Design and Field Evaluation of PassSec: Raising and Sustaining Web Surfer Risk Awareness

Melanie Volkamer[1,3], Karen Renaud[2], Gamze Canova[1], Benjamin Reinheimer[1], and Kristoffer Braun[1]

[1] Technische Universität Darmstadt, Darmstadt, Germany
name.surname@secuso.org
[2] University of Glasgow, Glasgow, U.K.
karen.renaud@glasgow.ac.uk
[3] Karlstad University, Karlstad, Sweden

Abstract. This paper presents PassSec, a Firefox Add-on that raises user awareness about safe and unsafe password entry while they surf the web. PassSec comprises a two-stage approach: highlighting as the web page loads, then bringing up a just-in-time helpful dialogue when the user demonstrates an intention to enter a password on an unsafe web page. PassSec was developed using a human-centred design approach. We performed a field study with 31 participants that showed that PassSec significantly reduces the number of logins on websites where password entry is unsafe.

1 Introduction

Web surfers can be at risk: (1) if the website itself is masquerading as the genuine entity; (2) the web page does not secure communications with the server by using `HTTPS`. In this paper, we focus on the latter as 10% of the top 100 sites in the study country currently fail to do this (including the 8^{th}, 9^{th} and 11^{th} most popular sites, including three major email providers). Insecure transmission has two consequences: communications being sniffed or the page itself being manipulated by third parties. Web browsers could refuse to load insecure pages but this relies on their being able to judge situations with 100% reliability, an unrealistic expectation. Failing this, users need to be wary, to protect themselves when pages are insecure.

Popular web browsers currently do a poor job of supporting users in this respect. *Firstly*, the main security indicator (`HTTP` or `HTTPS` with a padlock) is usually placed in the address bar where it is easily missed [2, 12, 15, 34, 23]. *Secondly*, web browsers usually reassure rather than signal problems, with indicators appearing only when communications *are* secured (padlock and/or highlighted in green). This is counter-intuitive since people's attention is generally deliberately drawn to risk; they are not only told to relax in similar contexts.

To support users more effectively we developed a Firefox Add-On called PassSec (see Fig. 1) to raise awareness in two stages: (1) highlight the password field either in red with an icon to *draw attention*, or in green with a lock icon to

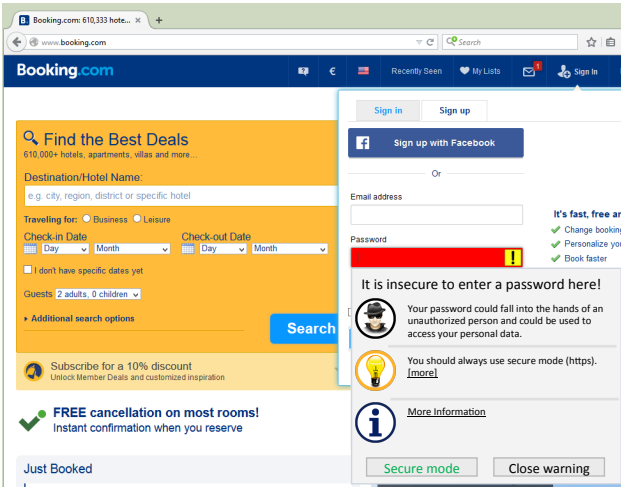

Fig. 1. Screenshot of PassSec: highlighted password field and helpful dialogue as `HTTPS` is not in place and the password field is focused.

reassure, as the web page loads; (2) bring up a helpful dialogue when the user is about to enter a password insecurely. The add-on was developed iteratively using a human-centred approach. We performed a field study with 31 participants and found that PassSec significantly reduced the number of logins on unsafe web pages.

2 Development Process

We derived a list of guidelines from the literature to inform effective implementation of PassSec's security indicators [6, 11, 13, 21, 29, 31, 32]. PassSec's *raison dêtre* is to raise awareness [17, 27], to make security visible, thereby helping people to understand risk. Guidelines apply either to the indicator mechanism as a whole, or are specific to the delivered message. The *overall* guidelines for warning indicators are that they should meet the following requirements:

Be noticeable. According to the C-HIP model [29] and the human-in-the-loop security framework [11], it is important to grab the user's attention and then maintain it [2, 12, 15, 34, 5].

Draw attention & reassure. The currently deployed `HTTPS` indicator and address bar padlock icon only reassure. One cannot expect users to interpret the lack of reassurance as something to be concerned about. Both must be provided.

Do not overstate. This risks habituation if people get used to dismissing advice because it appears gratuitously. For example [19] report on warning systems in hospitals and explain that when warnings appear too often or falsely they lead to confusion and irritation. Breznitz [7] explain that repeated alarms dull reactions so it is vital for indicators to signal genuine problems. This admonition is confirmed by [26].

Respect user autonomy. The final decision rests with the user, not with the software. Wichman [28] points out that autonomy is a universal psychological human need, which is related to well-being. Humans always strive to meet their needs, so not respecting this is bound to be less than helpful.

Minimise annoyance. Any advice that intrudes too often can be counterproductive. Politis *et al.* [20] tested speech warnings for drivers in terms of urgency, annoyance and effectiveness and argue for the importance of minimising annoyance in delivering warnings. Wogalter [30] also caution against causing annoyance since it interferes with the user's ability to interpret the communication.

The *message-specific* guidelines for security indicators are that they should:

Be explicit. Wolf *et al.* [33] recommend using simple and explicit language in communications. Wogalter *et al.* [31, 32] say interventions should identify the problem, explain the consequences and offer directives for how to avoid the problem. It is important for people to understand why wariness is recommended, maximising personal relevance [22].

