Proceedings of the Eighth International Symposium on
Human Aspects of Information Security & Assurance (HAISA 2014)

Users can't be Fooled – The Role of Existing vs. Fictitious Third Party Web Assurance Seals on Websites

N. Bär and J. Krems

Chemnitz University of Technology, Chemnitz, Germany
e-mail: {nina.baer; josef.krems}@psychologie.tu-chemnitz.de

Abstract

For secure online behaviour, individual attitudes like the users' trust in websites are just as important as technical security means. One possibility to accomplish trust in the web environment is the use of third party web assurance seals. Still, the effects of such security indicators are discussed controversially. Previous studies indicated that online users are vulnerable to visual deception; therefore might misleadingly place trust in insecure websites. In order to check the effectiveness of existing web assurance seals in comparison to fictitious graphical elements that could fool users, an online study (N = 131) was conducted. The participants had to estimate the trustworthiness of four different German websites which were equipped with either typical existing, fictitious or no web assurance seals. Results show that the existing seals provoked the highest level of users' trust while the fictitious seals did not yield any significant trust-promoting effects compared to the control group. However, qualitative feedback indicated that the users' knowledge about web assurance seals is rather unspecific which makes them vulnerable to manipulation.

Keywords

Web assurance seals, users' trust, user behaviour, website

1. Introduction

Security in online interactions is of major concern for users, website providers and governmental institutions. Implicitly, online users demand high security standards when they conduct any types of online business to prevent, e.g. unauthorized access to their personal information by unknown third parties, deception by phishing websites or similar. The possibility that negative consequences will arise from insecure online actions is both closely connected to the actual security provided on the website and the subjective evaluation of the situation by the user. Objective properties of the interface - like browser warnings, https identification or web assurance seals and certificates awarded by independent third parties - influence the subjective evaluation of the security on the website and can help to trigger the establishment of users' trust. Trust is an essential aspect for users' engagement in online actions (e.g. Bélanger and Carter, 2008; Beldad *et al.* 2010). It is defined as an "attitude that an agent will help to achieve an individual's goal in situations characterized by uncertainty and vulnerability." (Lee and See, 2004, p. 51). Depending on the perceptions during the interaction, a user might form the conviction that the interaction partner will support the user in achieving his or her goals. Mainly in transactional websites, when users are asked to disclose their

personal information or transfer money or any tangible objects, security ought to be of crucial importance for the achievement of the users' goals. To improve perceptions of security on transactional websites and therefore perceptions of trustworthiness, objective website elements like third party web assurance seals are used. Such security indicators should assure quality, serve as an independent recommendation and enhance trust. However, the effectiveness of such indicators is discussed controversially, as online users are vulnerable to visual deception (Dhamija *et al.* 2006). Therefore, users might even base their trust on spurious security indicators on websites. Considering the economic aspects of third party certification, the question if existing web assurance seals create higher users' trust than fictitious graphical web elements, is of particular relevance for website providers. Especially for small online shops or start ups it is crucial to know if expensive web assurance seals are effective in establishing a good reputation within their users. The aim of this study was to check if existing web assurance seals are effective when evaluating the trustworthiness of a website or if users can be fooled by any fictitious graphical elements. In an online study on different types of transactional websites, the effectiveness of existing web assurance seals in evoking users' trust was compared to fictitious web assurance seals as well as to a control condition without any security indicators.

2. Related work

Users are the key factor when it comes to online security. Especially young people – digital natives - feel secure and educated about e-safety risks (Atkinson *et al.* 2009). They even feel very confident in online security-related decisions although their subjective impression does not always correspond to the actual correctness of the decision. For instance, when differentiating phishing websites from real websites, participants were confident in their decisions, whether they were correct or incorrect (Dhamija *et al.* 2006). So, at a surface level users' confidence in online security issues appears to be high by all means. Looking closely at the users' awareness of online security threats and their resulting security practice, problems occur not only with novice users but also with those who consider themselves as experienced (Furnell *et al.* 2007). Even sophisticated users are not immune to attacks like visual deception (Dhamija *et al.* 2006). For everyday use and applicable for a large scale of online users, third party web assurance seals are one way of assuring certain standards in service and security. They can contribute to estimations of the trustworthiness of a website (e.g. Kim and Benbasat, 2010). However, only few users seem to check if the presented seals are genuine (Kimery and McCord, 2002). Recognition rates of third party web assurance seals are rather low, and even fictitious seals were recognized as familiar (Moores, 2005). Assuming that fictitious web assurance seals were mixed up with existing seals and the tendency of users to rely on the graphical image instead of the underlying certificate of approval, one could expect that fictitious seals might also induce users' trust. This would limit the meaning of third party web assurance seals as a way of generating trust in a website.

