# HTTPS-Only Modes: Improving warnings in Tor Browser and beyond

Killian Davitt
*King's College London*
United Kingdom
killian.davitt@kcl.ac.uk

Steven J. Murdoch
*University College London*
United Kingdom

***Abstract*—HTTPS-Only modes are new browser security features that present users with a warning page before proceeding to non-HTTPS websites. Despite these modes being available in most major browsers, little to no work has been done researching what these modes should be aiming to do, or how users react to these warnings. SSL Stripping attacks, which these modes mitigate are common in the Tor network. As a result, we studied these warnings in the context of Tor Browser. We deployed a survey of Tor experts and gathered their thoughts on these browser modes in general, as well as gaining specific feedback on 3 current warning pages. We report a number of potential improvements to HTTPS-Only mode warning pages. Future warning pages should mention specific types of attack that could occur. Warnings should also include discussion about the integrity of web content, not just confidentiality. The context of the website being visited is also not mentioned by current warning pages. Participants also highlighted that the warning as it appears in Tor Browser should feature some Tor specific advice. Finally, prompted by some participant responses, we engage in a discussion about whether the warnings should aim to deter non-HTTPS connections fully, or seek to empower users to make a determination themselves.**

***Index Terms*—SSL/TLS, HTTPS-Only, Tor Browser**

## I. Introduction

HTTPS-Only modes are web browser modes that show a warning page to users if the website they are visiting does not support HTTPS. Users must click through these warning pages to visit non-HTTPS websites [1]. This has been an optional mode in the Firefox browser since 2020 [2], as well as in Chrome [3] and Microsoft Edge [4] since 2021.

The primary function of HTTPS-Only modes is to notify users of potential man-in-the-middle attacks. HTTPS-Only modes also automatically upgrade connections to HTTPS when available, however, this is a feature that can be implemented without the intrusiveness of a warning page. The primary man-in-the-middle attack that can be conducted is an SSL stripping attack which can surreptitiously downgrade HTTPS SSL connections. If this attack is performed, a user's traffic can be subject to eavesdropping or alteration even if their browser normally upgrades all connections to HTTPS. Previously, it would be sufficient to automatically upgrade users' requests from HTTP to HTTPS. Websites that supported HTTPS would have secure connections to them, and thus the adversary would be defeated in as many cases as possible. With SSL stripping, protections must force connections to be HTTPS when possible, or, if this is not possible, warn users when the site they are visiting does not support HTTPS. This situation is particularly relevant to Tor, where bad exit nodes can intercept traffic. If a bad exit node does attempt an SSL stripping attack, an HTTPS-Only mode warning page can cause a user to rethink their decision to browse to the website.

HTTPS-Only modes are feasible because of the increased HTTPS adoption on the internet. The internet has rapidly been approaching a state of very high HTTPS adoption, although it may still be some time before the long tail of less popular websites adopts HTTPS in larger numbers [5].

There is current very little literature available on HTTPS-Only modes, this study serves as one of the first proper investigations into what information should and should not be included on HTTPS-Only mode warning pages. The specific focus of the study was risk in Tor Browser, however, some of the results are also applicable to other web browsers.

The open-ended survey in this project gathered a range of ideas specifically from Tor experts. The survey sought information both about general risks for web browsing without HTTP, as well as risks which are exacerbated when using Tor. The survey also presented participants with 3 example warning pages including the current Tor Browser warning page and elicited criticism on them.

The results of the survey produced a variety of themes which can provide insight into future designs of both Tor Browser and other browsers' HTTP-Only Mode warning pages.

82% agreed that the level of risk varies depending on the activity being performed. 61% specifically stated that non-HTTPS websites are less risky if no personal information or account information is being entered. 21% expressed in some form that users should be aware that alterations could be made to the website in question This risk from bad Tor exit nodes was persistently mentioned by participants. 17 of the 28 participants (61%) directly referenced this risk. 11% expressed the view that users should not necessarily be faced with decisions of this nature and that the best decision should be made for them.

For all three example warning pages included, many more participants believed the page was understating the danger than overstating.

## II. Research Questions

The first goal of this work (RQ1) is to elicit discussion of HTTPS-Only modes in general and to determine their goals. Given the limited work that is available on this topic and their limited deployment, exploring users general thoughts on the mode is an important contribution. For RQ2, we begin our Tor Browser specific work and investigate how the experience of HTTPS-Only modes can or should differ from other browsers. Finally for RQ3, we provide a more specific discussion of improvements that can be made to the warning pages to achieve their goals. We provide improvements that are Tor specific but also recommendations which can also be applied to other browsers.

1) RQ1: What should the goals of HTTPS-Only mode warning pages be?
2) RQ2: What issues effect HTTPS-Only mode warning pages for Tor Browser in particular?
3) RQ3: What improvements can be made to HTTPS-Only mode warning pages in general and specifically for Tor Browser?

## III. Background

### A. SSL Stripping Attacks

Although the authenticity guarantees provided by SSL mean an adversary cannot easily impersonate legitimate websites, an adversary can downgrade attempted HTTPS connections via a man-in-the-middle attack. This is known as SSL Stripping [6].

The simplest SSL Stripping attack is performed when the man-in-the-middle attacker does not forward a website's request to upgrade to HTTPS. The connection remains unencrypted and the attacker can view all of the traffic. This only works when the users web browser does not request HTTPS by default. More complex SSL Stripping attacks can also downgrade connections which were initially requested via HTTPS [7].

### B. HTTPS-Only Modes

HTTPS-Only modes are a relatively new option in most popular web browsers that forces HTTPS connections to websites. When enabled, this option first automatically attempts to load all web connections via HTTPS. Secondly, if the website does not support HTTPS, a warning is displayed to the user, and they can choose whether they wish to continue to the website without the protection of HTTPS. HTTPS-Only mode was first introduced in Firefox in 2020 [2], in Google Chrome in 2021 [8] and in Microsoft Edge in 2021 [4]. Safari does not include a mode that warns users about proceeding to HTTP pages; however, all requests are now automatically upgraded to HTTPS if it has been available since Safari 15 [9]. The Brave browser also includes a HTTPS-Only mode, it is the only major browser aside from Tor Browser to enable the mode by default [10]. All other browsers do not enable HTTPS-Only modes by default.

Automatically upgrading requests to HTTPS provides enhanced security at no cost or disadvantage to users. Displaying a warning to users can also help them recognise situations where it may be dangerous to proceed to a non-HTTPS website.

The adoption rate of HTTPS has increased dramatically over the past number of years. Websites with HTTPS as default rose from 26.9% in 2018 to 84.9% in 2024 [11]. It is also the case that smaller, less intrusive indicators to users are not as effective at convincing users not to proceed to websites [12].