Offer alternatives. Users do not like to abandon their intended action [16] so offering them an alternative (where possible) is preferable to advising abandonment.

Be understandable. Many active warnings fail in this respect [12] so we need to maximise understandability deliberately by using a human-centred design approach.

Be succinct & minimise effort. Too much text is likely to be daunting and become ineffective [3]. Humans are "cognitive misers" [14] meaning that they prefer to use intuition than to engage in effortful thinking. Moreover, we can not rely on people clicking on explanatory links such as "More Information" [2] so we should ensure that the most important information is displayed upfront.

These guidelines are not orthogonal. For example, understandability can help to raise awareness and offering alternatives minimises annoyance. On the other hand, a respect for autonomy can be taken too far: it could be used to justify removing interventions altogether, but that would not align with the 'raise awareness' guideline. In effect, for each design decision we had to rank the guidelines and use the most relevant one to guide our decision. This list helped us to make optimal design decisions, acknowledging the trade-offs that were sometimes unavoidable.

2.1 Design Decisions

When to Intervene? We identified relevant contexts for raising awareness. For each, we evaluated whether the password would be at risk while entering or sending (Table 1). We deliberately do not warn about certificate issues since these are only relevant when the website itself is fake, as is the case of websites masquerading as the genuine entities. Web browsers routinely warn about certificate issues and there is no point replicating this.

Table 1. Risk in different contexts and how it is addressed.

Context	At Risk		Current Browsers	With PassSec
	Entry	Send		
`HTTP` e.g. `http://edition.cnn.com`	Yes	Yes	– –	Draw Attention
`HTTPS` with unencrypted main page e.g. `http://www.booking.com`	Yes	No	– –	Draw Attention
`HTTPS` e.g. `https://www.amazon.com`	No	No	Reassures: lock icon	Reassures
`HTTPS` with mixed passive content [1] e.g. `https://www.answers.com`	No	No	Draw Attention: icon	Reassures
`HTTPS` with mixed active content [1] e.g. `https://www.answers.com`	No	No	Blocks active content, shield icon	Reassures
`HTTPS` with certificate issues	Maybe	Maybe	Active warning	Reassures

Redirect to HTTPS. It is technically possible to forward users to the secure web page automatically[4], if available, but automatic redirecting might be unnecessary if users do not plan to enter their password (*not overstate*). The other option is to advise them to switch. We decided on the second approach to let users decide, because it allows users to retain control: not treating them like children (*autonomy*). It also allows users to learn about securing communications and sustain awareness of insecure websites. Finally, it allows users to make the decision to use the unsecured web page, which they might do because they know that it is safe, despite appearances to the contrary (e.g. an internal company website or due to a trash account being used for this web page) (*autonomy*). We contemplated whether PassSec should provide an explanation or an easy-to-use button to authorise redirection. While the first option might be preferable with respect to raising awareness, we were concerned that it constituted too much effort for the user (*minimising effort*). We thus provide a button.

Keep History. The next decision is related to whether to ask users whether to switch to the `HTTPS` website every time an insecure web page is visited, or only once per specific page. Both have advantages (better awareness when asked each time) and disadvantages (likely to annoy). We incorporated a historical function to store details of those web pages where the user decided to switch to the secure option. Any time a user visits a web page that appears in the history, PassSec automatically redirects them to the secure web page (*minimising effort & annoyance*).

Intervention Strategy. PassSec deploys a two-stage approach to maximise effectiveness. The *first* stage is a specific passive security indicator that appears as soon as the web page is loaded to immediately draw attention to a problem. To achieve this, password fields are highlighted either to raise awareness or to provide reassurance (*raise awareness & reassure*). The *second* a helpful dialogue

[4] One could e.g. use the HTTPS-Everywhere Firefox Add-On `https://www.eff.org/https-everywhere` (last access: June 23, 2015)

appears next to the password field as soon as users start entering their password (just-in-time). Noticeability and effectiveness were evaluated in the field study.

2.2 Security Indicator Design

In [10], we showed that the combination of a red background and a yellow icon attracts attention effectively in an unsafe context (cf. Fig. 2). To reassure, we gave the input field a green border and a padlock icon (cf. Fig. 2). This proposal was developed through several iterations incorporating feedback from potential users. We started off with a green check mark but that confused people as they were accustomed to seeing it when they entered their data correctly. We settled on a padlock icon since it was perceived to be security-related. A green border was used instead of utilising a green background that was perceived to be too intrusive. The obvious concern with colour coding is that colour-blind users will be disadvantaged. It is true that the red background will not attract colour-blind users' attention as reliably, but the icon, being yellow, will serve to attract their attention. By using two independent indicators we make it less likely that colour-blind users will miss the signal.

Fig. 2. Highlighting of password fields to draw attention (left) if `HTTPS` is not in place; and to reassure (right) if `HTTPS` is in place.

2.3 Security Dialogue Design

The structure of the dialogues is based on Wogalter *et al.* [31, 32] who recommend that such dialogues should consist of four core components: (1) Signal word to attract attention, (2) Identification of problem, (3) Explanation of consequences, and (4) Directives to avoid problem. While this structure is in line with the guidelines, we adapted it slightly. First, we do not utilise one signal word to attract attention (1). Here, we share the opinion of Bauer *et al.* [4] that a signal word is not necessary but that a corresponding icon should suffice to draw attention. As an icon is already used in the highlighted field, we decided not to add another in the dialogue. Second, we provide additional information about the problem and the consequences for those who want to learn more (*understandability* and *raise awareness*). We ensure, however, that the most important information is available without any extra effort being expended. We decided to formulate the identified problem (2) as headline.

