On The Systematic Development and Evaluation Of Password Security Awareness-Raising Materials

Peter Mayer, Christian Schwartz, Melanie Volkamer
Why password security awareness is important

Average damage: $3.62 million

63% (2016) → 81% (2017)
Problems with existing awareness materials

- They demand impossible tasks from users
- Offer little actionable advice
- They do not represent the state of the art

Goal of this work:
Creation of effective awareness materials addressing the above problems
Our approach

Step 1: Development of initial version based on literature

Step 2: Incorporation of feedback from experts

Step 3: Incorporation of visual elements and feedback from lay-users

Step 4: Evaluation of the interventions in three SMEs

Step 5: Incorporation of feedback from the evaluation
Outline

Step 1: Development of initial version based on literature

Step 2: Incorporation of feedback from experts

Step 3: Incorporation of visual elements and feedback from lay-users

Step 4: Evaluation of the interventions in three SMEs

Step 5: Incorporation of feedback from the evaluation
Outline

- **Step 1:** Development of initial version based on literature
- **Step 2:** Incorporation of feedback from experts
- **Step 3:** Incorporation of visual elements and feedback from lay-users
- **Step 4:** Evaluation of the interventions in three SMEs
- **Step 5:** Incorporation of feedback from the evaluation
## Development of the material

<table>
<thead>
<tr>
<th>Step 1:</th>
<th>Development of initial version based on literature</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 11 attacks based on overview by Bonneau et al. (2012)</td>
<td></td>
</tr>
<tr>
<td>• Relevant defensive technologies</td>
<td></td>
</tr>
<tr>
<td>• Emphasis on important advice identified in the literature</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2:</th>
<th>Incorporation of feedback from experts</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Sent material to 30 experts in academia and the industry</td>
<td></td>
</tr>
<tr>
<td>• Received feedback from 13 experts</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3:</th>
<th>Incorporation of visual elements and feedback from lay-users</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Lab sessions with lay-users from our university</td>
<td></td>
</tr>
<tr>
<td>• Asked to read material and point out unclear or visually unappealing aspects</td>
<td></td>
</tr>
</tbody>
</table>
The awareness-raising material

Introductory sections

Attacks and actionable defences
The awareness-raising material

Introductory sections

Potential attackers

Possible consequences

Attacks and actionable defences
The awareness-raising material

Introductory sections

Potential attackers

Possible consequences

Attacks and actionable defences

- 11 attacks in ascending “distance” from user
- Dedicated icons and attack illustrations
- Relevant defensive technologies
The awareness-raising material

Introductory sections

Potential attackers

Possible consequences

Attacks and actionable defences

Angriff (1/11): „Gefährliche Nachricht“

Der Angriff versucht über eine gefährliche Nachricht (z.B. Phishing-E-Mail oder auch Anruf eines vorgelagerten Service-Mitarbeiters)

- entweder Sie dazu zu bewegen, Ihnen die gewünschten Daten direkt zuzusenden (z.B. Bankname oder das zugehörige Passwort),
- oder Sie dazu zu bewegen auf einen gefälschten Link zu klicken, der auf eine betrügerische Website mit einemtransparenten, aber falschen Design und auf der er alle Ihre Handlungen und die eingegebenen Daten dokumentiert kann.

Sollte sich der Betroffene auf einen gefälschten Link zu einem Problem der Schadsoftware führen lassen, ohne dass sie Ihrem etwas herausfinden oder erkennen müssten

Illustration

Attack

Defence

Further hints

Additional information on the threat of a „Frauliche Nachricht“

Additional information on the threat of a „Frauliche Nachricht“

More hints for the attack „Frauliche Nachricht“

There is a video, which shows the problematics of different attacks repeatedly.

https://www.youtube.com/watch?v=t4DFxLy4y4
Outline

Step 1: Development of initial version based on literature

Step 2: Incorporation of feedback from experts

Step 3: Incorporation of visual elements and feedback from lay-users

Step 4: Evaluation of the interventions in three SMEs

Step 5: Incorporation of feedback from the evaluation
Evaluation

- Evaluation of the materials in three German SMEs
- 90 participants overall, 30 in each SME
- Employees selected as lay-users by contact person in company
- One SME participated in retention after 6 months
Procedure

- Study performed completely in the employees’ real work environment
- Study material distributed by contact person as pdf file

**Goal:** Ensure the awareness-raising material’s effectiveness
Measures

Ability to assess behaviour as secure or insecure

- 22 scenarios
- One describing secure / insecure behaviour for each of the 11 attacks
- Participants must decide whether behaviour in scenario is secure / insecure
- Additional free-text field to justify answer

**Scenario 8:** Mr. Schmidt has problems remembering all the passwords he needs for his job and privately. Therefore, he uses walks on the keyboard, such as 1q2w3e4r

Mr. Schmidt behaves

- secure [ ]
- insecure [ ]

Why did you assess the behaviour of Mr. Schmidt as secure/insecure (a short answer is sufficient)?
Measures

Ability to assess security of passwords

- 12 passwords
- 7 weak passwords / 5 strong passwords
- Weak passwords: guessable within seconds using Hashcat + mangling rules
- Strong passwords: German diceware passwords

<table>
<thead>
<tr>
<th>#</th>
<th>Password</th>
<th>very insecure</th>
<th>very secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>@Q1w2e3r4#</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>samsung!!!</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>EimerKnirpsGoldSchelmerci</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>EssayRiesenrolleProbabilistisch</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Measures

Qualitative feedback: free-text questions

- Relevancy of the included information
- Additional information the participants would have wanted
- Helpfulness of the images in understanding content
- Effect of the material on the participant’s password management