As adoption grows, there has been a clear effort to have more users use HTTPS connections and to encourage users not to connect to non-HTTPS sites. This began with decisions to block mixed source content in web browsers, for example by Chrome in 2018 [13], and more controversially in 2019 with Google Chrome marking non-HTTPS sites as "insecure" [14]. In the last few years, HTTPS-Only modes have been the latest step by web Browsers to ensure more and more users' browsing activity is secured by HTTPS. The transition from URL bar indicators to full page warnings provided by HTTPS-Only modes provides users a much more explicit warning. It can alert them to danger in both cases where they may be visiting a new site that does not have HTTPS enabled or, perhaps more seriously, alerting them that a site they usually visit and normally does have HTTPS.

As the adoption of HTTPS continues to rise, the potential for harsher measures warning against non-HTTPS websites appears more likely. This follows from Krol's [15] work on false positive habituation. As warnings are seen by users less often, they can be more disruptive.

An analysis of the current HTTPS-Only mode Warning pages offered by major browsers is provided in Section IV.

### C. Tor Browser and HTTPS-Only Modes

Tor Browser has included the HTTPS Everywhere addon since 2010 [16]. This has meant that websites are automatically upgraded to HTTPS when available. HTTPS Everywhere also featured the 'EASE Mode' function, which provided a warning page exactly like HTTPS-Only modes; however, the Tor Project has never recommended enabling this option as selectively enabling it would make the users' browser fingerprint different to other Tor Browser users [17].

Reducing the danger that is faced from non-HTTPS websites has long been a priority of the Tor Project. Discussions have taken place since 2016 into how this would be achieved, however, adoption of a default non-HTTPS blocking mode did not occur until 2022 [18]. Tor Browser is ultimately an updated packaging of Firefox, and thus, the HTTPS-Only mode added to Firefox was imported into Tor Browser in 2022. It was also enabled by default in release 11.5 [19] fulfilling this long ambition to reduce the risk users faced from non-HTTPS connections, in particular due to the danger posed by bad exit nodes in the Tor network.

HTTPS-Only mode have particular relevance for Tor Browser, where exit nodes are in an ideal position to deploy SSL-Stripping attacks. SSL Stripping attacks have been deployed in the wild in the Tor network resulting in the loss of users' cryptocurrency [20]. At the same time, these attacks

are not restricted only to Tor and have been seen to cause many security problems in regular browsing, including some high-profile attacks [21].

We note that Tor hidden service connections do not support HTTPS[1] and are exempted from HTTPS-Only mode warnings.

### D. HTTPS Adoption

The effectiveness of HTTPS-Only modes could largely depend on the level of adoption of HTTPS on the Internet. If HTTPS adoption was low, users would frequently be faced with false positive warnings that interrupt their browsing experience, prior works shows that high false positive rates reduce the effectiveness of warnings [15]. High rates of HTTPS adoption ensures that users see false positive warnings infrequently, and the presentation of a warning has a higher chance of indicating that an attack is taking place.

HTTPS has become more widespread [22], after growing steadily for approximately the last decade. As a proxy for HTTPS availability, HTTPS adoption currently is measured at about 84.9% by W3Techs [23] for default protocol HTTPS and Google has measured 90% of navigations using the Google Chrome browser as being to HTTPS domains [24]. This means that while a large proportion of website visits are likely to be HTTPS, there are still a sizeable number of visits to HTTP sites under legitimate circumstances where the website has chosen not to implement HTTPS.

Felt *et al*. [25] attempted to measure HTTPS across the web in 2017. This proved a difficult challenge due to the many possible interpretations of HTTPS adoption. Nevertheless, the result showed a continuing increase in HTTPS adoption, which has continued in the years since the release of this paper.

## IV. Analysis of Current Warning Pages

I will next continue to an analysis of the currently deployed HTTPS-Only mode warning pages from a number of popular web browsers. Surveying the features of these warning pages provides insight into how improved warning pages could be designed.

### A. Google Chrome

The HTTPS-Only mode warning page included in Google Chrome as of version 118 is short relative to other browsers' warnings. It has a SMOG index of 10.1[2] and consists of only 2 sentences. The warning is displayed in Figure 1. It provides two simple statements: that the connection is not secure and that the warning has appeared because the site does not support HTTPS. A link to learn more is also provided[3].

Google Chromes standard insecure loading bar can also be seen in gray text. The grey text contrasts the green text provided for HTTPS websites, and the Red text provided for more severe SSL errors like expired certificates. This standard design is present even when HTTPS-Only mode is not enabled. It is noteworthy that the more serious 'red' branding is not used, potentially to differentiate a HTTPS-Only warning from a more serious warning which would indicate definite danger.

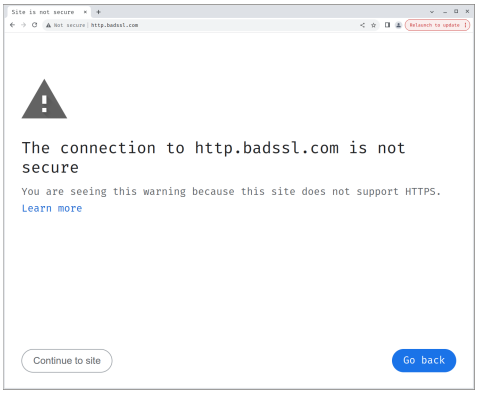


Fig. 1. Chrome HTTPS-Only mode warning page

### B. Brave

The Brave web browser [27] includes a HTTPS-Only mode [28]. Its behaviour and appearance are identical to that of Google Chrome due to Brave being based on the Chromium project. Much like Google Chrome, a link is provided for users to learn more[4]

### C. Microsoft Edge

The Microsoft Edge warning contains significantly more information than all other HTTPS-Only mode warning pages as can be seen in Figure 2. The information can be divided into three different sections: the initial information block, tips on what to try, and an additional details block, which is hidden until clicked on. The warning has a SMOG index of 9.7 which is lower than both Google Chrome and Firefox, despite its much longer length (16 sentences).

The warning page does not appear to warn the user of any actual danger, and it is likely not clear to users that a lack of HTTPS could be a sign of danger or attack. The first tip to users when seeing this page is to fall back to a HTTP connection, which likely encourages users to do exactly that and not to consider the issue any further.

### D. Safari

Safari does not provide an explicit HTTPS-Only mode; however, it does automatically upgrade all requests to HTTPS.

