“It builds trust with the customers” - Exploring User Perceptions of the Padlock Icon in Browser UI

Emanuel von Zezschwitz
Google Inc.
zezschwitz@chromium.org

Serena Chen
Google Inc.
sereeena@chromium.org

Emily Stark
Google Inc.
estark@chromium.org

***Abstract*—We performed a large-scale online survey (n=1,880) to study the padlock icon, an established security indicator in web browsers that denotes connection security through HTTPS. In this paper, we evaluate users' understanding of the padlock icon, and how removing or replacing it might influence their expectations and decisions. We found that the majority of respondents (89%) had misconceptions about the padlock's meaning. While only a minority (23%-44%) referred to the padlock icon at all when asked to evaluate trustworthiness, these padlock-aware users reported that they would be deterred from a hypothetical shopping transaction when the padlock icon was absent. These users were reassured after seeing secondary UI surfaces (i.e., Chrome Page Info) where more verbose information about connection security was present.**

We conclude that the padlock icon, displayed by browsers in the address bar, is still misunderstood by many users. The padlock icon guarantees connection security, but is often perceived to indicate the general privacy, security, and trustworthiness of a website. We argue that communicating connection security precisely and clearly is likely to be more effective through secondary UI, where there is more surface area for content. We hope that this paper boosts the discussion about the benefits and drawbacks of showing passive security indicators in the browser UI.

***Index Terms*—usable security, padlock, browser, security indicators, user perception**

I. Introduction

HTTPS is the fundamental cryptographic protocol used to provide connection security on the web [1]. Over the past years, HTTPS-support has proliferated[1] and nowadays most websites provide HTTPS to ensure data integrity and privacy between the communicating parties.

Most browsers show a padlock icon near the address bar to indicate connection security (see Figure 1, left). However, previous research has revealed that such icons are often neglected [2] and that the actual meaning of security indicators is not always obvious [3]. In fact, seeing a padlock is sometimes understood as a sign for general security and trustworthiness [4], [5]. This introduces the risk that users expect higher levels of protection that are not justified since a padlock does not guarantee that a site will behave in the user's best interest (for example, a phishing or malware site which uses HTTPS [6]). Such misconceptions challenge the benefit of showing the padlock as a passive security indicator. Indeed, in 2018, Google already announced plans to eventually remove secure indicators for HTTPS pages in Chrome[2].

To quantify the impact of modifying such established browser UI, we conducted the first large-scale online survey ($n = 1,880$) to systematically evaluate user perceptions of the padlock and modified iconography in a simulated encounter with an unfamiliar online shop. We designed different variations (see Figure 1) based on the most popular browser (i.e., Chrome) and tested the effects of replacing or removing the padlock icon. Our user study confirmed that the majority of users have misconceptions about the padlock's meaning, since only 11% of the respondents had exclusive expectations on connection security and it revealed opportunities to optimize browsers for better discoverability of secondary UI.

In this paper, we present the results of the online survey and discuss implications for the design of modern web browsers. Our results may not generalize to real-world browsing, since, for example, users may be more likely to contemplate the padlock icon when prompted to make a trust decision in a survey than in a naturalistic scenario. However, we believe that our results provide important up-to-date insights into users' perceptions and beliefs regarding the padlock icon. We hope that this paper provokes discussion about the benefits and drawbacks of showing passive security indicators in a HTTPS-enabled ecosystem, as it highlights the limitations of communicating fine-grained security information via simple iconography.

II. Related Work

In 2002, Friedman et al. [3] claimed that the padlock icon is a suboptimal choice to communicate connection security since it rather conveys “the idea of a 'place' that can be made secure” than data protection in transit. They concluded that the design of web browsers needs to be optimized in a way that helps users to better understand the accurate meaning of connection security.

