Rethinking Connection Security Indicators

Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, and Max Walker, *Google;* Christopher Thompson, *University of California, Berkeley;* Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo, *Google*

https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

This paper is included in the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016).

June 22–24, 2016 • Denver, CO, USA

ISBN 978-1-931971-31-7

Open access to the Proceedings of the Twelfth Symposium on Usable Privacy and Security (SOUPS 2016) is sponsored by USENIX.

Rethinking Connection Security Indicators

Adrienne Porter Felt[1], Robert W. Reeder[1], Alex Ainslie[1], Helen Harris[1], Max Walker[1],
Christopher Thompson[2], Mustafa Emre Acer[1], Elisabeth Morant[1], Sunny Consolvo[1]
Google[1], UC Berkeley[2]
security-enamel@chromium.org[1], cthompson@cs.berkeley.edu[2]

ABSTRACT

We propose a new set of browser security indicators, based on user research and an understanding of the design challenges faced by browsers. To motivate the need for new security indicators, we critique existing browser security indicators and survey 1,329 people about Google Chrome's indicators. We then evaluate forty icons and seven complementary strings by surveying thousands of respondents about their perceptions of the candidates. Ultimately, we select and propose three indicators. Our proposed indicators have been adopted by Google Chrome, and we hope to motivate others to update their security indicators as well.

1. INTRODUCTION

Security indicators are the most commonly seen browser security UI. Every major browser displays security indicators — a lock, a shield, or some other symbol — to summarize the security states of websites. (Figure 1 shows an example of a green lock in Google Chrome.) Yet, despite this ubiquity, people often find browser security indicators confusing.

Researchers have cautioned since 2002 that people don't always understand security indicators [7, 8, 16]. Two anecdotal experiences convinced us that the problem remained. While doing field work in India, we met many tech-savvy people who didn't associate Google Chrome's security indicators with security. Later, we discovered that one author's American sibling was similarly confused. This spurred us to formally revisit the problem of security indicators.

Our goal is to create new security indicators that non-expert browser users can understand. Ideally, security indicators should at least communicate whether a given website connection is currently secure or dangerous. We focus specifically on comprehension, leaving the question of how to draw attention to the indicators for future work [5].

In order to improve security indicators, we first needed to learn more about the shortcomings of existing indicators. We surveyed 1,329 people about Google Chrome's connection security indicators in the course of their normal web browsing. Although most of our tech-savvy (but non-expert) respondents had at least a basic understanding of the HTTPS indicator, many were unfamiliar with the HTTP indicator.

Symposium on Usable Privacy and Security (SOUPS) 2016, June 22–24, 2016, Denver, Colorado, USA.

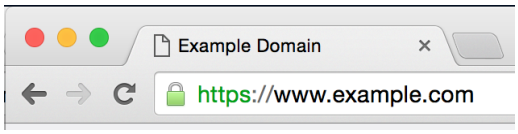


Figure 1: The green lock is a security indicator.

We then began the task of creating and testing new security indicators, working within the additional constraints posed by modern browser needs. Browsers are used by diverse audiences on diverse devices. Security indicators therefore face several design constraints:

- The indicators need to scale down for small devices. Icons should not rely on small decorations that become illegible when small. We can optionally use text, but there will not always be space to display it.
- The icon shape alone — without color — needs to communicate the level of risk to meet accessibility needs. 8% of men are colorblind [17], and many others have vision impairments.
- The indicator's meaning needs to be taught with words when possible. Millions of new Internet users have recently come online via smartphones without learning "standard" iconography from desktop browsers.

We identified forty candidate icons and seven accompanying strings that meet these constraints. Through a series of surveys, we narrowed the set down to the most promising icons and strings. Ultimately, we selected three sets of browser security indicators based on survey results, prior research, and our design constraints. Our proposed indicators will be deployed with Google Chrome 53.

Contributions. We contribute the following:

- Most security indicator research was performed in 2002 – 2008, but requirements have changed over time. We evaluate browsers' security indicators and determine whether they meet modern browser users' needs.
- We identify specific shortcomings of Chrome's connection security indicators with an in-the-moment survey of 1,329 respondents.
- We propose three new security indicators, based on multiple rounds of user testing and our constraints.

2. THE ROLE OF SECURITY INDICATORS

Browsers use security indicators to communicate connection security states, website trustworthiness, or a combination of the two. Security indicators are trusted browser UI, and they appear in or near the URL bar. They are distinct from website-controlled UI (such as favicons), although websites sometimes do use icons that appear similar to security icons. For example, the favicon for the website shown in Figure 1 looks extremely similar to Chrome's HTTP indicator.

2.1 Connection security

Connection security describes *how* a website was fetched over the network. Ideally, the HTTP connection should use well-authenticated TLS to protect end users' web traffic from eavesdroppers and attackers on the network.

Valid HTTPS. This is the best case scenario. The browser can establish a valid TLS connection to the server. The connection is private and tamper-free, even in the presence of malicious parties on the network. However, the website itself could be malicious or compromised; HTTPS only provides security guarantees about the connection.

HTTPS with minor errors. Although the browser was able to establish a valid TLS connection, there are minor problems (e.g., including an image over plain HTTP).

HTTPS with major errors. This is the worst case scenario. The website was supposed to load over HTTPS, but the certificate chain fails to validate. Most browsers show a warning that might (or might not) be overridable.

HTTP. The connection does not use HTTPS, so anyone on the network can see or modify the contents of the website. Although HTTP used to be the default for web browsing, more than half of page loads are now over HTTPS [9].

2.2 Website trustworthiness

In addition to connection security, browsers may also want to check whether the website itself is trustworthy.

EV HTTPS. A website can pay a certificate authority to confirm the website's identity, and the certificate authority will issue an Extended Validation (EV) certificate with the organization's name. EV was originally envisioned as a strong phishing defense.

Malware and phishing. Browsers may perform phishing and malware checks on websites. Services like Microsoft SmartScreen [2] and Google Safe Browsing [6] provide phishing and malware verdicts for browsers. Many browsers show full-page malware warnings.

3. RELATED WORK

Security indicators were well-studied in the mid-2000s, and this literature motivated a shift in how browsers treated security indicators. Security indicators used to be displayed in several areas (e.g., the bottom right corner of the browser), but browsers moved the indicators into the URL bar.

Warnings are complementary to indicators for communicating security issues to users, and have also received considerable research attention. While full coverage of the warnings literature is out of scope for this paper, readers may consult Sunshine et al. [21] and Sotirakopoulos et al. [20] as works specifically on connection security (i.e., SSL/TLS) warnings.

3.1 Connection security

Connection security indicators have received mixed results over the last fifteen years of research.

People look at indicators. Using eye tracking, Whalen and Inkpen found that most of their lab study participants looked at the lock icon while performing common online tasks [23]. Although some participants were confused about the significance of the icons, Whalen and Inkpen advised browser vendors against changing the lock. *"Making major modifications to this [lock] symbol, such as using a different object, may be disorienting: users now expect to find a lock in a browser window."*

Some people understand indicators. Friedman et al. interviewed people from a rural community in Maine, a suburb in New Jersey, and a Silicon Valley community [8]. Across these three communities, roughly half of participants could identify a secure connection from browser screenshots. While not terrible, we hope that someday more than half of users will understand how to differentiate secure and insecure connections. Lin et al. found similar results; some (but not all) of their participants knew about connection security indicators and checked them during study tasks [12].

No one heeds indicators. In contrast, Schechter et al. found that security indicators fail to change user behavior [16]. *None* of their participants withheld their passwords when asked to log in to their bank over HTTP. Similarly, several people incorrectly told Dhamija et al. that a lock icon is *"more important when it is displayed within the page than if presented by the browser"* [7].

Some mobile indicators are lacking. Amrutkar et al. studied SSL indicators in mobile browsers, where screen space is limited [3]. They found high rates of non-compliance with web security user interface standards on connection security indicators. In some cases, mobile browsers lacked any indicator at all of potential attacks, such that even experts would not have enough information to detect these attacks.