3. Method

The study was conducted in Germany as an online survey. Between three groups of participants the type of third party web assurance seals was manipulated. Participants were randomly assigned to one of the groups, facing four screenshots of different transactional website that either contained existing web assurance seals ('Existing Seals'), fictitious web assurance seals ('Fictitious Seals') or no trust inducing element that implied recommendations of third parties ('Control group'). In both experimental groups the manipulated third party web assurance seals were placed in the same spot where they had been in the original version of the website. In the control group the spot was not left blank but was covered by other elements of the website to keep a consistent design.

Participants. Of 149 people starting the online survey, N = 131 completed it and were included in the analysis. The sample consisted of 34 men and 97 women. All but one were psychology or sensor systems students of Chemnitz University of Technology, aged from 18 to 45 years (M = 22.2, SD = 4.1). All of them were well grounded in Internet use. 41% of the participants reported to have had bad experiences in the Internet, which have mostly been related to delivery problems of purchased products (no delivery or defect products delivered) and overlooked fees for website use. The most frequently used information to assess the trustworthiness of websites was recommendations of friends (87%). Another large proportion of 73% stated to use experience reports. Information by media was an important source of information for 53% of the participants, while ratings of previous users were relevant for 39%. Third party web assurance seals were the least frequently used trust cue (19%). The sample largely knew about the idea of web assurance seals to be awarded by independent third parties. However, about 20% of the participants stated to know nothing or only little about such seals. An equal proportion was aware of the limited meaning of assurance seals. The participants had also difficulties in recognizing third party web assurance seals. 55% of the sample recognized the fictitious 'Fairtrade' seal as an existing one and only 9% knew about the (existing) 'EHI' seal. The groups did not differ in control variables like system trust, propensity to trust, Internet usage habits or bad Internet experiences.

Material. In the online survey the participants saw four screenshots of websites where transactions or the disclosure of private data were requested: an online pharmacy, an online shop for electronic products, a travel website and a dating agency. Each of the websites contained at least one in Germany well-established third party web assurance seal in the original version. In the experiment, the original versions of the websites were equipped with only one existing assurance seal: the seal of 'Trusted Shops' or the 'TÜV' seal. Two of the four websites were equipped with the same seal, i.e. the participants saw each of the seals twice. The fictitious seals were designed using official-looking graphics such as a stamp of product testing, to ensure a certain plausibility of use. Still, they resembled the existing seals in appearance, form and size (Figure 1).

Figure 1: Existing (left) and fictitious seals (right)

Procedure. A 15 minutes online survey was implemented. In the beginning, participants were advised that this study was on security indicators. They were instructed to explore the screenshots and imagine a scenario where they were interested in what the single websites offered. After the presentation of the screenshot questions were asked if they noticed a third party web assurance seal on the website and for their intention to start a transaction at the website they had just seen. Then perceived trustworthiness and trusting intentions as well as system trust and propensity to trust were assessed using modifications of the Items of McKnight *et al.* (2002). At the end of the experiment general items on the user's knowledge about third party web assurance seals and their online habits were administered before demographical data was collected.

4. Results

To check for possible differences between the control and experimental group we analyzed the mean scores for perceived trustworthiness (Figure 2) and trusting intentions of those participants, who corresponded to the instruction and correctly identified the presence/ absence of the third party web assurance seals (N = 64). A two-way analysis of variance (ANOVA) for mixed designs revealed a significant main effect of the type of web assurance seals in trust scores ($F(2,61) = 4.04$, $p = .022$, $\eta^2 = .12$) with a power of 91%. In post-hoc multiple comparisons the Bonferroni correction was used to reduce the chances of obtaining false-positive results when several statistical tests are being performed simultaneously on a single data set. A significant difference between the control group and the group that saw the existing third party web assurance seals was detected ($p = .032$). The ratings on perceived trustworthiness for the fictitious seals did not differ from both the other groups.

