On the impact of warning interfaces for enabling the detection of Potentially Unwanted Applications

Vlasta Stavova & Vashek Matyas
Faculty of Informatics
Masaryk University, Czech Republic
Email: vlasta.stavova@mail.muni.cz, matyas@fi.muni.cz

Mike Just
School of Mathematical & Computer Sciences
Heriot-Watt University, United Kingdom
Email: m.just@hw.ac.uk

***Abstract*—We conducted a large-scale online study with 26,000 software installations during which we asked user (participants) whether they wanted to enable or disable the detection of Potentially Unwanted Applications (PUAs – potentially malicious software, such as *adware* or *spyware*). PUAs are notoriously difficult to manage, e.g., legal challenges can preclude default options that could otherwise be set for PUAs detection or removal. Our study was performed with an IT security software provider (ESET) who gave us access to the participants (antivirus product beta users). We used a between-subjects design with 15 conditions (a starting-point control interface, and 14 new "warning" interfaces). Despite the fact that many software companies (e.g., Microsoft, AVAST, AVG, McAfee, Kaspersky Lab) are struggling with PUAs detection, there are few studies focused on this topic.**

Our results indicate a strong desire for PUAs detection by users. In particular, enabling PUAs detection was chosen by 74.5% of our participants for our initial control interface. Further, a modified interface in which the option to enable PUAs detection was *presented first* resulted in 89.8% of participants choosing to enable PUAs detection (a *statistically significant increase* from the control).

I. Introduction

A *potentially unwanted application (PUA)* is software, such as *adware* or *spyware*, that can collect information about users [1]. PUAs are traditionally installed locally on a user's machine, though they can also operate via web-based mechanisms, for example using cross-site scripting [2]. Like malware, PUAs use computing resources, such as memory, processes and networks, and can also have a negative impact on user privacy, e.g., by collecting information such as page interactions and search queries. While malware is often deemed more malicious (e.g., supporting fraud, theft, denial-of-service), the direct results of PUAs are typically perceived as more benign and (legally or ethically) ambiguous. For this reason, PUAs are sometimes referred to as *greyware* [3]. While malware is typically subjected to automatic removal, the removal of *PUAs* will often depend upon the choice of a user [4].

While there has been a significant focus on malware over the years (e.g., [5], [6], [7]), there has been less focus on PUAs. Furnell et al. [8] highlight the impact that this has in terms of properly quantifying cybercrime, for example. However, recent research has provided an excellent first step, with a comprehensive analysis of the means and scale of adware injection [2]. Yet despite the fact that many software companies (such as Microsoft [9], AVAST [10], AVG [11], McAfee [12] and Kaspersky Lab [13]) are dealing with PUAs detection warnings, there appears to be no other study focused on this topic. In our paper, recognizing the importance of user involvement in deciding whether to accept a PUAs detection or not, we focus on the impact of warning interfaces for encouraging users to enable the detection of PUAs.

Deciding whether to enable PUAs detection is conceptually similar to other activities, such as controlling malware installation [14], evaluating whether mobile applications respect privacy [15], updating software [16] and click-through agreements [17], as each encourages a user to make an informed decision. Though due to the dubious legal standing of PUAs and their arguably lower risk (compared to malware) [18], it can be challenging to describe the threat of PUAs to users. For example, since the developers of PUAs actively defend their products, PUAs installation warnings that are overly biased (against their installation) can provoke legal challenges [3].

In this paper we report on a large-scale online study with 26,000 software installations in which we evaluated the effectiveness of a set of "unbiased warning" (i.e., warnings without intentionally stressed options) interfaces that asked participants (who were in the process of installing their antivirus software) whether they wanted to enable a feature that would thereafter detect the installation of PUAs.[1] Our designs were "unbiased" in the sense that we tried to present information and choices using non-judgemental language with regard to the acceptability of PUAs. Our goal was to *increase the number of participants who enabled PUA detection* when compared to the starting-point control interface. We were somewhat limited in the scale of interface changes that we could make (note that

[1]Full paper details and author contact information will be found at http://crcs.cz/papers/eurousec2016.

EuroUSEC '16, 18 July 2016, Darmstadt, Germany

http://dx.doi.org/10.14722/eurousec.2016.23003

these changes were made to the live system of our industry partner) so that more comprehensive changes were not possible for this experiment. Our interface designs and the evaluation study were performed in cooperation with the IT security software provider ESET who provided access to the study participants (antivirus product beta testers). Our 15 interface variations were based on four categories of warning features, namely (i) use of simple, jargon-free descriptions, (ii) warning images, (iii) enhanced text, such as with colour or bolding, and (iv) altering the order of option choices. Our reported results are quantitative and consist of the number of participants that decided to enable the PUAs detection feature (or not) for each of the interface variations.

In Section II we describe the related work in the area of warning design. Section III introduces principles and variables used during the design of proposed variants and also specifies the experiment design. Section IV explains the most significant experiment findings, while Section V discusses further observations. We conclude in Section VI. The appendix contains all proposed variants of PUAs detection user dialogs.

