Factors Influencing the Purchase of Security Software for Mobile Devices – Case Study

Vlasta Stavova[1], Vashek Matyas[1], Mike Just[2] and Martin Ukrop[1]

***Abstract*—We investigated whether we could *nudge* users to purchase a premium version of mobile security software after using a trial version for 2-3 months. Our three interface designs used two persuasion methods: two *decoy* interfaces that attempted to nudge users to purchasing longer duration licenses, and one interface that used *reciprocity* in order to determine the value that people associated with the security software. We had approximately 60,000 participants for our study who completed a questionnaire, and again we had approximately 60,000 who were exposed to proposed variants. There were 12,000 participants who intersected both data samples, from which we also analyzed purchase decision patterns across our wide participant range, including users of English, German, Slovak, and Czech language versions. Our results indicate that factors such as gender, age, home country, and attitudes towards privacy and data sensitivity each had a significant impact on whether or not a premium license was purchased.**

I. INTRODUCTION

Malicious software (malware) is a persistent problem on computing devices, leading to many security problems – such as denial of service, compromised passwords, and email spam – for which there are several mitigation approaches [6]. The impact of malware is of particular concern, especially since 80% of users use their devices to make financial transactions (electronic payments, online purchases, etc.), and 92% of users store private information on their devices (with 30% storing passwords and other login credentials) [11]. In this paper we focus on approaches that encourage users to purchase security software on their smart devices, thereby building upon the influence of response cost for the use of security software [4].

While research indicates that at least 75% of users recognize that their desktop computers and smartphones could use additional security software [10], user motivation to use security software is low, which is partly driven by the belief that such software can be costly and hinder device performance [16]. Further, when such software is used, users are challenged with its effective management (installation, use, updates) [6].

Encouraging the use of security protections, such as antivirus software, can be tricky, especially if users do not feel that viruses are directed specifically at them, such as with some denial of service attacks [1]. The problems stemming from malware and limited protection adherence are significant. Some have suggested more forceful deployment of security software, such as charging users for the right to manage their software, whereby users who don't pay would be subjected to mandatory, automatic system updates [3].

We investigate several factors that could cause users to purchase a security system (including antivirus protection) for their mobile devices. We collaborated with an IT security software provider ESET for access to study participants, and for the use of their existing mobile security system (MSS) software. We used a mixed-method approach from April to December 2015 consisting of a 2-3 month trial with a premium version of the MSS software (include a questionnaire), after which we ran a between-subjects study with four design conditions where we asked participants to either purchase the premium version, or to continue with reduced, basic MSS version. Our designs focused on two methods of nudging: *decoy* purchase options, and *reciprocity*. We chose to compare a premium MSS version, which offered more security features such as application audit, to a basic version with limited functionality due to challenges noted by others with regard to the user management of security software [6]. Our results include the purchase rates across the four design conditions, as well as the questionnaire results across a wide breadth of participants using English, German, Slovak and Czech language versions of the MSS. Overall we had approximately 60,000 participants across our four conditions, 12,000 of whom also completed our questionnaire.

In the following section, we describe the related work in the area of user security behavior and persuasion. The next section specifies the experiment design. Section IV reviews the most significant results and observations, followed by the overall conclusion.

II. RELATED WORK

Efforts to increase secure user behavior have for the most part focused on responses to security warnings (e.g., [18]), and we review some of this work below in relation to our designs. There has been some work in determining factors related to improving secure behavior [4], though little in terms of interface design improvements, especially for malware protection.

