The Impact of Security Cues on User Perceived Security in e-Commerce

Samuel N. Smith(✉), Fiona Fui-Hoon Nah, and Maggie X. Cheng

Missouri University of Science and Technology, Rolla, MO, USA
{snsww4, nahf, chengm}@mst.edu

Abstract. Users are expected to assess the level of security of e-commerce websites before conducting online transactions. In this research, we examine user assessment of security of e-commerce web pages based on cues presented on the web pages. A pilot study was conducted in which each subject assessed six e-commerce web pages with varying cues (i.e., HTTP vs. HTTPS, fraudulent vs. authentic URL, padlocks beside fields), and the findings are reported.

Keywords: Security cues · e-commerce · Cybersecurity · Information security

1 Introduction

For more than a decade, the information security research community has cited users as the "weakest link in the security chain" [1, p. 122]. In other words, a highly advanced security system—which typically consists of firewalls, email encryption, etc.—may not be effective at protecting an organization due to unintended behaviors of its users. For example, a robust email encryption software may not benefit an organization if users misuse or fail to use the encryption methods [2]. Hence, it is important to study and understand human factors in information security. Despite continuing research effort in cybersecurity, organizational information security continues to be negatively affected by human factors. In an IBM report titled "2014 Cyber Security Intelligence Index" [3], it was found that of the 109 security incidents IBM investigated for their clients throughout 2013, more than 95 % were found to "recognize 'human error' as a contributing factor" [p. 3]. Hence, we still have a long way to go in understanding and addressing human factors that lead to undesirable user behavior in information security.

In this paper, we are interested in examining user perceptions of security cues in e-commerce. We refer to security cues as elements of a web page interface that are intended to signal information security. For example, an HTTPS (Hypertext Transfer Protocol Secure) connection is indicated in a web browser window and signals to the user that the web page is using a connection which has been verified by a security protocol, typically SSL (Secure Sockets Layers). Although an HTTPS connection is a reliable way of determining web page security, other security cues also exist. For example, some interfaces, such as log-in screens, include images of padlocks within or near submission fields which are used for entering sensitive information (see Fig. 1).

However, the concern with a number of security cues in e-commerce is that they can be fabricated by a website designer and used for malicious purposes, such as

T. Tryfonas (Ed.): HAS 2016, LNCS 9750, pp. 164–173, 2016.
DOI: 10.1007/978-3-319-39381-0_15

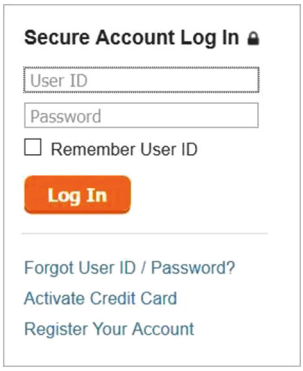

Fig. 1. Padlock displayed near login fields

signaling a false sense of security to lure a user into providing sensitive information, including information associated with a credit card number. Therefore, these cues become questionable or unreliable in certain contexts, such as phishing (i.e., the practice of directing users to fraudulent websites). When a security cue is indeed unreliable or fabricated, we refer to it as a security miscue. Given that information security is essential when conducting e-commerce, it is crucial to gain an understanding of how users assess and respond to various security cues (or miscues) in e-commerce. Hence, our research question is:

"How do users assess and respond to security cues in e-commerce?"

We explored this research question by conducting a pilot study in which subjects evaluated online checkout screens that contained variations in terms of security cues and miscues to determine changes in users' perceptions of e-commerce security. The cues we examined consist of: (1) an HTTP vs. HTTPS connection, (2) an authentic vs. fraudulent URL (Uniform Resource Locator), and (3) padlocks vs. no padlocks displayed next to credit card information input fields.