II. Related work

Previous work on security warnings tends to focus on either the *content* of the warning or the *presentation* of the warning. The end goal is to increase either adherence to a warning, or comprehension of the warning or its potential impacts. In some cases, where there are repeated requests for a user to respond to a warning, factors such as habituation are considered. While habituation does become an issue when managing each individual PUA, in this paper we focus primarily on the decision to enable (or not) a PUAs detection feature during one-time installation. Habitual choices related to each PUA acceptance decision will be considered in our future studies. In terms of warning message, there are conflicting results regarding the effectiveness of detailed explanations. Bravo-Lillo et al. [19] showed that a detailed explanation did not work well as an attractor in an experiment with other attractors (such as the use of pictorial symbols, colours, framing, etc.). Whereas Tan et al. [20] found that warning with a "purpose string" has a higher (but still not statistically significant) impact on a user over a warning without any purpose. Providing an example makes users pay more attention and consequently make more risk-aware choices [21].

Text structure may enhance readability too. Warning text in bullets or in an outline form is considered more readable than continuous text [22]. Use of simple language is also recommended. In terms of warning presentation, graphical improvements are often used to catch users' attention. For example, users are more likely to read salient, eye-catching warnings [23].

Wogalter et al. [24] note that warning visibility and readability can be enhanced by large or bold print that contrasts with the standard type and by adding signal colours, borders and special effects like flashing lights. User's comprehension can be increased also by adding pictorials to the warning [25]. Signal safety words, for example "Warning", "Danger", "Caution" or "Notice" also increase users' perceptions of a potentially risky situation [26].

Aspects such as colour, option order and pictorials have recently been used to *slightly influence*, or "nudge" users to use more secure options. For example, Turland et al. [27] designed a prototype for nudging users to select more secure wireless access points. Option order (the secure option comes first), option colour and the effect of pictorials were tested. There was a significant increase in choosing safer options depending on the colour of options, and their order, though a padlock pictorial had a negative impact (it tended to puzzle users).

Felt et al. [28] recently redesigned Google Chrome's SSL warning and tested the proposals with microsurveys and a field study. They used simple language, avoided technical jargon, targeted wording to a low reading level, and provided a short description. Despite using such (previously recommended) design features, they failed in designing a comprehensible warning, though they did increase adherence. The use of pictorial symbols and contrasting colours (yellow and gray) were main parts of the new design. In particular, the variant with a gray background and simple, jargon-free text had the best performance.

Other techniques such as *persuasion* [29] have also been used in computer security, such as for improving password choices, and anti-virus behaviour [30], [31]. There is also design example in which users are encouraged to update their first password choice by adding new characters [30].

III. Interface Design and Evaluation

A. Interface Design

For our studies, we used a baseline interface (see Fig. 1) that contained a short paragraph with a brief explanation of PUAs detection importance. "*ESET can detect potentially unwanted applications and ask for confirmation before they install. Potentially unwanted applications might not pose security risk but they can affect computer's performance, speed and reliability, or cause changes in behavior. They usually require user's consent before installation.*" People show their agreement by picking an option "Disable detection of potentially unwanted applications." or by choosing other option "Enable detection of potentially unwanted applications." To avoid potential legal challenges related to setting a default "enable detection" option, our interface designs used unchecked 'radio buttons' so that participants were required to choose one of the two options. There is one more user dialog that appears on the same screen that asks users to join "LiveGrid"[2]. Drawing on previous work on security warnings we tested 14 variations from the control interface that alter features such as the warning description (e.g., with hyperlinks, bullets) or presentation (e.g., with images, bolding, simple language, option order). We observed whether the application of these techniques to enabling PUAs detection had positive or negative

[2]ESET LiveGrid collects data submitted by ESET users worldwide and sends it to their malware research labs for analysis [32].

effects on user adherence, when compared to their use for other warning purposes.

Changes we made may seem subtle, but a conceptual redesign was out of question due to several limitations imposed by the company. However, we feel that even with our "subtle" changes we were able to incorporate some traditional warning design features.

Newly designed variants (marked A-N) are described in Appendix and are summarized in Table I along with their corresponding variant label. The interfaces of Variants A to K are shown in Figures 2 and 3 in the Appendix as they would have been viewed by our study participants (the LiveGrid portion of the screen is not shown in these images due to space constraints). Although the LiveGrid is strictly separate to our experiment, we wanted to investigate it's impact on our participants, hence Variants L and N do not include LiveGrid user dialog on the same screen as the PUAs detection user dialog.