Associating a value with security protections has often been performed for privacy protection, with results showing that users are willing to pay for privacy-enhanced web solutions [13] and smartphone apps [7]. For malware protection, Kaspersky [10] investigated factors influencing the purchase of antivirus software, noting increase purchase rates in North America, though this study did not evaluate different purchase interfaces and did not consider smart devices, such as smartphones or tablets. Overall, antivirus software purchase rates were low, with only 13% of desktop users purchasing a full license after a trial period. In terms of device security, 51%

Affiliation:
Masaryk University[1], Faculty of Informatics, Czechia.
Department of Computer Science, Heriot-Watt University[2], United Kingdom.
Email: vlasta.stavova@mail.muni.cz, matyas@fi.muni.cz, m.just@hw.ac.uk, mukrop@mail.muni.cz.
Manuscript first submitted on February 20, 2017.

of customers perceived a desktop computer to be "extremely unsafe" and requiring additional security software, whereas only 28% thought the same about smartphones. Kaspersky reports [11], [12] agree on differences in tablet and smartphone user security behavior. Tablet users protect their devices using special security software more often that the smartphone ones.

Our recent work [14] evaluated two purchase screen designs: one focusing on a simple text description focused on security and thus building upon the influence of perceived severity if not purchased [4], and the other supporting a purchase postponement with an "Ask me later" option. The simple description used the notion that the text structure greatly influences its readability and adherence [17]. The experiment ran in early 2015 with over 14,000 participants. The text change increased the number of license purchases from 1.96% to 3.18% (66% increase) in the first phase of our experiment, while the "Ask later" button increased from 1.96% to 2.65% (25% increase) in the same period.

A *persuasive* approach can be used to motivate users to make a preferred choice. Persuasion (or nudging) to improve user's security choices was used by J. Turland et al. [15] to improve user selection of WiFi access points. R. Cialdini [5] introduced six basic principles of persuasion including *reciprocity*, which can be implemented as a form of "Name your price" option for purchase decisions [8]. We use reciprocity in our designs, and to our knowledge, it has not previously been used to encourage security software purchases.

The decoy effect is another persuasive approach in which a decoy option is used to encourage the selection of another (non decoy) option by a user, so that the decoy can have the effect of causing an original option to appear more favorable. D. Ariely [2] describes an experiment to illustrate the decoy effect using newspaper subscription offers. The first option is to buy the online newspaper subscription for $59. The second option offers the subscription of a printed version for $125. The third offer is to buy both printed and online subscription for $125. While the second offer ($125 for printed version) naïvely seems pointless (it is unfavorable for the customer), it has an impact on the user decision. As a decoy, it nudges customers to select the third option. When respondents were choosing only between the first and third offer, 68% picked the first. After the introduction of the decoy option, more than 80% chose the third option. Adding the decoy option significantly changed the user's decision strategy. We are not aware of a decoy used to encourage security software purchases.

III. Experiment design

Our main experiment ran from April to December 2015 and included participants who installed English, German, Czech or Slovak versions of the mobile security system (MSS). Our experiment was undertaken in accordance with experimental and ethical regulations of our university. People who filled out a questionnaire participated with informed consent.

Experiment flow. We used a convenience sample of participants who downloaded and installed the (free) trial version of the company MSS on their mobile device. At the end of the installation process, participants were invited to complete a survey questionnaire, and were further rewarded with a 1-month trial extension (3 months instead of 2) for completing the survey. At the end of the trial period, each participant was asked to purchase a license for the premium MSS software as part of our user study, or "downgrade" to the basic version[1].

Questionnaire. The survey consisted of 10 questions that covered basic demographic features (age, gender, achieved education) and questions about attitudes toward privacy, smartphone safeness, price, user self-evaluation (Likert scale 1–6) as well as questions about smartphone use (e.g., storing passwords, accessing business data, internet banking). The questionnaire is in the Appendix section.

Experiment variants. We considered three new screen proposals and the original, control variant from our partner (see Figure 1). Each of the proposed variants differed from the original by their purchase options: Var. 1 and Var. 2 implemented a decoy purchase option. Var. 3 used reciprocity, where the user is asked to value her security. The user can select a price she wants to pay for the product out of three offers.