Indeed, various studies [4]–[10] have indicated that users often misunderstand the meaning of the padlock icon. Ruoti et al. [8] performed an interview study and found that such misconceptions can foster insecure behavior (e.g., ignoring TLS warnings). Based on the observation that the padlock

[1] transparencyreport.google.com/https/overview accessed: 2022/02/28

[2] blog.chromium.org/2018/05/evolving-chromes-security-indicators.html accessed: 2022/02/28

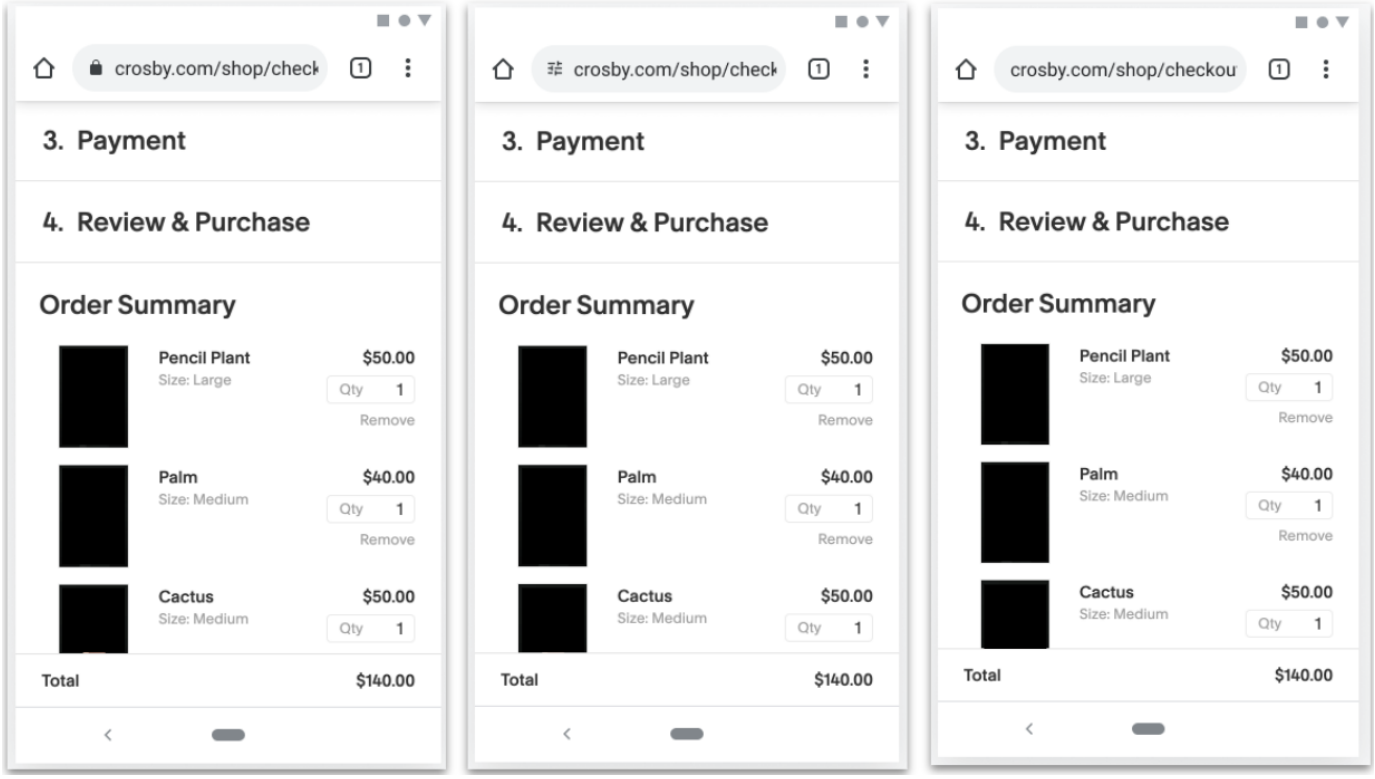

Fig. 1. The prototypes of the *Mobile* condition [*product images obfuscated*]. We tested three levels of *iconography*: padlock (left), tune (center), and no icon (right). Figure 3 (right) provides an example of the UI used in the *Desktop* condition.

icon was often perceived as an indicator for general safety of a website, they concluded that increasing user attention towards the padlock may be even counterproductive and put users at risk. In line with this finding, Ma et al. [6] found that more participants clicked on email phishing links or entered passwords on phishing sites when HTTPS-indicators were shown and concluded that the false perception of trustworthiness leads to "a fundamental divide between what users consider to be secure and the security actually provided by HTTPS." Recently, Spero and Biddle [9] argued that the padlock icon is incapable of communicating the complexity of connection security and suggested that software products need to increase the visibility of security information and communicate it in a way that is easier to understand.