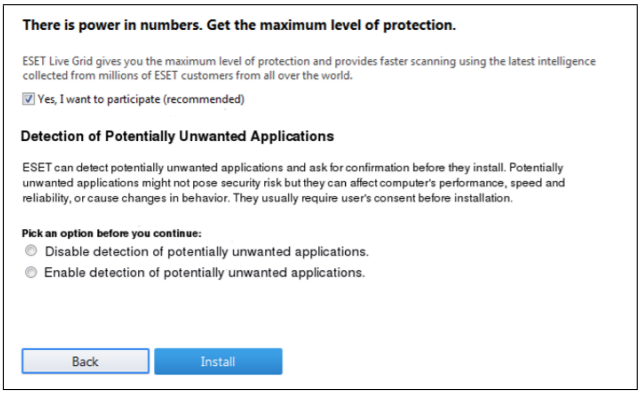


Fig. 1. The starting-point control variant.

1) Option order and language: In order to investigate the impact of changing options from the starting-point variant, we used three variants. In the first one, the order of the options was simply reversed (A in Fig. 2) so that "Enable detection of PUAs." came first and "Disable detection of PUAs." was second. In the second variant, we changed the wording so that "Disable detection of PUAs." became "Don't detect PUAs." and "Enable detection of PUAs." became simply "Detect PUAs" (B in Fig. 2). Since the formulation "Detect PUAs" is shorter and more straightforward than "Enable detection of PUAs", we had anticipated (based on previous research [28]) that variant B would increase the success rate. For the third variant, we reversed the order with the new wording to give the option of "Detect PUAs." first, and then "Don't detect PUAs." (C in Fig. 2). It is a combination of variants A and B.

2) Hyperlink: The role of explanation in warning design is still unclear. We wanted to investigate this issue so we designed three variants (D, E, F in Fig. 2) with a hyperlink connecting to the company website where a detailed PUAs explanation is provided. Variants D (Fig. 2) and E (Fig. 2) differ only in a text formulation of the hyperlink. Variant D (Fig. 2) states "What is a potentially unwanted application?", whereas variant E (Fig. 2) is "Why do we ask?" Variant F (Fig. 2) contains the hyperlink with the text "What is a potentially unwanted application?" but without the whole explanatory paragraph. The main aim of this variant was to investigate whether participants are influenced by moving the explanation from the warning body to an external web page or not.

3) Pictorials: Since related work considers pictures, pictorials or alert signs to be powerful attractors, we wanted to test this assumption also for the PUAs detection issue. We designed two variants (G, H in Fig. 3) where pictorials are added to the warning. Variant G (Fig. 3) uses the standard company warning sign, whereas variant H (Fig. 3) has the ANSI warning triangle.

4) Providing an example: People are more likely to adhere to a warning when they see a purpose. To provide a purpose to this warning, we decided to design a variant (I in Fig. 3) where an example is added at the end of the paragraph text. The sentence is: "**For example**, they may change your web browser's web page and search settings."

5) Signal word and signal red colour: As well as pictorial symbols, signal words and bright colours are also considered to be good attractors. To test this assumption, we designed the variant (J in Fig. 3) in which the paragraph text is introduced by the signal word "Notice" in red-coloured text. We expected that the combination of the colour and the signal word would catch users' attention and stress the importance of the user dialog.

6) Bulleted text: Since structured text is considered to be more readable than text in a single block, we designed variant K (Fig. 3), in which the text block is separated into bullet list. Also, the important words in the paragraph text – **"can affect your computer's:"** are presented in a bold type.

7) Complex combinations: Finally, we also included some more complex variants that combined or removed features of at least three existing variants. For these variants, we do not provide the corresponding images. In variant L, we investigated the influence of separating the PUAs detection and LiveGrid user dialog. We assumed that separating PUAs detection user dialog would enhance its visibility to participants. During the process of design, we identified a couple of variables that we wanted to test together to amplify their strength. The first combined variant, M, consists of a combination of text structure (K in Fig. 3), reformulated text in options (B in Fig. 2) and an explanatory hyperlink (D in Fig. 2). The other combined variant N has a similar structure to M, the only additional change being the removal of the previous (LiveGrid) user dialog.

8) Persuasion (not applied): For our purposes, persuasive techniques were viewed as too biased. For example, consider designs in which users are encouraged to update their first password choice by adding new characters [30] – we felt that it would be too much of a bias if a user were asked to reconsider their first choice of choosing to disable PUAs detection. Similarly, we considered an option whereby a user might be encouraged to follow the decision of others (e.g., by suggesting that "80% of other customers chose to enable PUAs

Var.	Description
Control	Text description with "Disable detection", then "Enable detection"(see Fig. 1).
A	*Option order reversed*: "Enable detection", then "Disable detection".
B	*Option text changed*: from "Don't detect" to "Detect".
C	*Option text changed & reversed*: Combines A and B.
D	*Added hyperlink*: "What is a potentially unwanted application?"
E	*Added hyperlink*: "Why do we ask?"
F	*Added hyperlink & no text description*: "What is a PUA?"
G	*Added warning image*: Warning image provided by the company.
H	*Added warning image*: ANSI warning triangle.
I	*Added example*: Added a practical example to end of description.
J	*Coloured warning text*: Added red *Notice* to start of text description.
K	*Bulleted text*: Text description bulleted, with partial bolding.
L	*LiveGrid user dialog*: LiveGrid user dialog removed from the screen.
M	*Hyperlink, bulleted text, & option text changed*: Combines B, D, K.
N	*Combination B, D, K, L.*

TABLE I
SUMMARY DESCRIPTION OF TESTED VARIANTS. SEE FIGS 2 AND 3 FOR SCREEN IMAGES OF VARIANTS A TO K.

detection"), though this too was felt to be overly biased (even though statistics would legitimately reflect previous customer behaviour).