2 Literature Review

We conducted a review of the literature on related work. Studies show that users are more concerned about the content of a web page (e.g., logos) than the security indicators on a web page [4, 5]. Hence, users become susceptible to fraudulent websites, i.e., phishing websites, whose content appears to be authentic. Previous research has examined the components of phishing and how to prevent users from falling victim to an attack. Dhamija et al. [6] took an experimentation approach by asking subjects to evaluate the security of different websites to determine how accurately the subjects could identify phishing attempts. A large number of phishing websites were undetected by the subjects, due to a lack of knowledge of the workings of computer systems and their associated security systems and indicators [6].

Similarly, Schechter et al. [7] explored the question of whether users would enter their passwords in an e-banking environment where security cues had been added, manipulated, or removed. The cues examined in their research comprise HTTPS indicators, site-authentication images (i.e., images generated by a website to authenticate its security and identity), and browser warning pages found within Internet Explorer 7. The results show that nearly every participant entered their password despite the removal of an HTTPS connection and site-authentication images. More than half entered their password even after being warned by the browser that the web page may not be secure.

Herzberg and Jbara [8] investigated how effectively users could identify fraudulent websites which varied in terms of HTTPS indicators and browser security certificates. In one phase of the testing, they examined browser security add-ons which could be customized by the user to fit their preferences. Their results show that the use of customizable security add-ons led to significantly higher user detection rates of fraudulent websites [8].

3 Methodology

To assess the impact of security cues on user perceived security in e-commerce, a pilot study was designed in which users rate their perceived sense of security, trustworthiness, and safety when viewing e-commerce web pages that contain various security cues and miscues. An e-commerce environment was utilized in the study because it is an online scenario where information security is crucial. The online checkout screen of a popular office supply store, Staples, was slightly modified to provide six different variations for subjects to evaluate in a within-subject experiment.

The original checkout screen did not display fields for payment and billing information until the user had entered their complete shipping information. We wanted to display still images of checkout screens to the user and determine how they perceive the security, trustworthiness, and safety of the web page. Therefore, we modified the original checkout screen to display all relevant input fields that a user would typically encounter when purchasing an item online (see Fig. 2). We also slightly modified the text in the tab near the top of the screen to display “Staples Checkout” since we felt it was more appropriate for the context. In addition, we changed the wording of the shaded checkout header above the input fields to “Shipping and Payment Info” to reflect the displayed input fields.

We manipulated three security cues: connection type (HTTP or HTTPS), the URL (fraudulent or authentic), and whether or not padlocks were displayed next to the credit card information input fields (i.e., these padlocks are miscues or invalid security cues). Although generating all combinations of these three cues would result in 8 variations of the checkout screen ($2 \times 2 \times 2$), we discarded two of them: (1) secure connection (HTTPS) with a fraudulent URL and no padlocks displayed next to input fields, and (2) secure connection (HTTPS) with a fraudulent URL with padlocks displayed next to input fields. We used the insecure connection (HTTP) scenario to assess the effect of a fraudulent vs. authentic URL. Thus, we used a total of 6 variations of the checkout screen (see Table 1). The security cues used in the study are shown in Figs. 3, 4, 5, 6 and 7.