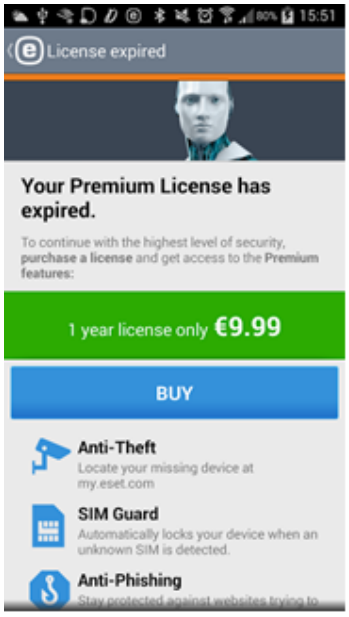

Fig. 1. The control variant.

Var. 0 (Original) Two options: free downgrade to the basic version, or purchase of 1-year premium license (€9.99).
Var. 1 (Decoy1) Three options: free basic version, 3-month license (€4.99) (decoy) and 1-year license (€9.99).
Var. 2 (Decoy2) Three options: free basic version, 1-year license (€9.99) (decoy) and 2-year license (€14.99).
Var. 3 (Reciprocity) Four options: free basic version, and all 1-year licence: €6.99, €9.99, or €12.99.

Apart from information about participants behavior towards one of randomly assigned proposed variant, we also collected

[1] At this stage, it is possible that participants could have uninstalled the basic version, though we were unable to confirm this[3].

system data (such as country, manufacturer, device type, resolution) about each participant in this phase. These attributes were collected automatically by company systems.

IV. RESULTS AND OBSERVATIONS

More than 60,000 users completed our survey questionnaire, and a similar number participated in our user study and were exposed to the proposed variants, with an overlap of 12,000 participants who performed both.

TABLE I
VARIANTS AND PREMIUM LICENSE PURCHASE RATE.

Variant	Downgraded	Bought license
Var. 0: Original	97.692%	2.308%
Var. 1: 3 moths + 1 year	97.464%	2.536%
Var. 2: 1 year + 2 years	97.453%	2.547%
Var. 3: 1 price	97.494%	2.507%

A. Influence of variants on purchasing a license

Our initial hypothesis was that persuasive principles used in screen design can influence user security decisions. We analyzed the final decision (a purchased license or downgraded) of over 60,000 study participants (see Table I). To distinguish significant differences in number of purchases, we used χ^2 test [9] at the significance level of $\alpha = 0.05$. While each proposed variant had a slightly higher conversion rate than Var. 0, the increase was not statistically significant ($\chi^2 = 2.202$, $p = 0.53$, $df = 3$).

We further investigated the influence of the decoy effect on a number of 1-year license purchases.

Var. 0: 354 of 15,339 purchased 1-year: 2.308%.
Var. 1: 347 of 15,161 purchased 1-year: 2.289%.
Var. 2: 261 of 15,076 purchased 1-year: 1.731%.

The difference in a number of sold 1-year licenses in Var. 0 and Var. 1 is not significant ($\chi^2 = 0.065$, $p = 0.8$, $df = 1$), which was contrary to our expectation since the 3-month license in Var. 1 was supposed to serve as a decoy that pushed participants to the 1-year license duration. We can also observe a significant drop between Var. 0 and Var. 2 ($\chi^2 = 10.526$, $p = 0.001$, $df = 1$) for the 1-year license (which was a decoy in Var. 2). We can observe a very small, insignificant improvement in the case when a 1-year license was accompanied by a 3-month decoy option, but 1-year license purchases went significantly worse with the 1-year license as a decoy. Based on these results, we conclude that in our case the decoy only nudges users towards the required option, but it also nudges them away from the decoy option. The difference between Var. 1 and Var. 2 (1-year license being non decoy versus decoy) is also significant ($\chi^2 = 11.456$, $p = 0.001$, $df = 1$).

1) Comparison between longest durations (non decoy options): We also investigated influence of nudging towards the longer duration licenses (the non decoy option) in Variants.

Var. 0: 345 of 15,339 purchased 1-year (only option): 2.249%.
Var. 1: 347 of 15,161 purchased 1-year (non decoy): 2.289%.
Var. 2: 111 of 15,076 purchased 2-year (non decoy): 0.736%.

