Melanie Volkamer, Fatih Karayumak, Michaela Kauer,
Dhanish Halim, Ralph Bruder:

Security versus Trust Indicators in 2011 in Germany

Published in:
Jähnke, von zur Mühlen, Rechert, von Suchodoletz:
Current Issues in IT Security 2012, Duncker & Humblot, 2012,
p. 79-96.
ISBN 978-3-86113-115-1
ISSN 1862-7625

MELANIE VOLKAMER, FATIH KARAYUMAK, MICHAELA KAUER,
DHANISH HALIM AND RALPH BRUDER*

Security versus Trust Indicators in 2011 in Germany

More and more people use the internet for online banking, online shopping, participating in online social networks, emailing and many other services. They are probably also aware that there are security and privacy problems in the internet. However, studies show that the average user is either not aware of the proper security indicators or does not know how to properly evaluate them on a visited webpage. The criteria users apply to judge the trustworthiness of a webpage (trust indicators) differ completely from these security indicators. In the past, various measures have been taken to improve this situation. We conducted an online survey in Germany to test whether these measures result in an improvement. The result of our study is that the situation has not really improved. Based on our results, we deduce first ideas to improve the situation in the future.

I. Introduction

Many studies show that users fail to distinguish trustworthy from non-trustworthy webpages (see e.g. Biddle et al., 2009; Jackson et al., 2007; Jakobsson et al., 2007). Consequently, users download viruses, become part of botnets, provide personal information to dangerous services, and fall for phishing pages. One reason for this is that many people are not aware of the relevant security indicators like HTTPS, proper URLs, security seals and extended validation certificates, or they do not understand their meaning. Moreover, several studies, such as by Schechter et al. (2007), Sobey et al. (2008), Tsow and Jakobsson (2007), show that people care more about the content of the webpage, i.e the logo and quality of the design (so called trust indicators) than about security indicators.

In the past, various measures have been taken to improve this situation. The new web browsers support users (in different ways) in identifying and analyzing security indicators. In this context, the CA/Browser Forum introduced the extended validation (EV) certificates in 2007, so that it would be possible to trust the authenticity of web service without checking the SSL certificates. In addition, especially in Germany, many initiatives and companies like "BSI for citizens", the D21, Tüv-IT, and banks tried to increase awareness of security indicators by explaining why and how to verify them in order to judge the trustworthiness of a webpage.

Correspondingly, the question we answer in this paper is whether the findings in previous studies regarding the security and trust indicators still apply and can

* Technical University of Darmstadt, Germany

in particular be applied for Germany (as existing studies have been mostly conducted in the US). Our aim is in particular to find out whether these findings do not apply anymore for special groups of users (experts, young people, etc.), for special groups of users, or for specific situations (e.g. when users enter personal data). Therefore, we conducted an online survey in German-speaking countries with 164 participants. In this study, two different web browsers (IE9 and Firefox 5) and four different categories of webpages (online banking, social networking, mail and shopping) were analyzed. From numerous security indicators, only the most relevant ones were tested: namely, HTTPS, SSL/EV SSL certificates, URLs and security seals. Furthermore, we asked the participants which criteria they use to evaluate the trustworthiness of a webpage in order to identify their trust indicators. In general, one must say that the situation has not really improved. Consequently, the type of measures taken in the past was not sufficient to improve the situation. Based on our results, we deduced first ideas to improve the situation.

The rest of the paper is as follows: We present related work in Section II. and introduce the survey layout in Section III. The demographics of the survey is shown in Section IV., the results for the security indicators in Section V. and thereafter trust indicators are presented and discussed in Section VI. General findings deduced from the results, conclusions as well as future work are proposed in Section VII. The appendix contains the screenshots and relevant tables of the survey.

II. Related Work

Several studies have tested the effect of URLs, third-party seals and extended validation SSL certificates on perceived trustworthiness.

There are some papers on security indicators. In a qualitative study with 18 participants, who were shown different legitimate and illegitimate webpages and emails, Jakobsson et al. (2007) found that users are able to detect ”syntactically peculiar” URLs, but were not suspicious about well-formed but illegitimate URLs. They also found that third-party trust logos were only effective in conveying trustworthiness for those participants who knew the brands. In a study by Schechter et al. (2007), all 63 participants entered their bank login password on their bank’s webpage, even in the absence of SSL. It has to be noted, however, that they had visited the same webpage in two previous tasks, where the connection was secured by SSL. Similar results have been shown by studies in the context of phishing Dhamija et al. (2006); Jakobsson (2007); Wu et al. (2006) where most participants fell for phishing, because they are either not aware or do not care about security indicators. Stebila (2010) identified the four most important security indicators and examined 125 popular webpages on whether these indicators are properly displayed. They showed that on most

of the webpages some of the security indicators are absent or suboptimal. This does not really support users in checking for security indicators and thus the above results are not very surprising.