We expand on prior literature by evaluating Google Chrome's existing security indicators at much larger scale. With more than a thousand respondents, we were able to collect a broad, nuanced set of qualitative data. Furthermore, all of the cited studies took place in laboratories as either semi-structured interviews or researcher-directed tasks. Our survey respondents naturally encountered security indicators in the course of browsing on their own computers.

3.2 Website trustworthiness

In the past, HTTPS was viewed as a sign of website trustworthiness; getting a valid HTTPS certificate was too difficult for typical phishing websites. Dhamija et al. challenged 22 people to identify phishing websites, and 17 of them failed to check the connection security indicator during the study [7]. This demonstrated that connection security indicators were ineffective at preventing phishing attacks. Subsequently, HTTPS has ceased to be a useful signal for identifying phishing websites because it is no longer unusual

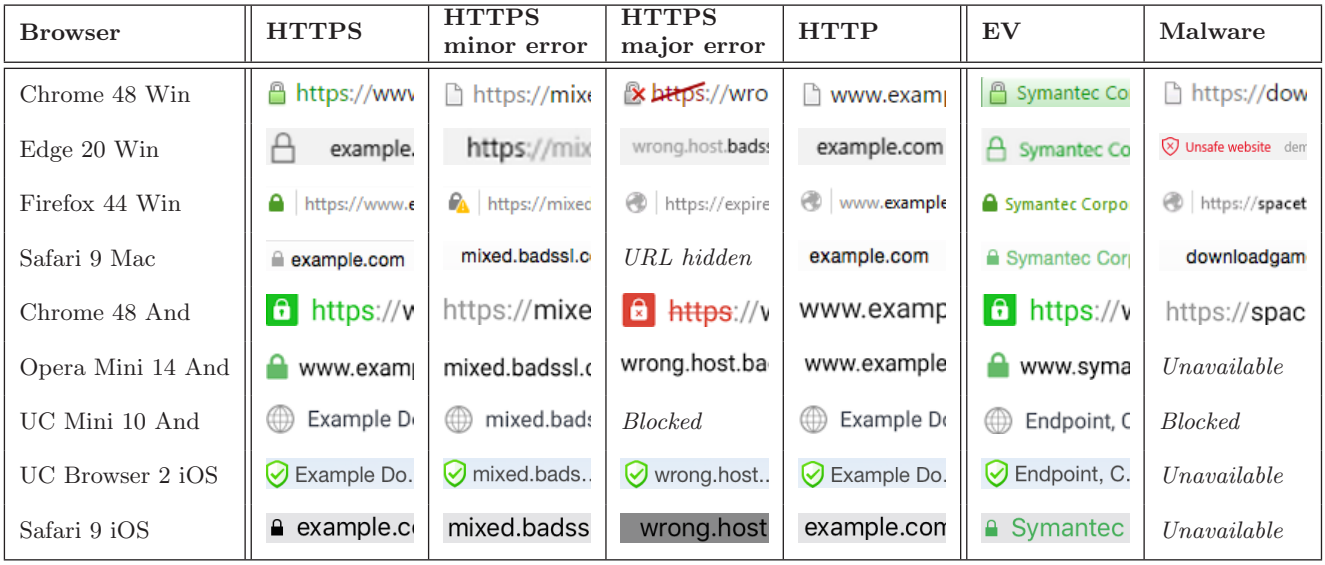


Figure 2: Security indicators for major browsers on Windows (Win), Mac, Android (And), and iOS. For categories that trigger warnings (e.g., malware), we include the security indicator state during the warning.

to find malicious websites that support HTTPS. We therefore do not aim to use HTTPS as an anti-phishing defense.

EV is an anti-phishing defense, although its use is limited by lack of support from popular websites and some major mobile browsers. All major desktop browsers display EV information, but some mobile browsers (including Chrome and Opera for Android) do not display EV information. Older literature suggests that EV indicators may need improvement. Jackson et al. asked study participants to identify phishing attacks and found that "extended validation did not help users defend against either attack" [10]. When testing new security indicators, Sobey et al. concluded that Firefox 3's EV indicators did not influence decision making for online purchases [19]. Improving EV indicators are out of scope for our current work.

3.3 Security indicator proposals

We propose changes to browser security indicators, and our proposal draws from prior research.

Sobey et al. suggested expanding security indicators into a "chip" that provides both an icon and explanatory text [19]. We like this format because it teaches and contextualizes the icon. However, Sobey et al. found that half of study participants did not notice the chip [19]. We have restricted our focus to comprehension, but their results suggest that we will need to do additional future work to draw attention to security indicators.

Maurer et al. proposed changing the entire toolbar to reflect the connection security state [14]. They surveyed participants about their proposal (and Firefox's existing security indicators) using a Firefox extension. With their proposal, study participants found valid HTTPS websites more trustworthy. In practice, however, we find it unlikely that a browser vendor would adopt a proposal that consumes the entire toolbar area as a security indicator. We took a similar methodological approach (using an extension) to survey people about Chrome's security indicators, but our surveys focused on comprehension instead of trustworthiness.

Although we specifically study security indicators, closely related UI also influences users' perceptions of security. For example, domain highlighting emphasizes the hostname in the URL bar (and de-emphasizes the potentially confusing path). Lin et al. found *"that domain highlighting works [to identify phishing], but nowhere near as well as we would like"* [12]. And what UI should be displayed when the user clicks on the security indicator? Biddle et al. proposed a way to display the identity information associated with the HTTPS connection [4]. Their proposal helped study participants find web site ownership and data safety information.

4. CURRENT BROWSER INDICATORS

Figure 2 illustrates how different security states are represented in major desktop and mobile browsers, according to our testing in February 2016. We describe and critique them to motivate the need for improved security indicators.

Similar shapes. Chrome and Firefox overload the meanings of shapes. Firefox's two lock icons have different meanings: a green lock for HTTPS, and a gray lock with a small yellow triangle for HTTPS-with-minor-errors. Chrome similarly has two locks: a green lock for HTTPS, and a red lock with a slash for HTTPS-with-major-errors. In both cases, the states look similar — particularly at small scale — unless the viewer is already familiar with the meaning. Chrome further compounds the problem by using colors that colorblind people commonly cannot distinguish.

Secure but untrustworthy. Most browsers use security indicators primarily to convey connection security information. If a browser's security indicator reflects only connection security, the browser can end up in a confusing state. When a user clicks through a warning to a malicious website, the browser will show a neutral or positive indicator in the URL bar. This might cause a user to believe the website is safe despite having seen the warning. Edge notably mitigates this by updating the security indicator to reflect malware or phishing verdicts.

Evergreen indicators. UCWeb's browsers (UC Mini and UC Browser)[1] stand out from other browsers by not displaying connection security information. Neither distinguishes between HTTP and HTTPS. UC Browser for iOS always displays a green shield regardless of the connection security state, which provides a sense of unmerited security.

Missing HTTP indicators. Many major browsers lack any indicator at all for HTTPS with minor errors or HTTP. As a result, the user does not have a click target to learn more about the connection security state. This is arguably reasonable on mobile, where small screens might necessitate removing or hiding indicators by default. However, desktop URL bars have sufficient space for an indicator.

HTTPS with minor errors. With the exception of Firefox, most browsers treat HTTPS with minor errors as if it were HTTP. We agree with this decision. This state is less risky than HTTP, but the website does not deserve to be displayed as fully secure. This state often occurs when websites are transitioning from HTTP to HTTPS. If we were to make the minor error state look *worse* than HTTP, it would discourage transitioning.

5. PERCEPTIONS OF CHROME'S SECURITY INDICATORS

We surveyed 1,329 people to understand user perceptions of Chrome's security indicators. We hoped to learn what people think Chrome's HTTPS and HTTP indicators mean, with an emphasis on identifying common misconceptions.