Previous work [7], [11], [12] has shown that many users focus on the content of a web page to understand its credibility and that the padlock is one of many trust signals users can use when evaluating the trustworthiness of a site [12]. Schechter et al. [13] performed a qualitative study to test the impact of removing passive security indicators during simulated online banking tasks. They found that all participants entered their passwords and completed the task even when the padlock icon and the HTTPS-prefix were not shown in the browser. Dhamija et al. [7] tested the effectiveness of phishing sites and found that 32% of the participants referred to the padlock icon when making trust decisions. Whalen and Inkpen [14] performed an eyetracker study to investigate which security indicators are typically noticed by users. They found that participants actually looked at the padlock but often ignored its interactive capability. Over a decade later, Stojmenoviæ and Biddle [10] confirmed that users often don't know that the padlock is clickable. Stebila [15] argue that the misuse of security indicators (e.g., showing a padlock icon in the content area) can train users to ignore such signals in practice. Finally, Thompson et al. [16] argued that passive security indicators like the padlock do not effectively help users to make security decisions and that negative, active indicators like warnings would be more promising.

The work presented in this paper complements the findings of previous research. We conducted the first large-scale ($n = 1,880$) study to systematically investigate how the presence or absence of the padlock influences users' trust decisions. We evaluated user perceptions of the padlock in a simulated encounter with an unfamiliar but legitimate online shop and tested the effects of removing or replacing the padlock icon in the browser UI. While we confirmed that the majority of users overestimates the security promises by the padlock, we extend the previous work by showing the reassuring effects of presenting security information in a secondary UI surface of the browser. Our findings indicate that replacing the padlock with a more neutral icon that communicates interactivity can be a promising way to 1) avoid displaying passive security indicators in secure-by-default states and 2) guide users to more verbose page information when making trust decisions.

III. Methodology

We conducted a between-groups survey study ($n = 1,880$). The survey was implemented in Qualtrics[3] and distributed via clickworker.com[4]. The median duration time for the survey was 347 seconds, all respondents were compensated with $0.85. To be eligible, respondents needed to be US-based, have a minimum age of 18, and provide informed consent. We screened out 319 participants who failed the attention check and respondents who did not use Chrome over the past week (self-reported). We followed our institution's guidelines for survey research. All respondents provided informed consent ahead of the survey and we did not collect any Personally Identifiable Information (PII). Figure 2 provides an overview of the procedure.

Conditions and Assignments

We tested three different levels (see Figure 1) of *iconography*: padlock (baseline), no icon (remove padlock), tune icon (replace padlock). In addition, we simulated a mobile *environment* and a desktop environment (2 levels, see Figure 3) resulting in overall six conditions. Respondents were assigned to the mobile or desktop condition based on the self-reported use of the respective platform. *Iconography* was randomly assigned.

Procedure

After passing the attention check, eligible respondents answered the survey based on a series of different scenarios.

Visual Inspection We simulated a visual inspection of the web site by asking *"Please review the web page and tell us how you would rate the trustworthiness and the security of the web shop without clicking."* Answers were collected on three Likert-scale items ranging from strongly disagree to strongly agree: *"The web shop seems trustworthy," "The web shop seems secure,"* and *"I would probably continue with my order."* In addition, we asked participants to share in a few words how they *" assessed the trustworthiness and security."*

Information Seeking We asked participants to imagine *"that the visual inspection was not enough to understand the security and trustworthiness of the web shop."* They were instructed to "[..] click on the region that you would usually click to learn more about the trustworthiness and the security of the web shop."

Secondary browser UI We showed participants an image of the Chrome page information surface. *"If you clicked the lock icon [..][5], you would see the following screen (see Figure 3). Please indicate the information (if any) that would help you most to make a purchase decision (i.e., continue or cancel the order).*" We collected click-patterns and asked the same three Likert-scale questions about trustworthiness and security.

[3]qualtrics.com accessed: 2022/02/17

[4]clickworker.com accessed: 2022/02/17

[5]Clicking in the padlock icon in Chrome opens a secondary UI surface with security information and other controls (e.g., cookies). The surface is called Page Info.

While the data was collected based on 5-point Likert-scales, we later transformed the ordinal data to nominal signals to emphasize the perception of trustworhiness and security. We coded agree and strongly agree as "agreed" and the rest of the data as "not agreed" before running statistical tests.