When comparing the longest duration license options (the 1-year licenses for Var. 0 and Var. 1 are shown above) the 2-year duration in Var. 2 was purchased by 111 out of 15,076 participants (0.736%), a significant drop from Var. 0 ($\chi^2 = 117.842$, $p = 0$, $df = 1$) and Var. 1 ($\chi^2 = 122.135$, $p = 0$, $df = 1$). We have observed a significant decrease comparing purchases of longest licenses in Var. 0 and Var. 2 ($\chi^2 = 117.842$, $p = 0$, $df = 1$) and a very similar observation when comparing Var. 1 and Var. 2 ($\chi^2 = 122.135$, $p = 0$, $df = 1$). Based on this results, we can't confirm an influence of decoy option towards the longest duration (non decoy option). Somewhat surprisingly, the most "economical" choice in terms of cost per license duration is the 2-year license option from Var. 2, though it was 2^{nd} lowest (lowest was the 3-month option of Var. 1) in terms of license purchase. Thus, a 2-year license may be a too long commitment for an ordinary user.

For Var. 3, there was a surprising variety, with 33% choosing the lowest price, 54% the middle (standard) price, and 10% the highest price. 3% purchased in other way (e.g., Google Play).

B. Questionnaire and system data analysis

For the following analysis, we took participants who both filled a questionnaire and were exposed to the tested screens (12,263 participants in total after performing data cleaning). We point out several aspects that may influence user's likelihood to purchase a license. These aspects are then statistically evaluated using the χ^2 test and variable correlation.

1) Gender: Men comprised the majority of our participants (69%). As far as differences in gender are concerned, the ratio of males purchasing the premium license (4.7%) is significantly higher than for women (3.6%) ($\chi^2 = 7.624$, $p = 0.005$, $df = 1$). Women's conversion rate was significantly higher in Var. 1 (3 months + 1 year) ($\chi^2 = 5.565$, $p = 0.018$, $df = 1$) over the zero variant. No significant preference for any of the variants was observed for men.

2) Age: We had 17.7% participants younger than 21 years, 34.2% participants were between 21 and 30 years, 19.6% between 31 and 40, 13.3% between 41 to 50 and 15.2% above 50. On the sample of 12,263 participants, we found a statistically significant correlation between age and purchasing a premium license ($r = 0.183$, $p = 0.000$, $n = 12,263$). *The older* a user is, the more likely she is to *buy* a premium license.

3) Education: To avoid misunderstanding between the education systems of all covered countries, our questionnaire offered only three options of achieved education level: primary, secondary and university. We used a sample of 12,263 participants, only 6.3% participants selected the primary education. Our further investigation found out that these were mostly young people in the process of their secondary education. 40.9% participants achieved the secondary education, and 52.8% the university level. We conducted a χ^2 test to detect significant differences in a level of education among people who purchased a license. The conversion rate is significantly *lower* for the participants with only *primary education* (2.3%), compared to secondary school and university participants with respective

conversion rates of 4.2% ($\chi^2 = 6.317$, $p = 0.011$, $df = 1$) and 4.7% ($\chi^2 = 9.053$, $p = 0.002$, $df = 1$).

4) Tablet/smartphone differences: For the analysis below, we use either device system data (data collected from participants exposed to the proposed screens) with the full sample of 60,000 study participants, or the questionnaire responses (also 60,000) related to study participants with more than 12,000 overlap responses. The majority of participants were smartphone users (88%), the others used tablets (12%), based on the collected device system data. 2.9% *tablet users* purchased the premium license, which was significantly more than the 2.4% *smartphone users* ($\chi^2 = 5.363$, $p = 0.021$, $df = 1$). This confirms results from Kaspersky [11], [12] reports, who also observed a difference in security software purchases among tablet and smartphone users.