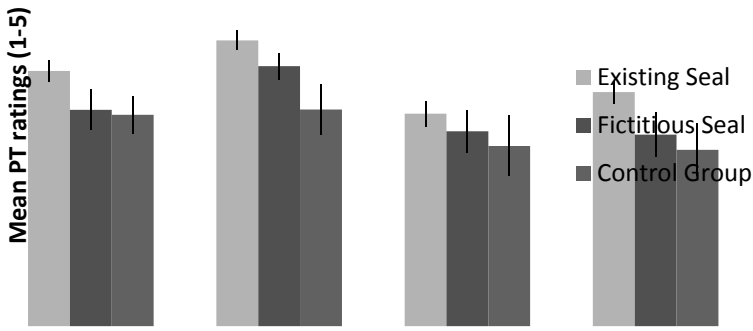

Figure 2: Mean scores in trust ratings (error bars indicate standard error)

Furthermore, a significant main effect of the type of website was found ($F(3,183) = 13.24$, $p < .001$, $\eta^2 = .18$, power = 1.0). All websites differed significantly in their scores on perceived trustworthiness apart from the dating website compared to the travel website (pairwise comparison, Bonferroni-corrected, all $p < .001$). The dating agency obtained the lowest ratings while the online shop for electronic products scored highest. The results for trusting intentions confirm the pattern found for perceived trustworthiness only for main effect for the website ($F(3,183) = 13.54$, $p < .001$, $\eta^2 = .18$). Except for the online pharmacy and the travel website all websites differed significantly from each other (pairwise comparisons, Bonferroni-corrected, all $p < .007$). There was no significant difference between the groups ($F(2, 61) = 2.86$, $p = .065$, $\eta^2 = .09$, power = .80). The participants' intention to engage in a transaction at the websites did not differ between the experimental groups ($F(2,61) = 2.95$, $p < .060$, $\eta^2 = .09$, power = .80) but for the websites ($F(3,183) = 32.64$, $p < .001$, $\eta^2 = .35$, power = 1.0). The online pharmacy did not differ from the travel website while the intentions to engage in a transaction for all other websites differed significantly from each other (pairwise comparison, Bonferroni-corrected, all $p < .001$). For none of the variables a significant interaction between the two factors could be detected.

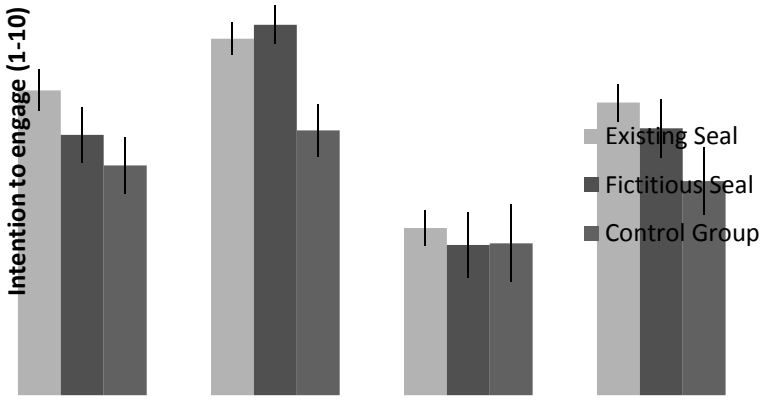

Figure 3: Mean scores in intention to engage in a transaction (error bars indicate standard error)

5. Discussion

The existing seals induced significantly higher scores of perceived trustworthiness than the websites in the control group without any seals of approval as security indicators. This supports the general positive effect of third party web assurance seals on perceived trustworthiness (e.g. Kim and Benbasat, 2010; Noteberg *et al.* 2003; Rifon *et al.* 2005). Fictitious seals did not yield any significant trust-promoting effects even when they were explicitly noticed as web assurance seals compared to the control group. The participants were instructed to pay attention to security-inducing website elements to make sure they did not overlook the manipulation. According to the Prominence-Interpretation Theory (Fogg, 2003) a website feature has firstly to be perceived to be interpreted and potentially influence appraisals of the website. Therefore only the data sets of participants who indicated to have noticed a third party web assurance seal were included in the analysis. This approach considerably reduced the sample size. Still, the calculated power was large enough to detect the effects in spite of the small sample size. For the existing seals the conscious perception did influence the ratings of perceived trustworthiness while the fictitious seals did not. This finding is somehow encouraging. Still, the participants were unsure in recognizing existing and fictitious seals of approval when asked if a seal was familiar to them. The general idea of third party web assurance seals was known by the majority of the participants while the knowledge appeared to be unspecific ("Seals signal quality"). Only a few participants stated that the criteria for awarding a third party seal are sometimes vaguely defined and seals are easily manipulable. A little percentage of participants reported that they knew about the possibility to check for the genuineness of seals of approval. For the trusting intentions and the intention to engage in a transaction at a certain website the different types of seals of approval did not make any difference. So, even when seals of approval positively affect users' appraisals of a website the actual behaviour is