Participants

Eligible participants were based in the US and between 18-64 years old (both factors were controlled by clickworker.com). In addition, respondents needed to report use of Chrome for at least one day over the past week. We collected 1,880 valid responses (sample sizes per condition varied slightly 295-330). Most (62%) respondents reported to use Chrome on a daily basis, 8% of the participants used Chrome only on mobile devices, 9% of the participants reported to use Chrome only on desktop devices.

IV. Results

In this section, we present the results of our survey. We focus on the perception of the padlock, the perception of removing or replacing the padlock, and the effects of showing the Page Info surface (secondary browser UI).

A. Padlock Expectations

At the end of the survey, we showed all participants the padlock and asked them to indicate the perceived meaning of the icon using a multiple choice question. The results are shown in Figure 4. The majority of the respondents (74%) indicated that "the website is secure." 70% mentioned that "the connection to the website is secure." 51% would expected that "it is safe to enter data on this web site." 30% of the respondents who indicated that "the website is secure" also expected that "The web site respects my privacy." Only 27% of the respondents who indicated that "the website is secure" indicated that "the connection to the website is secure." Categorizing the reported expectations shows that only 11% of the users expected exclusively connection security (i.e., target meaning). However, 59% of the users would expect connection security among other promises. Finally, 30% of the respondents did not expect connection security but other levels of protection (like phishing protection). Focusing on the target meaning of the padlock, we conclude that 11% were obviously well-informed, 59% tended to be over-confident, and 30% were misinformed. The feedback we collected during the study confirms that the padlock was often interpreted as a more universal trust signal. For example, one respondent highlighted that *"the padlock image in the URL suggests that the site is secure for e-commerce."* Such misconceptions can put users at risk as they lead to a false sense of security.

B. Visual Inspection

In the first part of the survey, the respondents reviewed the illustrated web shop (see Figure 5) and rated its trustworthiness and security. Since a Mann–Whitney U test did not indicate any significant differences ($p > .05$) between the *environments*, we will focus on the impact of *iconography*. To identify

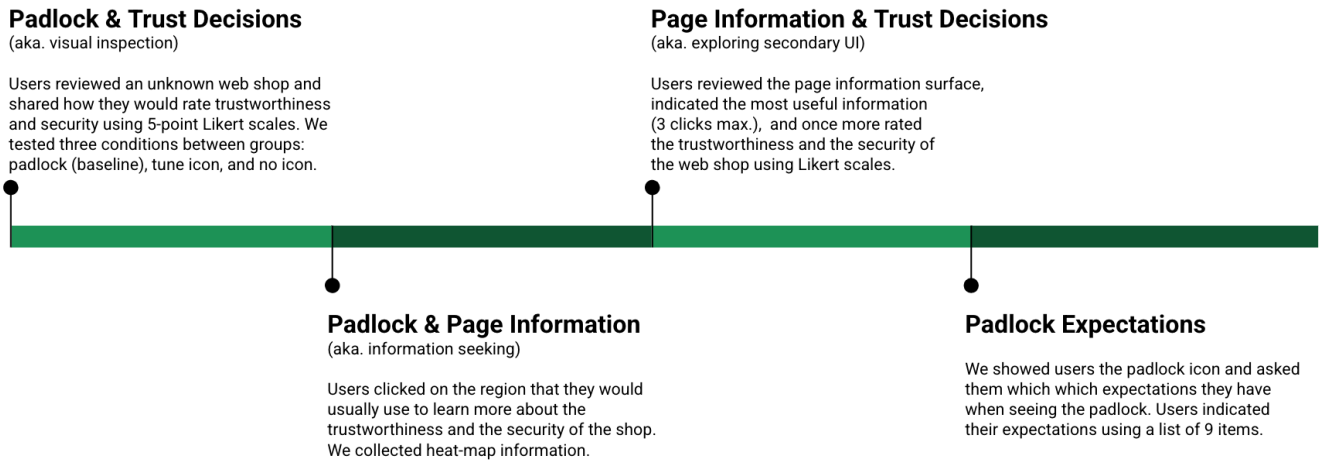

Fig. 2. The survey was based on a between-group design. The participants reviewed static mocks and provided feedback in free-text forms and via 5-point Likert scales.

