It is not about the design – it is about the content! Making warnings more efficient by communicating risks appropriately

Michaela Kauer[1], Thomas Pfeiffer[1], Melanie Volkamer[2], Heike Theuerling[1], and Ralph Bruder[1]
[1]Institute of Ergonomics
Technische Universität Darmstadt, Petersenstr. 30
64287, Darmstadt

[2]Department of Computer Science; Research Group IT-Security, Usability and Society
Technische Universität Darmstadt, Hochschulstr. 10
64289, Darmstadt

kauer@iad.tu-darmstadt.de; t.pfeiffer@iad.tu-darmstadt.de; melanie.volkamer@cased.de
h.theuerling@iad.tu-darmstadt.de; bruder@iad.tu-darmstadt.de

Abstract: Most studies in usable security research aim at a quantification of persons, who – depending on the subject – fall for phishing, pass on their password, download malicious software and so on. In contrast, little research is done to identify the reasons for such insecure behavior. Within this paper, the result of a laboratory study is presented in which participants were confronted with different certificate warnings. Those warnings were presented when the participants tried to access different websites with different criticality (online banking, online shopping, social networks and information sites). Besides quantitative analyses of participants who were willing to use a websites despite the warning, the main focus of this work is to identify reasons for their decision. As a result of our study those risks are identified which were unacceptable for most participants to take and thereby might help to prevent unsecure usage behavior in the web by rewording warnings according to the perceived risks.

1 Introduction

Many studies in the context of usable security show that users fail to distinguish trustworthy from non-trustworthy websites [DTH06, TJ07, DHC06, JTS+07]. Consequently, they download viruses, provide personal information to dangerous web services, and fall for phishing. One reason identified in these studies is that many people are not aware of security indicators relevant to identify non-trustworthy websites like proper URL and a communication secured by SSL, ideally based on extended validation certificates. These studies also show that people care more about the content of the webpage like the logo and the quality of the web design than about security indicators. Correspondingly, there is only a small overlapping between people's trust indicators and real security indicators.

Originally published in GI-Edition - Lecture Notes in Informatics (LNI), P-195.

As this situation is well known, browsers started supporting people in identifying untrustworthy websites, by displaying warnings, e.g., special phishing warnings and certification warnings. This is a first progress as the analysis is done automatically and the user is not in charge of it. However, studies [DTH06, ECH08, JSTB07, SDOF07, SEA+09] showed that people do not understand the content of certification warnings and thus tend to ignore them. Understanding certification warnings is particularly difficult, because trustworthy (in general less security critical) websites also cause "invalid" certificate warnings (which are, e.g., caused by self-signed or expired certificates or the fact that the root certification authority is not known to the browser). These warnings can be ignored without any serious risk. Research [ECH08, SEA+09] shows that especially people who have often seen certificate warnings on trustworthy websites, where ignoring the warning did not cause any problem, tend to ignore these warnings for any website including the untrustworthy ones, which then cause serious problems like losing money.

Bravo-Lillo et al. [BCDK11] developed a mental model of how people understand and react to security warnings. Within this paper, they found that there are big differences in the behavior of expert and novice users. Experts analyze security problems before proceeding, whereas novice users think of the consequences afterwards. Overall, the authors found SSL warnings to be the most confusing warnings. This implicates, that in particular SSL warnings need to be improved. Therefore, we decided to focus on these warnings.

While most existing studies aim at quantifying persons who fall for different attacks, this work aims at identifying reasons for such insecure behavior. Based on these results, improvements mainly regarding rephrasing warnings are deduced to prevent unsecure behavior in the future. We conducted a laboratory study in which participants were confronted with different certificate browser warnings when trying to access different websites with different criticality, namely online banking, online shopping, social networks and news websites. The participants were asked why they ignored the warning or stopped accessing a corresponding webpage. There was no usability assessment of the warnings. Our main result from this study is that people ignoring the warning underestimate the risk and are more likely to stop accessing web pages when warnings describe personal risks. Thus, based on our results, we recommend using these risk descriptions when rewording (certification) warnings, while also distinguishing different criticality classes of web pages in the text of the warning. This idea goes along the lines with those recommendations proposed by Wogalter in ([Wog06], page 6) claiming that warning needs to "tell exactly what the hazard is, what the consequences are, what to do or not to do".

