Poster: Towards an Instrument to Measure Everyday Privacy and Security Knowledge

Lydia Kraus, Tobias Hirsch, Ina Wechsung, Maija Poikela, Sebastian Möller
Quality and Usability Lab
Telekom Innovation Laboratories, TU Berlin
Ernst-Reuter-Platz 7, Berlin, Germany
lydia.kraus@telekom.de

1. INTRODUCTION

This paper presents the ongoing work on a questionnaire to measure privacy and security (P&S) knowledge amongst non-expert users. Whereas former work on the influence of privacy knowledge [1, 2] concentrated on self-reported knowledge, awareness, and behavior in the context of internet usage and protection against marketing companies, we measure how well everyday P&S advice, for instance provided in [3-6] and P&S concepts are known to users. Furthermore, we investigate whether there is a difference in mobile protection behavior between users with high, low, and medium P&S knowledge and privacy concern. The questionnaire was tested for difficulty and reliability in an online study with 154 participants. The study also contained questions regarding demographics, privacy concern, and mobile protection behavior. We find that many items have a low difficulty, that the reliability of the scale is acceptable to good, and that there is a difference in mobile protection behavior between participants of different P&S knowledge levels.

2. Methodology

2.1 Questionnaire design

To collect items for the questionnaire we accessed several webpages with recommendations for users during 2013 and 2014 [3-6]. Overall, we collected 27 recommendations which we compiled in a list. In addition, 4 experts met in a brainstorming session to determine P&S concepts to be used in the questionnaire. In the end, we were left with the 24 multiple choice items. Each item consists of one question and four suggested solutions, of which three are wrong and one is correct. In addition, each item includes a "don't know" option.

2.2 Online survey set-up

The online study consisted of seven parts: demographics, internet usage, smartphone usage, privacy concern (measured with the revised Global Information Privacy Concern Scale [7] on a 7 point scale, from 1 = *not concerned at all* to 7 = *very concerned*), P&S knowledge questions, and protection behavior (use of messenger apps with encrypted data transmission, anti-virus apps, anti-theft apps, privacy-protection apps, and decisions to install or de-install apps because of privacy-intrusiveness)

2.3 Participants

The survey was completed by 154 participants between 18 and 59 years (M = 29.61, SD = 9.19), recruited on a subjects portal. 67 participants (43.2%) were male and 86 (55.5%) were female, 2 (1.3%) did not report their gender. Participants with less than a secondary school degree (15.4%), secondary school degree (43.2%), and university degree (41.3%) were represented; there was a bias towards higher education levels. All kind of occupation groups were represented with a bias towards students (54.2%). 137 participants (89%) were smartphone users (88 Android (56.8%), 41 iOS (26.5%), and 8 "other" (5.8%)).

3. Results

3.1 Questionnaire analysis

The selected items (11 of 24) with means and standard deviations are given in the following. For the analysis the answers were either coded as correct (=1) or incorrect (=0). In the following, answer "A" is always correct, but during the survey the answer order was randomized.

- **How can a user protect herself against data misuse while surfing in a public network?** (M = .82, SD = 39; **A**: Avoid entering sensitive data on websites, **B**: Store the network password on the device, **C:** Delete the browser history after surfing, **D:** Disable location-based services on the device)
- **How can a device be protected from viruses**? (M = .82, SD = .38, **A:** Always keep software and OS up-to-date, **B:** Don't enter personal data on websites, **C:** Avoid using wireless networks, **D:** Only visit websites that were recommended by friends)
- **How can a smartphone be protected from malicious apps?** (M = 0.84, SD = .36, **A:** Only install apps from trustworthy sources, **B:** Check if the downloaded app provides legal info, **C:** Try to use apps only occasionally, **D:** Check if the app publisher has a website)
- **When using an online-banking app: how can the user protect herself against threats?** (M = 0.67, SD = .47, **A:** Secure the app with an additional password; **B:** Banking apps are always secure and don't need additional security means, **C:** Only use the app in urgent cases, **D:** Increase the security by modifying the source code of the app.)
- **What is the goal of encrypted data transmission?** (M = .61, SD = .49, **A:** The data can't be eavesdropped, **B:** The data is protected against viruses, **C:** The data can't be lost during transmission, **D:** Only the user herself can see the data)
- **What is malware?** (M = .83, SD = .38, **A:** Software which is unwanted and might be harmful, **B:** Software which is not working properly, **C:** Software which is automatically updating itself, **D:** A faulty technical device)
- **What is phishing?** (M = .77, SD = .43, **A:** The interception of personal information via faked routes, **B:** The analysis of user's browsing behavior **C:** The sending of unwanted ads, **D:** The uninstalling of software that needs too much resources)
- **What is social engineering*?** (M = .26, SD = .44, **A:** To spy out somebody's personal environment online with the goal to

use this information to undertake criminal activities such as identity theft or fraud **B:** To distribute software-testing tasks to several engineers in order to find security leaks, **C:** The development of software for social networks, **D:** The development of charitable apps which are free of charge) *Note: this item should be changed to “What is a social engineering technique?”

