Capturing Attention for Warnings about Insecure Password Fields – Systematic Development of a Passive Security Intervention

Nina Kolb, Steffen Bartsch, Melanie Volkamer, Joachim Vogt
TU Darmstadt, Germany
nina.kolb@stud.tu-darmstadt.de, steffen.bartsch@cased.de,
melanie.volkamer@cased.de, vogt@psychologie.tu-darmstadt.de

Abstract. Eavesdropping on passwords sent over insecure connections still poses a significant threat to Web users. Current measures to warn about insecure connections in browsers are often overlooked or ignored. In this paper, we systematically design more effective security interventions to indicate insecure connections in combination with password requests. We focus on catching the attention of the user with the proposed security interventions. We comparatively evaluate the three developed interventions using eye-tracking and report how effective these options are in the context of three different website designs. We find that one of the options – red background of the password field – captures significantly more attention than the others, but is less linked to the underlying problem than the yellow warning triangle option. Thus, we recommend a combination of the two options.

Keywords: security warnings, security interventions, morphological approach, attention.

1 Introduction

Business and leisure activities are to a large extent conducted via Internet – including critical tasks, such as online banking. Since most web sites still rely on passwords for authentication, the problem of eavesdropping on passwords over insecure connections, particularly on insecure networks such as airport Wi-Fi, is an imminent threat. Although current browsers offer several possibilities to check whether a connection is secured, many users neglect to do so before logging in with their password [8]. Hence, the user should be further supported in these decisions. So far, several attempts have been made in research to develop browser plug-ins that facilitate secure surfing behavior (e.g., [2, 7]). However, most of these attempts are of a rather exploratory nature and lack a theoretical foundation.

To close this gap, we chose a systematic procedure based on the morphological approach by Zwicky [16] and arrived at three promising security interventions, which follow psychological findings about attention. We comparatively evaluate the interventions using eye-tracking and report how the options play out with respect to three different websites as context. We find that one of the options captures significantly

more attention than the others, but is linked to the underlying problem to a lesser degree than another, alerting the user in a rather unspecific way. Thus, we recommend a combination of two of the options.

1.1 Security Interventions in the Web Context

Concerning warnings in Web browsers, researchers have particularly focused on the intervention strategies, that is, when and in which form to intervene. For example, Whalen and Inkpen showed how symbols as a passive form of interventions are seen, but not interacted with by the users [12]. Wu et al. argued that the right timing is important for interventions [15]. Similarly, Maurer et al. proposed to display warnings only if the user starts entering sensitive data and right where the data is entered [5].
Generally, active warnings have been shown to be more effective than passive indicators [8]. However, overly frequent active warnings (e.g. from false positives) lead to habituation effects [1]. Thus, there are many situations in which passive indicators seem to be more promising and should therefore be further investigated.
In general, even though new interventions have been proposed and evaluated, their development typically lacked a systematic approach. Therefore, the interventions proposed in this paper are systematically developed and evaluated.

1.2 Psychological Background

We based the development of the security interventions on psychological fundamentals of attention. Wolfe and Horowitz found that certain properties of objects can lead attention already in an early stage of perception [14]. This is particularly the case for color [9, 11, 14]. The color red has been found to have the strongest effect [13]. In addition, so-called "warning colors" – such as the combination of yellow and black – can create a similar level of attention [13]. There is good reason for the use of red and yellow-black for warning and traffic signs.

Biologically, humans perceive red stronger when it occurs in the center of the visual field, while yellow has a stronger effect in the periphery. The reason is the difference in the distribution of receptors for the red and yellow color over the visual field [11]. Moreover, colors also have a meaning: A study on the meaning of colors showed that 100% of the participants associated red with "Stop!" and 90% with "danger", while 81% of participants linked yellow to "Attention!" [11].

Another object property that guides attention is movement [14]. Movement is particularly powerful in the periphery of the visual field since it activates a biological alarm reflex (flank attack). This fundamental reflex makes it difficult for humans to ignore movements in the periphery [10] so that movement should be used sparingly in the Web context. Nielsen showed in an eye-tracking study that people "scan" websites in an "F pattern" – particular attention is thus paid to the upper and left sides of a website [6].