Tsow and Jakobsson (2007) analyzed trust indicators in a quantitative study with 398 participants. They found that many people only care about the look and design of the webpage (e.g. that it looks like always and the known logo is shown) and only start verifying other indicators in order to decide whether this page is trustworthy or not if the page looks strange or completely different.

There is also some literature in this context, analyzing whether education helps to improve the situation. Jackson et al. (2007) tested whether users, who saw Internet Explorer 7's indicator of the presence of an EV certificate (the location bar turns green) on a webpage, were more likely to identify spoofed versions of that page later (which did either not show that indicator or faked the whole address bar using a picture-in-picture attack), than those who had not seen them before. They found that knowing that the original webpage has the green address bar did not help the participants identifying the spoofed version, not even after reading documentation about what the bar means. Biddle et al. (2009) tried to break down the complexity of different statuses of SSL certificates (none, self-signed, basic and extended validation) to users by separating them into identity confidence and privacy, and explaining the different levels by using easier words. When they showed their redesigned information popup windows to users in comparison to regular SSL indicators in IE 7, users stated that it was easier to find and understand ownership and confidential information in the re-designed popups. However, in a study using this approach and employing eye tracking, Sobey et al. (2008) found that most participants hardly looked at the web browser chrome during the tasks and that, of those who did notice the SSL indicator, none clicked it to see the pop-up with extended information. Therefore users are unlikely to ever see the information presented in the popup by Biddle et al. (2009) in practice at all. Thus, these studies show that, at least for their participants, education does not improve the situation.

In the context of security and trust indicators, and motivated by previous mentioned study results, researchers have started to propose approaches supporting users in judging the authenticity of webpages. Herzberg and Jbara (2008) present TrustBar, a secure user-interface add-on for web browsers. This add-on tries to identify the SSL/TLS-protected webpages and the certificate authority using logos or at least names (not the URL) and displays highly visible warnings for unprotected webpages. Shi et al. (2011) present a new design for Extended Validation (EV) certificate interface in the Firefox web browser in their work, using affordance-based principles in their design of web authentication indicators. They evaluated this approach with three different versions of EV indicators in an exploratory, qualitative study and claim that these designs are more effective web authentication indicators. Fung and Cheung (2010), on the other hand,

propose a fundamentally different approach to sustain SSL protection. Their proposal, SSLock, is fired up by the idea that SSL, as a security-critical system, should not rely on user's judgement as the adversaries use this to their advantage. They claim that this proposal enhances an automatic protection by letting the service provider opt-in by operating its service in a secure sub-domain.

III. Survey Layout

We decided to run an online survey in order to collect as many distinguishing answers from as many people with different backgrounds as we could. We used the open-source content management system "Drupal" to build the webpage hosting the survey and MySql to store the data. The survey language was German. The survey consisted of six parts.

The *first* part of the survey contained demographic-screening-questions like age, gender, education level, etc. to enable classification of the participants. In the *second* part, we assessed the technical knowledge of the users in general and in particular regarding terms related to security indicators such as SSL, HTTPS, EV certificates, and seals of approval. There were also three invented terms; namely TLS registration, HTTPX und TCP/IT. We also asked them to explain the proper terms if they stated to know them. Note that once they decided to select one of these terms and they continued to the next page with the question to explain corresponding terms, it was not possible to go back again and to modify the selection. We used both measures to determine whether users really understood the terms.

In the *third* part, the participants were asked to evaluate twelve webpages from different contexts based on displayed screenshots. We distinguished between online banking (Deutsche Bank, Commerzbank, Hypovereinsbank, and Deka Bank), online social networks (Xing, Facebook, and StudiVZ), e-mail (Web.de and Gmx) and shopping (Neckermann, Amazon, and Epag). All twelve were shown to each of the participants. Seven of the screenshots were authentic screenshots and five screenshots were modified. We used different approaches to modify these screenshots; namely a typo in the domain name, real domain name as sub-domain of another domain, domain name as a folder in another domain name, slight modification of the domain name. Table 1 shows the faked webpages with the corresponding modification.

We asked participants for their browser preferences in order to show them screenshots using their own preference. The provided options were Internet Explorer, Firefox and others. According to their preferences, the screenshots were shown either in Internet Explorer 9 or in Firefox 5.0. The address bars of Firefox screenshots are displayed in Appendix A.