- **What is controlled by privacy settings in social networks?** (M = .84, SD = .36, **A:** The personal information that is shared with other people or apps, **B:** The personal information that can be seen by the provider of the network, **C:** The user data which is forwarded to other social networks, **D:** The user data which can be stored by the provider of the network)
- **What are web analytics?** (M = .66, SD = .47, **A:** Software which analyzes the behavior of website visitors, **B:** Software used by search engines to sort results by relevance, **C:** Software which automatically interlinks text on websites, **D:** Software, which analyzes HTML code for efficiency)
- **What is written in a privacy policy?** (M = .58, SD = .50, **A:** If and how a company processes personal information, **B:** What the user has to do in order to protect her data, **C:** How private data is classified in general, **D:** That personal information is always processed in anonymized form)

We measured a Kuder-Richardson 20 (KR-20) reliability (equivalent to Cronbach’s α for dichotomous items) of 0.76 for the scale with all 24 items. Items with a mean of more than 0.85, indicating that more than 85% of participants answered the item correctly, were removed as they do not allow for a good distinction between participants. After removing these items, the remaining scale with 11 items had a reduced KR-20 reliability of 0.67. A P&S score was calculated by summing up the number of correct answered questions of the 11 items. Descriptive statistics of the P&S score and privacy concern (PC) are given in Table 1. The quartiles were used to divide participants into categories of low, medium, and high P&S knowledge and privacy concern.

Table 1. Descriptive statistics: P&S score and Privacy Concern

Scale	Min	1st Qu	Mean	Median	3rd Qu	Max
P&S (N = 154)	1	6	7.71	8	9	11
PC (N = 154)	1	4	4.75	4.83	5.54	7

3.2 Mobile protection behavior

There was no correlation (Pearson product-moment correlation) between P&S knowledge and privacy concern, r = 0.106, N = 154, p = 0.190. Pearson χ^2- tests were computed to investigate the relation between P&S knowledge and mobile protection behavior as well as between privacy concern and mobile protection behavior (cf. Table 2).

Table 2. Differences in behavior between different groups of P&S knowledge and privacy concern[a]

Behavior	P&S	PC
1. Do you use messenger apps with encrypted transmission? (Yes[b] = 19%)	**high ↑; low ↓** $\chi^2(2, N=137) = 10.37; p=0.005$	**low ↓** $\chi^2(2, N=137) = 6.62; p=0.041$
2. Did you ever refrain from installing an app because the number of permissions was high compared to the features provided? (Yes[b]: 62.8%)	**high ↑** $\chi^2(2, N=135) = 7.23; p=0.027$	**low ↓** $\chi^2(2, N=135) = 6.04; p=0.041$
3. Did you ever refrain from installing an app due to unusual permissions? (Yes[b]: 75.9%)	-	**low ↓** $\chi^2(2, N=135) = 13.94; p=0.001$
4. Did you ever uninstall an app, after you heard that it is privacy-intrusive? (Yes[b]: 45.3%)	**high ↑; medium ↓** $\chi^2(2, N=135) = 7.83; p=0.021$	**high ↑; low ↓** $\chi^2(2, N=135) = 12.04; p=0.002$
5. Do you use the in-private browsing function of your browser? (Yes[c]: 33.6%)	**high ↑** $\chi^2(2, N=154) = 10.56; p=0.005$	-

[a] For cases 1-4 only smartphone users were considered. “low”, “medium” and “high” indicate the P&S knowledge or privacy concern group. Groups and behaviors without significant differences are not reported. The arrows indicate whether a group was either more likely to report a specific behavior (↑) or less likely (↓) compared to the complete sample (post-hoc tests with Bonferroni-correction).

[b] Refers to all smartphone users in the sample. [c] Refers to complete sample

4. DISCUSSION

The initial scale with all items had a good KR-20 reliability of 0.76; however, many items showed to have a low item difficulty. The reduced scale had an acceptable KR-20 reliability of 0.67; thus, further improvement is needed. Our results suggest that there is no correlation between P&S knowledge and privacy concern, but both where influential for mobile privacy protection behavior. Therefore, an improved version of P&S knowledge (or other digital literacy constructs) could be used in future studies to have an additional factor (besides privacy concern) to classify different user groups. However, with the given biases towards higher education levels and students in our sample, generalizations about the results should be made with caution and further studies are needed.

5. ACKNOWLEDGMENTS

This work has been supported by the EU FP-7 support action ATTPS under grant agreement no. 317665.

6. REFERENCES

[1] Park, Y. J.: "Digital literacy and privacy behavior online." *Communication Research* 40.2, 215-236, 2013

[2] Youn, S.: "Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents." *Journal of Consumer Affairs* 43.3, 389-418., 2009

[3] Data Privacy Day - http://www.staysafeonline.org/data-privacy-day/privacy-tips/mobile

[4] Hogben, G.,; Dekker, M.: Smartphones: Information security risks, opportunities and recommendations for users, *ENISA European Network and Information Security Agency*, 2010

[5] Microsoft Safety and Security Center: 4 safety tips for using Wi-Fi, http://www.microsoft.com/en-gb/security/online-privacy/public-wireless.aspx

[6] Consumer Action: How to Make Smart Wireless Choices and Avoid Problems: http://www.consumer-action.org/english/articles/cell_phone_ savvy_training_manual/#protect-info

[7] Malhotra, N. K.; Kim, S. S. & Agarwal, J.: Internet Users' Information Privacy Concern (IUIPC): The Construct, the Scale and a Causal Model. *Information Systems Research*, 15, 336-355, 2004