5.1 Method

We built a Chrome extension to deliver in-context surveys about Chrome's connection security indicators. The extension enabled us to survey respondents about indicators immediately after the respondents had an opportunity to see an indicator during normal browsing. Supplementary screenshots of the extension are in Appendix A, and the extension code is available on GitHub.[2]

5.1.1 How the extension worked

Setup. Immediately after installation, the extension displayed a consent form. If a respondent consented, s/he was then shown a short demographic survey, after which the extension shut down for a fifteen minute quiet period. Since the extension was intended for use with additional surveys later, we wanted respondents to learn that they would see surveys during regular browsing and not just upon installation of the extension.

Notification. After the quiet period ended, the extension waited until the respondent visited an HTTP or valid HTTPS website. (We avoided websites with major or minor errors by using a whitelist of popular websites without HTTPS errors.) When a qualifying website loaded, the extension prompted the respondent with a system notification to take a survey. If the respondent clicked on the notification, a survey would appear in a new window. Respondents were only notified once, and the extension stopped offering the survey after six hours from installation. So, not all people who installed the extension provided a survey response.

Survey. We created two versions of the survey, one for HTTP and one for HTTPS. The appropriate survey was selected based on the first website the respondent visited that triggered a survey notification.

5.1.2 Deployment

Our extension was publicly available for download in the Chrome Web Store, which is Google's official central repository for Chrome apps and extensions. We encouraged downloads via a press release, which was picked up by several popular tech news sources (e.g., [11, 18]) and a post in Chrome's help forum [13]. The promotional materials offered an opportunity to provide feedback on Chrome.

We collected surveys from May 11, 2015 to September 10, 2015 (122 days). We received 5,041 completed demographic surveys, and 1,329 completed HTTP(S) surveys, including 733 HTTPS surveys and 596 HTTP surveys.

To preserve respondent privacy, we chose not to monetarily compensate respondents. This decision allows us to collect data pseudonymously.

5.1.3 Questions

We asked respondents to describe the meaning of the indicators. To contextualize our question, the survey prominently included a screenshot of Chrome's URL bar with a red circle around the security indicator. The HTTPS and HTTP versions had screenshots of the appropriate indicators. Beneath the screenshot were the instructions:

> *You just now saw a URL bar like the one shown above. The following questions are about the URL bar.*

Each survey included three questions. In this paper, we focus on responses to the second question. (The other two are available in Appendix B, along with a screenshot of the survey in Appendix A.) We asked two versions, one for HTTPS and one for HTTP:

> HTTPS: *What does the green symbol to the left of the URL mean to you?*

> HTTP: *What does the white symbol to the left of the URL mean to you?*

5.1.4 Data coding

Seven security experts coded the qualitative responses. One team member (the *codemaster*) used open coding to create an initial codebook, in consultation with another expert. The remaining six coders did two partial coding rounds, each time giving feedback to the codemaster about shortcomings in the codebook. In the second round, all coders coded the same 40 responses to measure consistency. Fleiss's κ, a measure of inter-rater reliability, was 0.81, which we considered sufficiently consistent to proceed.

For the final round of coding, the codemaster divided the 1,329 responses between three pairs of coders. The coders

[1] `http://www.ucweb.com/company/about/`
[2] `https://github.com/GoogleChrome/experience-sampling`

worked in pairs so that two people independently coded each response. Each coder was responsible for approximately 400 responses, split between HTTP and HTTPS responses. Fleiss's κ was 0.89 before the codemaster reconciled remaining conflicts. Coders agreed on codes for 91% of responses, whereas 9% required resolution. The codemaster resolved the conflicting responses.

5.1.5 Demographics

While we hoped to reach a representative sample of Chrome users, our recruiting method may have provided a biased sample. In particular, we could not control which publishers ran our press release. Based on our demographic survey, respondents were most likely to learn about our survey from the Chrome Web Store, TechCrunch, omgchrome.com, and Reddit. These websites cater to technology enthusiasts, so our sample may be biased toward tech-savvy users. Furthermore, our decision to preserve respondent privacy by using non-compensated volunteers may have attracted a sample of people excited about improving Chrome.

Table 1 summarizes the demographics of our sample. Compared with Wash and Rader [22], a recent usable security paper that emphasized a representative sample of US Internet users, our sample skews young and heavily male. Educational level is closer to Wash and Rader's sample, though ours is skewed somewhat toward higher educational levels. Our sample was international (65% from outside the US), so cannot be expected to mimic Wash and Rader exactly, but we still note that the sample skews young and male.

Nevertheless, the sample is moderately large, at 5,041 installs and 1,329 survey responses. It is also diverse across age, educational level, and geography. Our survey was in English, and we filtered out non-English responses, but our respondents nonetheless were heavily international. The size and diversity of the sample suggest that the responses we received represent the understanding of a significant portion of the Chrome user population. And, since the bias is likely toward the tech-savvy, our results are likely an upper bound on the true understanding of security indicators amongst the general Chrome user population. That is, since our results show a lack of understanding of the indicators even amongst our sample, the understanding amongst all Chrome users is likely even lower. Our ultimate conclusion that users at large could benefit from a redesign of the indicators still holds.

5.1.6 Ethics

Consent. Respondents were shown a consent form that explained how the survey platform worked and how their answers would be used. If they did not consent, the extension would automatically uninstall itself. If they did consent, they proceeded to the demographic questionnaire. Respondents could view the consent form again later by clicking on "What is this?" in the extension notification.

Minors. Respondents needed to be age 18 or older. If a respondent claimed to be below the age of 18 in the demographic survey, the extension automatically uninstalled itself without sending any data to our server.

PII. We did not ask respondents to provide any personally identifiable information. The questions focus on the respondents' opinions of and beliefs about Chrome's security UI, as well as general demographic information. Each installation was assigned a random pseudonymous identifier to link demographic surveys with HTTP(S) surveys, but we cannot link the pseudonyms to individual people.

	Respondents	Installers
Male	90.4%	81.0%
Female	7.0%	14.2%
Other or not specified	2.6%	4.8%
Age 18-24	30.1%	25.8%
Age 25-34	40.7%	33.9%
Age 35-44	18.3%	20.0%
Age 45-54	6.9%	10.1%
Age 55-64	2.7%	6.3%
Age 65 or over	1.3%	3.8%
Some High School	2.6%	7.0%
HS or equiv	40.6%	48.9%
College degree	33.3%	28.2%
Graduate degree	20.2%	16.6%
Prefer not to answer	3.3%	6.4%
US	35.4%	27.8%
France	10.0%	6.8%
UK	5.9%	4.0%
Russian Federation	5.8%	4.4%
Germany	5.7%	3.7%
Canada	2.6%	3.6%
Other	34.6%	49.7%

Table 1: Demographics of the 1,329 respondents who provided completed surveys and of all 5,041 people who installed our extension.

Approval. Our organization does not have an IRB, but our study was internally reviewed before launch.

5.2 Results

We analyze responses to *What does the (white|green) symbol to the left of the URL mean to you?* by examining how many responses fall into each of our categories. We find that most respondents understand the HTTPS indicator, but are less sure about the meaning of the HTTP indicator. Table 2 summarizes the responses, including representative quotes.

5.2.1 HTTPS survey

Almost all of the 733 respondents mentioned security-related concepts when describing the green lock indicator. We categorized survey responses into seven high-level categories — CONNECTION, IDENTITY, PROTOCOL, SECURITY, ICON APPEARANCE, DON'T KNOW, and INCORRECT THEORIES — and ordered them by technical correctness and completeness, with CONNECTION demonstrating the most knowledge and INCORRECT THEORIES demonstrating the least. As shown in Table 2, most responses were at least partially correct; a majority fell in the first four categories, although the responses contain varying levels of technical depth and sophistication. We explain the categories, codes, and corresponding results in more detail below.