This paper is organized in the following way. In Section 2, we'll discuss related work. Afterwards, we will describe the methodology of the study in Section 3 and propose the result of the study in Section 4. Section 5 discusses these results and concludes the paper with an outlook for future work.

2 Related Work

The aspect of user's perceived consequences when submitting information to a fraudulent website has been studied extensively in the context of phishing attacks [JTS+07, ECH08, SEA+09, DHC07].

One of the most notable contributions in the area of SSL warnings is by Sunshine et al. [SEA+09]. They conducted an online survey followed by a laboratory study. In the online survey, they presented three different SSL certificate warnings (unknown issuer, certificate expired and domain mismatch) within the browser which the participants indicated they were using at the time. The warnings were displayed on either an anonymous forum or a shopping website (between-subjects) to 409 participants. Among other things they asked their participants "whether they understood what the warnings mean, what they would do when confronted with each warning and their beliefs about the consequences of ignoring these warnings". They did not find significant differences between the two websites. However, they did find that users who associated risks related to stolen information (e.g. identity theft, stolen credentials) with the warnings were more likely to heed them. To verify their findings, Sunshine et al. [SEA+09] conducted a laboratory experiment with 100 participants. Each participant completed tasks involving interaction with a library catalog and an online banking website (within-subjects) with one of five browsers: Firefox 2, Firefox 3, Internet Explorer 7 (IE7) and another two versions of IE7 with modified warning messages. The first modified warning message was altered visually to appear more severe and stated "An attacker is attempting to steal information that you are sending to [domainname]". The other modified warning first asked the user what kind of website she was visiting. In case of banks or web shops, the same warning as in the first modified version was displayed. In all other cases, the user was directed to the requested website. In the experiment, significantly fewer participants ignored the redesigned warnings than the existing warnings on the banking website. Nine out of eleven participants who heeded the first modified warning mentioned security of their information as the reason for doing so. No other significant effects of warning design were found.

We aim at replicating these findings in Germany with current browser versions as well as expanding on them by further investigating the risks associated with SSL warnings qualitatively.

3 Methodology

The herein presented study was a laboratory test and took place at the Technische Universität Darmstadt in Germany. The study consisted of two parts. Part one asked general questions on the participants' online usage behavior and their knowledge of security indicators. In part two, participants were instructed that they received an email with a link, which leads them to one out of twelve websites. The mail asked them to log in on the page and update some of their personal data.

Overall, three independent variables were varied: page type, web browser and warning

displayed. There were four different kinds of websites: online banking sites, online shopping sites, social networks and pure information sites. As in Sunshine et al.'s laboratory study [SEA+09], we expect users to react differently to warnings on different kinds of websites. Since Sunshine et al. only found differences in their within-subject study, we present different kinds of websites to each subject as well. It was expected that the number of participants who log in on a website and ignore the warning increases with decreasing criticality of the website.

Type and version of the web browser defines the second independent variable. The design of the warning varies significantly between different browser types and versions. The following four different browsers respectively browser versions were used: FireFox 2, FireFox 4, Internet Explorer 6, and Internet Explorer 9. Those browser types were selected as they are widely-spread at the time the survey was conducted. The versions were chosen to compare current with outdated warning design. Last, the type of certificate warning was varied. Three different certificate warnings were used within this study: certificate expired, certification authority unknown and wrong domain name. Figure 1-4 show examples for the warning "certification authority unknown" for each browser/version.

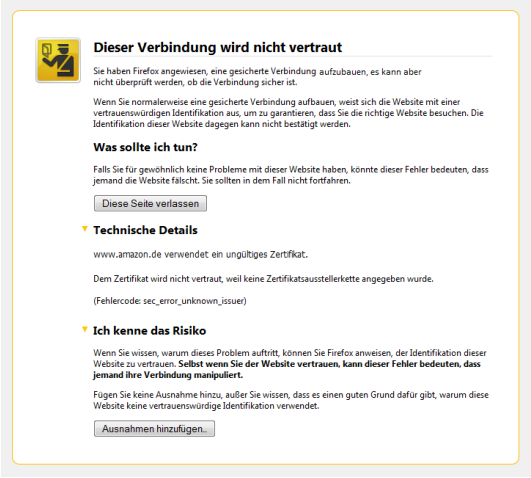

Figure 1: Certificate warning "certification authority unknown" for FireFox 4

Each participant was asked to access four different websites of at least three different kinds. The displayed warnings were in the design of each of the four browser types/versions. The warning contained each addressed certificate warning at least once. Participants were randomly assigned to the combination of type of website, browser type/version, and content of warning.