B. Experiment

The experiment ran in June and July 2015. We cooperated with ESET and used their proprietary system to measure a success rate of each variant. Since PUAs can have harmful effects, we defined our *success rate* as the percentage of antivirus installations where participants enabled PUAs detection during antivirus installation. We treated each variant as a condition in between-subjects experiment, including our 14 new design variants and the control one. Participants were product beta users who installed a beta version of ESET antivirus software. We had more than 26,000 SW installations in total, i.e. 1,755 per variant on average. Other more precise measurements, for example one case per device, were not possible in our study since we used the existing data collection interfaces of our industrial partner.

Each case in our dataset represented one antivirus installation. Unfortunately, we can not detect a situation when one same participant installed antivirus on multiple different devices.

Concerning that we are examining a beta version of a home end-point antivirus solution, we do not expect that many people will behave this way. For example, administrators usually do not install antivirus beta version across the entire site they administer. It is also hard to detect situations where somebody would have installed multiple times the beta version of the ESET antivirus solution on the same device. Since we collect for each installation the device IP address, CPU, RAM and OS platform, we found out that cases with same values in this attributes make only a small percentage of the whole dataset.

Each participant was randomly assigned to a variant. See Table II for a summary of our results of performing pairwise comparisons of each variant to the starting-point control interface.

Var.	No. of installations	Succ. rate	p-value	Sign.
Control	1,759	74.5%		
A	1,796	89.8%	0.001	YES
B	1,734	72%	0.1	no
C	1,755	83.9%	0.001	YES
D	1,766	72.8%	0.25	no
E	1,749	72.6%	0.21	no
F	1,688	72.7%	0.23	no
G	1,730	73.7%	0.6	no
H	1,735	73.1%	0.35	no
I	1,818	73.3%	0.41	no
J	1,772	71.1%	0.037	no
K	1,809	71.6%	0.052	no
L	1,699	73%	0.82	no
M	1,780	72.8%	0.25	no
N	1,737	73.6%	0.57	no

TABLE II
SUMMARY OF RESULTS FOR ALL VARIANTS. FINAL COLUMN INDICATES WHETHER THE SUCCESS RATE WAS SIGNIFICANTLY DIFFERENT (STATISTICALLY) FROM THE CONTROL VARIANT.

IV. FINDINGS

The control variant had a success rate 74.5%. The average success rate of all tested variants in total is 74.7%. The highest success rate, 89.8%, was achieved with the variant A (Fig. 2) where the order was changed (in comparison with the starting-point variant) – the first option is "Enable detection of PUAs." and the second is "Disable detection of PUAs." The lowest success rate was for variant J (see Fig. 3). To correct for the alpha error inflation resulting from multiple χ^2 testing, we used the significance level α=0.05/16=0.003 to find statistically significant differences among variants.

A. Option order and language

Observing the ordering and language for the "Enable detection of PUAs/Disable detection of PUAs" options, we evaluated and compared variants A, B and C (see Fig. 2) with the control variant (see Fig. 1). The control variant had a success rate 74.5%, while the rate changed to 89.8% for variant A with order changed, 72% for variant B where a shorter, reformulated text was used with the same order of the

control variant, and 83.9% for variant C which combined both language and order changes from the control variant.

1) Option order: We used χ^2 test at the significance level α=0.003 to find statistically significant differences among variants that differ only in the order of options. The order of options really matters for PUAs detection, as with other types of warnings, e.g., [27]. We showed that users have a strong tendency to choose the first option, irrespective of whether it is for a positive or negative installation choice. We used the χ^2 test to compare the control variant with variant A (Fig. 2) where "Enable detection of PUAs" came first and "Disable detection of PUAs" (χ^2=143, p<0.001, df=1, r=0.2, OR=3.02) came second. A statistically significant increase in the success rate towards the variant with switched order was observed. Then we used the χ^2 test to compare the control variant with variant C (Fig. 2) (χ^2=48, p<0.001, df=1, r=0.116, OR=1.79), and the result was very similar. Our subjects were more likely to pick the first option they were offered.

When we merged the results from the two variants, where the first option is positive (variants A and C) into one, and by a similar process we made with two variants, where the first option was formulated negatively (B and control), we used the χ^2 test and we found out that the position on the first place is a very strong aspect to influence the user to pick the preferred option (χ^2=206, p<0.001, df=1, r=0.171, OR=0.412).