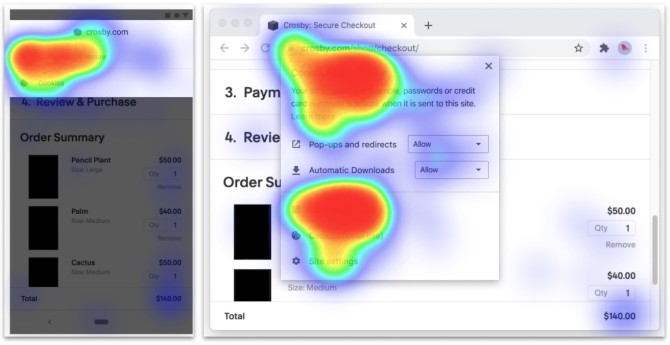

Fig. 3. The mobile prototype (left) and the desktop prototype (right) of the padlock condition [*product images obfuscated*]. After the review of the web shop, we showed the Page Info (secondary browser UI) which pointed out that the "connection is secure." The shown heat-maps represent the click patterns of respondents who were asked to indicate any information which was perceived helpful in the scenario.

padlock-aware users, we reviewed all free text responses and manually tagged the instances where the security indicator was mentioned. Since we were only focusing on one aspect (i.e., padlock references) and since most participants referred to the padlock as "lock," "padlock," or "security icon," we were able to perform a simplified content analysis where one researcher went through all responses. We asked the respondents to evaluate the website's trustworthiness and evaluated the weight of the padlock icon. Across conditions, the majority of the respondents did not refer to the padlock icon while evaluating the trustworthiness of the website. In the baseline condition, where the padlock icon was present, 44% mentioned it. When it was replaced, 23% mentioned the absence of the security indicator. When the padlock was removed, 26% mentioned the absence while making trust decisions.

Most respondents referred to the look and feel of the web shop, its structure, or the actual content:*"It looks professional enough to have adequate security."* Across conditions, only a subset of users (6%) mentioned the absence of a warning as an important signal.

Baseline Condition - Showing the Padlock

In the baseline condition, 74% of the respondents indicated that they would probably continue their order. A complete content analysis of the free-text responses revealed that 52% of them mentioned the presence of the padlock when justifying their assessment.

Comparing the respondents who mentioned the padlock and to those who did not, we found that the first group reported significantly more often that they would continue with their order (89% vs. 63%, $\chi^2(1, N = 633) = 57, p < .001$). In addition, we found that those users who 1) had misconceptions about the padlock's meaning and 2) mentioned the padlock during the visual inspection, were significantly more likely to agree that "the web shop seems trustworthy" than users who mentioned the padlock but had a correct understanding of the icon (88% vs. 75%, $\chi^2(4, N = 566) = 60, p < .001$). The quote of one participant illustrates the overconfidence some users have when seeing the padlock: *"the website has the lock security icon by the website name. It builds trust with the customers."*

Replacing the Padlock

When a tune icon was present, significantly fewer respondents (53% vs. 74% in the baseline condition) agreed that they "would probably continue with [their] order" ($\chi^2(1, N = 1255) = 64, p < .001$). While 23% of all respondents in this condition mentioned the absence of the padlock when justifying their assessment, only 21% of those users who referred to the padlock would proceed with their order. This suggests that the absence of a passive security indicator could negatively impact users' transactions in real-world browsing: *"This website isn't trustworthy because there isn't a lock symbol before the URL."* Respondents who thought less critically