Participants were asked if they would use the website as normally, which included entering their user name and password to log in. In case of the pure information sites, this would have meant getting access to forums or customized information. Additionally, they were asked to give reasons for their decision. In a second step, each participant was confronted

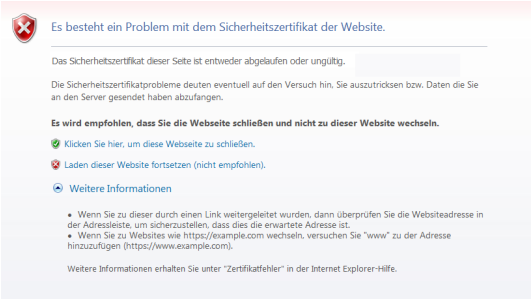

Figure 2: Certificate warning ”certification authority unknown” for Internet Explorer 9

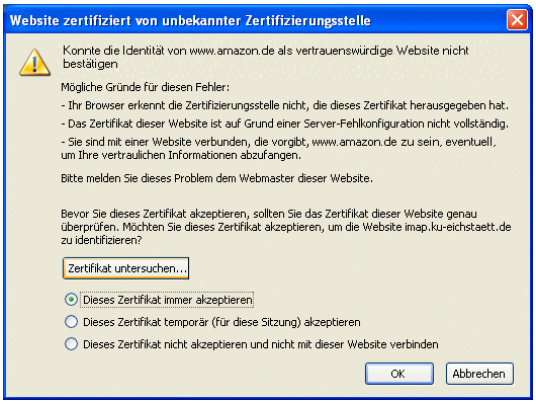

Figure 3: Certificate warning ”certification authority unknown” for FireFox 2

with each of these four combinations again and had to answer two questions for each of them, namely ”What does the warning mean?” and ”Which risk comes along with this warning?”.

4 Results

The results are a combination of quantitative and qualitative data. All calculations on the quantitative data were done with SPSS 19. Qualitative data was quantified by grouping similar answers to be able to somehow quantify the prevalence of the different answers.

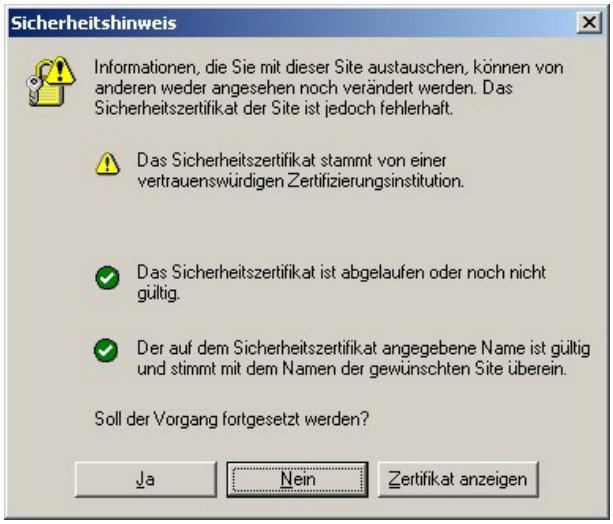

Figure 4: Certificate warning ”certification authority unknown” for Internet Explorer 6

4.1 Participants

30 participants attended the laboratory study. 14 participants were female. The participants were aged between 16 and 68 years, with an average of 35.50 years (SD = 15.94). One third of the participants stated to use the internet several times a day, 56.7% daily and only three participants stated to use it between once and four times a week. None of the participants stated not to use the internet at all. Participants were asked about their online shopping behavior. One participant responded to buy weekly at shops like Amazon, 90% of the participants ordered less than once a week and two participants stated that they never use online-shopping.

Out of the 30 participants 26.7% stated not to use online banking at all. One third of the participants are not active in social networks whereas 16.7% use social networks several times a day. 26.7% participants use social networks at least once a day, 13.3% three to four times a week and 3.3% once a week. 6.7% stated to use social networks less than once a week. 60% of the participants used Firefox as internet browser, 23.3% used the Internet Explorer. 6.7% used other browsers and 10% did not respond to the question.