2) Option language: Considering the option text language, the formulation "Enable detection of PUAs" (A in Fig. 2) has a higher influence (χ^2=27, p<0.001, df=1, r=0.087, OR=0.592) on users than "Detect PUAs" (C in Fig. 2), though both offer the option for enabling detection first. This difference is statistically significant.

In contrast, the control variant compared with variant B is not statistically significant (χ^2=2.66, p=0.1, df=1, r=0.027, OR=0.882).

B. Warning image

According to previous research, a warning picture would catch the user's attention and would increase the success rate more than the control variant [25]. We compared the variant without the pictorial symbols (the control one) and with the pictorial (G in Fig. 3) – the company's warning sign (χ^2=0.27, p=0.6, df=1, r=0.009, OR=0.96), we observed that there is no significant difference in user behaviour. Similarly, when doing a comparison between the control variant and variant H (Fig. 3) with the ANSI warning triangle (χ^2=0.87, p=0.35, df=1, r=0.016, OR=0.93), no statistically significant difference is observed.

Finally, we compared both variants with the pictorial symbol (χ^2=0.17, p=0.68, df=1, r=0.007, OR=0.969). There is no significant difference in use of the standardized ANSI pictorial or the company's own warning sign.

C. Coloured warning text

We chose the red signal colour in combination with the warning word "Notice". Both the use of a red colour and warning text has previously shown to be a good attractor [24]. Thus, we had expected that this attractor would increase the success rate. However, when comparing the "Notice" variant (J in Fig. 3) with the control variant (χ^2=5.06, p=0.024, df=1, r=0.037, OR=0.843), we found that the variant with "Notice" had no significant effect on the success rate from the control variant. This variant has the lowest success rate 71.1% from all variants (the control has 74.5%). One possible explanation for this result may be that some users misinterpreted the red colour as a warning to not add the PUAs detection feature, and thus clicked on the first option ("Disable detection of potentially unwanted applications'). This possibility also supports previous work on SSL warnings. Bravo-Lillo et al. improved SSL warnings adherence by stressing important parts by adding contrast color [19]. Despite the fact that this variant did not have best performance, still was better than the control one. Felt et al. [28] used signal color in warning design and significantly improved adherence of SSL warning. But both used "safe option" as the first option, whereas the safe option in our case was the second.

V. Other findings

A. Hyperlink

1) Text in a hyperlink: We were curious whether participants would be interested in more information and would be more likely to enable the PUAs detection in the variant that contains a hyperlink to the explanatory webpage. We also tested two variants of a descriptive hyperlink text. Current research considers explanation to be a bad attractor; on the other hand, users are more likely to behave securely if they see a purpose to this behaviour. We tested two possible formulations of this link. The company's question mark pictorial symbol is appended to both sentences. The first is "Why do we ask?" (E in Fig. 2) and the second is "What is a potentially unwanted application?" (D in Fig. 2). We observed that there is absolutely no difference in user behaviour when formulations differ. (χ^2=0.01, p=0.92, df=1, r=0.001, OR=1.00). Unfortunately, our industry partner couldn't provide us information whether users clicked on the hyperlink.

2) Hyperlink and no description: We expected that the version with the explanatory paragraph text (the control one) would increase the success rate more than the version without the explanatory paragraph text, but with a hyperlink only (F). The χ^2 test proved that there is no statistically significant difference between the variant with the explanatory paragraph text (the control variant) and the variant without explanatory text, only with the hyperlink following to the company's web page with detailed explanation (χ^2=1.41, p=0.23, df=1, r=0.02, OR=0.912).

B. Providing an example

We expected that the variant with the PUA example explicitly mentioned (I) in the text would increase the success rate over the control variant, because participants would see the purpose of PUAs detection clearly. Despite our expectations, providing the example in a bold type did not significantly

improve the success rate (χ^2=0.67, p=0.41, df=1, r=0.013, OR=0.939).

C. Text structure

We decided to structure the paragraph with the explanatory text into bullet points to enhance its readability and text comprehension. Since structured text is more readable by participants, we expected also an improvement in the success rate over the control variant. The very unexpected result was that the variant with the structured text (K in Fig. 3) has the second lowest success rate 71.6% and we observed no significant difference in comparison with the control variant with an unstructured text (χ^2=3.7, p=0.052, df=1, r=0.032, OR=0.863).

D. Complex combinations

We expected that the variant without the previous LiveGrid user dialog (L in Fig. 3) would be more effective, as it would catch the user's attention better and increase the success rate. Comparing the control variant with the corresponding variant without the previous LiveGrid question (χ^2=0.05, p=0.82, df=1, r=0.003, OR=0.928), we observed no difference in user behaviour.

We expected that the variant with a combination of several principles would increase the user success rate more than variants with only one aspect used. Comparing the control variant with the "combined variant" (M in Fig. 3) that contained structured text, the hyperlink and a shorter text in options (χ^2=1.355, p=0.25, df=1, r=0.019, OR=0.915), no significant change in user behaviour was observed.