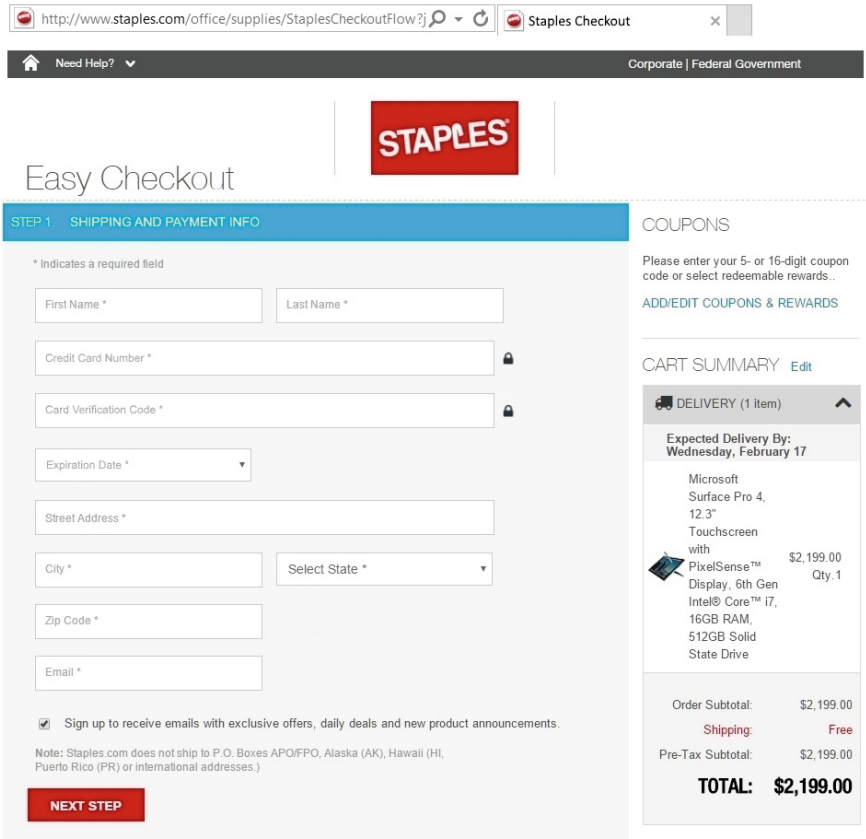

Fig. 2. A checkout screen for the pilot study

Table 1. Checkout screen variations.

1	Unsecure connection (HTTP), phishing URL, no padlocks displayed next to credit card input fields
2	Unsecure connection (HTTP), phishing URL, with padlocks displayed next to credit card input fields
3	Unsecure connection (HTTP), authentic URL, no padlocks displayed next to credit card input fields
4	Unsecure connection (HTTP), authentic URL, with padlocks displayed next to credit card input fields
5	Secure connection (HTTPS), authentic URL, no padlocks displayed next to credit card input fields
6	Secure connection (HTTPS), authentic URL, with padlocks displayed next to credit card input fields

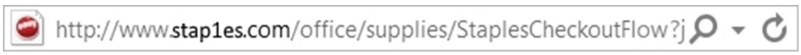

Fig. 3. HTTP connection with a fraudulent URL

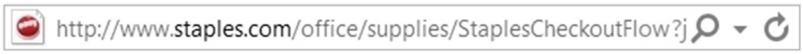

Fig. 4. HTTP connection with an authentic URL

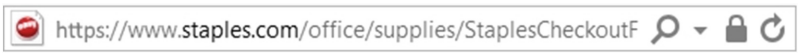

Fig. 5. HTTPS connection with an authentic URL

Fig. 6. Credit card information input fields without added padlocks

Fig. 7. Credit card information input fields with added padlocks outside the fields (miscues)

After examining each checkout screen, the participant was given a set of questions (see Table 2) to answer using a 7-point Likert scale (i.e., 1 = strongly disagree to 7 = strongly agree) to assess the following variables:

1. **Intended Purchase Behavior:** The likelihood that the user would carry out the transaction.
2. **Trust:** The degree to which the user perceives the web page to be trustworthy.
3. **Security:** The degree to which the user perceives the web page to be secure.
4. **Safety:** The degree to which the user perceives the web page to be safe.

After all six checkout screens had been evaluated, the participant was asked to provide demographic information and any open-ended comments or feedback.

Table 2. Measurement of variables.

Variable	Items
Intended Purchase Behavior	1. I would perform the transaction on this web page 2. I would carry out the transaction on this web page 3. I would complete the transaction on this web page
Trust	1. I would enter my personal information into the web page 2. I trust the web page 3. I believe that the web page is trustworthy
Security and Safety	1. The web page appears to be (secure/safe) 2. The web page gives me a sense of (security/safety) 3. I believe that the web page is (secure/safe)

4 Data Collection

Fourteen undergraduate and graduate students were recruited from a Midwestern university to participate in the pilot study. Their ages ranged from 18-34. Of the fourteen subjects, seven were female and seven were male. Upon arrival, each participant was provided with an informational document on the experiment. They were given a scenario in which they had to imagine that they were about to begin a new career and were shopping online to purchase a new laptop. They were told that they would be shown six checkout screens for the laptop and that they would be given a questionnaire after each screen to determine whether or not they would proceed with the online purchase. All subjects viewed the checkout screens in the order listed in Table 1.