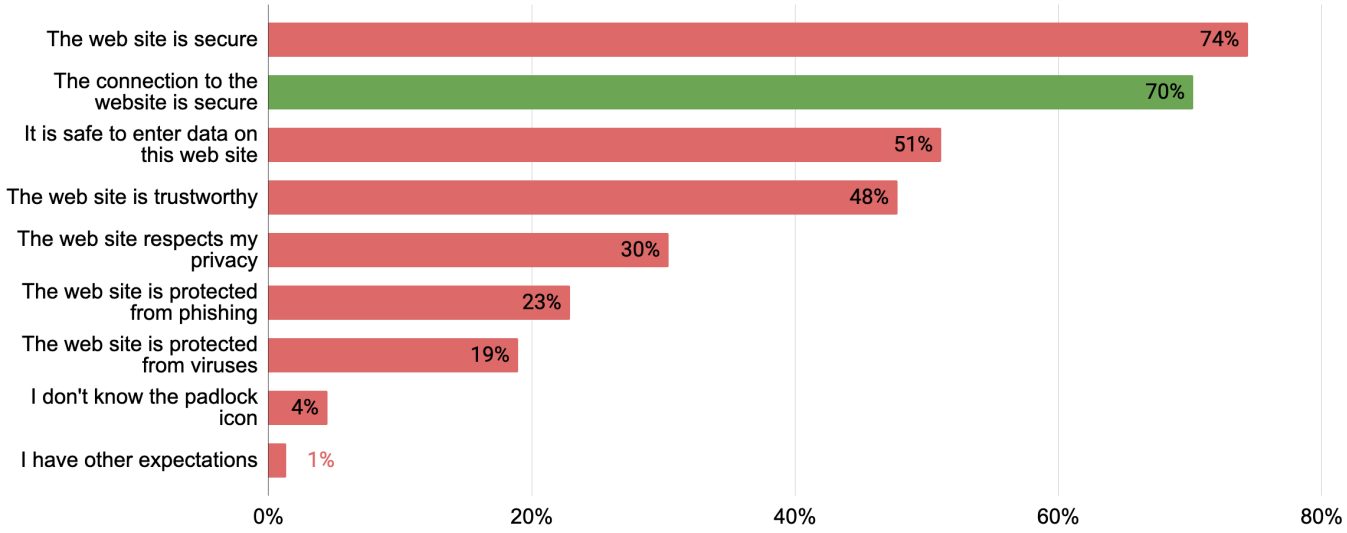

Fig. 4. The respondents were asked to indicate the meaning of the padlock [multiple choice]. While 70% would expect connection security, most of them expected more than one security promise. Indeed, only 11% of the respondents reported connection security as their only expectation (not represented in the figure).

about the absence of the padlock often relied on other factors: *"I see that the web address doesn't have the lock icon on it, but the website looks nice and expensive [..]."*

Removing the Padlock

With no icon being present, 50% of the respondents indicated that they would continue with their order. Compared to the baseline condition (74%), users in the "no icon"-condition were less likely to proceed ($\chi^2(1, N = 1258) = 86, p < .001$). 27% of the respondents in this condition mentioned the absence of padlock: *"It doesn't seem to be secure since I don't see a lock in the address bar. That makes it slightly less trustworthy but doesn't necessarily rule it out."* Again, users who referred to the absence of the padlock were significantly less likely to report that they would proceed with their purchase than users who did not mention the padlock icon (17% vs. 61%, $\chi^2(1, N = 625) = 96, p < .001$).

C. Information Seeking

In the next scenario, we asked users to imagine that the visual inspection was not sufficient. The participants were prompted to indicate where they would click to get more information about the security and the trustworthiness of the website. We analyzed the participants' click-patterns.

Baseline Condition

While the padlock icon was the most frequently clicked element[6] in the baseline condition (50% clicked on the padlock), the data suggests that half of the users would visit other areas of the screen to learn more about the website. Independent from the *environment*, only a minority (6%) of the users would review the URL, 7% (desktop) to 11% (mobile) would visit the overflow menu of Chrome. Besides such Chrome surfaces, reviewing web content (14%) and visiting external sites (8%) were further important sources of truth for the respondents. The majority of users (81%) who mentioned the padlock during the visual inspection also clicked on it to get further information. In contrast, only 26% of the respondents who did not mention the padlock clicked on it. This indicates that the general awareness for the padlock is an important factor when it comes to finding this secondary security-UI.

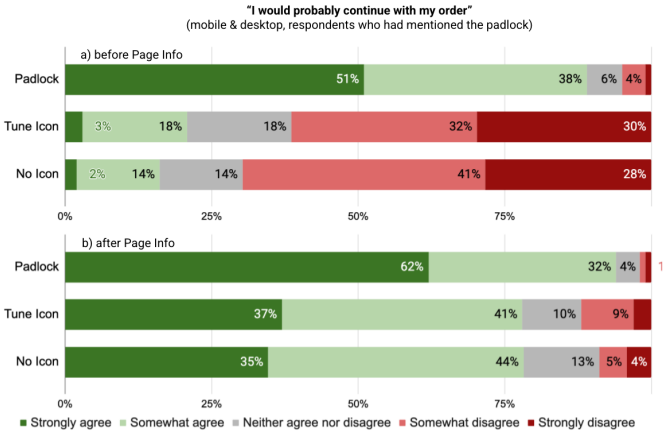

Fig. 5. The respondents rated the web shop (a) after the visual inspection and (b) after reviewing the secondary browser UI (i.e., page Info). Showing the security information in the secondary browser UI was reassuring across conditions. This figure illustrates the impact on users who mentioned the padlock during visual inspection.