The combination of four aspects (N in Fig. 3) (a structured text, a hyperlink, a shorter option text and previous user dialog removal) also did not lead to significant improvements (χ^2=0.32, p=0.57, df=1, r=0.009, OR=0.957) in comparison with the control variant.

VI. Conclusions

We conducted our user experiment in the unexplored area of the acceptability of potentially unwanted applications (PUAs). PUAs are notoriously difficult to manage, e.g., legal challenges can preclude default options that could otherwise be set for PUAs detection or removal. Our large-scale experiment was completed with 26,000 SW installations. It was conducted in cooperation with antivirus product beta version users of the IT security software provider ESET. Drawing on previous security warning literature, we tested the impact of 15 warning screen variations for their ability to encourage participants to enable PUAs detection during the process of antivirus installation.

Starting with the control variant, we determined that 74.5% of participants wanted to enable PUAs detection. Further, from our 15 variants, we obtained an even larger percentage by presenting a positive option first (for enabling the PUAs detection), resulting in a statistically significant increase to 89.8% adherence (an increase of 15.3 percentage points). This best variant also has the highest effect size (odds ratio) 3.02. Further research will be needed to evaluate user trust level towards security products and his behaviour during its installation.

The remaining variants, covering effects such as warning images, bolding, red-coloured "Notice" and simplified warning text were surprising for not providing any increase in the number of participants who enabled PUAs detection. Odds ratios in this cases were around 0.9. In fact, the use of a signal word *Notice* in a contrasting red colour resulted in the lowest success rate 71.1%. While the results about the order of options may not seem that surprising, the variability of success between all options, some of which we would have also expected an increase, e.g., option J (coloured warning text) is very surprising, especially given the previous positive effects of these warning techniques, e.g., for SSL warning adherence.

The main conclusion from our results is that the order of available options is crucial. The design change with the greatest impact in a limited design space is to simply put the "safe option" in the first place.

Our study focuses only on the behavior of beta users. It could be enhanced by collecting statistics about clicking on hyperlinks in variants D, E and F and also by more precise distinction between multiple installations under single user credentials in our dataset. This was not possible in the current study as we used the existing data collection interfaces of our industry partner.

In future work, there are a number of areas for potential improvement and further advancement. We plan to perform a similar evaluation on a more diverse set of participants (e.g., not only beta users, but also real product users), and also to collect further data, including qualitative feedback from participants. We also plan to investigate more on antivirus users demography and security and privacy attitudes.

Acknowledgment

The authors acknowledge the support of the Masaryk University (MUNI/M/1052/2013). Thanks also to the reviewers for their excellent feedback, and to our shepherd (Paul Gerber) for his assistance in greatly improving the presentation of our results.

References

[1] J. C. Sipior, B. T. Ward, and G. R. Roselli, "The ethical and legal concerns of spyware," *Information Systems Management*, vol. 22, no. 2, pp. 39–49, 2005.

[2] K. Thomas, E. Bursztein, C. Grier, G. Ho, N. Jagpal, A. Kapravelos, D. Mccoy, A. Nappa, V. Paxson, P. Pearce, N. Provos, and M. Abu Rajab, "Ad injection at scale: Assessing deceptive advertisement modifications," in *Security and Privacy (SP), 2015 IEEE Symposium on*, May 2015, pp. 151–167.

[3] J. Malcho, "Is there a lawyer in the lab?" in *Proceedings of the 19th Virus Bulletin International Conference*, 2009.

[4] A. Butcher, J. Garms, K. Azad, M. Seinfeld, P. Bryan, S. Reasor, and A. Loh, "Identifying and removing potentially unwanted software," Mar. 23 2010, uS Patent 7,685,149. [Online]. Available: https://www.google.com/patents/US7685149

[5] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, 2011, pp. 3–14.

[6] E. Gandotra, D. Bansal, and S. Sofat, "Malware analysis and classification: A survey," *Journal of Information Security*, vol. 2014, 2014.

[7] M. Wagner, F. Fischer, R. Luh, A. Haberson, A. Rind, D. A. Keim, W. Aigner, R. Borgo, F. Ganovelli, and I. Viola, "A survey of visualization systems for malware analysis," in *Eurographics Conference on Visualization (EuroVis) State of The Art Reports*. EuroGraphics, 2015, pp. 105–125.

[8] S. Furnell, D. Emm, and M. Papadaki, "The challenge of measuring cyber-dependent crimes," *Computer Fraud & Security*, vol. 2015, no. 10, pp. 5–12, 2015.

[9] "How Microsoft antimalware products identify malware: unwanted software and malicious software," https://www.microsoft.com/security/portal/mmpc/shared/objectivecriteria.aspx, accessed: 2016-06-17.

[10] "Avast: Enable detection of potentially unwanted programs (PUPs)," http://ccm.net/faq/15731-avast-enable-detection-of-potentially-unwanted-programs, accessed: 2016-06-17.