5 Findings

In this study, we assessed the effects of (i) HTTP vs. HTTPS connection; (ii) an authentic vs. fraudulent URL; (iii) padlocks vs. no padlocks displayed next to credit card information input fields. We averaged the item responses for the same variable in each condition and used paired t-tests to compare them across different conditions.

To assess the effects of HTTP vs. HTTPS connection, we carried out paired t-tests to compare user responses of:

- Screenshots 4 and 6 (HTTP vs. HTTPS with padlocks displayed next to credit card information input fields)
- Screenshots 3 and 5 (HTTP vs. HTTPS with no padlock displayed next to credit card information input fields)

Table 3 shows the descriptive statistics and paired t-test results for comparisons of screenshots 4 and 6 (HTTP vs. HTTPS with padlocks), whereas Table 4 shows the descriptive statistics and paired t-test results for comparisons of screenshots 3 and 5 (HTTP vs. HTTPS with no padlock).

The results show that when padlocks were displayed next to the credit card fields, subjects perceived the HTTPS connection to offer an increased level of security and

Table 3. Descriptive statistics and paired t-tests for screenshot 4 vs. 6 (HTTP vs. HTTPS with padlocks).

Variable	Mean	Standard deviation	p-value (1-tailed)
Behavior (screen 4)	4.98	1.61	0.07
Behavior (screen 6)	5.50	1.37	($p > 0.05$)
Trust (screen 4)	4.93	1.55	0.05
Trust (screen 6)	5.48	1.33	(marginal)
Security (screen 4)	4.76	1.53	0.03*
Security (screen 6)	5.43	1.31	($p < 0.05$)
Safety (screen 4)	4.90	1.58	0.03*
Safety (screen 6)	5.55	1.34	($p < 0.05$)

* $p < 0.05$

Table 4. Descriptive statistics and paired t-tests for screenshot 3 vs. 5 (HTTP vs. HTTPS with no padlock).

Variable	Mean	Standard deviation	p-value (1-tailed)
Behavior (screen 3)	4.50	1.87	0.15
Behavior (screen 5)	5.14	1.51	($p > 0.05$)
Trust (screen 3)	4.38	1.83	0.14
Trust (screen 5)	5.07	1.48	($p > 0.05$)
Security (screen 3)	4.29	1.87	0.13
Security (screen 5)	5.00	1.47	($p > 0.05$)
Safety (screen 3)	4.38	1.84	0.12
Safety (screen 5)	5.12	1.50	($p > 0.05$)

sense of safety than the HTTP connection (see Table 3). As presented in Table 3, the difference in trust perceptions is marginal and the difference in behavior is not significant. When there were no padlocks displayed next to the credit card fields, subjects did not perceive any difference between the HTTPS connection and the HTTP connection (see Table 4). These results are interesting in that the presence of padlocks next to the credit card fields (i.e., miscues or invalid security cues) sensitized subjects to perceive HTTPS to be safer and more secure than HTTP, but when no padlock was present, subjects did not perceive any difference between HTTPS and HTTP.

To assess the effects of an authentic URL (i.e., staples.com) vs. a fraudulent URL (i.e., staples.com), we conducted paired t-tests to compare user responses of:

- Screenshots 2 and 4 (a fraudulent URL vs. an authentic URL with padlocks displayed next to credit card information input fields)
- Screenshots 1 and 3 (a fraudulent URL vs. an authentic URL with no padlock displayed next to credit card information input fields)

Table 5 shows the descriptive statistics and paired t-test results for comparisons of screenshots 2 and 4 (fraudulent vs. authentic URL with padlocks), whereas Table 6 shows the descriptive statistics and paired t-test results for comparisons of screenshots 1 and 3 (fraudulent vs. authentic URL with no padlock).

Table 5. Descriptive statistics and paired t-tests for screenshot 2 vs. 4 (fraudulent vs. authentic URL with padlocks).