Icons. Based on feedback on first mockups of our dialogues, we realised we had to incorporate meaningful icons. Wolf *et al.* [33] advise the use of icons to reduce the amount of text (*minimise effort*). Thus, instead of using headlines for the different elements of our dialogues we use corresponding icons. The icons were chosen from other areas to maximise ease of association with the type of

information being provided (*understandable*). We used a light bulb to denote recommendations and the well-known "i" icon with blue background for information. After some iterations with potential users, we settled on a spy icon to depict the potential consequences.

Options. Users receiving dialogues have two options. One is to dismiss the dialogue and the other is to detour to the safe route, which is only possible if `HTTPS` is available. We facilitated the latter (secure) course of action by providing a button with green font based on findings about the efficacy of colour in this respect [10]. We allowed them to add exceptions when `HTTPS` was not available.

Background colour. We considered two background colours: neutral (grey) or yellow. The first is less *annoying* while the second is more likely to be *noticed*. We decided to go with the grey background since the dialogue already comes with the password field highlighted in red. The design of a PassSec dialogue is shown in Fig. 3.

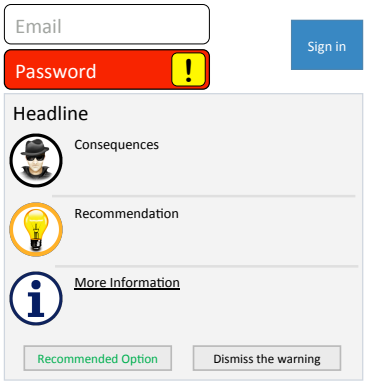

Fig. 3. Design proposal for dialogues

2.4 Dialogue Content

We conducted a feasibility study in order to test the viability of different terms for different aspects as well as different phrases for different parts of the intervention to maximise understandability and effectiveness. We studied in surveys:

Term for 'Eve': The following terms were studied to find a common usage term for what we understand by 'Eve': Unauthorised people, criminals, hackers, attackers, and con men. The most promising common-usage term for 'Eve' turned out to be '*unauthorised person*'.

Headline. The following headlines were evaluated: 'You are not protected here', 'Your password is endangered here', 'The connection is not encrypted' as potential titles of the dialogue. 'Your password is endangered here' was promising, but it turned out that some people thought that 'endangered' was the wrong term. Therefore, we rephrased this proposal to '*It is insecure to enter a password*'.

Consequences. A number of alternative phrases were mooted to find a common usage phrase that is concrete, understandable and effective in depicting Eve's actual action: access, capture, reveal, publish, forward, distribute personal data *as well as* use, have access to, abuse the account/data at your account. To describe her malicious actions in the consequence 'access your personal data' was the preferred option. Furthermore, during the discussion we realised the importance of mentioning the password again to explain how access is granted. The final consequence reads: '*Your password could fall into the hands of unauthorised persons and could be used to access your personal data*'.

Recommendation. The recommendation depends on whether `HTTPS` is available, or not. The dialogue text recommends switching to `HTTPS` whenever possible. This is the only recommended option (see Fig. 3) and the consequence is that the web page will, in future, always be opened using `HTTPS`. Note, we decided to use the term '*Secure mode*' instead of using the term `HTTPS` to avoid technical terms and maximise *understandability*. The actual text is: "*You should always use secure mode (https). Click on the 'secure mode' button and you will be redirected to secure mode automatically in the future.*"

If `HTTPS` *is not* available, the risk can be reduced by not re-using the password entered on this web page. Consequently, the text reads: "*This website does not offer a secure option (https). If you decide to log in anyway, you should at least use a different password for other websites.*" We are aware of the fact that this lacks substance, but being more explicit and prescriptive would result in a long paragraph and might lead to users not reading it at all (*minimise effort* and *annoyance*).

Options. The options provided in the dialogue depend on whether `HTTPS` is available, or not. The recommended option for our context is to open the web page via `HTTPS` whenever available, that is, the secure option. If `HTTPS` is not available, there are two options. The first is for the user to add an exception. This ensures that the decision is recorded and PassSec does not annoy the user by asking him or her to re-affirm every time they access the page. The other option is for the user to dismiss the dialogue by clicking on 'Close'. The risk of the first option is that an HTTPS option might be available in the future and the exception would prevent PassSec from checking for the availability of HTTPS. On the other hand, if the exception is not added this will lead to a dialogue appearing every time, which is bound to lead to annoyance.

Amount of visible text. To balance *succinctness* and *understandability*, we show the headline, the entire consequence, and the first part of the recommendation (when `HTTPS` is available) as well as the entire recommendation (when `HTTPS` is not available); with a link to more information. We ensure that the most important information is always visible and does not require any additional action by the user as clicking on a link such as "More Information".

2.5 Firefox Add-On

The described concepts were implemented as a Firefox Add-On called *PassSec*. The dialogues are depicted in Figures 4 and 5. PassSec acts after the browser

has judged the web page (what the browser blocks, stays blocked). In summary, PassSec satisfies the guidelines identified in Section 2 as depicted in Table 2.

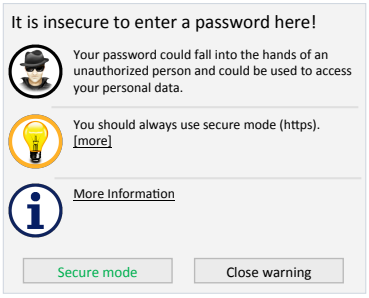

Fig. 4. A PassSec screenshot for when `HTTPS` is available. The default version is shown.