### E. Firefox

The Firefox HTTPS-Only mode warning page in Figure 3 is also currently shared by Tor Browser. The warning contains a large header, followed by a statement reminding the user that they have turned on HTTPS-Only mode and that the current website does not support HTTPS. The warning has a SMOG index of 10.7 and includes 8 sentences. Two scenarios are

[1]Hidden Service connections are already encrypted and so TLS is not required.

[2]SMOG [26] is a reading comprehensibility score, higher scores indicate more complex, difficult text.

[3]https://support.google.com/chrome/answer/10468685#https-only-mode

[4]https://support.brave.com/hc/en-us/articles/15513090104717

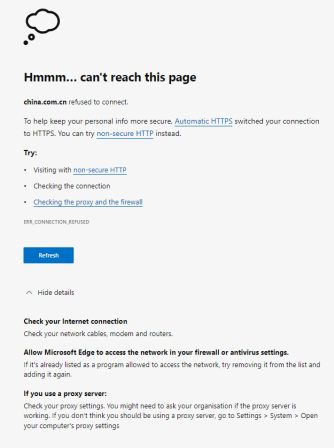


Fig. 2. Edge HTTPS-Only mode warning page

given, informing the user what might be happening to cause the error; either the website does not support HTTPS, or an attacker could be involved. The user is urged not to enter sensitive information if they continue.

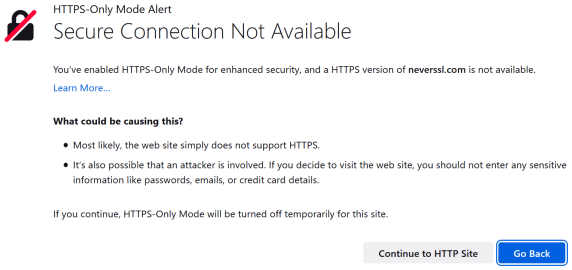


Fig. 3. Firefox HTTPS-Only mode warning page

Some changes to the standard text have been made in previous years [29] but no widespread survey or testing has been conducted on these texts.

### F. HTTPS Everywhere (EASE Mode)

The HTTPS Everywhere browser addon has long provided 'EASE Mode' (Encrypt All Sites Eligible) which warns users when connecting to non-HTTPS websites. This warning can be seen in Figure 4 This warning page is substantially different to the other warnings discussed. In particular, the information is contained effectively in one large paragraph, in contrast to Firefox and Edge's bullet points or Google Chrome's short length. The warning additionally contains little advice to users, and does not describe any specific warnings or risk scenarios

## V. Survey Design

### A. Recruitment

As stated, the goal of this survey is to consult individuals who are already knowledgeable about Tor Browser and are familiar with browser security. Discussing this topic with participants who understand the technology allows us to properly


Fig. 4. HTTPS Everywhere (EASE Mode) warning page

evaluate what risks are relevant for non-HTTPS connections and what is missing from the current warnings Participants were recruited directly from the Tor community. Our three main avenues of recruitment were a recruitment message sent to the official Tor mailing list, a post on the Tor forums, and a tweet sent out by the Tor project Twitter account. After deploying and advertising the survey, we waited for approximately 3 weeks until no new submissions were being received, and the final number of responses was 31. Our goal was to have a smaller number of higher quality participant responses. Our survey consisted mainly of open-ended text questions, and the study aimed to encourage participants to be as verbose as they could be and to include any thoughts they had on the subject. We opted not to collect any demographic information on participants as Tor users and experts are more likely to be unwilling to provide this information. Including these questions may have discouraged participants from completing the survey.

Although this was an effective method of finding participants who were exceptionally knowledgeable about Tor and Tor Browser, the participants cannot be guaranteed to be experts. Data from these participants was assessed to ensure that participants with incorrect or incomplete knowledge of Tor were not included in our results.

### B. Ethics

This survey received ethical approval from the UCL Ethics Committee. No personal data was collected from participants, except if they optionally agreed to provide their name to be credited in publication. Participants were warned not to provide any other personally identifiable information aside from this. All parts of the survey were optional.

### C. Questions

The survey itself consists of nine open ended questions about HTTPS-Only modes in general, before presenting participants with three different examples of HTTPS-Only mode warning pages and asking three open ended questions about each page. The full list of questions can be seen in Appendix A.

The questions cover the risks from visiting non-HTTPS websites, how these risks change for Tor Browser users,

whether specific criteria make this more risky or not. Participants are also asked what they personally do as regards non-HTTPS websites. The survey then asks about the concepts of Confidentiality, Integrity and Authenticity and whether it is necessary to understand these to make a safe determination. Confidentiality, Integrity and Authenticity (CIA) are three of the main guarantees that TLS offers. A complete assessment of whether TLS is required in a certain situation should therefore require an understanding of what TLS offers.

Finally, the three current warning pages are presented[5] and participants are asked if the page is accurate, if anything is left out, or if it overwarns users.

The selected warning pages to display are:

1) The current Firefox HTTPS-Only mode warning page (as of version 96)
2) The HTTPS Everywhere EASE mode warning page as was previously displayed in Tor Browser (Figure 4)
3) A previously used Tor Browser HTTPS-Only mode warning page (version 11) (Figure 5)

The previously used Tor Browser warning page is in fact an old version of the Firefox warning page. Tor Browser is a variant of Firefox, and due to the nature of the build process which incorporates Firefox's long term support release, it includes an older version of the warning. The current Firefox warning was selected as it was likely to be included in Tor Browser in the future. Some months after the completion of the survey, this warning page became the current Tor Browser warning in version 11.5. HTTPS Everywhere was previously included as an addon in every Tor Browser build. Before the advent of Firefox's HTTPS-Only mode, this addon fulfilled the same task when the 'EASE Mode' (Encrypt All Sites Eligible) was enabled.

The current Firefox warning and the Tor Browser warning are textually very similar, they warn the user that an attacker could be involved and not to enter any sensitive information. These two warning are aesthetically different with some different visual design choices. The HTTPS Everywhere EASE mode features different text and does not include any warnings about sensitive information.

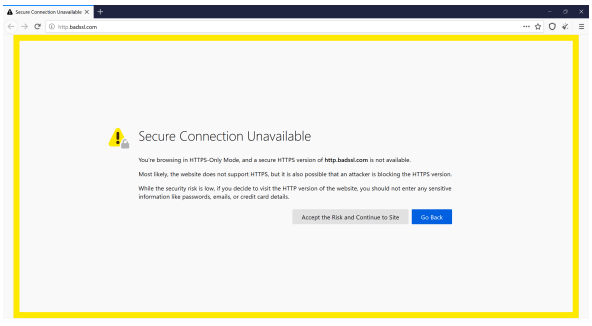


Fig. 5. Older Tor HTTPS-Only mode warning page (version 11)

[5]Note that some of the warning pages show the url that was visited by the user. This may have some effect on participants reaction, but is not possible to control for.