Connection and Identity. Responses in these categories are the most technically sophisticated and nuanced. CON-

HTTPS Category	Responses	Representative Quotes
CONNECTION	40.1%	
Encrypted connection	18.8%	"a secure encripted page"; "Connection is encrypted by HTTPS/SSL."
Secure connection	17.0%	"Secure connection"; "Secure connection I associate with the https vs http"
Safe to enter data	2.2%	"this site is safe to proceed to send data"
Private connection	1.5%	"The connection is private"; "It's a secure and private session"
Connection in general	0.6%	"https connection"
IDENTITY	13.4%	
Valid certificate	8.6%	"Secured connection, valid certificate"
Verified or authenticated	2.6%	"it's a verified domain – it's safe"
Trusted site	1.0%	"that is's a trustworthy page with a known identity."
Authority/Root CA/Chain of trust	1.0%	"...the certificate is in my database of trusted CA."
Identity applies only to name	0.3%	"does not guarantee the identity of the recipient (other than the hostname that is)"
PROTOCOL	34.4%	
HTTPS	18.7%	"HTTPS-using website."; "Secured via HTTPS"
SSL	12.1%	"SSL"; "SSL is enabled on the current site"
TLS	2.5%	"The page was served over TLS"; "That the site is SSL/TLS"
Secure form of HTTP	1.0%	"secure http"; "Site using encripted http"
SECURITY	35.7%	
Security or safety in general	23.7%	"Security."; "Security, safe, protection"
Secure site or page	12.0%	"The website is secure"; "Is a secure page"
ICON APPEARANCE	0.4%	
Lock	0.4%	"locked"; "closed lock = locked..."
DON'T KNOW	0.6%	
Don't know	0.6%	"I do not Know."
INCORRECT THEORIES	0.4%	
Miscellaneous	0.4%	"it is password?"; "website has user secured information on it"

HTTP Category	Responses	Representative Quotes
NOT SECURE	21.2%	
Not secure in general	10.9%	"This web page is purely a web page with no security"; "The page is unsecure"
Not encrypted	6.8%	"An unencrypted connection to the site."; "Unencrypted transmission of the page."
Insecure connection	2.0%	"white symbol to me means unsecure connection and page info."; "Unsecure connection"
PROTOCOL	17.4%	
Not HTTPS	6.6%	"Means that it is not https"; "Unencrypted connection (non-HTTPS)"
HTTP	4.3%	"unencrypted page transmitted over http protocol"; "http"
HTTP and not HTTPS	1.9%	"HTTP, not HTTPS"; "The site is being served via HTTP rather than HTTPS"
Protocol in general	1.5%	"Web protocol + Certificate"; "It represents either the favicon or the security protocol..."
HTTPS	0.6%	"security something (https?)"; "https I think?"
Not TLS	0.4%	"It's not TLS/SSL secures. so no https"
ABOUT SECURITY	7.1%	
Security in general	6.2%	"Security"; "Safety!"
Connection in general	0.6%	"The type of connection that was made with the server."
Site identity in general	0.4%	"Whether or not the identity of the site is verified"
REGULAR WEBPAGE	8.4%	
Regular webpage	8.4%	"regular web page"; "I am looking at a regular web page with no known issues"
CONTEXT MENU ITEMS	23.8%	
Site information	11.8%	"Provides Site Information"; "Click - see details for website"
Cookies	4.7%	"cookies"; "It gives a quick glance at permissions and cookies."
Permissions	2.4%	"information about privacy permissions"
SSL certificate status	1.9%	"Information on current page (cookies, ssl certificat)"
Connection	1.7%	"Access to the details of the connection to the site."
Security status	1.3%	"It offers information about the security of the webpage you are visiting."
ICON APPEARANCE	5.3%	
Document	2.6%	"document"; "Something to do with paper or a document..."
Page	1.3%	"page icon"
Piece of paper	0.9%	"Something to do with paper or a document..."
File icon	0.4%	"For me this symbol is the 'computer' file symbol..."
FAVICON	9.4%	
Website with no favicon	6.8%	"no favicon"; "No favicon for the current website."
Is the favicon for the site	2.4%	"Favicon"; "the site icon"
OTHER FUNCTIONALITY	1.7%	
Make a bookmark	1.1%	"A link to easily create a shortcut."
Drag the URL	0.6%	"THat's where I click whan I want to drag the URL..."
DON'T KNOW	7.1%	
Don't know	7.1%	"i just dont know."; "no idea"
NO MEANING	0.9%	
No meaning	0.9%	"nothing"; "...It mean nothing."
INCORRECT THEORIES	2.4%	
Bookmark indicator	0.6%	"I think it signifies that the page is saved as a bookmark."
Page loading	0.4%	"The page is loaded."; "The page hasn't loaded entirely."
Trouble loading	0.4%	"Trouble loading page"
SECURE	1.5%	
Secure page	1.3%	"secure site"; "Th url is safe"

Table 2: The percentage of responses that fell into each category, and representative quotes. Percentages do not add up to totals because some responses received multiple codes. Responses are verbatim, except as indicated by ellipses.

NECTION was the most-mentioned category, applying to 40.1% of responses. IDENTITY, at 13.4%, was the fourth most-mentioned. An expert would ideally mention both.

The CONNECTION category is the most unambiguously correct category. Responses within this category fell into five sub-codes, four of which explicitly mention connection security: *Encrypted connection*, *Secure connection*, *Private connection*, and *Connection in general*. A fifth code, *Safe to enter data*, was assigned to responses that did not explicitly mention the connection but indicated that the data exchanged with the server could not be intercepted.

The IDENTITY category is more complex. With an HTTPS connection, the browser verifies the server's identity to make sure the client isn't accidentally talking to a man-in-the-middle attacker. Some IDENTITY codes correctly refer to this process by talking about a *Valid certificate*, *Authority/root CA/chain of trust*, or how the *Identity applies only to domain*. However, HTTPS alone does not provide any guarantees that the website is trustworthy or the right website for the user's task. Some respondents mentioned identity but incorrectly said that HTTPS vouched for the website's trustworthiness (*Verified or authenticated*, *Trusted site*). This is an unfortunate misconception, although it was rare (about 3% of the total).

Protocol. A third of responses (34.4%) correctly mentioned the protocol. These responses mentioned *HTTPS*, *SSL*, *TLS*, or a *Secure form of HTTP*, which demonstrates an association between the indicator and protocol. However, we cannot tell whether a respondent understands what HTTPS is just by mention of the name, so these codes do not necessarily indicate an understanding of the protocol.

Security. The second most-mentioned category at 35.7%, SECURITY, included responses that mentioned security in a general sense, without necessarily mentioning the TLS guarantees or any of the protocols. Some responses in this category mentioned *security or safety in general*, while others mentioned security or safety in the context of a site or page.

Icon appearance, Don't know, Incorrect theories. The last three categories were rarely assigned for the HTTPS indicator. Responses in ICON APPEARANCE mentioned the literal appearance of the icon, namely that it depicts a *lock*. Responses in DON'T KNOW explicitly stated that respondents did not know what the HTTPS indicator meant. Responses in INCORRECT THEORIES suggested miscellaneous incorrect meanings for the indicator.

5.2.2 HTTP survey

Codes for the HTTP survey reflect a greater variety of responses than we observed for the HTTPS survey, and respondents displayed less knowledge about HTTP. Table 2 shows results from the HTTP survey.

We grouped responses into 12 categories, ordered by decreasing technical correctness and completeness: NOT SECURE, PROTOCOL, ABOUT SECURITY, REGULAR WEBPAGE, CONTEXT MENU ITEMS, ICON APPEARANCE, FAVICON, OTHER FUNCTIONALITY, DON'T KNOW, NO MEANING, INCORRECT THEORIES, and SECURE. We explain categories, codes, and corresponding results for the HTTP study below.

Not secure. About a fifth of responses (21.2%) correctly say that the security guarantees of TLS are not in place. Most of the NOT SECURE responses indicated that something (the page, the site, or no subject at all) was *not secure in general*. Others more specifically named the connection and noted that it was *not encrypted* or *insecure*.

Protocol and About security. As with our HTTPS survey, many responses mentioned a protocol or talked about security in general (17.4% for PROTOCOL, 7.1% for ABOUT SECURITY). Within the PROTOCOL responses, people talked about HTTP using various synonyms, and the ABOUT SECURITY responses touched generally on connection security or identity. Unfortunately, a few of the PROTOCOL responses incorrectly suggested *HTTPS* was in use.