For the evaluation, the users took part in a small role play, where they supposedly receive an email with a link. In this e-mail they were asked to follow

Table 1: Webpage - type, name, URL and type of modification

Type	Name	URL	Type of Modification
Online Banking	Hypovereinsbank	https://my.hypvereinsbank.de	The letter "o" is taken out
Online Social Network	StudiVZ	http://www.studivz.net.secure-login.de/login.html	StudiVZ is subdomain of the secure-login.de domain
Shopping	Amazon	https://www.einkaufen.info/-user/www.amazon.de/-login.html	www.amazon.de as a folder in the server of einkaufen.de
Shopping	Neckermann	http://www.neckermann-login.de/-on/demandware.store/Sites-DE-Site/	neckermann-login.de instead of the original neckermann.de domain name
Mail	Web.de	http://www.secure-login.de/-user/www.web.de/login.html	www.web.de as one folder at secure-login.de

a link to a webpage. They were told that they already have an account on this webpage and were asked to log in, in order to see the alterations and the general terms and conditions of the webpage. Then, twelve webpages were shown to the participants while they were asked to answer the following questions for each screenshot;

- whether they have an account on the displayed webpage;
- whether they would log on to these webpages and use them as usual (yes or no), and how certain they are about their decision, on a scale from 1 to 7 (1 being not sure and 7 very sure);
- whether the webpage and the information transmissions on the webpage are encrypted (yes or no) and how certain they are about their decision on a scale from 1 to 7 (1 being not sure and 7 very sure).

In the *fourth* part, we concentrated further on SSL certificates. Users were shown the details of an SSL certificate (authentic certificate which belongs to facebook.com and signed by DigiCert) and asked

- whether they know how to open this SSL certificate window,
- for which type of webpages they check this information (while providing the options: none, login pages, online banking, webshops, all HTTPS pages, all HTTPS pages without EV certificate)

The *fifth* part focused on seals of approval in the context of webshop security. The participants were presented with 15 icons. These icons are shown in Figure 14 in Appendix F. We confronted the participants with five different categories of icons, while not stating anything about the categories to the user. In the first category 'A' holds four of the seals ("Trusted Shops", "TÜV Süd Safer

Shopping", "EHI Euro Label", "EHI bvh"), which were officially accredited by D21[1] and had clearly defined quality criteria for web-shop security. In the second category 'B' are three seals of approval ("Verisign", "Protected Shops", "United SSL-Secure Site") which are not evaluated by D21. However, Verisign is also very well established and accepted in the context of webshop security. United SSL-Secure Site seal ensures that the data connection of the webpage is secured via HTTPS. The security criteria used by Protected Shops is not clearly stated. In the third category 'C' are four seals, which are related to webshops, but do not make a statement about the security of the webshop ("Idealo" is for price comparison; "Paypal" and "Verified Visa-Master Card Securecode" are for the availability of the corresponding payment methods; and "United SSL Secure Site"). In the fourth category 'D' has two seals for aspects other than webshops or the Internet ("Self Certified" for the security of the rainforest trees, "TÜV Berlin" for car security). In the last category 'E' were two fake seals, which we invented (the seals with the padlock symbol and the seal with the letters 'TP'). Then users were asked which of the seals were important for them to determine whether a webshop is secure.

The *sixth* and last part of the survey addressed trust indicators. We asked the participants what would indicate that a webpage is not trustworthy. We provided 14 different options: namely 'Too many advertisements', '"about us" page does not exist', 'Loading of the page takes too long', 'Not possible to log in', 'There is no seal of approval', 'Appearance of the webpage does not seem to be right', 'The address in the address bar has a typo', 'The address in the address bar is different than the one in the email', 'The address in the address bar is too long', 'The address in the address bar is other than the name in the logo', 'The data transmission is not encrypted with HTTPS', 'The web-browser shows an error message', 'The displayed webpage is not previously known', and 'The padlock symbol is not closed'. However, only the option with the typo in the addressbar is a clear indicator that the webpage is not to be trusted. All other options may occur on a legitimate webpage, too.

At *the end of the study* we asked the participants whether they answered the questions on their own and if not, what kind of help they received. The study was online for one week between July 23rd and July 31st 2011.

IV. Demographics

In total 138 people participated in the study. 26 stated that they did not answer the questions on their own. Therefore, we excluded these 26 participants. From the remaining participants, 32 used Internet Explorer and 80 Firefox. We had 50.9% female (75.0% with IE, and 41.3% with Firefox) and 49.1% male participants. The average age of the participants was 33.43 (SD = 11.47); the

[1] http://www.internet-guetesiegel.de/index.html [11.01.2012].