## VI. Results

Over 2 weeks from 18th January 2022[6], we received 31 responses to our survey[7], of which 28 were usable. The three discarded responses were blank, or had very minimal text which was not considered useful to analyze. The mean word count from the used responses was 330. The shortest was 67 words and the longest was 646. This demonstrates the amount of data provided by participants which provided a lengthy insight into their views on HTTPS-Only modes. The data was then organized and coded, providing some quantitative insight into participants' views on the provided HTTPS-Only mode warning pages.

The data was analyses using a Grounded Theory approach. Due to the clear nature of the themes being studied and the lack of complex or subjective codes being applied, a single coder was considered sufficient for this data.

The codebook is provided in Tables I and II.

| Code | Count |
|---|---|
| http_okay_if_no_personal_info/account | 28 |
| risk_level_does_vary_on_activity | 23 |
| tor_is_riskier_because_of_exit_nodes | 18 |
| users_need_to_understand_cia | 16 |
| am_i_interacting_or_providing_info_to_the_site | 14 |
| exit_nodes_are_a_risk | 10 |
| risk_of_data_being_altered | 9 |
| loss_of_account_info_is_a_http_risk | 8 |
| users_dont_need_to_understand_cia | 8 |
| mitm_attacks_are_a_http_risk | 7 |
| tor_users_dont_understand_cia | 6 |
| tor_is_riskier_http | 6 |
| users_should_know_data_could_be_altered | 6 |
| risk_from_isp | 5 |
| sometimes_I_just_need_to_access_the_site | 5 |
| downloading_files_is_riskier | 5 |
| tor_users_are_technical | 5 |
| users_not_need_understand_browser_should_make_decisions | 5 |
| users_should_know_dont_enter_data | 5 |
| risk_varies_but_is_never_zero | 4 |
| reputation_of_site_matters | 4 |
| cryptocurrency-as-a-risk | 3 |
| injection_of_ads_is_a_risk | 3 |
| isps_versus_exit_nodes | 3 |
| tor_is_riskier_because_of_user_demographic | 3 |
| tor_users_understand_c_but_not_ia | 3 |
| users_should_know_exit_nodes_are_a_risk | 3 |
| users_should_never_proceed | 3 |
| wont_login_to_http_sites | 3 |
| blocking_javascript_reduces_risk | 2 |
| home_versus_public_network | 2 |
| risk_depends_on_type_of_site | 2 |

TABLE I
CODEBOOK FOR PARTICIPANTS VIEWS ON RISK FROM NON-HTTPS, AND SPECIFIC RISK TO TOR USERS.

### A. General HTTP Risks

*1) Logging in Presents Risk:* 23 participants (82%) agreed that the level of risk varies depending on the activity being performed. One of the most common reasons highlighted was the use of login credentials.

[6]In the 3 years since deploying the survey there have been no changes to the analyzed warning pages, except that Tor Browser has adopted the "current Firefox warning" as it's warning

[7]Results data is available here: https://osf.io/xgm97

| Code | Count |
|---|---|
| HTTPS Everywhere | |
| inaccurate | 16 |
| accurate | 13 |
| should_give_specific_risks | 11 |
| understates_risks | 9 |
| overstates_risks | 2 |
| should_warn_about_risk_of_contexts | 1 |
| confusing | 2 |
| too_long | 2 |
| Old Tor Browser Warning | |
| accurate | 12 |
| understates_risks | 10 |
| could_link_to_specific_anonymity_information | 8 |
| should_give_specific_risks | 6 |
| should_warn_of_contextual_threats | 2 |
| inaccurate | 1 |
| overstates_risks | 1 |
| Current Firefox/Tor Browser Warning | |
| accurate | 11 |
| understates_risks | 10 |
| should_give_specific_risks | 8 |
| inaccurate | 7 |
| overstates_risks | 2 |

TABLE II
CODEBOOK FOR PARTICIPANTS VIEWS ON THE 3 PROVIDED WARNING PAGES.

*2) Risk for Personal Information:* 28 participants (100%) specifically stated that non-HTTPS websites are less risky if no personal information or account information is being entered. All either stated that there was less risk or no risk for users who did not log in or provide personal information. P11 stated this succinctly: *"If an important website is HTTP while also holding people's accounts ... then data can be easily taken off of the data packets by someone with ill intentions."*

P22 conveyed this using the term *"read-only website"* which may be a useful analogy for users in the future. They also further stressed that this reduced risk is not no risk *"Visiting a non-HTTPS site is never fully safe."*.

*3) Risk from Downloading Files:* One risk which was only mentioned by five participants (18%) is the risk of downloading files. P3 specifically mentions executable binary files being riskier for users.

*4) Risk is Never Zero:* 4 participants (14%) took the opinion that while the level of risk does vary, it is never zero. For some sites, it would be very unwise to proceed without HTTPS, but even when browsing a website where no personal data is entered, and where no level of trust is assumed for the content, there are still risks.

*5) Integrity of the Website:* 9 participants (32%) discussed the risks of data being altered by a third party. The principle of integrity is of course provided by SSL and thus is something that is not available with HTTP connections. P9 states the risk succinctly *"A malicious party can alter the website content."*. P10 then outlines their criteria for deciding if this is a risk for them *"Safe example would include visiting a store's website to check their opening hours, or reading a Wikipedia page; it is unlikely that an attacker modifying this information would cause any harm."*

*6) Injection of Advertising:* Participants 1,12,13, and 24 highlighted the risk of injection of advertising. Most responses discuss this risk in the context of Internet Service Providers rather than Tor exit nodes. Both Tor exit nodes and ISPs have the ability to modify unencrypted traffic to insert advertising. P13 claimed direct experience with this: *"I've experienced, first hand, MITM attacks from US companies. They hijack the connection to insert JavaScript powered advertising"*. No participants specifically mentioned seeing this practice performed by Tor exit nodes. Injecting advertising would also further contribute to the perverse incentives outlined below in Section VI-B2.

*7) Users Should be Aware that websites could be altered without HTTPS:* Opinions from participants were varied on this topic. No one theme appeared to be dominant in the data. Six participants (21%) expressed in some form that users should be aware that alterations could be made to the website in question. Some participants note in a general sense that *"The contents of the page might have been modified from what the site tried to send."*( P21).

P9 warns that *"Website content, especially things like bank account number, contact data should not be trusted."*.