Context menu items and other functionality. Surprisingly, the most popular topic was about what the HTTP icon can do if clicked or dragged. 23.8% of responses talk about the CONTEXT MENU ITEMS that appear when someone clicks on the icon, and another 1.7% talk about OTHER FUNCTIONALITY. We did not see these types of responses for the HTTPS indicator, even though it has the same behavior when clicked or dragged. One potential explanation is that respondents who were unfamiliar with the HTTP icon clicked on it after reading our question, and then told us what they found.

Regular webpage. 8.4% of responses called HTTP websites "regular" or "normal." This reflects the prevalence of HTTP on the web.

Don't know, no meaning, and icon appearance. Some respondents simply didn't know what the HTTP indicator means. 7.1% responses said they DON'T KNOW, 1% said the icon has NO MEANING, and 5.3% simply described the ICON APPEARANCE without commenting on its functionality or meaning. These types of responses were more common than for the HTTPS survey.

Incorrect responses and secure. A small but still too-large number of respondents provided incorrect descriptions of the HTTP indicator. 9% of respondents thought the indicator was the default FAVICON, rather than a security indicator, and 2.4% had miscellaneous other incorrect theories. Unfortunately, 1.5% of responses thought that the HTTP indicator meant the opposite: that the page is SECURE.

6. EVALUATING NEW ICONS

With our survey (Section 5), we learned that even tech-savvy people hold incomplete or incorrect beliefs about Chrome's HTTP indicator. Since we see shortcomings in other browsers' security indicators as well (Section 4), we decided to create new security indicators. We began by searching for icons for our proposal and evaluating them with Google Consumer Surveys (GCS) [15]. Our goal was to determine which icon shape and color best represented secure and insecure connections to websites. We ultimately selected three shapes: a green lock, a black circle, and a red triangle.

In our analysis, we performed thirteen tests for statistical significance. To account for multiple testing, we adjusted our levels of significance using the Holm-Bonferroni method.

Figure 3: The candidate indicator shapes, split between positive (top) and negative (bottom).

6.1 Candidate icons

We began with forty candidate icons. They varied in three dimensions: shape, historical connotation, and color.

Shape. We selected eight shapes (Figure 3) that are commonly used in road signs or Google products to communicate safety information. They are all simple shapes that scale, and their profiles can be distinguished from one another.

Connotation. Four of the shapes have historically been used to communicate safety, and four of the shapes have historically been used to communicate danger. We considered the former to be candidates for a security icon, and the latter to be candidates for an insecure icon.

Color. We chose five colors: black, blue, green, orange, and red. We produced each shape in five colors.

6.2 Survey method

Questions. We ran two sets of surveys in September 2015 to evaluate which icons best represent a secure connection or insecure connection. The questions were, respectively:

- *Imagine each of the icons below next to a URL in your browser address bar. Which of the icons best represents a connection to the website that IS secure?*
- *Imagine each of the icons below next to a URL in your browser address bar. Which of the icons best represents a connection to the website that is NOT secure?*

To answer the question, respondents had to pick an icon from a pair. The two icons were different shapes but the same color. Each respondent answered the same question five times, once for each color. For example, a respondent might have to pick between a green lock and a green shield, then pick between a blue triangle and a blue checkmark, and so on. A screenshot in Appendix C.1 shows what the pairwise comparison looked like.

Recruitment. GCS surveys are published on news, reference, and entertainment websites. Respondents answer the survey questions to gain access to free content, in lieu of subscribing or upgrading. We did not directly pay respondents. Google paid the publisher for the responses.

Sample. Five hundred participants answered each variant of each question, which yielded a total of 7,000 responses from 1,000 respondents. We did not ask any demographic or personal questions, although Appendix D contains inferred demographics. All of our respondents were physically located in the United States at the time of the survey.

	Positive icons				*Negative icons*			
...IS secure?								
Black	**23%**	20%	18%	13%	8%	8%	5%	5%
Blue	20%	**21%**	17%	17%	7%	7%	5%	6%
Green	**23%**	20%	16%	12%	8%	10%	6%	4%
Orange	19%	**20%**	18%	18%	6%	9%	6%	4%
Red	19%	**20%**	19%	18%	7%	7%	5%	5%
...is NOT secure?								
Black	4%	8%	10%	6%	19%	14%	**21%**	19%
Blue	5%	8%	7%	8%	**21%**	19%	16%	16%
Green	3%	10%	7%	8%	19%	17%	**20%**	16%
Orange	6%	8%	9%	7%	**19%**	17%	17%	16%
Red	7%	6%	7%	6%	**21%**	18%	16%	19%

Table 3: How often each icon "won" when the respondent answered, *Which of the icons best represents a connection to the website that...* N=1000

Google Consumer Surveys are typically representative of the Internet-using population in the United States [15].

6.3 Survey results

Although respondents exhibited strong associations between icon shape and (in)security, no individual shape-color combination stood out. Table 3 shows our results.

Preconceived beliefs. We hypothesized that respondents would have preconceived beliefs about the icon shapes based on past experiences, and our data substantiates this hypothesis. Prior to running the experiment, we categorized our icon shapes as "positive" or "negative" based on how they are used in existing products. The "positive" icons were more likely to be considered secure than insecure, and the "negative" icons were more likely to be considered insecure than secure. We found a significant difference between between the positive icons' scores across the secure and insecure questions ($\chi^2 = 57.06, df = 3, p < 0.01$). Similarly, we found a significant difference between the negative icons' average scores in the secure and insecure questions ($\chi^2 = 42.91, df = 3, p < 0.01$).

Secure connection. Respondents did not have a clear favorite for a color-shape combination that represents a secure connection. The "positive" icons won at similar rates for the secure connection question, although the shield or lock won the most across colors.

Insecure connection. Respondents also did not have a clear favorite for a color-shape combination that represents an insecure connection. There "negative" icons won at similar rates for the insecure connection question, although the triangle placed either first or second across the five colors.

6.4 Icon selection

We had hoped that three clear winners would emerge from the forty icons: an icon strongly associated with a secure connection, an icon strongly associated with an insecure connection, and an icon moderately associated with an insecure connection. Although that did not happen, we can still look at the pairwise rankings to identify candidates.

Secure connection. The shield and lock consistently performed well across all colors, which suggests that either shape should be meaningful to people who are colorblind. We break the tie by considering that many browser users have already been taught to look for locks, and our tech-savvy extension survey respondents related it to security (Section 5). Over ten years ago, Whalen and Inkpen cautioned against changing the lock shape because their interviewees had begun to expect it [23]. Thus, we propose to continue using a green lock for HTTPS.

Insecure connection. The triangle and slash both tested as viable candidates. They jointly won all of the insecurity comparisons, and the slash ranked among the lowest on the security question. We break the tie by considering scalability and contrast; the blockier triangle will be easier to recognize at small scale on different backgrounds. Thus, we propose to use a red triangle for insecure connections.

Slightly insecure connection. To represent HTTP, we want to choose an icon from the "negative" group that is not strongly associated with either end of the spectrum. The circle with an exclamation point fits that criteria and also appears similar to the ISO symbol for information. We hope that the similarity would encourage people to click on it to find out more information about connection security. Thus, we propose to use a black circle with an exclamation point for connections over HTTP.

7. EVALUATING NEW TEXT

We hope that text can aid user comprehension of security indicators, particularly for new Internet users who do not have preexisting expectations of icons. But which strings should we use? Using Google Consumer Surveys, we tested a set of strings to see which helped comprehension the most.

7.1 Candidate strings

We paired each of the three icons with seven strings. The strings are simple phrases that convey slightly different threat models. The sets of candidate strings are:

- For the green lock: *"https," "private," "secure," "safe," "encrypted," "secure and private," "secure site"*
- For the black circle: *"http," "not private," "not secure," "not safe," "not encrypted," "not secure, not private," "site not secure"*
- For the red triangle: *"~~https~~," "not private," "not secure," "not safe," "not encrypted," "not secure, not private," "site not secure"*

Two designers selected the strings in consultation with security experts. Their simplicity should make them (relatively) easy to translate correctly. The black circle and red triangle strings are similar because they are both conveying insecure states, of different degrees of severity.