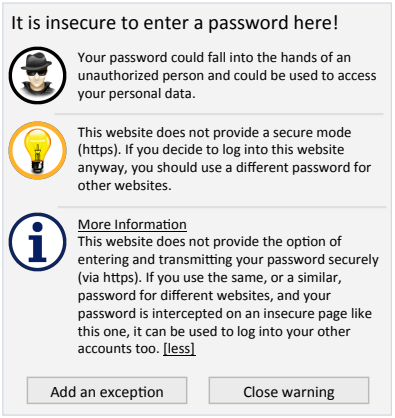

Fig. 5. A PassSec screenshot for when `HTTPS` is not available. The expanded version is shown.

Table 2. Mapping guidelines to PassSec Add-On design.

GUIDELINE	HOW ACHIEVED
noticeability	locate next to password field
draw attention & reassure	highlight field and add icon
not overstate	redirect not enforced
respects user autonomy	user decides whether to redirect or not
minimise annoyance	appear only when password field focused
explicit	dialogue design
offer alternatives	'Secure mode'
understandability	feasibility testing
be succinct	'[more]' links
minimise effort	remember whitelist decisions

3 Field Evaluation

Testing security-related behaviour in a laboratory setting leads to unrealistic and overly positive results. We thus carried out a field test to evaluate PassSec's noticeability, understandability and the succinctness of the dialogue text. Acceptability was also considered in terms of the System Usability Scale[5] (SUS)

[5] `http://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html` (last access: June 23, 2015)

and feedback questions as this would be a necessary pre-condition for PassSec's potential success in the future. One cannot test security-related behaviour reliably in a laboratory setting since you get unrealistic and overly positive results.

3.1 Study Design

Participants were told that the study was part of our research into Internet-related warnings but we did not specify the types of risky situations we were interested in. The field study comprised three phases. Participants used a deactivated Add-On to record baseline performance. After three to four weeks, participants installed a logging PassSec. A link to a web page detailing the functionality of PassSec, including information about the logging, was provided. Two weeks later participants uninstalled PassSec and filled out an online survey. The online survey elicited demographics, posed SUS usability-related questions [8] and questions relating to PassSec acceptability and the choices they made during their usage of PassSec.

3.2 Study Prototype

The Pre-Study Add-On logged the following information together with timestamps whenever users focused on a password field: (1) Hash of the domain (sub and top level domain) of the visited website, (2) Whether this was done via `HTTPS`, (3) Whether users submitted their password via `HTTP` and (4) Whether `HTTPS` was available (if not used by default). The PassSec Add-On additionally logged whether and which of the buttons in the dialogue were pressed, whether participants clicked on the 'more information' link, whether they submitted their passwords via `HTTP` or `HTTPS`. The hashed domains were destroyed once they were tallied to support analysis to preserve the privacy of our participants.

3.3 Recruitment, Reimbursement, and Ethics

Flyers were distributed across town, emailed to mailing lists, posted on web pages and to social networks. Those we reached were asked to advertise the study to get more participants, using a snowball approach. We did not pay participants but they could win one of two iPad minis if they participated in all three phases. Guidelines on ethical issues regarding research involving humans are provided by an ethics commission at the host University. The relevant requirements for this research relating to respondent consent and data privacy were satisfied. Logged data, as well as survey data, was not linked to individuals and only used for the purposes of this research. Visited domain details were hashed. Participants could withdraw at any time and request that their stored logs be deleted.

4 Results

In total, 51 participants installed the Pre-Add-On and 37 installed the PassSec Add-On. The final online survey was completed by 31 participants (sixteen female and fifteen male), whose data informed our analysis. The average age was

31, ranging from 19 to 73 with a standard deviation of 10.64. Out of the 31 participants, 14 people had something to do with IT (e.g. postgraduate or undergraduate degree). The free-text responses were independently coded by two of the authors using an inductive coding approach. Both reviewed the answers and identified categories from participants' responses. These were discussed and iteratively developed.

4.1 Noticeability

There are two ways of testing noticeability. If one tests something in the lab you can use eye-tracking equipment to see if people look at the part of the screen where the dialogue appears, or you can ask people if they saw it. With a field evaluation you cannot do this, so you have to use an indirect measure to detect noticeability. In our case we tested whether people carried out fewer insecure actions with the PassSec dialogues appearing. If we see a reduction in insecure actions, one can assume that the dialogue must have been noticed, and affected behaviour. We studied the impact of PassSec on participants' behaviour. For the purposes of this discussion we will use the following terms: for access via `HTTP` we will use the term *insecure* and for access via `HTTPS` we will use the term *secure*. Table 3 presents participants (P), attempting (A) to login to websites on different domains (D) in phase-1 (Pre-Add-On) and phase-2 (PassSec). Fig. 6 provides an overview of participants' behaviour with PassSec (based on the logs and survey responses).

Table 3. Number of insecure login attempts with and without PassSec.

	HTTP Login Attempts	By Participants	At Domains
`HTTPS` Available	476	19	19
`HTTPS` Available (PassSec)	30	9	15
`HTTPS` Unavailable	105	7	9
`HTTPS` Unavailable (PassSec)	87	19	24

Insecure logins (`HTTPS` available:): In total there were 476 insecure login attempts executed by 19 participants on 19 different domains. With PassSec there were 30 insecure login attempts by nine participants on 15 different domains. Seven of these attempts happened after the participant had previously switched to 'secure mode' to log in. This might have happened if participants used PassSec on different devices. Seven of the nine participants subsequently switched to secure mode. One participant only logged in once insecurely (he/she did not return to the website thereafter). Another logged in five times on the same insecure website. For the evaluation, we considered for each participant (who – at least once – logged in insecurely) the difference between insecure login attempts *without* and *with* PassSec. We first used the Kolmogorov-Smirnov test

to determine whether these differences were normally distributed. This hypotheses had to be rejected ($p = 0.011$, $p < 0.001$). Therefore we applied a one-tailed Wilcoxon signed-rank test to determine statistical significance. These differences differ from zero in a highly significant manner ($p < 0.001$). Thus PassSec was successful.