### B. Does Tor Browser Come with Greater Risk?

Many users mentioned circumstances where Tor Browser users could experience higher levels of risk than other non-Tor browsers. The vast majority of these situations involved bad Tor exit nodes which could act as adversaries against Tor users. This risk from bad Tor exit nodes was persistently mentioned by participants. 18 of the 28 participants (64%) directly referenced this risk.

*1) Contrast Between Trust Models of ISPs and Tor Exit Nodes:* When someone is not using Tor to connect to the internet, the users' ISP has broadly the same powers as a Tor exit node to intercept, modify or read non encrypted traffic. Five participants (18%) did express concern that ISPs could perform some form on traffic sniffing on unencrypted connections.

Although ISPs may be more trustworthy because they have an economic incentive to maintain the trust of their user base it is also typically difficult to change ISP quickly, in contrast, Tor exit nodes have much less incentive to maintain trust, however they can be changed out with extreme ease. P10 reminds us that the effort required for a bad actor to set up a bad exit node is dramatically less than the effort required to set up an ISP. P1 compared the risk of bad exit nodes to an ISP interfering in traffic. *"Exit nodes are in a position to attack and they are known to do so... your ISP is in the same position, and they are also known to do bad things... You can't change ISP quickly, but they have reputation and tend not to want to lose it."*

*2) Perverse Incentives for Exit Node Operators:* Providing a concrete example of the risk users face from bad Tor exit nodes, P3 mentions the SSL stripping attacks which occurred throughout 2020 in the Tor network [20]. These attacks focused mainly on cryptocurrency based websites and

were an effort to steal users cryptocurrency. This highlights attackers' economic motivation for attacks, perhaps users are at greater risk when conducting activities where an attacker could gain real financial benefit. P4 also mentions the ability of exit nodes to insert affiliate links to websites in order to gain a financial benefit.

P9 highlights the risk of law enforcement deterring legitimate exit node operators. If legitimate operators have to constantly fear action from law enforcement, they are less likely to continue operating their exit node, thus bad exit nodes, which do not have to worry about this risk are encouraged.

Other participants provided other worries about the legitimacy of exit nodes and their ability to attack users. P23 notes that as exit nodes are run by volunteers, they may have malicious motives for running the node. P10 noted that there is very limited oversight processes for exit node operators.

*3) Demographic Risk:* Although the risk of bad exit nodes was the primary concern raised by participants, some respondents were concerned of the demographic risk to users. P8,17 both agreed that users of Tor are more at risk specifically because of the type of person that uses Tor. P8 believed that: *"many people use Tor for sensitive research."*, P8 did not elaborate on this but the implication of this would be that they believe that those accessing sensitive information may be more at risk of being monitored or attacked. P17 simply states that a Tor Browser user is more likely to be under surveillance. Despite this being a potential factor in the risk facing Tor users, it is a non specific risk and is not necessarily limited to a particular browsing scenario.

### C. Heuristic Measures of Risk

A number of participants discussed different heuristics they used for deciding whether a website was risky or not. As opposed to clear cut indicators of risk, these heuristics provide a inexact assistance to users.

P18 provides an interesting perspective into when one can expect non-HTTPS. They cite the example of a small organization who do not have the proper IT resources required to set up a HTTPS enabled website.

Only one participant, P20 raised the issue of home versus public Wi-Fi networks. The participant is likely referring to non-HTTPS connections which are not over the Tor network as using Tor would negate any risk from a local network adversary.

Four participants (14%) discussed the reputation of the website being a factor. Three participants (11%) expressed that they would be more likely to continue to the website if they held it in high regard, as P18 stated *"If I know who owns the website, the organization behind it, I might proceed."*

This reasoning does not protect against man-in-the-middle attacks from Tor exit nodes, a high reputation website will not be safer than a low reputation website when this warning appears.

Only one participant, P10 reports *"whether the site was previously available over HTTPS."* as being a factor for them proceeding past the warning or not.

### D. Other Factors

*1) Users Should not be Faced with this Decision & Potentially Warned Away:* Five participants (18%) expressed the view that users should not necessarily be faced with decisions of this nature and that the best decision should be made for them. P24 states: *"I don't think non technical users can really understand the risks because the risks are mostly invisible."*. This comports somewhat with previous design choices by Tor Browser which seek to minimize users' cognitive load however it may be the case that all cognitive load cannot be removed from users in this scenario and users must be informed somewhat about the risks so they can make an informed choice on whether to proceed or not.

Similarly, three participants (11%) advocated strongly warning users away from proceeding under any circumstances. P15 states *"A user must avoid a non-HTTPS site at all times except when it is really necessary"* and P17 states *"A good rule of thumb is 'don't do it."'*.

*2) Blocking of JavaScript as a Defense:* As a defence against some non-HTTPS risks, P3 and P27 propose blocking JavaScript. JavaScript can be a significant attack vector for malicious sites, and Tor Browser does include the NoScript addon for blocking JavaScript [30]. By default it is not enabled, but changing the security level of Tor Browser from *'Standard'* to *'Safer'* causes JavaScript to be blocked on non-HTTPS websites [31]. Elevating this to *'Safest'* causes all JavaScript to be blocked.

*3) No Clear Answer on Whether Users Need to Understand CIA:* There was a clear divide between participants on this topic; the majority (16) (57%) believed that understanding *cia* was necessary for users, whilst eight participants thought that it was not needed. In arguing for the point, P3 states *"for example, you shouldn't download a file over HTTP without checking its integrity. So a warning explaining which potential risks can happen is important."*

For users to understand that files being downloaded over HTTP are more risky, there must be an inherent understanding of integrity. Users must understand that an attacker could alter the file in any way and it would not be flagged by their system (the exception to this being signed software).

*4) Overwhelming Need to Access the Site:* Another factor which was seen from participants is the expression that sometimes the need to access a website is particularly great, and thus users will continue, even if they were not confident in it's safety. Five different participants (18%) expressed this view in some form. P2 states: *"How much I need to access it to complete whatever task brought me to that resource."*. P8 states *"How much I care about the content (ex, was the headline really interesting?)"* this shows that the factors which contribute to proceeding past a warning can go beyond just the level of perceived risk, users can tolerate greater risk if the reason is important [32].

### E. Current Tor Browser warning page (Firefox)

There was mixed opinions amongst participants on whether Firefox's current warning page accurately portrays the correct

level of risk to users. 11 participants (39%) stated that the page did provide accurate information, while 7 (25%) disagreed with this. Most participants did not elaborate on their opinions.

*1) Specific Tor Risks Should be Mentioned:* When asked what was left out of the page, 18 participants (64%) provided an answer. 8 (29%) of these responses specifically mentioned adding mention of the specific risks which are faced by users. Another two participants (7%) stated that it should be indicated that this could be an issue with the exit node being used and users should be guided to change to a new Tor circuit. P15 stated that the page could be improved by mentioning specific risks that are faced when using Tor.