[6]Clicking on the padlock icon does show the Page Info which provides site-related information. On Chrome mobile, the Page Info is additionally accessible via overflow menu (i.e., the three dots).

Replacing the Padlock

With the tune icon being present, the ratio of users who clicked the icon significantly decreased from 50% to 40% ($\chi^2(1, N = 1255) = 12, p < .001$). Assuming that mobile users would be able to discover the Page Info via the overflow menu, we find discoverability rates between 42% (desktop) and 52% (mobile) when the tune icon is displayed. Respondents who referred to the absence of the padlock icon before were more likely to click on tune than users who did not mention the padlock (65% vs. 32%, $\chi^2(1, N = 622) = 51, p < .001$). This indicates that padlock-aware users have a higher chance to discover the secondary browser UI even when a tune icon is shown. In addition, the fact that 32% (versus 26% in the baseline condition) of the users who did not mention the padlock actually clicked on the tune icon to evaluate the security and the trustworthiness of the website indicates a slightly better click-affordance for users who are not aware of the padlock as an entry point to site-related security information.

Removing the Padlock

Compared to both other conditions, removing the padlock icon led to a significantly reduced discoverability of the page information surface even if we assume that the surface would also be accessible via overflow menu (39% vs. 51% (tune and baseline), $\chi^2(2, N = 1,880) = 166, p < .001$). 16% of the respondents still clicked into the (empty) original icon region near the address bar. Another 23% clicked on the overflow menu to learn more about the web shop. Assuming that users on both platforms would be able to discover the Page Info via the menu and the address bar, leads to theoretical discoverability rates between 36% (desktop) and 42% (mobile). Even without the visual access point, 36% of the respondents who mentioned the absence of the padlock icon clicked on the icon region to get further information. In contrast, only 9% of the users who did not refer to the padlock icon did the same. It is worth noting that the motivation to explore this browser region can be expected to fade over time if no visual entry point is present.

D. Secondary Browser UI - Page Information

In the last scenario, the respondents saw the page information surface and indicated up to three areas which are important to make trust decisions (see Figure 3). Afterwards, they reassessed the security and trustworthiness of the webshop using the 5-point Likert scales. In the desktop conditions, the certificate info (30%), the TLS header (23%), and the TLS info text (13%) were most frequently indicated as helpful information. Despite being perceived as an important cue, the written feedback indicated that certificates are not well understood. Most respondents mentioned them as generally "security related." In the mobile condition, the TLS info (49%), the cookie information (21%), and the embedded padlock icon (19%) were perceived as important signals.

Across conditions, Wilcoxon signed-rank tests indicate that showing the secondary browser UI did significantly increase the likelihood to proceed with a purchase. Focusing on the users who mentioned the padlock during the assessment (see Figure 5) reveals that +5pt in the baseline condition ($94\%, Z = -4.870, p < 0.001$), +57pt in the tune condition ($78\%, Z = -9.096, p < 0.001$), and +62pt in the "no icon"-condition ($78\%, Z = -10.170, p < 0.001$) agreed that they would probably continue the order: *"I am not familiar with that icon [tune], however clicking on the icon and reading the result did give me more confidence in purchasing."*

V. Discussion and Conclusion

We performed the first large-scale online survey ($n = 1,880$) to systematically investigate users' understanding of the padlock icon and to evaluate the impact of modifying this established browser UI. The participants reviewed an unfamiliar web shop and rated the perceived trustworthiness and security using 5-point Likert scales. The results indicated that the majority of users have misconceptions about the meaning of the padlock. This confirms prior findings [4], [5], [8] and shows that it is challenging to communicate fine-grained information via iconography [9], [17].

In our survey, only a subset of respondents (23%-44%) actually referred to the padlock (absence or presence) when asked to evaluate trustworthiness. Nevertheless, users who noted the absence of this established security indicator often reported that it would change their decision to proceed with their order. This indicates that removing the padlock from the address bar may indeed unsettle users and raise concerns even on legitimate web sites. However, as soon as the users saw security information on the Page Info surface, they were reassured and significantly increased their trust ratings. Browser designers should therefore prioritize secondary UI discoverability if looking to remove or replace the padlock. As shown in our survey, modified iconography can be used to increase click affordance.