The amount of attention attracted by a stimulus also depends on the environment: The larger the difference among the surrounding distractors, that is, objects close to the stimulus, the smaller is the effect of that stimulus. Conversely, the stimulus is

more pronounced in case of a larger difference to the distractors [3]. Accordingly, the goal is to employ a stimulus that is as different to its surrounding as possible. Since the stimulus does not fit with the surrounding, it creates surprise that leads to attention [4].

2 Development of the Security Interventions

Based on the psychological fundamentals laid out in the previous section, we developed security interventions to better protect Web users from eavesdropping on their passwords. The situation is the following: The user visits a web page which contains a password field. There is either no https in place or there is a problem with the https certificate. Since password fields are widespread on websites and often not used to actually login, we decided to develop passive, that is, non-interrupting, interventions. Since our focus at this stage of work lies on the capturing of attention, we developed visual and nonverbal interventions.

We chose a systematic procedure based on the morphological approach by Zwicky [16] – identifying all possible solutions for the different parts of the problem individually and combining them the most promising way – and arrived at the three interventions shown in Figure 1.

In the first intervention, the **password field is highlighted red**. Red creates the most attention as an individual color and is also associated with "Stop!" and "Danger". The intervention is located within the password field, since this should receive attention as part of the login procedure. Moreover, the location creates a semantic connection to the login procedure and, particularly, with entering the password.

The second intervention is a **yellow warning triangle**, containing a black exclamation mark, which should remind of the commonly-used warning sign and should symbolize "Attention!".

The third intervention is a **yellow warning bar**, located below the browser chrome. It shows the above-mentioned warning triangle and the word "Attention!". Text and symbol were added to the bar to provide context and additional information. We deliberately limited the text to a minimum to allow for a comparison between all three interventions. The warning bar is located on the left and upper side of the browsing window, since users look there most while scanning a website, according to Nielsen [6]. To create additional attention, the intervention is only shown 0.5 seconds after the page is displayed and moves into the window from the top left. Since this is a short one-time movement, the movement should not overly distract from the website contents.

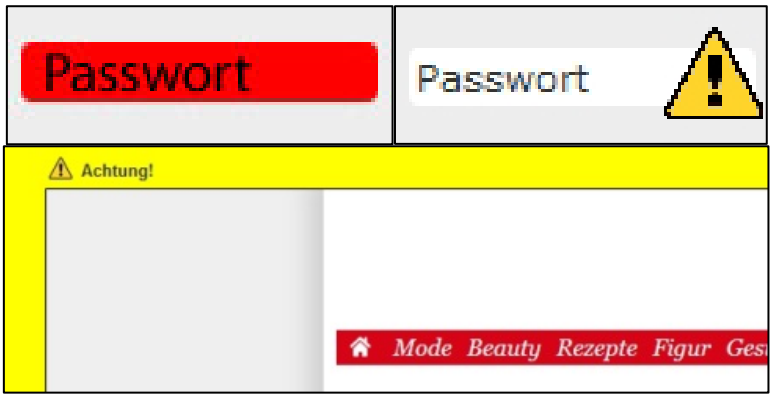

Fig. 1. Passive security interventions tested in our study (red password field, warning triangle, warning bar).

3 Hypotheses

We tested these interventions in a psychological experiment to determine which one attracts the most attention.

Based upon the psychological background given above, we developed the following hypotheses. Color as an object property works best to guide attention [14]. Since the color red has the strongest effect [13], we hypothesize:

H1: Intervention 1 (red password field) generally attracts most attention.

The effect of stimuli furthermore depends on the surrounding of the stimuli [3], so that:

H2: There is an interaction between the attention effect of the individual intervention and the website design. The amount of attention of the interventions thus depends on the website.

Furthermore, we studied for which of the tested interventions potential users understand its meaning best, even without an additional explanatory text.

4 Method

4.1 Participants

In total, 29 people (23 female, 6 male) took part in the study. For technical reasons, the eye-tracking data of only 28 participants could be used in the analysis. All participants are psychology students who took part for course credit. The mean age was 24.21 years (SD=5.76). The participants estimate their experience in using the Web browser applied in the study (Mozilla Firefox) as 4.86 on average (SD=1.21; scale from 1 to 7, with 1 for very low and 7 for very high experience).