7.2 Method

Questions. We asked three GCS questions in November 2015 about website safety, each intended to capture a different aspect of security indicators. We wanted to understand how respondents perceive the safety of the page, threat model, and desired action given different security indicators. Our questions were:

1. *If you saw this browser page, how safe would you feel about the current website?*
   Not at all safe
   A little safe
   Somewhat safe
   Very safe
   Extremely safe
2. *If you saw the below icon and message in the browser's address bar, that would be that someone might...*
   Try to put a virus or malware on your PC
   Modify the content of the page
   Have created a technical bug on the site
   Steal the things you read and type
   None of the above
3. *If you came across a site in your browser and saw this in the address bar, how would you most likely proceed?*
   I'd browse normally
   I'd leave the site
   I wouldn't enter any credit card details
   I'd look for more information about the site
   I'd browse quickly, then leave

Each question was accompanied by a mock browser screenshot that included an icon, string, and blurred URL. We made 21 variants of each question because we had 21 combinations of icons and strings. An individual respondent answered all three questions for the same icon-string pair. For Q2, respondents could select multiple choices *or* "None." Responses were either randomly flipped (Q1) or randomly ordered (Q2 and Q3). Appendix C.2 shows an example question.

Q3 asks respondents how they would react to an indicator. Since this is self-reported data, it likely does not reflect actual behavior in the field. However, it gives us insight into how respondents *perceive* the indicators' calls to action.

Recruitment. GCS surveys are published on news, reference, and entertainment websites. Respondents answer the survey questions to gain access to free content, in lieu of subscribing or upgrading. We did not directly pay respondents. Google paid the publisher for the responses.

Sample. Three hundred respondents took each of our twenty-one variants, each of which consisted of three questions. This yielded 19,386 responses from 6,462 respondents. We did not ask any demographic or personal questions, although Appendix D contains inferred demographics. All of our respondents were physically located in the United States at the time of the survey.

7.3 Results

Respondents had different perceptions of page safety, threat models, and calls to action depending on the strings. Table 4 shows the full results.

7.3.1 Valid HTTPS

We find that "secure" and "https" are the most promising companions to a green lock icon.

Q1:		Not at all	A little	Somewhat	Very	Extremely
	https	23%	9%	**32%**	26%	10%
	Private	24%	16%	**35%**	18%	7%
	Secure	12%	19%	**40%**	24%	5%
🔒	Safe	20%	16%	**34%**	20%	10%
	Encrypted	23%	12%	**42%**	19%	4%
	Secure and private	20%	19%	**36%**	21%	4%
	Secure site	18%	17%	**32%**	24%	8%
	http	**40%**	20%	27%	11%	3%
	Not private	**60%**	17%	15%	4%	4%
	Not secure	**58%**	14%	19%	6%	4%
❗	Not safe	**61%**	12%	16%	7%	4%
	Not encrypted	**52%**	19%	18%	5%	6%
	Not secure, not private	**57%**	17%	18%	6%	2%
	Site not secure	**63%**	14%	14%	6%	3%
	~~https~~	**63%**	16%	12%	5%	4%
	Not private	**68%**	14%	11%	3%	5%
	Not secure	**61%**	22%	11%	2%	4%
⚠	Not safe	**65%**	14%	14%	5%	3%
	Not encrypted	**53%**	18%	19%	6%	5%
	Not secure, not private	**64%**	20%	11%	3%	2%
	Site not secure	**64%**	15%	12%	6%	4%
Q2:		**Malware**	**Steal**	**Bug**	**Modify**	**None**
	https	15%	10%	12%	14%	**64%**
	Private	24%	22%	16%	14%	**51%**
	Secure	15%	12%	12%	13%	**65%**
🔒	Safe	24%	19%	16%	14%	**54%**
	Encrypted	22%	15%	12%	16%	**56%**
	Secure and private	23%	18%	15%	17%	**53%**
	Secure site	18%	12%	9%	14%	**60%**
	http	30%	24%	22%	27%	**41%**
	Not private	41%	**48%**	29%	26%	21%
	Not secure	**51%**	37%	29%	24%	22%
❗	Not safe	**53%**	39%	29%	22%	25%
	Not encrypted	**36%**	38%	24%	23%	32%
	Not secure, not private	**50%**	42%	32%	26%	22%
	Site not secure	**48%**	40%	30%	25%	24%
	~~https~~	**47%**	34%	30%	26%	23%
	Not private	46%	**49%**	30%	27%	21%
	Not secure	**54%**	46%	32%	33%	20%
⚠	Not safe	**61%**	39%	25%	23%	20%
	Not encrypted	**43%**	39%	23%	28%	26%
	Not secure, not private	**50%**	37%	25%	23%	23%
	Site not secure	**61%**	43%	35%	29%	22%
Q3:		**Leave site**	**More information**	**No credit card**	**Normally**	**Quickly**
	https	20%	12%	12%	**51%**	5%
	Private	**28%**	19%	18%	25%	9%
	Secure	17%	15%	18%	**41%**	9%
🔒	Safe	26%	14%	14%	**37%**	10%
	Encrypted	28%	14%	18%	**33%**	7%
	Secure and private	25%	15%	20%	**31%**	9%
	Secure site	23%	16%	14%	**40%**	8%
	http	**38%**	10%	22%	21%	10%
	Not private	**53%**	13%	17%	9%	8%
	Not secure	**58%**	10%	16%	9%	7%
❗	Not safe	**66%**	6%	16%	7%	5%
	Not encrypted	**49%**	8%	25%	9%	9%
	Not secure, not private	**51%**	13%	21%	8%	7%
	Site not secure	**59%**	8%	20%	7%	7%
	~~https~~	**60%**	12%	14%	6%	8%
	Not private	**60%**	11%	15%	7%	7%
	Not secure	**54%**	12%	17%	11%	7%
⚠	Not safe	**68%**	9%	14%	6%	4%
	Not encrypted	**53%**	11%	21%	10%	5%
	Not secure, not private	**59%**	12%	17%	5%	8%
	Site not secure	**64%**	8%	15%	7%	7%

Table 4: Responses to the three GCS questions with both icons and strings. N=6462

Safety. Respondents associated different levels of safety with different strings, based on comparing all of the different outcomes to Q1 (chi-square = 101.30, $df = 24$, $p < .01$). "Secure" yielded the highest number of respondents who felt that the website was at least somewhat safe and the lowest number of participants who felt not safe at all.

Threat. Respondents were most likely to trust a page with the "https" and "secure" strings. The strings influenced the number of respondents who chose "none of the above" (vs. any other response) when asked what kinds of risks might exist on the page (chi-square = 68.23, $df = 6$, $p < .01$). Additionally, across all strings, respondents were unlikely to think that a website with a green lock might try to install malware. This suggests that our indicators are broadly perceived as security indicators, not specifically as connection security indicators.

Action. Respondents claimed they would take different actions depending on the strings (chi-square = 17.40, $df = 6$, $p < .01$), with "https" resulting in the highest number of respondents browsing normally and "secure" having the fewest respondents who would leave the website. We do not assume that respondents would necessarily take these actions, but this demonstrates differing perceptions of the strings.

7.3.2 Invalid HTTPS

We find that "not secure" and "site not secure" are the most promising companions to the red triangle.

Safety. There was a significant difference in how respondents perceived the safety of the website across all strings (chi-square = 71.62, $df = 24$, $p < .01$). Respondents viewed "~~https~~," "not secure", and "not encrypted" as the least safe.

Threat. For invalid HTTPS, "none of the above" is not a desirable answer. We compared how many respondents answered "none of the above" (vs. any other response) and observed a significant difference between the strings (chi-square = 18.51, $df = 6$, $p < .01$). The "not secure" and "site not secure" strings yielded the most respondents who believed at least one of the negative actions could occur.