Switch to `HTTPS`: 17 participants switched to secure mode a total of 43 times. Ten did so whenever the option was offered. In the online survey participants were asked why they did not switch to the 'Secure Mode' (if applicable). Five of the seven participants who failed to switch stated that they always switched to the 'secure mode' before they logged in and two stated that they switched to secure version of the website themselves.

Insecure logins (`HTTPS` unavailable:) There were 105 insecure login attempts on nine different domains without PassSec. Seven participants did this at least once. There were 87 login attempts on 24 domains with PassSec. Fifteen participants did this at least once.

Exceptions Added: Ten exceptions were added by five participants. Participants were asked to share their reasons for adding exceptions. One participant cited the irrelevance of the dialogue for the specific website. Another said that he/she was annoyed by the dialogue. Three said they had no alternative because they wanted to log into their account so abandonment was not an option. Some entries in the logfiles showed that dialogues were ignored whereas the expected log entry detailing the dialogue was missing. We tried to reproduce this exception and noticed that we had failed to anticipate the fact that some people allow the browser to store their passwords. In this case the browser populates the credentials automatically and the dialogue would not appear since it is triggered only when the password is focused.

Background colour: The survey contained a screenshot of the dialogue, as shown in Fig. 4 and one with the same content but with a yellow background. We asked participants to rate their appeal and ability to grab attention and asked which one they would recommend. In terms of appeal and recommendation, both performed equally. With respect to grabbing attention, the yellow one was much preferred. We tested the difference in grabbing attention with a two-tailed Wilcoxon signed-rank test and it reached significance with $p = 0.028$.

4.2 Understandability and Succinctness

Participants were asked whether the message texts were easy to understand. On a scale from 1 (not at all) to 5 (very understandable), the median of the answers was 4. For the boxplot see Fig. 7. Participants were also asked whether they were aware of the PassSec recommendation to consider changing their other passwords One was indeed aware of the message text but 23 were not and two were unsure. We also asked whether they changed their password based on the recommendation. Seven answered 'no' and 19 argued that there was no recommendation.

Confusion regarding the '*Close*' button was identified from the free text answers on feedback. Some participants seemed unsure of the consequences of click-

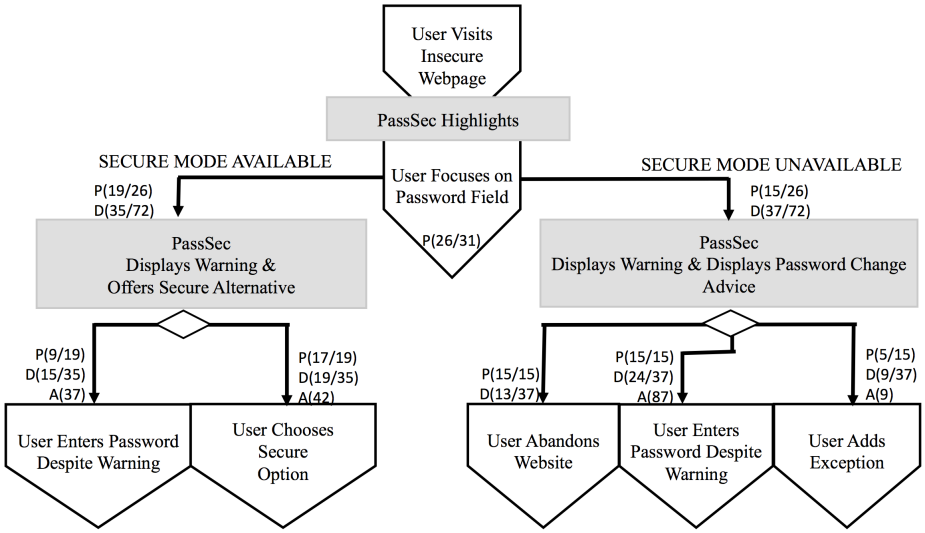

Fig. 6. Impact of PassSec on participants behaviour when faced with either of the messages (P=Participants, D=Domains, A=Attempts/ Number of Actions).

ing on this button. It was sometimes interpreted as "leave this web page". Participants were asked whether the dialogues had the right amount of text. On a scale from 1 (totally agree) to 5 (totally disagree), the median of the answers is 2. For the boxplot see Fig. 7. The survey also contained a screenshot of a shorter message text version (only headline and buttons and a link to get more information) and a long version (as shown in Fig. 4). Participants were asked whether the long version should be displayed immediately, or not. The longer version was preferred by the majority of participants (21 out of 31).

4.3 Acceptability

Satisfaction. PassSec received an SUS score of 81.91. A score over 80 implies a good-to-excellent result. Besides the SUS score, we asked the participants several questions about its usability. Responses and ratings are depicted in Fig. 7. For most of the questions the rating was *very good* (median). This includes helpfulness in detecting unsafe contexts, appreciating reassurance, not disturbing, not irritating, and not annoying.