motivated by various factors and the influence of the trustworthiness of a website is limited. For all experimental groups, the dating agency obtained the lowest ratings of both trustworthiness and intentions to engage in a transaction, while the online shop for electronic products scored highest. This might be due to the relevance of both topics in the student sample's daily life. It is assumed that the shop might be close to the real interests of the sample whereas the dating agency touches a highly sensitive topic. Therefore, social desirability might have biased the ratings. As stated in the questions on frequently used recommendations of the trustworthiness of a website, the opinion of friends, experience reports of previous users and media reports are the preferred ones. Third party web assurance seals are considered only little when estimating a website. The importance of peer opinion and a website's reputation have been found to be crucial for website usage decisions even when users possess profound knowledge about information security risks (Kline *et al.* 2011).

In summary, the effectiveness of existing third party web assurance seals as security indicators in promoting trustworthiness on websites could be confirmed. However, the method used in this study entails certain limitations. The sample size was rather small and only a few websites were investigated. Therefore, the generalization of the results is limited. Still, the effects that were found were large enough to be detected, even with the number of participants. It is assumed, that a replication of this study with a larger sample size would strengthen the findings. The fact that the participants have almost exclusively been students should not be a disadvantage of the study, as students are typical Internet users. Furthermore, most studies on online users' trust report student samples, which makes the results comparable to previous studies. Further studies on the effectiveness of web assurance seals could extend to samples with different demographics. Then, the experimental surrounding could be complemented by a field study to gain a higher real-life correspondence.

6. Conclusion

In summary, third party web assurance seals have a positive effect on perceived trustworthiness compared to no seals used. Fictitious seals do not obtain any trust-promoting effects compared to websites without such graphical elements. This supports the system of third party approval. For website providers who want to improve their reputation and communicate trust cues to their users, third party web assurance seals seem appropriate. Still, the users reported to have difficulties in differentiating between existing and fictitious seals. That circumstance makes them vulnerable to manipulation. To prevent manipulation of third party web assurance seals, more transparent information about third party approval is needed.

7. References

Atkinson, S., Furnell, S., & Phippen, A. (2009). Securing the next generation: enhancing e-safety awareness among young people. *Computer Fraud & Security*, *2009*(7), 13–19. doi:10.1016/S1361-3723(09)70088-0

Bélanger, F., & Carter, L. (2008). Trust and risk in e-government adoption. *The Journal of Strategic Information Systems, 17*(2), 165–176. doi:10.1016/j.jsis.2007.12.002

Beldad, A., de Jong, M., & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior, 26*(5), 857–869. doi:10.1016/j.chb.2010.03.013

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590).

Fogg, B. J. (2003). Prominence-interpretation theory: Explaining how people assess credibility online. In *CHI'03 extended abstracts on Human factors in computing systems* (pp. 722–723).

Furnell, S. M., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security*, *26*(5), 410–417. doi:10.1016/j.cose.2007.03.001

Kim, D., & Benbasat, I. (2010). Designs for effective implementation of trust assurances in internet stores. *Communications Of The ACM*, *53*(2), 121-126.

Kimery, K. M. & McCord, M. (2002). Third Party Assurances: Mapping the Road to Trust in eRetailing. *Journal of Information Technology Theory and Application* 4(2).

Kline, D., He, L., & Yaylacicegi, U. (2011). User perceptions of security technologies. *International Journal of Information Security and Privacy*, *5*(2), 1-12

Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors, 46*(1), 50–80.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research, 13*(3), 334–359. doi:10.1287/isre.13.3.334.81

Moores, T. (2005). Do consumers understand the role of privacy seals in e-commerce? *Communication of the ACM*, *48*(3), 86–91.

Noteberg, A., Christiaanse, E., & Wallage, P. (2003). Consumer trust in electronic channels: the impact of electronic commerce assurance on consumers' purchasing likelihood and risk perceptions. *E-service Journal, 2*(2), 46-67.

Rifon, N. J., LaRose, R., & Choi, S. (2005). Your privacy is sealed: effects of web privacy seals on trust and personal disclosures. *Journal of Consumer Affairs, 39*(2), 339-362.