Table 2: Percentage of participants who use the corresponding service

Service	Total	Firefox	IE
Surfing / Searching / Getting Infos	95.5%	96.3%	93.8%
Online banking	71.4%	67.5%	81.3%
Shopping	70.5%	66.3%	81.3%
Online games	31.3%	32.5%	28.1%
Online Social Networks	75.9%	72.5%	84.4%
Others	37.5%	41.3%	28.1%

oldest one was 68 and the youngest one was 11 (for IE the corresponding numbers are 11/68 years, mean = 36.88, SD = 13.69 and for Firefox 18/68 years, mean = 32.05, SD = 10.23). 62.5% had a university degree, 31.3% finished Fachhochschule or Hochschule, and 6.2% were less educated. 25% of the participants were students; 8.8% of them in the IT area. 16.1% worked in the IT industry (for IE the corresponding numbers are: 50.0% university degree, 27.5% Fachhochschule or Hochschule, 12.6% less educated and for Firefox: 67.5% university degree, 28.8% Fachhochschule or Hochschule, 3.8% less educated). 70.6% of the participants use the Internet several times every day or stated being online most of the time (70.0% for Firefox and 71.9% for IE). The remaining stated that they are less frequent online. Table 2 provides an overview of the services the participants use.

V. Results for Security Indicators

In this section, we present the results for part two to five, which deal with questions and tasks related to security indicators. Note that we do not mention the difference between participants having selected FF and those who are in favor of the IE if the browser preference should not have an influence on the study results, like with general knowledge of terms or the displayed seal icons.

Knowledge of security indicators in the context of encrypted and authentic communication. Participants were asked whether they know the named security indicators, including three faked terms. Table 3 shows the results, i.e. percentage of participants who stated that they know a particular term and percentage of those who answered the question for a particular term with yes and could properly explain it. Wrong answers included programming language for SSL, secure homepage implementation for HTTPS, a certified SSL version for SSL certificate, and a new type of spam for phishing. It is notable that more than 50% of the participants used online banking in their explanation for phishing. In total, only five participants claimed to know all the proper ones; four of them were also able to properly explain these. 39 participants did not select any of the existing security indicators.

SSL certificate information. The question, whether it is known how to open

Table 3: Percentage of participants who know the terms and could explain it properly

Terms	Total Yes	Total Yes and Correct Descr.
SSL	57.75%	33.93%
SSL certificate	53.07%	24.11%
HTTPS	67.35%	43.75%
EV certificate	18.25%	18.25%
Phishing	62.0%	41.96%
TCPIT	36.6%	–
HTTPX	10.7%	–
TLS/Registration	16.1%	–

Table 4: SSL certificate checking depending on the type of webpage

Type of webpage	Number of participants
None	79
Login	12
Online banking	30
Online Shopping	18
All HTTPS webpages	8
All HTTPS webpages without EV	3

the certificate information window was answered by 35% of the participants (12.5% IE and 45.5% FF) positively. 79 participants stated that they never check the SSL-certificates. Only three participants said that they check all the HTTPS webpages, which do not use EV certificates. Two of them also marked the option "all of the https webpages" which does not really make sense, as this would include those with EV certificates. The other participant who marked the option "all the HTTPS without the EV certificate" did not mark the option "all of the HTTPS webpages", but has in addition marked login and shopping. Thus, there is only one participant who behaves properly, namely checking login and shopping pages when it is only secure by basic HTTPS. Table 4 shows an overview of the selections.

SSL - Basic versus Extended Validation. The participants were explicitly asked whether they know the difference between basic and extended validation certificates. 14.3% stated that they do know the difference (with Firefox 18.8% and with IE 3.1%). This matches with the results from part three of the study. Here 19.5% of the participants on average were able to detect those webpages using HTTPS based on an EV certificate. However, when it comes to the explanations, only 4.5% of the participants made proper statements.

No - basic - EV HTTPS. On an average of 53.2%, for all the screenshots, the participants (46.6% for IE and 56% for FF) selected the proper encryption type out of the three possible choices (no, basic, EV). An overview of the results of each screenshot is shown in 5. The results show that only few people can distinguish between SSL basic and SSL with EV certificate. Regardless of whether basic or EV was the proper answer, more people selected SSL basic