The number of 30 participants was chosen because the main focus of this study lies on the qualitative analysis of the perceived risk. According to Morgan et al. [MFBA01] this sample size is large enough to be likely to reveal at least once any belief held by 10 percent or more of the population.

4.2 Quantitative Reactions to Certificate Warnings

The aim of this section is to quantify the number of people who decided to log in on a website despite the warning. The number of logins is distinguished between browser type/version (cmp. Table 1), content of warning (cmp. Table 2), and type of website (cmp. Table 3).

Browser Type/Version	**Would you log in?**	
	Yes	No
FireFox 2	10	20
FireFox 4	8	22
Internet Explorer 6	11	9
Internet Explorer 9	9	21

Table 1: Number of participants who decided to log in according to the browser type/version.

Warning Type	**Would you log in?**	
	Yes	No
wrong domain name	11	29
certificate expired	13	27
unknown authentication authority	14	26

Table 2: Number of participants who decided to log in according to the warning type.

Kind of Website	**Would you log in?**	
	Yes	No
online banking	2	28
online shoping	8	20
social network	13	19
information site	15	15

Table 3: Number of participants who decided to log in according to type of website.

With the help of cross tables a χ^2 statistic was computed to test if there is an effect of the browser type/version, the content of the warning, and the type of website respectively on the number of participants who would log in on the page despite the warning. The test revealed no significant difference between different browser types/versions (χ = 0.770, df = 3, p = .857). The same holds for the content of the warning (χ = 0.539, df = 2, p = .764). The last independent variable was the type of website on which the certificate warning occurred. Here a χ^2 test revealed highly significant differences between the different website types (χ = 14.636, df = 3, p = .002). Table 3 shows that the number of people who are willing to log in on a certain website despite an occurring warning decreases with increasing criticality of the deposed data.

4.3 Qualitative Reactions to Certificate Warnings

Within this study qualitative data was collected which is evaluated in this subsection.

Reasons for and against logging in. Besides the decision whether to log in or not on a certain page with a warning, participants were asked to give reasons for their decision. With 30 participants and four pages per participant an overall of 120 reasons were given. Similar reasons were grouped. This led to an overall of 10 different groups of reasons for log in and 13 different groups of reasons against log in. Five reasons are present in both groups, due to the fact that some people decided to log in because of those reasons, whereas other participants decided against logging in. Table 4 gives an overview of the reasons combined with the number of participants giving that reason.

a) Reasons for log in	**Number**
trust in this website	15
no personal data existent	6
risk unknown/unclear	6
interested in content/usage of page	3
illusion of inviolability (I am sure nothing will happen/Nothing never happened before)	2
warning incomprehensible	2
website looks secure	1
certificate unknown/invalid	1
coping strategies (close site and open again; try again later)	1
general caution	1
b) Reasons against log in	**Number**
general caution	31
personal data existent	10
attacks feared	10
high risk for banking/websites	7
faked website	6
warning incomprehensible	5
page is insecure	4
coping strategies (close site and open again; try again later)	4
warning exists	1
design of warning	1
problems with the content of the page	1
certificate unknown/invalid	1
risk unknown/unclear	1

Table 4: Number of participants who decided to log in on a website despite the warning (a) or not to log in on a website (b) separated according to the reason for their decision.

The reason ”trust in this website” which led in majority to a visit of a website despite showing a warning was further investigated and divided according to the website for which

this reason was mentioned. Trust was used as reason to log in on banking sites (one participant), on shopping sites (three participants), in social networks (five participants) and on information sites (six participants) despite the warnings.

Associated Risk. The second part of the qualitative analysis was concerned with the question which risk participants associate with ignoring the warnings. Each participant had to name the risk he would take if he ignored the warning for each warning he was presented. That made a total 120 named risks. Again, risks were grouped to simplify the evaluation.

A total of eight different risk groups emerged. Those groups and the according number of mentions are shown in Table 5. The higher a risk is represented in the table, the more participants in total mentioned the risk.