Action. When faced with an insecure connection, the ideal user behavior is to leave the website. As a result, we compared the ratio of respondents who chose "I'd leave the site" to the total of the other options. The chi-square reveals a significant difference (chi-square = 35.40, $df = 6$, $p < .01$), with "not safe" and "site not secure" ranking highest.

7.3.3 HTTP

Our HTTP security indicator needs to communicate a state that is mildly insecure, but not as insecure as invalid HTTPS or a known malware page. Using "http" would yield the least alarming indicator, and "site not secure" the most alarming.

Safety. Respondents felt at least somewhat safe with the "http" string, whereas "not private" and "site not secure" had the lowest percentage of respondents who felt at least somewhat safe. The differences between strings were statistically significant (chi-square = 116.59, $df = 24$, $p < .01$).

Threat. Respondents were most likely to select "none of the above" (vs. any other response) with the "http" string, which we interpret to mean they felt safest with the "http" string. On the other hand, they were most likely to choose at least one negative consequence with "not private." The differences between the set of strings was statistically significant (chi-square = 110.68, $df = 6$, $p < .01$).

Action. When using an HTTP page, we want respondents to seek more information and/or avoid entering their credit card. Across the strings we observed a significant difference in responses when comparing the number of respondents who say they would perform one of the actions compared to browsing normally (chi-square = 63.08, $df = 6$, $p < .01$), with respondents most likely to browse normally with "http."

8. DISCUSSION

We draw out the implications from our extension survey, Google Consumer Surveys, and prior work.

8.1 Shortcomings of HTTP indicators

We want indicators to teach people that HTTP is less secure than HTTPS. Conveying the threat of a network attacker with an icon and three words is challenging, and we don't think that browsers are currently succeeding.

Most of our extension survey respondents did not relate Chrome's HTTP indicator to connection security, despite their tech-savvy demographics. It was a disappointing but unsurprising finding. We can't say *why* they failed to mention connection security; it could be lack of knowledge, or that it did not come to mind at the moment of the survey. Either way, indicators are supposed to be immediately recognizable and understandable without significant thought.

Although we did not test other browsers' security indicators, we would not expect them to fare better at explaining HTTP. Edge and Safari don't display any indicator at all for HTTP, and UCWeb browsers don't distinguish between HTTP and HTTPS. Firefox's globe is neutral, so we suspect people would view it much like Chrome's neutral page icon. This means that we do not think Chrome can solve its problem by copying other browsers' HTTP indicators.

We did learn, however, that understanding security icons is not impossible for non-experts. Nearly all of our extension survey respondents associated Chrome's green lock with HTTPS and security. Their beliefs — particularly around identity — were not always complete or correct, but they still understand the general concept of the indicator. Although these respondents were tech-savvy, they were not security experts, which makes us hopeful that others will also learn the meanings of indicators with sufficient nudges.

8.2 Proposed connection security indicators

We propose three security indicators, shown in Figure 4. The strings should smoothly collapse or re-appear, depending on the page state and device screen size.

Section 6.4 describes how we narrowed down our icon choices to the lock, circle, and triangle. After testing, we modified the circle icon to more closely resemble the ISO Information Symbol; we hope that it will attract clicks from curious users seeking further information about the website.

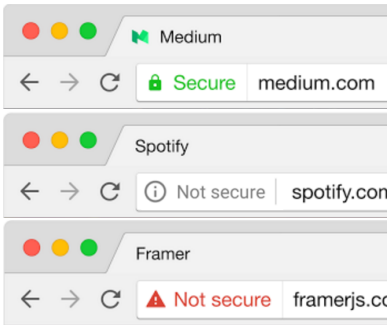


Figure 4: Proposed connection security indicators.

We chose strings after selecting the icons. For the positive security state, "secure" and "https" performed well across all three metrics (Section 7.3). Between the two, we preferred "secure" because it is less technical. We chose "not secure" for the neutral and negative states because it performed reasonably well and has a pleasing symmetry with "secure."

Chrome will launch our proposed connection security indicators with Chrome 53. However, we hope that our indicators are not limited to Chrome's URL bar. We would like to see other products that convey connection security adopt similar shapes to reinforce the meaning of the indicators. All of the icons are free to use as part of Material Design.[3]

Although we believe our changes are an improvement, open questions about HTTP remain. Our extension survey respondents did not connect HTTP with a lack of connection security. Despite our desire to teach people that HTTP is not secure, we do not want to frighten people from using the Internet. We therefore plan to gradually ease into the "not secure" label to avoid panicking people, beginning with private browsing mode because users are presumably performing privacy-sensitive tasks. Whether this is too conservative (or too aggressive) remains to be seen.

8.3 Malware security indicators

We can easily imagine why some end users do not distinguish between connection security indicators and website trustworthiness indicators. It is confusing, even to an expert, that clicking through a malware warning does not yield a negative security indicator in most browsers. In the extension survey, many tech-savvy people mistakenly believed that HTTPS identity guarantees pertain to website trustworthiness. Many GCS respondents similarly did not distinguish between the threat models.

Edge displays a negative security indicator for malware and phishing websites (Table 2). We recommend that other browsers, including Chrome, also use a negative security indicator for known malware and phishing websites.

8.4 Future work

Internationalization. One of our primary goals is to help new Internet users learn the meaning of security indicators. We added strings to the indicators specifically for this demographic. However, we have not yet tested the indicators in countries with many new Internet users; we only tested our icons with English-speaking Americans. Translation, cultural differences, or prior computing experiences might cause our results to not hold across countries. We need to do further work to find out whether we have achieved our full set of goals, although we expect that this will require a longitudinal field study to see whether people learn the meanings of the indicators over time. Thus, our next step is to test these indicators outside of the United States.

Repeat the survey. Once people have had time to acclimatize to the new icons, we should repeat the extension survey to see whether results remain the same. Will people be more likely to understand the HTTP indicator?

Attention. How might we draw users' attention to security indicators at the right time? (And when is the right time?) People sometimes ignore security indicators at crucial moments, or — worse — look within the content area of the website for the indicators [7]. Even if we were to train people to only look for security indicators in trusted browser UI, there are exceptions. Websites can add favicons to tabs, extensions can add icons near the URL bar, and so on. How might we teach people to look — and look in the right place?

9. CONCLUDING SUMMARY

We surveyed 1,329 people about Google Chrome's security indicators using a custom Chrome extension. Although our moderately tech-savvy respondents could relate Chrome's green lock to security, they had varying thoughts on the meaning of Chrome's neutral page icon. This motivated the need for new security indicators. Since existing security indicators from other browsers didn't entirely meet our design constraints, we set out to create new indicators.

We evaluated forty icons and seven complementary strings by surveying thousands of Google Consumer Survey respondents. Ultimately, we selected and proposed three indicators: Secure for HTTPS, Not secure for HTTP, and Not secure for invalid HTTPS. Our proposed indicators have been adopted by Chrome, and we hope to motivate others to update their security indicators as well. Our next step is to evaluate the indicators internationally, once they have been in use for several months.

10. ACKNOWLEDGMENTS

We thank Emily Stark and Lucas Garron for their help coding the extension survey responses, Chris Palmer for his input into the security icon redesign, and the rest of the Chrome security team for their feedback and support.

11. REFERENCES

[1] Inferred demographics. `https://support.google.com/consumersurveys/answer/6218151`.

[2] SmartScreen Filter: Frequently asked questions. `http://windows.microsoft.com/en-us/windows/smartscreen-filter-faq#1TC=windows-7`. Accessed February 2016.

[3] C. Amrutkar, P. Traynor, and P. C. van Oorschot. Measuring ssl indicators on mobile browsers: extended life, or end of the road? In *Information Security*, pages 86–103. Springer, 2012.

[4] R. Biddle, P. C. van Oorschot, A. S. Patrick, J. Sobey, and T. Whalen. Browser interfaces and Extended Validation SSL Certificates: An Ampirical Study. In

[3] `https://design.google.com/icons/`

Proceedings of the ACM Cloud Computing Security Workshop, 2009.