Table 5: Percentage per type of encryption (no, basic, EV) for each screenshot

		Unencrypted			Basic			EV		
Webpage	Encryption	Total	FF	IE	Total	FF	IE	Total	FF	IE
Deutsche-Bank	EV	26.8%	16.3%	53.1%	57.1%	65%	37.5%	16.6%	18.8%	9.4%
Commerz-bank	EV	27.7%	17.5%	53.1%	50.0%	53.8%	40.6%	22.3%	28.8%	6.3%
Hypo-vereins-bank	SSL	41.1%	31.3%	65.6%	49.1%	56.3%	31.3%	9.8%	12.5%	3.1%
Xing	unen-crypted	80.4%	78.8%	84.4%	15.2%	16.3%	12.5%	4.5%	5.0%	3.1%
StudiVZ	unen-crypted	75.9%	72.5%	84.4%	17.0%	20.0%	9.4%	7.1%	7.5%	6.3%
Facebook	SSL	37.5%	28.8%	59.4%	51.8%	57.5%	37.5%	10.7%	13.8%	3.1%
Amazon	SSL	29.5%	18.8%	56.3%	58.9%	66.3%	40.6%	11.6%	15.0%	3.1%
Epag	EV	28.8%	20.0%	50.0%	51.8%	57.5%	37.5%	19.6%	22.5%	12.5%
Necker-mann	unen-crypted	77.7%	73.8%	87.5%	18.8%	21.3%	12.5%	3.6%	5.0%	0.0%
Web.de	unen-crypted	75.9%	70.0%	90.6%	21.4%	26.3%	9.4%	2.7%	3.8%	0.0%
Gmx.de	SSL	33.9%	23.8%	59.4%	52.7%	61.3%	31.3%	13.4%	15.0%	9.4%
Deka Bank	SSL	33.0%	25.0%	53.1%	59.8%	66.3%	43.8%	7.1%	8.8%	3.1%

than SSL with EV. However, 77.5% of the participants selected 'no encryption' if the screenshots only displayed 'http'. At least people are much better in distinguishing between no with any encryption than between basic and EV based HTTPS. Note, regarding the differentiation between EV based and basic https, participants using FF got better results than participants using IE. The opposite is the case for distinguishing between encryption and no encryption. This could be caused by the different concepts in place for IE and FF to display no, basic, and EV based HTTPS (see Figure 1 for the different concepts). However, the FF interfaces for EV and basic HTTPS are very similar and can only be distinguished by the color, while the IE interface for EV based HTTPS with the green bar differs much from the other two. Therefore, it is unclear how to explain this result.

Figure 1: Screenshots of web browser adress bars for no, basic, and EV based HTTPS

We also asked the participants how certain they were. The results are shown in Table 6. The average for all screenshots is 4.9, on a scale from 1 to 7 (1 being not sure and 7 very sure). This value occurred to be very similar for all the screenshots and does not vary for any of the encryption types. In general

Table 6: Certainty of participants regarding properly having answered the questions

		Average users certainty that their answer encryption is correct (7 very certain)			Average users certainty that their answer regarding the usage as usual (7 very certain)		
Webpage	Encryption	Total	FF	IE	Total	FF	IE
Deutsche Bank	EV	4.75	4.8	4.625	4.7500	4.8000	4.6250
Commerzbank	EV	5.0357	5.2	4.625	5.3839	5.5625	4.9375
Hypovereinsbank	Phishing SSL	4.5982	4.7625	4.1875	5.1696	5.2875	4.8750
Xing	unencrypted	4.9911	5.2125	4.4375	5.1339	5.2375	4.8750
StudiVZ	unencrypted Phishing	5.0982	5.325	4.5312	5.2321	5.3625	4.9062
Facebook	SSL	5.0893	5.25	4.6875	5.4196	5.5250	5.1563
Amazon	Phishing SSL	4.9554	5.15	4.4687	5.3750	5.5625	4.9063
Epag	EV	4.7946	4.925	4.4688	5.0714	5.1375	4.9063
Neckermann	unencrypted Phishing	4.9732	5.1125	4.625	5.2054	5.3125	4.9375
Web.de	unencrypted Phishing	4.9107	5.05	4.5625	5.1071	5.1750	4.9375
Gmx.de	SSL	4.9732	5.175	4.4688	5.3125	5.5375	4.7500
Deka Bank	SSL	4.7768	4.8875	4.5	5.3214	5.5000	4.8750

the participants using FF seem to be a bit less certain, than those using IE (4.2 with FF and 4.5 with IE). This is somehow surprising as the FF users performed better in properly identifying the encryption type.

Screenshots - Authenticated versus manipulated/phishing webpages. In this part the participants had do decide whether it is a faked/phishing page or an authentic one. An overview of the results per screenshot is shown in Table 7. There were only six participants who had answered all of the questions correctly regarding the faked pages. 37.5% of the participants did not recognize any of the fake webpages (78.1% IE, 21.3% FF). On average 64.96% of the participants would access the shown faked pages (for IE it would even be worth with 87.5% on average). The category of the webpage as well as the type of modification has no significant impact on the decision to login as usual. The lowest percentage of people who would access one of our faked pages belongs to the email service (web.de) and the highest to the social network (StudiVZ). With respect to the type of modifications, the application of a subdomain was the one with the highest percentage of people who stated that they would access the page as usual and the application of subfolders was the one with the lowest percentage. There is no correlation between the fact that someone has an account at any of the services and their decision to use the service as usual (neither in general nor for the faked pages). The only significance we can identify is the one between Firefox and IE users. As both web browsers show the modified URLs in an equal way, the browser interface itself cannot have caused this difference. However, the other results of the study give reason to assume, that the (or at least our) Firefox users are more educated in Internet security questions than the IE users. This might have caused these different results.