*2) No Mention of Content Alteration Risk:* One participant mentioned that there is no mention of the risk of content being altered *"It leaves out the risk of an attacker tampering with the content. Downloads could be swapped out with malware"*.

*3) Understating Risk:* When asked whether the warning page was understating or overstating the risk the opinion of participants was much clearer. 10 (36%) of the 25 participants answering clearly indicated that they believed the page as understating the risks, while only 2 participants (7%) indicated it was overstating the risk. One participant believed that the page was understating the risks due to the lack of information of Tor specific attacks. From this it is extrapolated that the participant is referring to the lack of information available on bad Tor exit nodes in the warning page.

One participant who believed that page overstated the warning, said so because *"the dangers are highly dependent on the nature of the visited website."*.

### F. HTTPS-Everywhere

*1) The warning is too technical:* 11 participants (39%) wrote that the effectiveness of the HTTPS Everywhere warning page could be improve by citing specific risks that users face, instead of giving broad technical description of the attacks that could occur. P3 summed this up as follows: *"'network-based downgrade attacks' is term that users probably wouldn't understand, so changing that to real examples like: an attacker could steal your login credentials, tamper your download...that would be more easy to understand."*.

P27 has a similar concern: *"yes it informs accurately but that does not mean all users will necessary appreciate all the risks language such as 'downgrade attacks' is probably opaque to a subset of users"*. P20 complained that the text was confusing and suggested that overall it should be simplified and state only basic facts.

9 participants believed the warning understated the danger and 2 believed it overstates.

### G. Old Tor Browser warning page

Generally, participants did not express concerns that were much different than the current Firefox warning page.

When asked what was left out of the Tor Browser warning page, 16 participants (57%) provided an answer. 6 (38% of those) of these participants once again believed that the warning page should include more specific risks. One participant highlighted risks to privacy and also more disastrous JavaScript issues *"An attack can still monitor what you do and run scripts."*. Three participants (11%) highlighted the lack of explanation of the risk of content alteration. *"No explanation about the risks of page content being altered (like banking account number, contact details, downloaded app being replaced with a malicious one)."*.

*1) Generally Understated Risk:* As with the previous two warning pages, many more participants believed the page understated the risk rather than overstated. 10 participants (36%) considered the page to be understating the risk and 1 believed it overstated. Another 12 (43%) believed the warning was okay, or did not have strong opinions. Participants were terse in their descriptions but most followed the sentiment of one participant saying the page was *"de-emphasizing the possibility that something might actually be going wrong."*. Another participant specifically discussed the style and design of the page stating *"It could be designed even better to grab the users attention. If I were to see this, I would barely even read this page..."*

## VII. Discussion

### A. Context is a Key Indicator of Risk from non-HTTPS Websites

In earlier sections of the survey, participants discussed the different risk factors for non-HTTPS websites and in particular what factors influence whether or not they will continue to the website. The strongest indicator of risk for participants was the need to enter personal information. This ranges from basic information like names or addresses to banking information or credit card numbers. This risk was discussed by a large number of respondents, both as a general risk and when asked about the factors that participants considered themselves when visiting non-HTTPS websites. Other contextual risks were also raised by participants.

Some participants mentioned cryptocurrencies as a risk factor. Since cryptocurrencies are typically transferred by reading a users address (potentially from a website). Non-HTTPS requests could have altered addresses and could redirect users' payments. This may mean users should not participate in cryptocurrency activities on non-HTTPS websites.

A small number of participants mentioned the size of the website being accessed as an indicator of risk. This is most succinctly put by P18 *"Sometimes I am accessing a small coop or small organisation website ... and they just don't have https enabled because of lack of IT resources"*. Although users are still vulnerable to all of the same attacks when using smaller websites, it may be the case that a lack of HTTPS is less surprising and is not indicative of an attack being performed. On the contrary, a large enterprises website would be fully expected to implement HTTPS and being faced with a warning there would indicate a high likelihood of an attack being performed against the user.

### B. Should Users be Encouraged not to Proceed

Currently, HTTPS-Only modes attempt to offer a reasonable choice to users when faced with websites that do not support HTTPS. In some cases, it may be acceptable to proceed past the warning to a non-HTTPS website, and in other cases, it may be dangerous to do so. Some participants argued that this distinction should be disregarded, and that in fact, warning pages should completely discourage proceeding to non-HTTPS websites of any kind.

Always blocking non-HTTPS websites, or designing warnings in a way that always discourages users from proceeding would preclude users from accessing legitimate websites that do not provide HTTPS. It is not clear what the level of disruption this would cause currently; approximately 84.9% of websites currently provide HTTPS [11] which potentially could cover the vast majority of websites visited by users however it is not known whether the distribution of websites visited by Tor users aligns with this figure.

Current SSL warnings follow this paradigm of discouraging users from proceeding in any circumstance. The success of SSL warning pages is measured purely as the percentage of users who do not proceed past the warning. Key work on SSL warnings by Felt [33], [34] only uses this metric.

As the percentage of HTTPS enabled websites grows higher and higher, the argument for discouraging proceeding becomes more powerful. As HTTPS adoption becomes very high, the number of cases where a user is warned away from a legitimate website that does not implement HTTPS becomes lower. This debate forms the basis of our answer to RQ1.

### C. Comparison between Warning pages

Of the 3 warning pages surveyed, it is clear that users have more issues with the older two warning pages rather than the newer Firefox warning. There still are however common issues which are not addressed in any of the warning pages and which will need to be addressed in future.

### D. Improved Warning Pages

The purpose of this survey was to scope out potential factors which could help in designing improved warning pages which are specific to Tor Browser. While analyzing the responses to the survey, we identified 5 different general themes which were highlighted multiple times by participants and which could form the basis of an improved warning page. It is important to note that while these themes can provide useful additions to warning pages, adding too much extra information could also fatigue users and cause them to disengage from the warning. Excessive warning text has been identified as a contributor to user fatigue [35]. The following sections answer RQ3 by suggesting these warning page improvements.

*1) Integrity of Content: Downloads:* A number of participants mentioned the integrity of downloaded files, (in particular executable files or binary programs) as being an important aspect of HTTPS. Upon examining the current warning pages provided, participants remarked that this was not warned about to any extent.

Google Chrome has recently included a new measure which aims to address this issue in their browser [36]. This new optional feature, much like HTTPS-Only modes will cause a warning to be displayed when a file download is attempted over a non-HTTPS connection. The feature, if adopted in Tor Browser would alleviate the concerns posed by the survey participants by ensuring users are properly warned when downloading files over an insecure connection which would make it unnecessary to include this risk in warning page texts.