Variable	Mean	Standard deviation	p-value (1-tailed)
Behavior (screen 2)	4.10	2.06	0.03*
Behavior (screen 4)	4.98	1.61	($p < 0.05$)
Trust (screen 2)	4.02	1.98	0.03*
Trust (screen 4)	4.93	1.55	($p < 0.05$)
Security (screen 2)	3.74	1.87	0.02*
Security (screen 4)	4.76	1.53	($p < 0.05$)
Safety (screen 2)	3.98	2.00	0.02*
Safety (screen 4)	4.90	1.58	($p < 0.05$)

* $p < 0.05$

Table 6. Descriptive statistics and paired t-tests for screenshot 1 vs. 3 (fraudulent vs. authentic URL with no padlock).

Variable	Mean	Standard deviation	p-value (1-tailed)
Behavior (screen 1)	4.83	1.62	0.27
Behavior (screen 3)	4.50	1.87	($p > 0.05$)
Trust (screen 1)	4.60	1.75	0.36
Trust (screen 3)	4.38	1.85	($p > 0.05$)
Security (screen 1)	4.29	1.67	0.50
Security (screen 3)	4.29	1.87	($p > 0.05$)
Safety (screen 1)	4.56	1.86	0.39
Safety (screen 3)	4.38	1.84	($p > 0.05$)

The results show that when padlocks were displayed next to the credit card fields, subjects were able to distinguish between the fraudulent vs. authentic URL in all aspects assessed, i.e., e-commerce purchase behavior (i.e., transact or not), trust, security and sense of safety (see Table 5). When there were no padlocks displayed next to the credit card fields, subjects did not perceive any difference between the fraudulent and authentic URL (see Table 6). These results are interesting in that the presence of padlocks next to the credit card fields (i.e., miscues or invalid security cues) sensitized subjects to become more cautious in identifying fraudulent vs. authentic URLs to avoid phishing whereas subjects did not perceive the security of fraudulent vs. authentic URLs differently when there was no padlock.

To assess the effects of padlocks vs. no padlocks displayed next to credit card information input fields, we conducted paired t-tests to compare user responses of:

- Screenshots 5 and 6 (padlocks vs. no padlocks with HTTPS connection)
- Screenshots 3 and 4 (padlocks vs. no padlocks with HTTP connection)

Table 7 shows the descriptive statistics and paired t-test results for comparisons of screenshots 5 and 6 (padlocks vs. no padlocks with HTTPS connection) whereas Table 8 shows the descriptive statistics and paired t-test results for comparisons of screenshots 3 and 4 (padlocks vs. no padlocks with HTTP connection).

Table 7. Descriptive statistics and paired t-tests for screenshot 5 vs. 6 (padlocks vs. no padlocks with HTTPS).

Variable	Mean	Standard deviation	p-value (1-tailed)
Behavior (screen 5)	5.14	1.51	0.14
Behavior (screen 6)	5.50	1.37	($p > 0.05$)
Trust (screen 5)	4.07	1.48	0.10
Trust (screen 6)	5.48	1.33	($p > 0.05$)
Security (screen 5)	5.00	1.47	0.08
Security (screen 6)	5.43	1.31	($p > 0.05$)
Safety (screen 5)	5.12	1.50	0.08
Safety (screen 6)	5.55	1.34	($p > 0.05$)

Table 8. Descriptive statistics and paired t-tests for screenshot 3 vs. 4 (padlocks vs. no padlocks with HTTP).

Variable	Mean	Standard deviation	p-value (1-tailed)
Behavior (screen 3)	4.83	1.87	0.10
Behavior (screen 4)	4.50	1.61	($p > 0.05$)
Trust (screen 3)	4.60	1.85	0.06
Trust (screen 4)	4.38	1.55	($p > 0.05$)
Security (screen 3)	4.29	1.87	0.07
Security (screen 4)	4.29	1.53	($p > 0.05$)
Safety (screen 3)	4.56	1.84	0.08
Safety (screen 4)	4.38	1.58	($p > 0.05$)

Subjects did not perceive any difference between having padlocks and not having any padlock next to the credit card fields, regardless of whether the URL indicated HTTPS or HTTP connection. The results are consistent with actual security because padlocks next to the credit card fields do not change or enhance actual security.