Furthermore, the results show that it does not make any difference whether

Table 7: Percentage of participants with account & who would login

	Part. with account (%)			Part./ would use it (%)		
Webpage	Total	FF	IE	Total	FF	IE
Deutsche Bank	22.3%	21.3%	25.0%	86.6%	81.3%	100%
Commerzbank	22.3%	17.5%	34.4%	84.8%	80.0%	96.9%
Hypovereinsbank	32.1%	32.5%	31.3%	66.1%	58.8%	84.4%
Xing	38.4%	41.3%	31.3%	78.6%	72.5%	93.8%
StudiVZ	31.3%	30.0%	34.4%	68.8%	60.0%	90.6%
Facebook	51.8%	52.5%	50.0%	92.0%	88.8%	100%
Amazon	33.0%	31.3%	37.5%	65.2%	56.3%	87.5%
Epag	17.0%	15.0%	21.9%	78.6%	71.3%	96.9%
Neckermann	24.1%	25.0%	21.9%	63.4%	53.8%	87.5%
Web.de	22.3%	20.0%	28.1%	61.6%	51.3%	87.5%
Gmx.de	22.3%	21.3%	25.0%	86.6%	81.3%	100%
Deka Bank	22.3%	21.3%	25.0%	86.6%	81.3%	100%

the manipulated URL uses HTTPS or not. Thus, for phishers it is still not necessary to use HTTPS for their faked web pages, as the success rate at least for the study is the same for HTTPS as without HTTPS. It is also interesting to see that 75% of the participants noticed that the connection to Xing is not secured by SSL. However, 78.6% percent of the users stated that they would log in.

Regarding the certainty question (compare to Table 6), the participants on average were more certain that their answer is correct than with respect to the type of encryption question (on average, in total: 5.2 on a scale from 1 to 7; 5.3 for FF and 4.9 for IE). While for the type of encryption question the value for the IE was higher on average, here it is the opposite. This might be due to the same explanation regarding FF holding the more educated participants. For the IE users, the manipulated StudiVZ shreenshot got the worst result: 90.6% of the IE participants stated that they would login as usual (the worst result for all manipulated results), while the average certainty value is 5.2 (the highest for all twelve screenshots). In general, from the two questions related to the twelve screenshots it can be deduced that, the fact of many participants being able to distinguish between HTTP and HTTPS connections, does not mean that these people would not login to HTTP webpages.

Seals. Participants were asked whether they know Internet security seals of approval and whether they can explain what they are. 40.18% stated that they know these seals. 9.82% of those who answered with yes could also properly explain it. Wrong answers were mainly related to the certified good quality of the sold products. It is notable that, from the 45 participants stating they know seals of approvals, only 27 stated that they are important for them when deciding whether a webpage is trustworthy or not. Furthermore, 65 of the participants did not select any of the D21 approved seals. The most popular seal approved by the D21 is the TÜV Süd Safer Shopping. One reason, why this icon looks

Table 8: Seal of Approval Knowledge

Seals	Number of participants	Category
EHI accepted Online Shop	14	A
e-Trusted Shop	30	A
TÜV Süd Safer Shopping	32	A
EHI bvh	6	A
Verisign	30	B
Protected Shops	0	B
Idealo Gelisteter Partner	2	C
Paypal	38	C
Verified Visa/Mastercard Securecode	30	C
United SSL Secure Site	1	C
Safe Certified	2	D
TÜV Berlin	17	D
Padlock Symbol Seal	3	E
Seal with shield and TP letters	1	E

familiar to the participants could be the fact that it looks similar to the TÜV seal they are used to from the TÜV test for their cars. This would also explain why TÜV Berlin was selected by 17 participants (which is a much higher number than any of the other wrong icons (category D and E) got). The results also show that Verisign is well known, as well as the seal from e-Trusted Shop. The overall results are displayed in Table 8.