A limitation of our survey study is that our numeric results may not apply to real-world browsing behaviors. We suspect that, in real browsing, people are less likely to contemplate the lock icon or even make conscious trust decisions at all compared to when they are prompted to contemplate website trustworthiness in a survey. In addition, users in a real shopping scenario may be more motivated and thus more likely to proceed with their order even in the absence of a padlock. Still, our results provide insight into users' beliefs and reactions to security iconography when they do evaluate website trustworthiness.

Future work could report on recent field experiments[7] using browser telemetry to explore how removing or replacing the padlock icon in the address bar affects real-world browsing behavior. Another area of future work is to explore good candidates for replacing the padlock. Ideally, a new icon would have a strong affordance to be clickable and thus help users to discover the secondary UI when in need.

[7]https://blog.chromium.org/2021/07/increasing-https-adoption.html, https://www.neowin.net/news/microsoft-might-replace-the-https-lock-icon-in-the-edge-address-bar-to-avoid-confusion/ accessed: 2022/02/28

REFERENCES

[1] A. P. Felt, R. Barnes, A. King, C. Palmer, C. Bentzel, and P. Tabriz, "Measuring {HTTPS} adoption on the web," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1323–1338.

[2] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, 2007, pp. 51–65.

[3] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum, "Users' conceptions of web security: A comparative study," in *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '02. New York, NY, USA: Association for Computing Machinery, 2002, p. 746–747. [Online]. Available: https://doi.org/10.1145/506443.506577

[4] A. P. Felt, R. W. Reeder, A. Ainslie, H. Harris, M. Walker, C. Thompson, M. E. Acer, E. Morant, and S. Consolvo, "Rethinking connection security indicators," in *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, 2016, pp. 1–14.

[5] K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. von Zezschwitz, "" if https were secure, i wouldn't need 2fa"-end user and administrator mental models of https," in *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019, pp. 246–263.

[6] Z. Ma, J. Reynolds, J. Dickinson, K. Wang, T. Judd, J. D. Barnes, J. Mason, and M. Bailey, "The impact of secure transport protocols on phishing efficacy," in *12th {USENIX} Workshop on Cyber Security Experimentation and Test ({CSET} 19)*, 2019.

[7] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*, 2006, pp. 581–590.

[8] S. Ruoti, T. Monson, J. Wu, D. Zappala, and K. Seamons, "Weighing context and trade-offs: How suburban adults selected their online security posture," in *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)*, 2017, pp. 211–228.

[9] E. Spero and R. Biddle, "Out of sight, out of mind: Ui design and the inhibition of mental models of security," in *New Security Paradigms Workshop 2020*, 2020, pp. 127–143.

[10] M. Stojmenoviæ and R. Biddle, "Hide-and-seek with website identity information," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018, pp. 1–6.

[11] B. J. Fogg, J. Marshall, O. Laraki, A. Osipovich, C. Varma, N. Fang, J. Paul, A. Rangnekar, J. Shon, P. Swani *et al.*, "What makes web sites credible? a report on a large quantitative study," in *Proceedings of the SIGCHI conference on Human factors in computing systems*, 2001, pp. 61–68.

[12] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, and Y.-K. Lim, "What instills trust? a qualitative study of phishing," in *International Conference on Financial Cryptography and Data Security*. Springer, 2007, pp. 356–361.

[13] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, "The emperor's new security indicators," in *2007 IEEE Symposium on Security and Privacy (SP'07)*. IEEE, 2007, pp. 51–65.

[14] T. Whalen and K. M. Inkpen, "Gathering evidence: use of visual security cues in web browsers," in *Proceedings of Graphics Interface 2005*. Citeseer, 2005, pp. 137–144.

[15] D. Stebila, "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*, 2010, pp. 248–251.

[16] C. Thompson, M. Shelton, E. Stark, M. Walker, E. Schechter, and A. P. Felt, "The web's identity crisis: understanding the effectiveness of website identity indicators," in *28th {USENIX} Security Symposium ({USENIX} Security 19)*, 2019, pp. 1715–1732.

[17] H. Habib, Y. Zou, Y. Yao, A. Acquisti, L. Cranor, J. Reidenberg, N. Sadeh, and F. Schaub, "Toggles, dollar signs, and triangles: How to (in) effectively convey privacy choices with icons and link texts," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, pp. 1–25.