Subdomain

<table>
<thead>
<tr>
<th></th>
<th>Before</th>
<th>After</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subdomain</td>
<td>✗</td>
<td>✓</td>
<td>❗</td>
</tr>
</tbody>
</table>

amazon.shopping.com
V. Discussion

b. Individual URLs/Levels

2) Letter swapping trick **mircosoft.com**

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>×</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>
V. Discussion

b. Individual URLs/Levels

3) Legitimate URLs

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
<th>Retention</th>
</tr>
</thead>
<tbody>
<tr>
<td>👎 Overcaution</td>
<td>✅ Certainty</td>
<td>⚠ Overcaution</td>
</tr>
</tbody>
</table>
VI. Conclusion

- Game-based education app
- Phishing detection training
- 3 different points in time
- Significant better performance
- Subdomains Repetition
- More focus on letter swapping
- Comparative Studies
- Perceived app as usefull
References


"Gnome-logviewer" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-logviewer.svg#mediaviewer/File:Gnome-logviewer.svg

"Gnome-application-exit" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-application-exit.svg#mediaviewer/File:Gnome-application-exit.svg

References

"Gnome-accessories-text-editor" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-accessories-text-editor.svg#mediaviewer/File:Gnome-accessories-text-editor.svg

"Gnome-input-gaming" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-input-gaming.svg#mediaviewer/File:Gnome-input-gaming.svg


"Gnome-face-cool" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-face-cool.svg#mediaviewer/File:Gnome-face-cool.svg

References

"Gnome-emblem-important" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-emblem-important.svg#mediaviewer/File:Gnome-emblem-important.svg


"Gnome-application-certificate" by GNOME icon artists - HTTP / FTP. Licensed under CC BY-SA 3.0 via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Gnome-application-certificate.svg#mediaviewer/File:Gnome-application-certificate.svg