[11] "What are Potentially Unwanted Programs (PUP)," https://support.avg.com/SupportArticleView?l=en_US&urlName=What-is-Potentially-Unwanted-Program-PUP, accessed: 2016-06-17.

[12] "Potentially Unwanted Programs (PUPs)," http://www.mcafee.com/us/threat-center/resources/pups-configuration.aspx#VSE7, accessed: 2016-06-17.

[13] "Kaspersky Internet Security 2011," http://support.kaspersky.com/3914, accessed: 2016-06-17.

[14] D. Modic and R. Anderson, "Reading this may harm your computer: The psychology of malware warnings," *Computers in Human Behavior*, vol. 41, pp. 71–79, 2014.

[15] O. Kulyk, P. Gerber, M. E. Hanafi, B. Reinheimer, K. Renaud, and M. Volkamer, "Encouraging privacy-aware smartphone app installation: Finding out what the technically-adept do," 2016. [Online]. Available: http://eprints.gla.ac.uk/116161/

[16] K. E. Vaniea, E. Rader, and R. Wash, "Betrayed by updates: how negative experiences affect future security," in *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2014, pp. 2671–2674.

[17] V. C. Plaut and R. P. Bartlett III, "Blind consent? a social psychological investigation of non-readership of click-through agreements." *Law and human behavior*, vol. 36, no. 4, p. 293, 2012.

[18] "What is a potentially unwanted application or potentially unwanted content," http://support.eset.com/kb2629/, 2015, accessed: 2016-06-17.

[19] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, "Your Attention Please: Designing Security-decision UIs to Make Genuine Risks Harder to Ignore," in *Proceedings of the Ninth Symposium on Usable Privacy and Security*, ser. SOUPS '13. New York, NY, USA: ACM, 2013, pp. 6:1–6:12. [Online]. Available: http://doi.acm.org/10.1145/2501604.2501610

[20] J. Tan, K. Nguyen, M. Theodorides, H. Negrón-Arroyo, C. Thompson, S. Egelman, and D. Wagner, "The effect of developer-specified explanations for permission requests on smartphone user behavior," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '14. New York, NY, USA: ACM, 2014, pp. 91–100. [Online]. Available: http://doi.acm.org/10.1145/2556288.2557400

[21] M. Harbach, M. Hettig, S. Weber, and M. Smith, "Using personal examples to improve risk communication for security & privacy decisions," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2014, pp. 2647–2656.

[22] E. N. Wiebe, E. F. Shaver, and M. S. Wogalter, "People's beliefs about the internet: Surveying the positive and negative aspects," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 45, no. 15, pp. 1186–1190, 2001. [Online]. Available: http://pro.sagepub.com/content/45/15/1186.abstract

[23] J. A. Strawbridge, "The influence of position, highlighting, and imbedding on warning effectiveness," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 30, no. 7. SAGE Publications, 1986, pp. 716–720.

[24] M. S. Wogalter, V. C. Conzola, and T. L. Smith-Jackson, "Research-based guidelines for warning design and evaluation," *Applied ergonomics*, vol. 33, no. 3, pp. 219–230, May 2002.

[25] J. S. Wolff and M. S. Wogalter, "Comprehension of pictorial symbols: Effects of context and test method," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 40, no. 2, pp. 173–186, 1998.

[26] M. S. Wogalter, M. J. Kalsher, L. J. Frederick, and A. B. Magurno, "Hazard level perceptions of warning," *International Journal of Cognitive Ergonomics*, vol. 2, no. 1-2, pp. 123–143, 1998.

[27] 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*. ACM, 2015, pp. 193–201.

[28] A. P. Felt, A. Ainslie, R. W. Reeder, S. Consolvo, S. Thyagaraja, A. Bettes, H. Harris, and J. Grimes, "Improving ssl warnings: Comprehension and adherence," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 2015, pp. 2893–2902.

[29] R. Cialdini, *Influence: The Psychology of Persuasion*. HarperCollins, 2009.

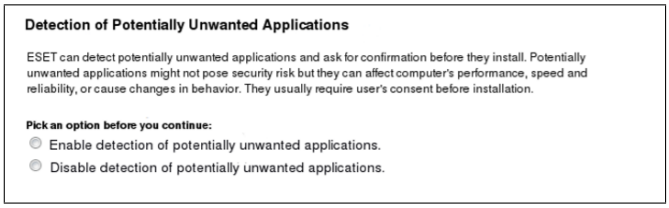
[30] L. Zhang-Kennedy, S. Chiasson, and R. Biddle, "The role of instructional design in persuasion: A comics approach for improving cyber security," *International Journal of Human-Computer Interaction*, no. just-accepted, 2016.

[31] A. Forget, S. Chiasson, P. C. van Oorschot, and R. Biddle, "Persuasion for stronger passwords: Motivation and pilot study," in *Persuasive Technology*. Springer, 2008, pp. 140–150.