Risk	**Number**	**Log in?**	
		Yes	No
spying out personal data	58	11	47
risk unknown	22	7	15
manipulation of website/connection/own PC due to insecure connection	15	8	7
no risk	14	9	5
malware	7	2	5
loss of money	3	1	2
website not accessible	1	0	1

Table 5: Risks mentioned as being associated with ignoring the warning with number of participants who would log in despite the risk or not.

Out of all 120 mentions a total of 38 led to a log in on a page with warning. Excluding nine participants who stated that there is no risk associated with the warning[1], 29 participants remain who decided to log in on a page, despite the fact that they were able to name an occurring risk. The most often named risk was ”spying out personal data”. Therefore this risk was further investigated. Four out of the eleven participants who were willing to log in even by taking the risk of spying out personal data stated that they would take the risk for accessing an online shopping site, five participants for social networks and two for information sites. Nobody was willing to take that risk for an online banking site. It is noteworthy that one participant was willing to log in on an online shopping page even though he associated a potential loss of money with it.

As a next step, we compared answers which explicitly mentioned a personal risk with those that did not mention any personal risk (excluding those that saw no risk at all). The groups ”Spying out personal data” and ”Financial loss” were identified as ”personal risk”, all other groups except ”no risk” as ”no personal risk”. Then we investigated if personal risks were more likely to prevent participants from logging in. A χ^2 test revealed significant differences between personal and no personal risk (χ = 4.272, df = 1, p = .039), with personal risk being more effective in preventing login (see Table 6).

[1]It is noteworthy that four participants associated no risk even with warnings on the bank website.

Kind of risk	Would you log in?	
	Yes	No
personal risk	12	49
no personal risk	17	28

Table 6: Number of participants who decided to log in on the website despite the warning or not, separated according to whether they associated personal or technical risks with it.

5 Discussion

Some of our findings concur with those by Sunshine et al. [SEA+09], while others do not. In both studies, risks associated with ignoring SSL warnings played a key role in the decision to heed the warning or not. However, Sunshine et al. report no statistical tests for the correlation between risk perceptions and decisions relating to warnings. Consistent with their laboratory experiment but in contrast to their online survey, we found significant differences in behavior between the different types of websites. This can be explained by the fact that both our and their lab experiment tested the website type as a within-subjects factor whereas it was a between-subjects factor in their survey. Therefore participants were probably more aware that there are different kinds of websites and their different security preferences were more salient. Since visiting different types of websites in a row is more akin to usual web browsing behavior than visiting only one kind, we conclude that this finding has a higher external validity than the survey finding.

In contrast to Sunshine et al. we found no different reactions to the different kinds of warnings. This can be explained by our participant's lack of knowledge about SSL and related warnings, as Sunshine et al. reported much larger differences between reactions to the different types of warnings for experts than for non-experts.

21 times, participants gave "risk unknown or unclear" as answer to the question which risk is associated with ignoring the warning. Out of these 21 participants six participants decided to log-in. This is about a quarter of the participants. It can be assumed that those participants would not have logged in, if they would have been informed on the risks they were taking. *This leads to the conclusion that the risk should be clearly communicated to the users.*

For the communication of the risk, the wording is essential for the success of the warning, as can be seen in Table 6. Here, nine out of 17 participants who associated the technical risk "Manipulation of website/connection/own PC due to insecure connection" with logging in to the website did log in. The *communication of the risk* should therefore not only be formulated in terms of technical risks (e.g. the connection is insecure,) but in terms of *personal risks* (e.g. therefore, someone might be able to spy out your personal data).

A similar approach is needed for those who enter a website just because of their trust in the page regardless of warnings (as 15 of our participants did). To inhibit this unsecure behavior the risks should be clearly named and additionally, it is necessary to communicate that the look of a page alone is not sufficient to guarantee its trustworthiness.

Furthermore, nine participants were sure that there is no risk associated with the displayed

warnings. Some pointed out that there was no personal data to spy out (on information sites and social networks), some stated that they are familiar with the warning and until now, nothing had ever happened. This is partly true, because some of the presented warnings come along with low risk. Still, even our information sites had a log-in area, in which additional information was provided. To enter this log-in page a password and a user name were required. It is alarming that spying out passwords is not perceived as potential risks by our participants, especially because many people tend to use the same password for several applications [CVOB06]. Therefore, for a number of participants the theft of a password in this application would enable or at least simplify attackers the access to other applications used by the same participant. For this reason, it is essential to inform people about possible risks.