4.2 Study Design

We used a 3x3 mixed within-and-between-subjects design, varying intervention type within and website design between subjects. Each participant interacted with one of three different forum websites designed either in a predominantly red (bfriends.brigitte.de), purist (forum.golem.de) or cluttered way (community.bravo.de). We carefully chose these design criteria for their possible influence on the attentional effect of the interventions. We conducted the study using Mozilla Firefox as this is one of the most common Web browsers. The study was conducted in Germany and therefore in German; the original questions were translated for this publication.

The experiment consisted of two parts. In the first part, participants completed tasks like posting a text or editing their profile (comparable tasks for the different websites), with each task requiring the participants to log in first on the corresponding page with provided credentials. On the login page, the intervention was presented. Each participant saw all three interventions, though in a random order. Due to this within-subjects variation, the consideration of an attentional baseline was not necessary. We used an eye-tracking system (FaceLAB 5.0) to check if the participants had looked at the intervention at all, and – if they had – how long they had focused it.

In the second part of the study, we conducted a semi-structured interview, asking the participants if they had noticed the interventions, how much they had attracted their attention plus several questions about the anticipated meaning of the interventions. To facilitate the interview, we showed the participants screenshots with the different interventions on the websites that they had interacted with in the first part (stimulus recall technique). We carefully referred to the interventions as "modifications" in the attempt to weaken the subjects' tendency to build hypotheses themselves about independent variables. The questions obtaining our dependent variables included:

- "On a scale from 1 to 7, how noticeable did you find this modification [show screenshot], with 1 for very little, 7 for very strong?"
- "What do you think does this modification [show screenshot] mean for you as a user?"
- "If you would be browsing the Web at home and you would notice this modification [show screenshot], would this influence your behavior? If yes, in which way?"
- "The modifications should warn you that the connection is unprotected and thus a third party could eavesdrop e.g. on your password. Would you link this modification [show screenshot] with this situation?"

5 Results

5.1 Eye-Tracking

To determine which intervention attracted the most attention, we measured the total amount of time (in milliseconds) the participants focused on the particular intervention.

In total. Results show that participants focused longest on the red highlighted password field; followed by the yellow warning triangle and the yellow warning bar (see Table 1). We conducted a repeated measures two-way analysis of variance (ANOVA) with the intervention type as within-subject factor and the website design as between-subjects factor. The analysis showed a significant difference regarding the time that participants focused the interventions, $F(2,50) = 11.41$, $p < .001$, partial $\eta^2=0.31$. In addition, our analysis shows an interaction between the attention effect of the intervention and the website design, $F(4,50) = 4.05$, $p < .05$, partial $\eta^2= 0.25$.

Table 1. Focus times by intervention.

	Time (in ms) for focus of intervention	
Intervention type	M	SD
Intervention 1 (red password field)	2855. 67	2497.76
Intervention 2 (yellow triangle)	1397.07	1013.94
Intervention 3 (yellow warning bar)	894.13	1325.27

Per website. We also conducted analyses per website design individually. A repeated measures one-way analysis of variance with the intervention type as within-subject factor did not show significant differences for the time of focus for the red design (bfriends). The same analyses for the purist (golem) and the cluttered (bravo) design did show significant and a trend to significant differences, respectively (cf. Table 2). For the latter two designs, participants focused longest on the red password field. Table 3 lists the focus times by website design. Overall, participants spent the most time focusing interventions in the cluttered design.

Table 2. Significance of intervention type as within-subject factor per website design.

	df	F	p	partial η^2
Red design (bfriends.brigitte.de)	2, 18	0.30	.785	0.03
Purist design (forum.golem.de)	1.250, 11.247	12.29	.003	0.58
Cluttered design (community.bravo.de)	1.191, 8.339	4.50	.061	0.39

Table 3. Focus times by intervention and website design.