Overall, our findings suggest that displaying padlocks next to the credit card fields sensitized subjects to look for other security cues in assessing security. Even though the display of padlocks by themselves did not change users' perceived sense of security, they changed users' sensitivity to security cues.

6 Discussion and Conclusions

Our findings are interesting in that user perceptions of the security of a connection (HTTP vs. HTTPS) and the detection of fraudulent vs. authentic e-commerce websites are moderated by fabricated padlocks displayed next to input fields. We did not expect such findings. Padlocks displayed in the body of a web page do not affect the security of that web page; they are simply images that any web designer can place into a web page. However, they primed our subjects to look for important security cues (i.e., HTTP vs. HTTPS and authenticity of the URL). Even though these padlocks do not increase security, they help to sensitize subjects to important security cues. However, four of the fourteen subjects specifically mentioned that the padlocks next to the credit card fields

increased their sense of security. As one participant noted, "The locks next to some fields make it seem like it goes further to protect your security." The perceptions that these padlocks have created for these subjects could pose a serious problem since padlocks in the body of the web page are unreliable security cues, i.e., miscues, that can be easily fabricated for malicious purposes. Also, three out of fourteen subjects mentioned that they use online website reviews when deciding whether or not a web page is secure. It would be intriguing to further examine the degree to which users trust online website reviews when evaluating the security of a web page.

There are several limitations in this pilot study. Since we used a fixed order of screenshots in the study, there could be an ordering effect. As subjects progressed through the screenshots and noticed differences between them, they may have learned to become more proficient in assessing the security of web pages based on these cues. For example, it is possible that the increases in the degrees to which subjects perceived the web pages to be trustworthy, secure, and safe were the results of exposure bias to the checkout screens. Since we only had a small sample size in this pilot study, it was not feasible to include variations in the order of checkout screens to entirely rule out the possibility of ordering effects. This pilot study was carried out to explore user perceptions of basic security cues, and to help us refine the experimental procedures for the full-scale study. In our full-scale study, we will address the above issues by counterbalancing the order of screenshots and using a sample size that provides good statistical power.

Acknowledgements. This research is supported by National Science Foundation grant CNS/1537538 and the Laboratory for Information Technology at Missouri University of Science and Technology.

References

1. Sasse, M., Brostoff, S., Weirich, D.: Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security. BT Technol. J. **19**(3), 122–131 (2001)
2. Whitten, A., Tygar, J.D.: Why Johnny can't encrypt: a usability evaluation of PGP 5.0. In: Proceedings of the 8th USENIX Security Symposium, pp. 169–184 (1999)
3. IBM Corporation: IBM Security Services 2014 Cyber Security Intelligence Index, pp. 1–12. IBM Global Technology Services, Somers, NY (2014)
4. Kauer, M., Pfeiffer, T., Volkamer, M., Theuerling, H., Bruder, R.: It is not about the design—it is about the content! making warnings more efficient by communicating risks appropriately. In: Proceedings of the 6th Annual Conference of the Department of Security and of the Society for Computer Science, pp. 187–198 (2012)
5. Darwish, A., Bataineh, E.: Eye tracking analysis of browser security indicators. In: International Conference on Computer Systems and Industrial Informatics, pp. 1–6 (2012)
6. Dhamija, R., Tygar, J.D., Hearst, M.: Why phishing works. In: Conference on Human Factors in Computing Systems, pp. 581–590 (2006)
7. Schechter, S., Dhamija R., Ozment, A., Fischer, I.: The emperor's new security indicators. In: IEEE Symposium on Security and Privacy, pp. 51–65 (2007)
8. Herzberg, A., Jbara, A.: Security and identification indicators for browsers against spoofing and phishing attacks. ACM Trans. Internet Technol. **8**(4), 1–36 (2008). Article 16