[5] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter. Your attention please: designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, page 6. ACM, 2013.

[6] G. Developers. SafeBrowsing API. `https://developers.google.com/safe-browsing/`. Accessed February 2016.

[7] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of ACM CHI*, 2006.

[8] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum. Users' conceptions of web security: A comparative study. In *Proceedings of ACM CHI*, 2002.

[9] I. Grigorik. HTTPS navigations in Chrome. `https://plus.google.com/+IlyaGrigorik/posts/7VSuQ66qA3C`, November 2014.

[10] C. Jackson, D. R. Simon, D. S. Tan, and A. Barth. An evaluation of extended validation and picture-in-picture phishing attacks. In *Proceedings of the International Conference on Financial Cryptography and International Conference on Usable Security*, 2007.

[11] F. Lardinois. Google launches Chrome extension to solicit user feedback about its browser. TechCrunch. `http://techcrunch.com/2015/05/11/google-launches-chrome-extension-to-solicit-user-feedback-about-its-browser`, May 2015.

[12] E. Lin, S. Greenberg, E. Trotter, D. Ma, and J. Aycock. Does domain highlighting help people identify phishing sites? In *Proceedings of CHI*, 2011.

[13] K. M. Help improve Chrome with this extension. `https://productforums.google.com/forum/#!category-topic/chrome/sUwEcHPygFU`, May 2015.

[14] M.-E. Maurer, A. De Luca, and T. Stockinger. Shining chrome: Using web browser personas to enhance SSL certificate visualization. In *Human-Computer Interaction – INTERACT*, 2011.

[15] P. McDonald, M. Mohebbi, and B. Slatkin. Comparing Google Consumer Surveys to existing probability and non-probability based Internet surveys. Technical report, Google Inc., 2015.

[16] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer. The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies. In *Proceedings of IEEE Symposium on Security and Privacy*, 2007.

[17] L. T. Sharpe, A. Stockman, H. Jagle, and J. Nathans. Opsin genes, cone photopigments, color vision and color blindness. In K. R. Gegenfurtner and L. T. Sharpe, editors, *Color Vision: From Genes to Perception*. Cambridge University Press, 1999.

[18] J.-E. Sneddon. Google's latest Chrome extension wants to ask you stuff. OMG!Chrome! `http://www.omgchrome.com/chrome-user-experience-surveys-extension/`, May 2015.

[19] J. Sobey, R. Biddle, P. C. van Oorschot, and A. S. Patrick. Exploring user reactions to browser cues for Extended Validation certificates. In *Proceedings of ESORICS*, 2008.

[20] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. On the challenges in usable security lab studies: lessons learned from replicating a study on ssl warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, page 3. ACM, 2011.

[21] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying wolf: An empirical study of ssl warning effectiveness. In *USENIX Security Symposium*, pages 399–416, 2009.

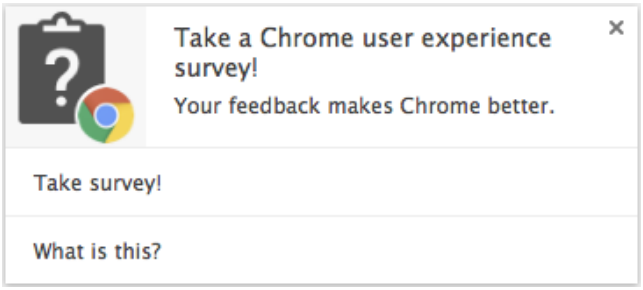
[22] R. Wash and E. Rader. Too much knowledge? Security beliefs and protective behaviors among United States Internet users. In *Proceedings of SOUPS*, 2015.

[23] T. Whalen and K. M. Inkpen. Gathering evidence: Use of visual security cues in web browsers. In *Proceedings of Graphics Interface*, 2005.

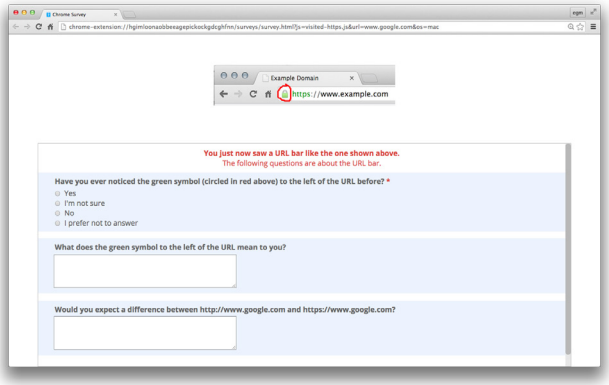
APPENDIX

A. EXTENSION SCREENSHOTS

When the survey criteria were met, the extension would generate a notification that looked like:



After clicking on the notification, the respondent would see a survey that looked like:



B. EXTENSION QUESTIONS

The full list of questions for the extension survey.

B.1 HTTP survey questions

1. Have you ever noticed the white symbol (circled in red above) to the left of the URL before?
   Yes
   I'm not sure
   No
   I prefer not to answer

2. What does the white symbol to the left of the URL mean to you? [Short answer]
3. Would you expect a difference between http://www.example.com and https://www.example.com? [Short answer]

B.2 HTTPS survey questions

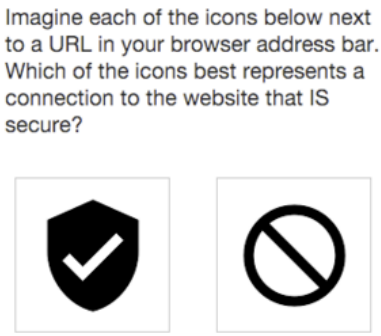
1. Have you ever noticed the green symbol (circled in red above) to the left of the URL before?
   Yes
   I'm not sure
   No
   I prefer not to answer
2. What does the green symbol to the left of the URL mean to you? [Short answer]
3. Would you expect a difference between http://www.example.com and https://www.example.com? [Short answer]

C. GCS SURVEY QUESTIONS

Examples of what the questions looked like to respondents.

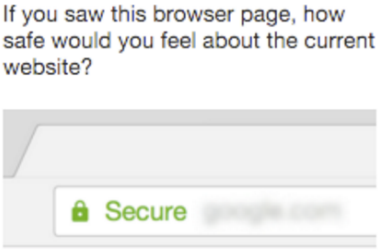
C.1 Icon questions

An example pairwise icon question:



C.2 Text questions

An example text question:



D. GCS SURVEY DEMOGRAPHICS

For completeness, we provide the *inferred* demographics of our survey respondents as provided by the GCS platform. We urge caution in interpreting inferred demographics. GCS assigns demographic characteristics to respondents based on their browsing history, which is an imperfect process [1].

D.1 Icon questions

	N	% of total
Male	496	49.6%
Female	349	34.9%
Unknown	155	15.5%
Age 18-24	131	13.1%
Age 25-34	178	17.8%
Age 35-44	157	15.7%
Age 45-54	132	13.2%
Age 55-64	109	10.9%
Age 65 or over	54	5.4%
Age Unknown	239	23.9%
Income $0-$24,999	80	8.0%
Income $25,000-$49,999	545	54.5%
Income $50,000-$74,999	250	25.0%
Income $75,000-$99,999	64	6.4%
Income $100,000-$149,999	24	2.4%
Income $150,000+	9	0.9%
Income Unknown	28	2.8%

D.2 Text questions

	N	% of total
Male	3006	46.5%
Female	2186	33.8%
Unknown	1270	19.7%
Age 18-24	918	14.2%
Age 25-34	1283	19.9%
Age 35-44	956	14.8%
Age 45-54	724	11.2%
Age 55-64	642	9.9%
Age 65+	312	4.8%
Unknown	1627	25.2%
Income $0-$24,999	576	8.9%
Income $25,000-$49,999	3421	52.9%
Income $50,000-$74,999	1624	25.1%
Income $75,000-$99,999	434	6.7%
Income $100,000-$149,999	151	2.3%
Income $150,000+	51	0.8%
Income Unknown	205	3.2%