	Time (in ms) for focus of intervention	
Intervention type	M	SD
Red design		
Intervention 1 (red password field)	676.80	1236.37
Intervention 2 (yellow triangle)	1033.60	902.08
Intervention 3 (yellow warning bar)	918.40	817.84
Purist design		
Intervention 1 (red password field)	3451.20	2121.85
Intervention 2 (yellow triangle)	1001.60	409.26
Intervention 3 (yellow warning bar)	648.00	996.10
Cluttered design		
Intervention 1 (red password field)	4375.11	2469.06
Intervention 2 (yellow triangle)	2156.00	1282.65
Intervention 3 (yellow warning bar)	992.00	2049.14

5.2 Interviews

Conspicuity. During the interviews, most of the participants rated the red-highlighted password field as the most conspicuous, followed by the yellow warning triangle. The yellow warning bar was rated the least conspicuous. Hence, the results gathered via eye-tracking are in line with the subjective statements. The results from the question are shown in Table 4, also differentiated by website design. The conspicuity of the interventions differs significantly, $F(2, 48) = 43.04$, $p < .001$, partial $\eta^2 = 0.64$. We could not find an interaction between the conspicuity and website design, $F(4, 48) = 2.00$, $p = .110$, partial $\eta^2 = 0.14$.

Table 4. Results from interview question on conspicuity.

	Conspicuity rating, scale 1 to 7	
Intervention type	M	SD
Total		
Intervention 1 (red password field)	5.95	1.04
Intervention 2 (yellow triangle)	4.26	1.65
Intervention 3 (yellow warning bar)	2.30	1.92
Red design		
Intervention 1 (red password field)	5.70	1.16
Intervention 2 (yellow triangle)	3.40	1.71
Intervention 3 (yellow warning bar)	1.88	1.73
Purist design		
Intervention 1 (red password field)	6.00	1.05
Intervention 2 (yellow triangle)	4.10	1.45
Intervention 3 (yellow warning bar)	3.10	2.13
Cluttered design		
Intervention 1 (red password field)	6.17	0.94
Intervention 2 (yellow triangle)	5.39	1.22
Intervention 3 (yellow warning bar)	1.78	1.72

Meaning. Asked about the anticipated meaning of the interventions, most of the participants (78%) thought the red-highlighted password field indicated an incorrect login, such as a wrong password. For the yellow warning triangle, 56% thought of an incorrect login. 22% of the participants thought they would need to pay more attention to the login and to be more careful with their password. The yellow warning bar was most frequently (21%) linked with the detection of malware on the currently visited website, 17% interpreted the symbol as an indication that the website is generally “insecure”.

Behavior at home. In case that the participant would be confronted with the red password field on their own PC at home, 45% would still login and 21% would be irritated and hesitate before entering their password. For the warning triangle, 41% report that they would still login, 21% would look for the reason of the intervention and 14% would be more attentive when entering the password. For the warning bar, 21% would still login, another 21% would close the page and not log in, and 17% would look for the reason of the intervention.

Fit for the situation. The participants consider the yellow warning triangle as the best fit for the situation of an insecure connection (17% say fitting, 59% not fitting, others are unsure). The warning bar is more often considered fitting than the red password field (14% vs. 7%), but the warning bar is also more often considered not fitting (76% vs. 72%). All participants mentioned that they would like a short explanatory note as an addition for the interventions.

6 Discussion

6.1 Summary of Findings

Overall, the participants spent most eye fixation time on the red password field. We thus can assume that this is the intervention that receives most attention – at least visually.

However, the time participants look at the intervention also depends on the website design. In case of a cluttered design, the interventions are generally looked at longer. Both, for a cluttered and for a purist design, the red password field is the intervention which attracted the longest visual attention. There is no significant difference between the interventions for the red design. The red password field thus appears to be best suited to capture the attention of the user independent of the design: Even for the predominantly red design, it is not significantly shorter looked at than the other interventions, and it is also the most successful attractor of fixation time in the other two designs.

In line with this, we found in the interviews that the red password field is considered the most conspicuous, followed by the yellow triangle. The subjective data thus reflect the eye-tracking data. However, we did not find an interaction with the website design for the subjective rating.

H1 (the red password field generally receives the highest attention) is thus both supported by the eye-tracking and interview data. The assumed interaction between the attention effect of the intervention and the website design (H2) could only be shown for the eye-tracking data, not for the subjective data. One possible explanation could be the fact that the number of participants who interacted with one website is rather small.

None of the interventions appears to be self-explaining. Among the presented solutions all failing to be intuitive, the yellow triangle was considered the best fit to the

situation. For this intervention, most participants would try to find the reason for its appearance.