5) Purchase differences: We found several correlations with premium license purchase:

- Those participants who purchased a premium license consider the devices to be *less secure* against online attacks ($r = 0.049$, $p = 0.000$, $n = 12,263$) based on the questionnaire data, confirming the importance of security for the purchase decision.
- In terms of data privacy, we found the following. Participants who bought the premium license have *more private* data in their devices ($r = -0.032$, $p = 0.000$, $n = 12,263$), and are also *more sensitive* about their privacy ($r = -0.030$, $p = 0.001$, $n = 12,263$), both based on questionnaire data.
- The longer the duration of device ownership is, the fewer the participants who buy a premium license ($r = -0.024$, $p = 0.009$, $n = 12,263$).
- Those who did not buy a premium license, consider the price of €9.99 too high for the mobile security solution ($r = 0.084$, $p = 0.000$, $n = 12,263$), indicating that the magnitude of the purchase cost had an impact on the decision to not purchase the premium version.
- Participants who buy premium license consider smartphones to be a less secure device than those who did not buy the license ($r = 0.049$, $p = 0.000$, $n = 12,263$).
- There is no significant difference in self-evaluation between the people who decided to purchase a license and those who do not ($t = -0.153$, $p = 0.878$, $df = 12,261$).

6) User activity: There is a correlation between activities a user performs on a device and the willingness of buying a license ($r = 0.037$, $p = 0.000$, $n = 12,263$). As far as particular activities are concerned, there is always a statistically significant correlation between people who use a device for online activities (e.g., web browsing, email, Internet banking) and purchasing a license. The only activity that shows no statistically significant correlation with license purchase is, surprisingly, the use of the device for storing passwords ($r = 0.009$, $p = 0.309$, $n = 12,263$).

7) Country: Finally, we had 31.2% participants from the USA, 20.2% from Slovakia, 18.9% from Great Britain, 8.3% from the Czech Republic and 8% from Germany, covering more than 86% of our study participants. Since the information about country and purchases was involved in the system data, the data sample covers 60,000 participants. Slovakia and the Czech Republic had very similar conversion rates (3.0% and 3.1%, respectively). The USA and Great Britain also showed similarities in conversion rates (2.3% and 2.5%, respectively). A significantly *higher conversion rate* was observed for *Germany* (about 12.1%). We conducted ANOVA with the Bonferroni Post Hoc Multiple Analysis [9] which pointed out that our sample in Germany showed a significantly higher age than samples in other countries ($F = 14.001$, $p = 0.000$, $df = 4$). Germans from our study also considered smartphones as the least safe device ($F = 157.7$, $p = 0.000$, $df = 4$) (comparing with other countries). They also use smartphones less than in other countries ($F = 81.995$, $p = 0.000$, $df = 4$). No other significant difference (based on gender, education or privacy sensitivity) was observed. All these aspects may play a role in the decision whether to purchase a license or not. See Table II for an overview.

TABLE II
OVERVIEW OF FACTORS WITH INFLUENCE ON ANTIVIRUS PURCHASE.

Factors	Significant influence on purchases
Use of decoy option	No
Reciprocity	No
Gender	Yes
Age	Yes
Country	Yes
Security perception	Yes
Security self-evaluation	No
Privacy sensitivity	Yes
Private data on device	Yes
Password stored on device	No
Online activities	Yes

C. Study limitations

Our study concerned various approaches of nudging users to obtain an antivirus premium license. We included 60,000 product users into the study, so the sample size is more than sufficiently large, but we also see some limitations of our study.

Our study focused on design changes in final screen. Changes may seem too subtle and also no other antivirus features that may have an influence on purchasing a license such as overall satisfaction with the product were discussed.

Our measure of security software purchases is not necessarily indicative of secure user behavior. For example, participants who did not purchase the software may have chosen to use an alternative antivirus solution. In addition, there are other ways to define security behavior, other than their use of security software that we did not consider, e.g., web surfing behavior.

The questionnaire was distributed in English, German, Czech and Slovak language only. Respondents were recruited only from people using one of these antivirus language version that may cause a bias. We used a 1-month free antivirus use as a motivation to fill out the questionnaire, but we made a careful data cleaning to avoid meaningless and too quick responses.

Moreover, there could be additional facts that also influence purchase preference such as financial status of the participant. Unfortunately, we were not allowed to ask for such sensitive information. Similarly, we did not investigate factors of age and cost of devices.