VI. Results for Trust Indicators

In this section, we present the results regarding the question which properties of a webpage would indicate that it is untrustworthy to the participants. We provided 15 different options to choose from while multiple choices were allowed. Table 9 shows the results per option and browser. These results support the ones from Tsow and Jakobsson (2007), i.e. people care most about the look and design of the webpage, as 64.3% selected 'Appearance of the webpage does not seem to be right'. Surprisingly, 67.9% percent of the participants stated that they pay attention to the webpage's URL. If we compare this result with previous ones, it can be shown that participants do not practice their theoretic knowledge, as only 34% identified the URL typo in the Hypovereinsbank screenshot. In total, only 29 out of the 76 participants who stated that they check for typos detected the problem within the Hypovereinsbank screenshot.

VII. Conclusion

We conducted an online study to test whether the results of previous studies on security and trust indicators still remain valid, even in German speaking countries. We analyzed how well the most popular security seals are known. We showed that only 43.75% of the 112 participants knew HTTPS and the oth-

Table 9: Percentage of participants who selected each of the listed trust indicator

Options	Total	Firefox	IE
Too many advertisements	33.0%	33.8%	31.3%
”about us” page does not exist	33.9%	33.8%	34.4%
Loading of the page takes too long	13.4%	13.8%	12.5%
Not possible to log in	23.2%	26.3%	15.6%
The address in the address bar has a typo	67.9%	63.8%	78.1%
There is no seal of approval	21.4%	25.0%	12.5%
Appearance of the webpage does not seem to be right	64.3%	58.8%	78.1%
The address in the address bar is different than the one in the email	53.6%	48.8%	65.6%
The address in the address bar is too long	15.2%	18.8%	6.3%
The address in the address bar is other than the name in the logo	57.1%	55.0%	62.5%
The data transmission is not encrypted with HTTPS	34.8%	43.8%	12.5%
The web browser shows an error message	47.3%	38.8%	68.8%
The displayed webpage is not previously known	39.3%	42.5%	31.3%
The padlock symbol is not closed	25.0%	30.0%	12.5%

ers are less known. Only 35% of the participants stated that they know how to open the SSL certificate information window and 79 of the participants that they never check this information. Only 4.5% could explain properly the difference between basic and EV based HTTPS. For the twelve shown screenshots only 53.2% were in average properly answered with respect to the type of encryption. While people were with an average of 77% able to detect the screenshots without https and only very few could distinguish those screenshots with basic https and EV based HTTPS. 37.5% of the participants did not identify any of the fake webpages and on average 64.96% of the participants would have accessed the known faked pages as usual. There was no significant difference for different categories of web pages or the different type of modifications we applied to the URLs. Furthermore, the study showed that seals do not improve the situation or help the average users. In addition, we showed that trust indicators still differ from the real security indicators.

Since the study shows that the situation has not improved compared to earlier studies, we propose the following steps to support users: Checking URLs is already difficult as shown in Stebila (2010) due to the lack of a standard in domain name patterns. For instance Commerzbank uses www.commerzbanking.de and Deutsche Bank uses meine.deutsche-bank.de. Therefore, a corresponding standard for domain names could improve the situation. One possibility is that every provider gets only one domain per country and the domain name should match the logo. Furthermore it is confusing that most, but not all banks use EV certificates, also do some shops, but most don't. Thus, it should be required (e.g. by law) that service providers, which store or proceed personal data (like banks, shops, online social services) need an EV certificate, thus the user is not required to check the certificate information. In addition, it should be enforced that certification authorities become liable for issuing certificates to unauthorized domains. It would also help integrating the type of service as statement

into the certificates.

Afterwards, it will be necessary to educate people in verifying URLs and to only enter personal data if the connection is secured by HTTPS based on EV. Thus, it is not required to distinguish between basic SSL and EV based HTTPS, but only between EV based and non-EV based HTTPS. In addition, standardized interfaces for all browsers would also help verifying the proper HTTPS encryption.

Seals make a different statement about the web service than HTTPS. Therefore, applying and understanding these also pays off. However, displayed seals need to be automatically verified by browsers, as these icons can also easily be faked. Now, the remaining question is how to implement such steps, as many different parties and disciplines need to be involved.

References

BIDDLE, R. AND VAN OORSCHOT, P. C. AND PATRICK, A. S. AND SOBEY, J. AND WHALEN, T. (2009), Browser interfaces and extended validation SSL certificates: an empirical study, *in* 'Proceedings of the 2009 ACM workshop on Cloud computing security', CCSW '09, ACM, New York, NY, USA, pp. 19 – 30.

DHAMIJA, R. AND TYGAR, J. D. AND HEARST, M. (2006), Why phishing works, *in* 'Proceedings of the SIGCHI conference on Human Factors in computing systems', CHI '06, ACM, New York, NY, USA, pp. 581 – 590.

FUNG, A. P. H. AND CHEUNG, K. W. (2010), SSLock: sustaining the trust on entities brought by SSL, *in* 'Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security', ASIACCS '10, ACM, New York, NY, USA, pp. 204 – 213.