This feature does not however protect users from copy and pasting code or scripts from insecure websites. Another similar, but less powerful feature was rolled out by default in 2021 [37] which warns users against mixed content downloads of executable files. Only insecure downloads which are initiated from a secure connection are considered by this feature however.

*2) Integrity of Content: Untrustworthy Information:* Content integrity was not mentioned by many participants. For the most part, risk to users financial data occurs when entering financial information like bank card details online and thus users focus more on this. One exception however, is cryptocurrencies or direct bank transfers where account numbers/wallet addresses could be maliciously altered and result in a payment to the wrong account. This is an example of a serious harm that results from lack of content integrity.

In future warning pages, it may be helpful to include warnings about the integrity of websites. For example, a warning could include *"It's possible the information on this site has been altered by an attacker"* A sentence like this would inform users of integrity risks. Other survey participants did discuss the economic value of attacks and as such alteration of information on websites could potentially be less lucrative to attackers and thus less frequent in practice.

*3) Examples of Specific Risks:* One of the strongest themes throughout the survey was the request for more specific risks to be described in the warning pages. The main description of risk in the Firefox page for example is "It's also possible that an attacker is involved.", HTTPS Everywhere as well as the old Tor Browser page state "it is also possible that an attacker is blocking the HTTPS version".

The overall main drive of the three warning pages examined seems to be: its possible an attack is taking place, do not enter sensitive data. This appears to be good advice for users and covers some of the issues with using non-HTTPS pages however all three pages avoid mentioning any specific problems or attacks that could occur if the user continues to that website. As P4 suggested of the HTTPS Everywhere page: *"It should communicate the risks of using an HTTP version, like password theft, phishing, adding spyware, etc."*. P24 also mentions *"page modification, credential stealing, malware shimming"*. These examples of specifically identified risks could be integrated into the warning page. A naive example of this could be "If you continue to this website, an attacker could view and passwords you enter. If an attack is taking place, your machine could be vulnerable to malware". These statements convey the risk of real dangers to users as

opposed to the previous generalised statements.

A danger with this approach is however over-warning based on the context. The insightful comment from P25 sums up this concern, when asked if the Firefox warning page was overstating the danger, they replied *"Unknown, since the dangers are highly dependent on the nature of the visited website."*. This comment accurately conveys the difficult of describing real risks to users through the warning pages, warning users of malware from a website is likely to cause them to abandon visiting the website, even when the context indicates that there is little risk of an attack occurring.

*4) Contextual Risk Depending on Type of Website:* Given that many survey participants highlighted context as an important factor in the safety of non-HTTPS connections, it is reasonable that an improved HTTPS-Only mode warning page could attempt to convey this to users. Such a warning could aim for either a specific or a general warning text. Specific examples could include mentioning the dangers of entering login information or personal details which could be stolen by an adversary. More general warnings could advise users that the danger from non-HTTPS websites will vary depending on the website, and that more critical web browsing should not be done on non-HTTPS websites.

*5) Lack of Discussion of Tor Specific Risks:* One of the most cited risk factors for browsing non-HTTPS websites using Tor was the potential for bad Tor exit nodes to either passively listen to, or alter traffic passing through them. As mentioned, without HTTPS malicious exit nodes can view in plaintext all of the traffic passing through them. They can also go further and attempt active attacks by altering the content of the website being returned to the Tor user. These risks are very specific to Tor and as many participants mentioned are not featured in any of the sampled https-only-mode warning pages. Answering RQ2, we can see that HTTPS-Only mode warning pages should be different in Tor Browser.

## VIII. Related Work

### A. User Habituation to Warnings

*1) False Positives Drive Habituation:* In a seminal work on the subject by Krol *et al*. [15], users' response to security warnings on PDF downloads is evaluated.

The authors argue that the content or style of security warnings have almost no impact on users' decisions and that users mostly relied on their own set of heuristics for deciding whether the task was risky or not.

The authors believe that the lack of effectiveness of these warnings is caused by habituation and excessive false positive warnings.

*2) Warning Text Matters in Absence of Habituation:* In contrast to the work by Krol, Akhawe and Felt [38] published a study only one year later that studies users click-through rate on SSL, malware and phishing warnings in Firefox and Google Chrome. The results show that Firefox had a much lower lower click-through rate than Google Chrome, showing that warning pages do have an effect and disprove Krol's assertion that security warnings are largely ineffective.

We can see that this was later corroborated by Felt *et al*.in 2015 [34] where this high level of Google Chrome click through relative to Firefox was partially rectified by improving the warning design.

*3) Changes in Style are Temporary Fixes:* Bohme [39] produced a study on user habituation to warning pages, in particular with reference to EULA style agreements. Bohme argues that users are highly habituated to longer textual, EULA style warnings and are likely to click through them without properly reading or understanding their content.

The authors advocate for more sparing use of warnings in other to prevent habituation.

*4) Reputation:* Reeder *et al*. [40] discovered that a large proportion of Firefox users that continued through SSL warnings did so because of site reputation. Many participants commented that they had visited the site before and they trusted it, and therefore did not need to heed the warning. A lesser but still significant number of participants noted that they had proceeded due to the necessity of visiting the site, and despite the warning they still had a task they wished to complete.

Overall Reeder *et al*. [40] conclude that despite some issues, web browser SSL warnings are effective in changing user action.

*5) Malware & Phishing Warnings:* Kirlappos *et al*. [32] studied online phishing attempts and conducted a user study on users' mental models of website trustworthyness. Flaws in users evaluation of website trust were found, primarily, users looked for elements of the website to confirm the trustworthiness like the quality of the website design, rather than looking for negative elements which should have called into question their trust.

Egelman [41] found that methods to increase user attention to phishing warnings did not actually improve compliance. The authors conducted a user study of 59 participants, and recruited them under the guise of an email web client usability evaluation.

Almuhimedi *et al*. [42] conducted a study on the factors that cause users to proceed through Google malware warnings. The study focuses on browsing history and finds that users are less likely to proceed through a warning for a website they have never been to before and conversely are sometimes more likely to proceed through a malware warning for a website they have visited in the past.

### B. User Comprehension of Warnings

Felt *et al*. [34] present a study, which attempts to create SSL warnings that are well understood by users. Previous work focused purely on convincing users to adhere to SSL warnings and not proceed to the website in question. This study attempts to go further by ensuring users understand what is going on and why it might be dangerous for them to proceed.

In crafting this new SSL warning page promoting user understanding, the authors draw on literature from the wider design literature [35], [43]–[45, ] which advise on techniques for increasing the comprehension of warnings.