V. CONCLUSION

We conducted an experiment with a trial version of a mobile security system in cooperation with an IT security software provider ESET. We investigated the influence of several aspects to user's willingness to purchase the premium license at the end of a trial period. We used different persuasive approaches to design three new variants of the screen that appeared to the user at the end of the trial period.

On one hand, we observed no significant impact of screen designs on participant's behavior. It seems that use of decoy options or reciprocity did not play a substantial role in observed user security decisions. On the other hand, we found a significant correlation of user's gender, education, country and age with purchasing the premium license.

Also, the type of device used plays a significant role in the decision whether to purchase a license. Tablet owners are significantly more likely to buy the premium license than ordinary smartphone users. The more actively the participants use their device, the more likely they are to obtain a license (with the surprising exception of password storage that did not prove to be statistically significant).

One's individual privacy sensitivity is also a strong factor to obtain the premium license. In terms of limitations, premium purchases are not necessarily indicative of secure behavior, and we have no further information about participants' behavior after declining a license purchase.

ESET acknowledged the results and decided not to experiment with persuasion principle further at this point. They considered namely the differences we found in user behavior across different countries to be of (their) primary interest.

To conclude, despite the persuasive approaches deployed, user dialog design seems to have a minor effect in comparison to other aspects such as participant's sensitivity to privacy, their gender, age, education, country or device type.

VI. ACKNOWLEDGEMENTS

The authors acknowledge the support of Masaryk University (MUNI/M/1052/2013) and involvement of colleagues from the Faculty of Social Studies in the experiment design.

REFERENCES

[1] R. Anderson and T. Moore. The Economics of Information Security. In *Science*, volume 314, pages 610–613. AAAS, 2006.

[2] D. Ariely. *Predictably Irrational, Revised and Expanded Edition: The Hidden Forces That Shape Our Decisions*. Harper Perennial. Harper Collins, 2010.

[3] T. August, R. August, and H. Shin. Designing user incentives for cybersecurity. In *Communications of the ACM*, volume 57, pages 43–46. ACM, 2014.

[4] T. Chenoweth, R. Minch, and T. Gattiker. Application of Protection Motivation Theory to Adoption of Protective Technologies. In *HICSS'09*, pages 1–10. IEEE, 2009.

[5] R. Cialdini. *Influence: The Psychology of Persuasion*. Harper Collins, 2009.

[6] L. Cranor and N. Buchler. Better Together: Usability and Security Go Hand in Hand. In *IEEE Security & Privacy*, number 6, pages 89–93. IEEE, 2014.

[7] S. Egelman, A. Felt, and D. Wagner. Choice architecture and smartphone privacy: There's a price for that. In *WEIS 2013*, pages 211–236. Springer, 2013.

[8] S. Fay. Partial-Repeat-Bidding in the Name-Your-Own-Price Channel. In *Marketing Science*, volume 23, pages 407–418. INFORMS, 2004.

[9] A. Field and G. Hole. *How to Design and Report Experiments*. SAGE Publications, 2002.

[10] Kaspersky Lab. Perception and knowledge of it threats: the consumer's point of view. https://www.kaspersky.com/downloads/pdf/kaspersky-lab_ok-consumer-survey-report_eng_final.pdf, 2012. Accessed: 2017-02-01.

[11] Kaspersky Lab. Consumer security risks survey 2014: Multi-device threats in a multi-device world. http://media.kaspersky.com/en/kaspersky_lab_consumer_security_risks_survey_2014_eng.pdf, 2014. Accessed: 2017-02-01.

[12] Kaspersky Lab. Consumer security risks survey 2016: Connected but not protected. https://press.kaspersky.com/files/2016/10/B2C_survey_2016_report.pdf, 2016. Accessed: 2017-02-01.

[13] S. Preibusch. The Value of Web Search Privacy. In *IEEE Security & Privacy*, volume 13, pages 24–32, 2015.