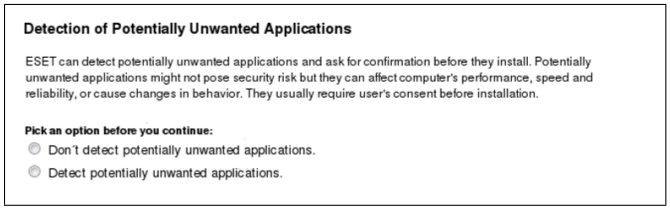
[32] "The ESET Advantage," http://www.eset.com/us/about/eset-advantage/, 2006, accessed: 2016-06-17.

APPENDIX
PROPOSED PUAS DETECTION USER DIALOGS

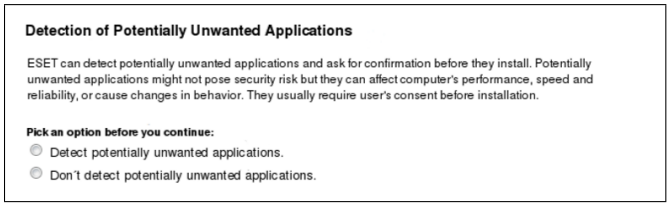
A



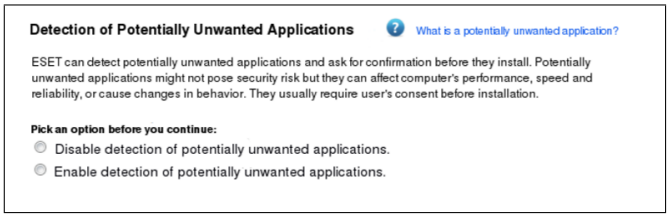
B



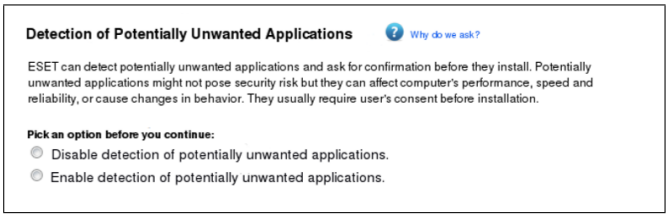
C



D



E



F

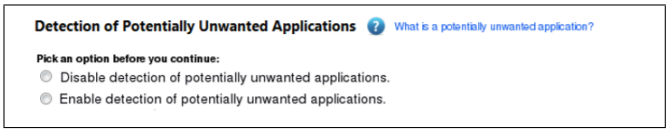
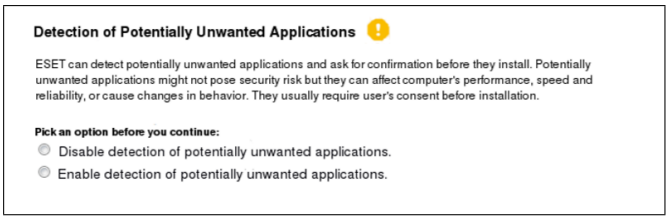
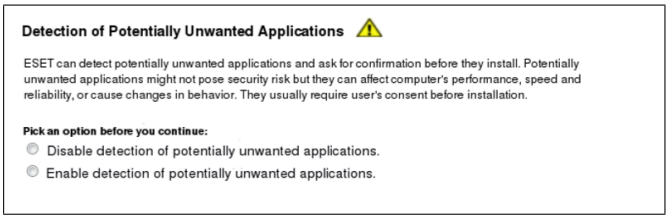


Fig. 2. Variants A-F.

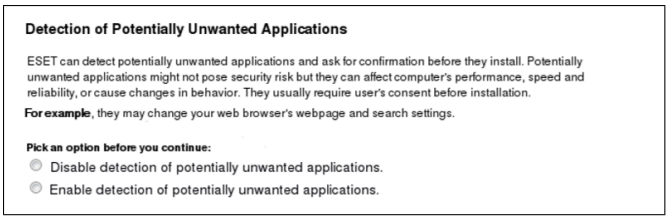
G



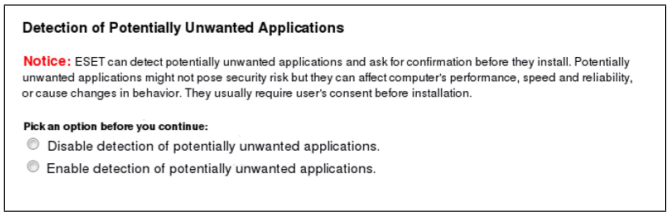
H



I



J



K

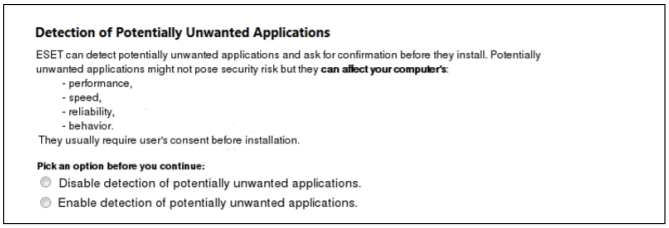


Fig. 3. Variants G-K.