Intention to use PassSec in future. 18 participants wanted to continue to use PassSec after the study; and ten were undecided. Three did not plan to use it in future (all male). Examples of positive comments were: '*easy to notice*', '*increased attention that passwords are also requested on* `HTTP` *websites*', '*feeling more secure*', '*does not disturb me but helpful*', and '*easy to switch to* `HTTPS`'. Examples of negative comments: '*too few technical details*' '*Firefox was only used to participate in the study*', '*design should be improved first*', '*other Add-Ons installed such as https-everywhere*', '*slows down browser*', and '*not enough*

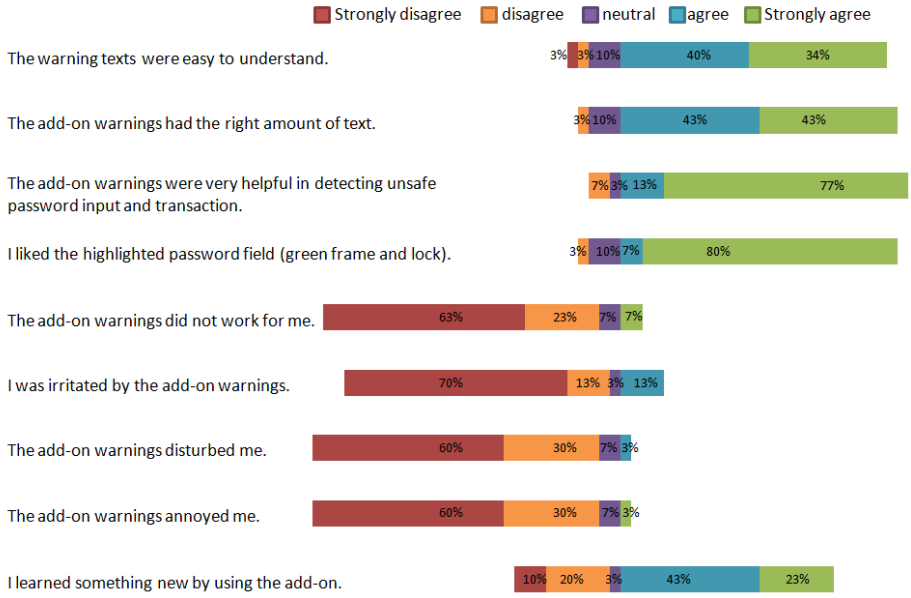

Fig. 7. Result for the survey questions related to amount and understandability of the provided text, as well as satisfaction related questions.

protection'. We categorised them as negative and positive and not according the three groups (wants to use it, not decided, does not want to use it again) because in all three groups we found both negative and positive arguments.

Nice to have features. In order to collect input regarding possible future functionality and modifications, we requested suggestions for improvement from the participants. They responded: '*cover more critical form fields; e.g. bank account details*', '*allow users to enable* `HTTPS` *everywhere*', '*provide more information about algorithms/criteria*' '*improve performance*', '*not easy enough to see whether* `HTTPS` *is available or not*', '*option to close does not function as expected*' (as the dialogue is displayed every time the password field is focused) and '*improve recommendation for insecure situation*'. Furthermore, we provided a list of possible *form fields* which could also trigger PassSec dialogues in future versions. Bank account number and credit card were selected 28 times, TANs 25 times, email addresses 16 times, postal addresses 15 times, and name 13 times.

5 Discussion

Noticeability: PassSec significantly reduced the number of insecure login attempts. Most participants who logged in insecurely either dismissed the dialogue or added an exception. The dialogues must have been noticed. It also became clear that the highlighting of the password field was insufficient indication since

participants with stored passwords logged in despite the password field being highlighted in red. Thus, in PassSec 2.0 we need to ensure messages are also displayed in this context, to improve noticeability. There are actually two options: (1) detect the auto-fill of the password field and then show the dialogue (not two-stage but still passive) or (2) detect the auto-fill of the password field and show the dialogue when user clicks the login button. In this case the login would not be executed when clicked. It would be enabled again once the dialogue was displayed (two-stage but active since it interferes with the user's activity and demands attention). Both require evaluation in a future study. The survey answers indicate that noticeability could be further improved by using a yellow background colour for the text which seems to improve noticeability without increasing annoyance or decreasing appeal.

Understandability: The overall understandability rating was good but we identified a number of areas for improvement. The semantics and consequences of the 'close' and the 'add exception' buttons were unclear. There was no explanation in the dialogue, an unfortunate omission. 'Close' may have confused participants because it reappeared every time the user focused the password field. This may also explain why one participant became annoyed by the dialogue. We propose renaming the 'close' button to 'Ok, got it' in PassSec 2.0, and adding a sentence: 'If you do not want to see this dialogue again, add an exception'. Moreover, we will ensure that the dialogue only appears once per page. Another issue was the recommendation to 'change' passwords on other websites. The phrase '*If you decide to log into this website anyway, you should use a different password your other websites*' was unclear. We propose to rephrase this to '*If you decide to log into this website anyway and you use the same password for other website accounts, you should change them immediately.*'

Succinctness: Users accepted the amount of text and most voted against showing less text. PassSec 2.0 will provide an option to switch to the short version. Participants complained that it was difficult to distinguish between websites that could be opened securely from websites which could not, at first glance. Initially the only difference was the green font versus the black font on the other button. To make the difference more obvious, PassSec 2.0 will use a green background for the secure mode button and a red one for the exception button.

Acceptability: PassSec performed very well with respect to usability. The free text answers revealed a number of positive comments revealing ease of use, minimal disturbance and low annoyance. Many will continue to use PassSec, others wanted their comments about usability addressed before they would consider adoption. The main areas for improvement were performance and the amount of information displayed. The performance issues were caused by the logging as well as by the way that PassSec was implemented: It initially loaded the `HTTP` page, then checked whether the user had previously elected to be redirected, and, if so, loaded the `HTTPS` page. If not, it checked for the domain on the exception list. The performance was particularly poor with slow Internet connections. This has been improved in PassSec 2.0 by optimising the checks and directly loading the `HTTPS` page if the website is in the secure mode list. We plan to extend the pro-

vided information and to provide a link to the website in the 'More information' part of the dialogue.