[14] V. Stavova, V. Matyas, and K. Malinka. The challenge of increasing safe response of antivirus software users. In J. Kofroň and T. Vojnar, editors, *Mathematical and Engineering Methods in Computer Science, Volume 9548 of the series Lecture Notes in Computer Science: 10th International Doctoral Workshop, MEMICS 2015, Revised Selected Papers*. Springer, 2016.

[15] J. Turland, L. Coventry, D. Jeske, P. Briggs, and A. van Moorsel. Nudging towards security: Developing an Application for Wireless Network Selection for Android Phones. In *Proceedings of the 2015 British HCI Conference*, pages 193–201. ACM, 2015.

[16] M. Volkamer, K. Renaud, O. Kulyk, and S. Emeröz. A Socio-Technical Investigation into Smartphone Security. In S. Foresti, editor, *Security and Trust Management, Volume 9331 of the series Lecture Notes in Computer Science: 11th International Workshop, STM 2015, Proceedings*. Springer, 2015.

[17] E. Wiebe, E. Shaver, and M. Wogalter. People's Beliefs about the Internet: Surveying the Positive and Negative Aspects. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, volume 45, pages 1186–1190, 2001.

[18] M. Wogalter, V. Conzola, and T. Smith-Jackson. Research-based guidelines for warning design and evaluation. In *Appl. Ergon.*, volume 33, pages 219–230, 2002.

Vlasta Stavova is postgraduate student in Center for Research on Cryptography and Security, Masaryk University. Her research is focused on usable security and human aspects in IT security, especially on ordinary end users.

Václav (Vashek) Matyáš is a Professor at the Masaryk University, Brno, CZ, and Vice-Dean for Industrial and Alumni Relations, Faculty of Informatics. His research interests relate to applied cryptography and security, where he published over 150 peer-reviewed papers and articles, and co-authored several books. He was a Fulbright-Masaryk Visiting Scholar with Harvard University, Center for Research on Computation and Society in 2011-12, and previously he worked also with Microsoft Research Cambridge, University College Dublin, Ubilab at UBS AG, and was a Royal Society Postdoctoral Fellow with the Cambridge University Computer Lab. Vashek edited the Computer and Communications Security Reviews, and worked on the development of Common Criteria and with ISO/IEC JTC1 SC27. He received his PhD degree from Masaryk University, Brno and can be contacted at matyas AT fi.muni.cz.

Mike Just is an Associate Professor in the School of Mathematical & Computer Sciences at Heriot-Watt University in Edinburgh, UK. His research focuses on using human-computer interaction and machine learning techniques in order to make better computer security tools.

Martin Ukrop is postgraduate student at Masaryk University, Brno, Czech Republic in the field of information security. Involved in Center for Research on Cryptography and Security since 2012. His research now focuses mainly on making security

VII. APPENDIX

A. *Questionnaire*

What is your gender? *[Single choice]*

- male
- female

How old are you? *[Text field: 13-99]*

Please indicate your highest level of education. *[Single choice]*

- Primary school
- Secondary school (high school)
- University/College

How long have you been using this smartphone? *[Single choice]*

- less than month
- less than 3 months
- less than 6 months
- less than a year
- less than 2 years
- longer

Do you consider yourself to be a skilled smartphone user? *[Likert scale]*

Extremely skilled o o o o o o Not at all skilled

Do you use this smartphone for… *[Multiple choice]*

o visiting websites?
o e-mail?
o social networking sites (e.g. Facebook)?
o online games?
o Internet banking?
o accessing business contacts?
o accessing business data?
o storing passwords?

Do you consider the data in this smartphone private? *[Likert scale]*

Extremely private o o o o o o Not at all private

In general, are you sensitive about your privacy? *[Likert scale]*

Extremely sensitive o o o o o o Not at all sensitive

In general, do you consider smartphones to be safe devices against online attacks, e.g. viruses, hacking, phishing, etc.? *[Likert scale]*

Absolutely safe o o o o o o Not at all safe

In general, do you consider 9.99 EUR for antivirus mobile software to be … *[Likert scale]*

Extremely high o o o o o o Not at all high