6.2 Implications for the Intervention Design

A possible solution for the final design of the intervention could consist of a combination of the red-highlighted password field to gain attention and the yellow warning triangle for the meaning. Furthermore, we propose to add a short explanatory text, since all participants mentioned that this would be of great use. The question remains, how many words are efficient for this purpose and where to place them.

As follow-up work, we will develop and evaluate the placement of the explanatory texts. Moreover, we will measure whether or not symbol and text actually keep users from logging in over unprotected connections instead of only asking whether or not they would login at home.

6.3 Limitations

An important limitation of this work is that its scope refrains to the effect of the interventions on visual and subjective attention. Since this study is only an intermediate step in the development of the final intervention, we did not investigate whether the interventions actually prevent users from logging in.

Another potential limitation lies in the selection of three intervention types and three website designs. We employed a systematic approach for the design of the interventions and the selection of websites to cover the relevant influence factors. We consider this a good start, however, we cannot exclude that better interventions and other relevant influence factors for the website design exist.

A third limitation is that our study took place in a controlled laboratory environment. Also, the participants used others' login data. Thus, the conclusions which were drawn with respect to everyday handling of one's own login data need further studies. For the time remaining, the password field as elaborated in this study is the best solution.

6.4 Conclusion

This paper contributes to the ongoing effort of developing effective and appropriate interventions for Web browsing. While interventions are typically developed intuitively and then evaluated afterwards in this context, we chose a systematic approach. We developed interventions based on psychological fundamentals regarding human attention, systematically selected the interventions with the morphological approach, and took the final decision based on study results. In this way, we were able to propose a well-founded solution for warning against sending passwords over unprotected connections.

Acknowledgments. The work presented in this paper is supported by funds of the Federal Ministry of Food and Agriculture (BMEL) based on a decision of the Parliament of the Federal Republic of Germany via the Federal Office for Agriculture and Food (BLE) under the innovation support programme.

References

1. Amer, T.S., Maris, J.B.: Signal Words and Signal Icons in Application Control and Information Technology Exception Messages – Hazard Matching and Habituation Effects. Nothern Arizona University (2006)
2. Chou, N. et al.: Client-Side Defense Against Web-Based Identity Theft. Presented at the NDSS 2004 (2004)
3. Duncan, J., Humphreys, G.W.: Visual search and stimulus similarity. Psychological Review. 96, 3, 433–458 (1989)
4. Horstmann, G.: Die Unterbrechungsfunktion der Überraschung: ein neues experimentelles Paradigma und eine Überprüfung der Automatizitätshypothese. Uni Bielefeld (2001)
5. Maurer, M.-E. et al.: Using data type based security alert dialogs to raise online security awareness. Presented at the SOUPS '11 , New York, NY, USA (2011)
6. Nielsen, J.: F-Shaped Pattern For Reading Web Content, http://www.nngroup.com/articles/f-shaped-pattern-reading-web-content, (2006)
7. Ross, B. et al.: Stronger password authentication using browser extensions. Presented at the , Berkeley, CA, USA (2005)
8. Schechter, S.E. et al.: The Emperor's New Security Indicators. Presented at the IEEE Symposium on Security and Privacy Mai (2007)
9. Treisman, A., Gormican, S.: Feature analysis in early vision: Evidence from search asymmetries. Psychological Review. 95, 1, 15–48 (1988)
10. Ungerleider, G.L., Mishkin, L.: Two visual cortical systems. MIT Press, Cambridge, Mass. (1982)
11. Wandmacher, J.: Software-Ergonomie. De Gruyter, Berlin, New York (1993)
12. Whalen, T., Inkpen, K.M.: Gathering evidence: use of visual security cues in web browsers. Presented at the , School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada (2005)
13. Wirth, T.: Missing Links. Über gutes Webdesign. Hanser Verlag, München (2002)
14. Wolfe, J.M., Horowitz, T.S.: What attributes guide the deployment of visual attention and how do they do it? Nat Rev Neurosci. 5, 6, 495–501 (2004)
15. Wu, M. et al.: Do security toolbars actually prevent phishing attacks? Presented at the CHI '06 , New York, NY, USA (2006)
16. Zwicky, F.: Discovery, Invention, Research Through the Morphological Approach. The Macmillian Company, Toronto (1969)