All participants recommended extending the mechanism to cover other kinds of data entry. PassSec 2.0 identifies banking data related fields as well as name, address, and email address fields. While most of these issues can, and will, be addressed, there is a trust issue that appears when trying to recruit users. People tend to mistrust Add-Ons in general, since they do not know whether additional information is collected. This issue can be addressed if PassSec's functionality is integrated into browsers.

Limitations: Participants used PassSec for different lengths of time due to recruitment difficulties and a fixed end date. Due to the fact that we conducted a field evaluation, we do not know whether we logged data only from the actual participant or whether he/she shared the device with others (which six stated they did, three on a daily basis). Participants were told that we were going to log their actions, and this might have influenced their behaviour, perhaps biasing them towards behaving more securely than usual.

6 Related Work

Researchers have come up with a variety of innovative mechanisms to make users aware of the dangers to their data while using the Internet. Based on the literature there seem to be three ways of approaching this problem: (1) Educating web surfers, (2) passive (non-blocking) security indicators, and (3) using active (blocking) warnings that interrupt the user's current workflow. A prominent *educational* approach is Anti-Phishing Phil by Sheng *et al.* [24]. Their game was designed to help users to differentiate between secure and fake URLs in a playful way. They were able to show that their approach was superior to existing teaching material. As other Phishing detection mechanisms cannot provide 100% protection, it is important not to discount the benefits of education; it is an essential first step in making users more aware of threats. To warn about insecure communications, technology can reliably check whether `HTTPS` is in place or not and then either reassure or warn, augmenting the educational approach. Some notable approaches in the field of *passive* approaches are LinkExtend[6] and research such as published by Shepherd *et al.* [25]. LinkExtend is a Firefox Add-On considering many different security indicators including whether `HTTPS` is in place or not. However, it displays the relevant information at the top of the web browser while other research has shown that indicators in the address bar are unlikely to be noticed [2, 12, 15, 34]. Their approach is unlikely to be effective.

Active warnings have been studied e.g. by Brustoloni and Villamarín-Salomón [9]. They evaluated their approach in a user study with 26 participants and this led to participants being more risk averse. The active approach is likely to annoy people in our case as they would get a warning even though they only want to surf on the corresponding page. Maurer *et al.* [18] use a mix of passive and active

[6] `https://addons.mozilla.org/de/firefox/addon/linkextend-safety-kidsafe-site/` (last access: June 23, 2015)

warnings. A warning dialogue is displayed whenever critical data type fields are focused and the corresponding website is not yet white listed. They call their approach "semi-blocking" as it does not actively interrupt the user's current workflow but requires deliberate action before submission is possible. Their main purpose is to make users aware that they are about to enter sensitive data and that they should make sure it is transmitted securely and the website is not a Phishing website. Users can elect to add the web page to a whitelist in order to reduce warnings, or just dismiss the warning. The system aimed to reduce warnings and only display them when really required in order to reduce both annoyance and minimise habituation effects. Their solution was comprehensibly tested, both in the lab and in the field. In the lab, they tested whether people could detect Phishing web sites with the help of their warning system. In the seven day field study they focused on how their approach was perceived by real users. As opposed to our work, their field study did not quantitatively evaluate whether the tool reduced insecure behaviours in the wild but rather on whether the number of warnings decreased over time.

In summary, education is definitely worthwhile in our context but augmenting it with warnings is likely to improve matters even further. Existing approaches proposing passive and passive indicators have their limitations. The approach that most closely mirrors ours is the semi-blocking approach written about by Maurer *et al.* [18]. Their main focus was on masquerading websites. They have yet to test its effectiveness in reducing insecure behaviours in the field.

7 Conclusion and Future Work

We developed a Firefox Add-On, called PassSec, to effectively support users in detecting insecure communications. By ensuring that we satisfied a number of guidelines identified from the literature, and by applying a human-centered design approach (both for the content and design of its dialogue) we were able to achieve our aim. PassSec significantly reduced the number of insecure logins. We have identified ways to improve PassSec 2.0. We delivered dialogues using a Firefox Add-On, but it would be preferable for this functionality to be embedded within current browsers. The results for the first phase of the field study indicated that passwords are at risk in many situations and it became clear that such an Add-On could lead to more secure behaviour. While PassSec is not the first Add-On to attempt to support users in this respect, it is, to the best of our knowledge the first that has been evaluated in a field study which is as close to ecological validity as is possible in a controlled field study. For future work, we plan to distribute PassSec 2.0. Since PassSec significantly reduced insecure logins we hope that PassSec 2.0 will improve the situation even further.