2. Which additional information would you have hoped to find in the material?
**H1a:** The awareness-raising material significantly increases the users’ ability to discern secure from insecure password-related behaviour in different scenarios known to the participant before reading through the material.
**Hypotheses - Assess behaviour as secure or insecure**

**Pre-Treatment**  
11 Scenarios (random)

**Treatment**  
- H1a: 11 Scenarios (same as in Pre)
- H1b: 11 Scenarios (not in Pre)

**Post-Treatment**  
11 Scenarios (same as in Pre)

**6 Months**

**Retention**

**H1b:** The awareness-raising material significantly increases the users’ ability to discern secure from insecure password-related behaviour in different scenarios unknown to the participant before reading through the material.
Hypotheses - Assess behaviour as secure or insecure

H1c: The awareness-raising material significantly increases the users’ ability to discern secure from insecure password-related behaviour in different scenarios known to the participant before reading through the material even six months after reading it.
Hypotheses - Assess behaviour as secure or insecure

**H1d:** The awareness-raising material significantly increases the users' ability to discern secure from insecure password-related behaviour in different scenarios **unknown** to the participant before reading through the material even six months after reading it.
Hypotheses - Ability to assess security of passwords

Pre-Treatment | Treatment | Post-Treatment | 6 Months | Retention

12 Passwords | H2a | 12 Passwords | 12 Passwords |

**H2a:** The awareness-raising material significantly increases the users’ ability to correctly assess the security of passwords.
H2b: The awareness-raising material significantly increases the users' ability to correctly assess the security of passwords even six months after reading it.
Results - Assess behaviour as secure or insecure

11 Scenarios (random) → H1a → 11 Scenarios (same as in Pre) → H1b → 11 Scenarios (not in Pre) → H1c → 11 Scenarios (same as in Pre) → H1d → 11 Scenarios (not in Pre)

H1a (Pre → Post known)
- Significant improvement
- $r = 0.378$ → medium effect

H1b (Pre → Post unknown)
- No significant improvement
- $p = 0.07$
Results - Assess behaviour as secure or insecure

H1c (Pre ➔ Retention known)
- Significant improvement
- $r = 0.363$ ➔ medium effect

H1d (Pre ➔ Retention unknown)
- Significant improvement
- $r = 0.482$ ➔ medium effect
Results - Ability to assess security of passwords

H2a (Pre → Post)
- Significant improvement
- $r = 0.423 \rightarrow$ medium effect

Secure → Insecure
- Significant difference in Pre
- Significant difference in Post
Results - Ability to assess security of passwords

H2b (Pre ➔ Retention)
- Significant improvement
- $r = 0.603$ ➔ large effect

Secure ➔ Insecure
- Significant difference in Retention
Results - Hypotheses Overview

- **Pre-Treatment**: 11 Scenarios (random)
- **Treatment**: 11 Scenarios (same as in Pre)  
  - H1a
- **Post-Treatment**: 11 Scenarios (not in Pre)  
  - H1b
- **6 Months**: 11 Scenarios (same as in Pre)  
  - H1c
- **Retention**: 11 Scenarios (not in Pre)  
  - H1d

- **Pre-Treatment**: 12 Passwords
- **Treatment**: 12 Passwords  
  - H2a
- **Post-Treatment**: 12 Passwords
- **6 Months**: 12 Passwords  
  - H2b
Results - Hypotheses Overview

Pre-Treatment: 11 Scenarios (random)

Treatment:
- H1a: 11 Scenarios (same as in Pre)
- H1b: 11 Scenarios (not in Pre)

Post-Treatment: 11 Scenarios (same as in Pre)

6 Months:
- H1c: 11 Scenarios (same as in Pre)
- H1d: 11 Scenarios (not in Pre)

Retention:
- H2a: 12 Passwords
- H2b: 12 Passwords

12 Passwords (random)
Results - Qualitative Data

Relevancy of the included information
- 90.6% found the material relevant and helpful

[The material] was very helpful.
I have learned a lot!
- P7

Most helpful topics
- Password composition and guessing attacks
- Information on regular changes
- Password managers
Results - Qualitative Data

Additional information the participants would have wanted

- More concrete advice on creating passwords
- More information on password managers

[I want] concrete suggestions regarding software which can be used to generate secure passwords, about good password managers.

- P78
Results - Qualitative Data

Helpfulness of the images

Participants found the images helpful

*The images were very helpful in understanding the [awareness-raising material's content].*

- P53
Results - Qualitative Data

Effect of the material on the participant’s password management

- Dominant theme were password managers
  - 20.3% stated to start using one
  - 61.0% stated to continue using one
- 9.8% stated to use different management
- 8.9% stated not their change password management
Outline

Step 1: Development of initial version based on literature

Step 2: Incorporation of feedback from experts

Step 3: Incorporation of visual elements and feedback from lay-users

Step 4: Evaluation of the interventions in three SMEs

Step 5: Incorporation of feedback from the evaluation
Outline

Step 1: Development of initial version based on literature

Step 2: Incorporation of feedback from experts

Step 3: Incorporation of visual elements and feedback from lay-users

Step 4: Evaluation of the interventions in three SMEs

Step 5: Incorporation of feedback from the evaluation
Limitations

- Sample
  - German Participants
  - SME employees

- Participants could not be supervised in their real work environment
  - Participants might have used material when filling questionnaires
  - Material might have been read only partially, different amounts of time spent
  - Participants in the same SME might have “worked together”
Questions?

Step 1: Development of initial version based on literature

Step 2: Incorporation of feedback from experts

Step 3: Incorporation of visual elements and feedback from lay-users

Step 4: Evaluation of the interventions in three SMEs

Step 5: Incorporation of feedback from the evaluation

Already deployed in 48 companies to overall 578 employees