HERZBERG, A. AND JBARA, A. (2008), 'Security and identification indicators for browsers against spoofing and phishing attacks', *ACM Trans. Internet Technol.* 8, pp. 16:1 – 16:36.

JACKSON, C. AND SIMON, D. R. AND TAN, D. S. AND BARTH, A. (2007), An evaluation of extended validation and picture-in-picture phishing attacks, *in* 'Proceedings of FC'07/USEC'07', Springer-Verlag, Berlin, Heidelberg, pp. 281 – 293.

JAKOBSSON, M. (2007), The Human Factor in Phishing, *in* 'Privacy and Security of Consumer Information '07'.

JAKOBSSON, M. AND TSOW, A. AND SHAH, A. AND BLEVIS, E. AND LIM, Y.-K. (2007), What instills trust? a qualitative study of phishing, *in* 'Proceedings FC'07/USEC'07', Springer-Verlag, Berlin, Heidelberg, pp. 356 – 361.

SCHECHTER, S. E. AND DHAMIJA, R. AND OZMENT, A. AND FISCHER, I. (2007), 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'.

SHI, P. AND XU, H. AND ZHANG, X. (L.) (2011), Informing security indicator design in web browsers, *in* 'Proceedings of the 2011 iConference', iConference '11, ACM, New York, NY, USA, pp. 569 – 575.

SOBEY, J. AND BIDDLE, R. AND OORSCHOT, P. C. AND PATRICK, A. S. (2008), Exploring User Reactions to New Browser Cues for Extended Validation Certificates, *in* 'Proceedings of the 13th ESORICS Conference', Springer-Verlag, Berlin, Heidelberg, pp. 411 – 427.

STEBILA, D. (2010), Reinforcing bad behaviour: the misuse of security indicators on popular websites, *in* 'Proceedings of the 22nd Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction', OZCHI '10, ACM, New York, NY, USA, pp. 248 – 251.

TSOW, A. AND JAKOBSSON, M. (2007), Deceit and Deception: A Large User Study of Phishing, Technical report.

WU, M. AND MILLER, R. C. AND GARFINKEL, S. L. (2006), Do security toolbars actually prevent phishing attacks?, *in* 'Proceedings of the SIGCHI conference on Human Factors in computing systems', CHI '06, ACM, New York, NY, USA, pp. 601 – 610.

A Online banking screenshots

Figure 2: Screenshot of the webpage Commerzbank-legitimate

Figure 3: Screenshot of the webpage Deutsche Bank-legitimate

Figure 4: Screenshot of the webpage Hypovereinsbank-fake: typo in the url

B Online social network screenshots

Figure 5: Screenshot of the webpage Facebook-legitimate

Figure 6: Screenshot of the webpage Studivz-fake: subdomain of secure-login.de

Figure 7: Screenshot of the webpage Xing-legitimate

C Shopping screenshots

Figure 8: Screenshot of the webpage Amazon-fake: folder of the einkaufen.de

Figure 9: Screenshot of the webpage Neckermann-fake: false url

D Webpages with login screenshots

Figure 10: Screenshot of the webpage Deka-legitimate

Figure 11: Screenshot of the webpage Epag-legitimate

E Mail screenshots

Figure 12: Screenshot of the webpage Gmx-legitimate

Figure 13: Screenshot of the webpage Web.de-fake: folder of the secure-login.de

F Seals of approval screenshot

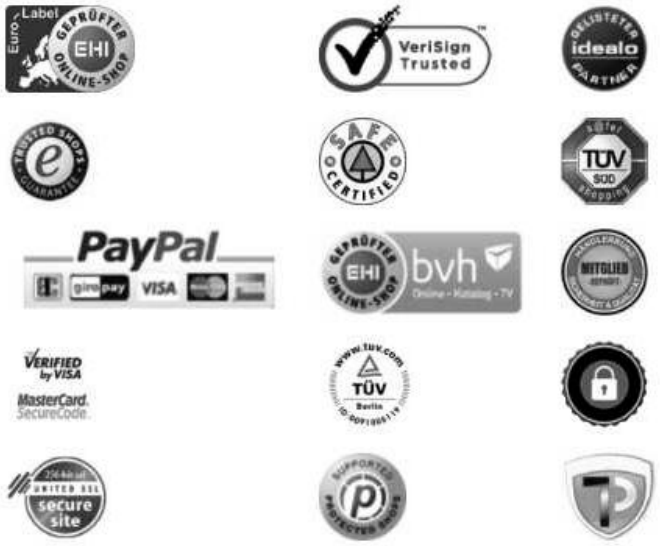

Figure 14: Screenshot of icons of possible seals of approvals for webshop security