References

1. Mixed Content Blocking Enabled in Firefox 23! `https://blog.mozilla.org/tanvi/` (2013), (last access: June 23, 2015]

2. Akhawe, D., Felt, A.P.: Alice in warningland: A large-scale field study of browser security warning effectiveness. In: Usenix Security. pp. 257–272. Washington DC (14-16 August 2013)
3. Ayres, T.J., Gross, M.M., Wood, C.T., Horst, D.P., Beyer, R.R., Robinson, J.N.: What is a warning and when will it work? In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. vol. 33, pp. 426–430. SAGE Publications (1989)
4. Bauer, L., Bravo-Lillo, C., Cranor, L., Fragkaki, E.: Warning design guidelines. Tech. rep., Carnegie Mellon University (2013), CMU-CyLab-13-002
5. Bravo-Lillo, C., Cranor, L.F., Downs, J., Komanduri, S., Sleeper, M.: Improving computer security dialogs. In: Human-Computer Interaction–INTERACT 2011, pp. 18–35. Springer Berlin Heidelberg (2011)
6. Bravo-Lillo, C., Komanduri, S., Cranor, L.F., Reeder, R.W., Sleeper, M., Downs, J., Schechter, S.: 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. pp. 6:1–6:12. SOUPS '13, ACM (2013)
7. Breznitz, S.: Cry wolf: The psychology of false alarms. Psychology Press (2013)
8. Brooke, J.: SUS: A Retrospective. Journal of Usability Studies 8(2), 29–40 (2013)
9. Brustoloni, J.C., Villamarín-Salomón, R.: Improving security decisions with polymorphic and audited dialogs. In: Proceedings of the 3rd symposium on Usable privacy and security. pp. 76–85. ACM (2007)
10. Canova, G., Volkamer, M., Bergmann, C., Borza, R.: NoPhish: An Anti-Phishing Education App. In: Security and Trust Management, pp. 188–192. Springer, Wroclaw, Poland (10 September 2014)
11. Cranor, L.F.: A framework for reasoning about the human in the loop. In: Proceedings of the 1st Conference on Usability, Psychology, and Security. pp. 1:1–1:15. UPSEC'08, USENIX Association (2008)
12. Dhamija, R., Tygar, J.D., Hearst, M.: Why phishing works. In: Proceedings of the SIGCHI conference on Human Factors in computing systems. pp. 581–590. ACM (2006)
13. Egelman, S., Cranor, L.F., Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 1065–1074. ACM (2008)
14. Kahneman, D.: Thinking, Fast and Slow. Farrar, Strauss, Giroux (2011)
15. Lin, E., Greenberg, S., Trotter, E., Ma, D., Aycock, J.: Does domain highlighting help people identify phishing sites? In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. pp. 2075–2084. CHI '11, ACM (2011)
16. Locke, E.A.: Relationship of success and expectation to affect on goal-seeking tasks. Journal of Personality and Social Psychology 7(2), 125–134 (1967)
17. Maurer, M.E.: Bringing effective security warnings to mobile browsing. In: 2nd International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (in Conjunction with Pervasive 2010), Helsinki, Finland (2010)
18. Maurer, M.E., De Luca, A., Kempe, S.: Using data type based security alert dialogs to raise online security awareness. In: Proceedings of the Seventh Symposium on Usable Privacy and Security. p. 2. ACM (2011)
19. Meredith, C., Edworthy, J.: Are there too many alarms in the intensive care unit? An overview of the problems. Journal of Advanced Nursing 21(1), 15–20 (1995)
20. Politis, I., Brewster, S., Pollick, F.: Speech tactons improve speech warnings for drivers. In: Proceedings of the 6th International Conference on Automotive User Interfaces and Interactive Vehicular Applications. pp. 4:1–4:8. AutomotiveUI

'14, ACM, New York, NY, USA (2014), http://doi.acm.org/10.1145/2667317.2667318
21. Potgieter, M., Marais, C., Gerber, M.: Fostering content relevant information security awareness through browser extensions. In: Information Assurance and Security Education and Training, pp. 58–67. Springer, Auckland, New Zealand (July 8-10 2013)
22. Ruiter, R.A., Abraham, C., Kok, G.: Scary warnings and rational precautions: A review of the psychology of fear appeals. Psychology and Health 16(6), 613–630 (2001)
23. Schechter, S.E., Dhamija, R., Ozment, A., Fischer, I.: The emperor's new security indicators. In: Security and Privacy, 2007. SP'07. IEEE Symposium on. pp. 51–65. IEEE (2007)
24. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J., Nunge, E.: Anti-phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In: Proceedings of the 3rd symposium on Usable privacy and security. pp. 88–99. ACM (2007)
25. Shepherd, L.A., Archibald, J., Ferguson, R.I.: Reducing risky security behaviours: Utilising affective feedback to educate users. In: International Conference on Cyber Forensics. Glasgow, UK (23-24 June 2014)
26. Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., Cranor, L.F.: Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In: USENIX Security Symposium. pp. 399–416 (2009)
27. West, R.: The psychology of security. Communications of the ACM 51(4), 34–40 (2008)
28. Wichmann, S.S.: Self-determination theory: The importance of autonomy to well-being across cultures. The Journal of Humanistic Counseling 50(1), 16–26 (2011)
29. Wogalter, M.S.: Communication-Human Information Processing (C-HIP) Model. In: Wogalter, M.S. (ed.) Handbook of Warnings. Lawrence Erlbaum Associates (2006)
30. Wogalter, M.S., Conzola, V.C.: Using technology to facilitate the design and delivery of warnings. International Journal of Systems Science 33(6), 461–466 (2002)
31. Wogalter, M.S., Desaulniers, D.R., Brelsford, J.W.: Consumer products: How are the hazards perceived? In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. vol. 31, pp. 615–619. SAGE Publications (1987)
32. Wogalter, M.S., Godfrey, S.S., Fontenelle, G.A., Desaulniers, D.R., Rothstein, P.R., Laughery, K.R.: Effectiveness of warnings. Human Factors: The Journal of the Human Factors and Ergonomics Society 29(5), 599–612 (1987)
33. Wolf, M.S., Davis, T.C., Bass, P.F., Curtis, L.M., Lindquist, L.A., Webb, J.A., Bocchini, M.V., Bailey, S.C., Parker, R.M.: Improving prescription drug warnings to promote patient comprehension. Archives of internal medicine 170(1), 50–56 (2010)
34. Wu, M., Miller, R.C., Garfinkel, S.L.: Do security toolbars actually prevent phishing attacks? In: Proceedings of the SIGCHI conference on Human Factors in computing systems. pp. 601–610. ACM, Montreal, Canada (April 22 - 27 2006)