Within this study, personal risks (namely spying out personal data and financial loss) were found to be more effective in terms of preventing users from visiting a website despite a warning than impersonal risks, like a generalized manipulation of the communication or malware or an unknown risk. This is consistent with a study by Hardee et al. [HWM06] where participants mostly mentioned "Protecting Information" and "Protecting Money/Property" as the gains from making conservative security decisions. Therefore, "spying out personal data" or "financial loss" should be mentioned in warning massages directly. We believe that the effectiveness could even be further increased, if it is possible to make content-sensitive warnings which indicate the kind of data (e.g. banking data) that would be spied out on the type of web page that the user tries to access.

6 Conclusion and Outlook

We conducted a study on certificate warnings. A website was shown to the participants with an according warning. Participants were then asked to either log in or not. Afterwards, they were asked to justify their decision. The study revealed the following four items: First, the general section on security indicators confirmed that most people are not familiar with them. Then, the qualitative part of this research revealed that people are often not aware of actual risks. As a third result, we showed that the perceived risk of personal data being spied out prevented most participants from entering the corresponding website. From this result, we conclude that risks need to be more clearly communicated. The fourth result of the study allows us to further concretize this statement, as we showed that it is more effective to communicate personal risks than technical risks. Correspondingly, we can conclude that personal risk descriptions should be used when rephrasing warnings.

These findings confirm and expand upon the major findings by Sunshine et al. [SEA+09]. Building upon our findings we are currently preparing a study that tests newly designed warnings which incorporate information about the personal consequences of submitting data to a fraudulent site of a certain kind. We hope that these warnings will be even more effective than the ones designed by Sunshine et al., which still remained on an impersonal level ("An attacker is attempting to steal information").

7 Acknowledgements

The authors like to thank Tim Protzmann for the conduction of the study and Jurlind Budurushi for the formatting. We also thank the reviewers for their constructive feedback.

References

[BCDK11] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie S. Downs, and Saranga Komanduri. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy*, 9(2):18–26, April 2011.

[CVOB06] Sonia Chiasson, P.C. Van Oorschot, and Robert Biddle. A usability study and critique of two password managers. In *15th USENIX Security Symposium*, page 1–16, 2006.

[DHC06] Julie S. Downs, Mandy B. Holbrook, and Lorrie Faith Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, page 79–90, New York, NY, USA, 2006. ACM.

[DHC07] Julie S. Downs, Mandy Holbrook, and Lorrie Faith Cranor. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, eCrime '07, page 37–44, New York, NY, USA, 2007. ACM.

[DTH06] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, page 581–590, New York, NY, USA, 2006. ACM.

[ECH08] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, CHI '08, page 1065–1074, New York, NY, USA, 2008. ACM.

[HWM06] Jefferson B. Hardee, Ryan West, and Christopher B. Mayhorn. To download or not to download: an examination of computer security decision making. *interactions*, 13(3):32–37, May 2006.

[JSTB07] Collin Jackson, Daniel R. Simon, Desney S. Tan, and Adam Barth. An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. In Sven Dietrich and Rachna Dhamija, editors, *Financial Cryptography and Data Security*, volume 4886, pages 281–293. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[JTS+07] Markus Jakobsson, Alex Tsow, Ankur Shah, Eli Blevis, and Youn-Kyung Lim. What instills trust? a qualitative study of phishing. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security*, FC'07/USEC'07, page 356–361, Berlin, Heidelberg, 2007. Springer-Verlag.

[MFBA01] M. Granger Morgan, Baruch Fischhoff, Ann Bostrom, and Cynthia J. Atman. *Risk Communication: A Mental Models Approach*. Cambridge University Press, 1 edition, July 2001.

[SDOF07] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The Emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, 2007.

[SEA+09] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. Crying wolf: an empirical study of SSL warning effectiveness. In *Proceedings of the 18th conference on USENIX security symposium*, SSYM'09, page 399–416, Berkeley, CA, USA, 2009. USENIX Association.

[TJ07] Alex Tsow and Markus Jakobsson. Deceit and Deception: A Large User Study of Phishing. *Indiana University. Retrieved September*, 9:2007, 2007.

[Wog06] Michael S. Wogalter. *Handbook of warnings*. Routledge, January 2006.