The authors found no significant improvement in their warning for comprehension of false positives or data risk. There is a minor significant improvement in threat source understanding, but the overall ability of participants to choose the correct answer was still about the same as chance.

### C. Warning Text & Style

*1) Formality of Language:* Stokes *et al*. [46] conducted a recent study on how the level of language formality and professional style affected security notice compliance. This study focused on having participants grade both the formality and their likeliness to comply with security notices on a range of the most popular websites. The study finds that increasing formality tends to be a useful guideline for writing new warnings, the exception being when formality causes the length of the warning to be excessive, which can in turn cause users to stop reading the warning and take an uninformed action.

*2) Both Text and Appearance Alter Behaviour:* In Felt *et al*. [33], various experiments are conducted in an attempt to improve adherence to HTTPS error warnings in Google Chrome. The study is unique in that the authors had the ability to deploy their techniques directly to the Google Chrome browser. The experiments are run on users in the real environment of everyday browsing, and as such, it would be difficult to doubt the correctness of the results.

The authors note that Firefox had a much higher adherence rate to SSL warnings than Google Chrome. The authors produce a direct replica of the Firefox SSL warning page and bring it to Google Chrome to test the adherence rate for this page.

The key finding of the study is that the visual appearance of the warning page causes almost half of the large difference between the adherence rate of SSL warnings in Firefox and Chrome.

The authors note that the Firefox warning does not use technical jargon, identifies actions users can take to mitigate risk, and hides technical details from users which may account for Firefox's more successful warning page.

### D. Decision Retention

Whenever a user proceeds through a HTTPS-Only mode warning, a temporary exception will be saved by the browser. Both Google Chrome and Firefox only retain the exception for the current session, meaning that when the browser is closed and reopened, the warning will display again for that web page.

The benefits of longer exception retention are clearly outlined in work by Weinberger and Felt [47]. When considering SSL warnings, the study arrives at 1 week as a reasonable retention time for warning exceptions.

## IX. Limitations

### A. Limited Information on Study Sample

The Tor experts sampled in this project are not likely to experience Tor and Tor Browser in the same way as the average Tor user. Given that we are attempting to design better warning pages for all Tor Browser users, there may be a mismatch between what is desired by the Tor experts and the general userbase.

The sample is also non-exhaustive, there may be many more interesting themes that could be drawn out on this topic but the limited scope of the sample may not have achieved this.

Finally, due to the private nature of Tor users, we did not choose to ask for demographic information as it may have discouraged users from participating. This prevents us from completing any demographic based analysis.

### B. Lack of knowledge of HTTPS-Only modes

HTTPS-Only modes are a relatively new feature to web browsers. In particular, while the mode was enabled by default in Tor Browser, the survey was conducted before this occurred. As a result, participants in this survey may not have been fully familiar with HTTPS-Only mode before taking the survey, and thus, their views on the warning pages may not be well developed. This was mitigated by explaining the modes to participants during the survey. Future work could be more effective as users have had time to deal with HTTPS-Only mode in Tor Browser. Prospective survey participants will likely have more developed thoughts on HTTPS-Only modes and provide improved survey responses.

## X. Conclusion

This paper described the current state of HTTPS-Only modes in web browsers, in particular the content of their warning pages. From this, a broad scoping survey was drawn up in an attempt to gain insight into the views of Tor experts on the risks from non-HTTPS connections. We outlined the results of qualitative coding that was performed on the data and discussed the themes that emerged from this. The results and final discussion showed that more specific risks should be identified in future warning text, and that the concept of integrity potentially could be introduced where currently only confidentiality is mentioned. We also brought new discussion to whether users should have a choice in proceeding to non-HTTPS websites in the future.

Overall, we have presented a study and discussion which adds significant insight to HTTPS-Only modes, a new relatively new and not well studied security mode in web browsers.

## XI. Acknowledgments

This project was supported by the HDI Network Plus grant.

This work was supported by EPSRC (EP/R045178/1 Human Data Interaction: Legibility, Agency, Negotiability). Killian Davitt and Steven J. Murdoch are funded by the Royal Society (RGF/EA/80191 and UF160505).

We thank the Tor Project for their help in this work.

## References

[1] Christoph Kerschbaumer, Julian Gaibler, Arthur Edelstein, and Thyla van der Merwey. HTTPS-Only: Upgrading all connections to https in Web Browsers. In *Proceedings 2021 Workshop on Measurements, Attacks, and Defenses for the Web*, Virtual, 2021. Internet Society.

[2] Christoph Kerschbaumer, Julian Gaibler, Arthur Edelstein, and Thyla van der Merwe. Firefox 83 introduces HTTPS-Only Mode, November 2020.
[3] Shweta Panditrao, Devon O'Brien, and Emily Stark. Increasing HTTPS adoption, 2021.
[4] Microsoft Edge Blog. Available for preview: Automatic HTTPS helps keep your browsing more secure, June 2021.
[5] Ariana Mirian, Christopher Thompson, Stefan Savage, Geoffrey M. Voelker, and Adrienne Porter Felt. HTTPS Adoption in the Longtail. Technical report, Google and UC San Diego, 2018.
[6] Moxie Marlinspike. Some Tricks for Defeating SSL in Practice, 2009.
[7] Moxie Marlinspike. moxie0/sslstrip, October 2023. original-date: 2011-04-24T06:40:08Z.
[8] Chris Thompson. Enable HTTPS-First Mode flag by default, August 2021.
[9] Jen Simmons. New WebKit Features in Safari 15, October 2021. Section: News.
[10] Brave Privacy Team. Brave: HTTPS by Default, February 2023.
[11] Q-Success. Historical yearly trends in the usage statistics of site elements for websites, January 2024.
[12] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. The Emperor's New Security Indicators. In *2007 IEEE Symposium on Security and Privacy (SP '07)*, pages 51–65, Oakland, CA, USA, May 2007. IEEE. ISSN: 2375-1207.
[13] Emily Stark and Carlos Joan Rafael Ibarra Lopez. No More Mixed Messages About HTTPS, October 2019.
[14] Emily Schechter. A milestone for Chrome security: marking HTTP as "not secure", July 2018.
[15] Kat Krol, Matthew Moroz, and M. Angela Sasse. Don't work. Can't work? Why it's time to rethink security warnings. In *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, pages 1–8, Cork, Ireland, October 2012. IEEE. ISSN: 2151-478X.
[16] Mike Perry. HTTPS Everywhere Firefox addon helps you encrypt web traffic | Tor Project, June 2010.
[17] Matthew Finkel. New Release: Tor Browser 9.0.7 | Tor Project, March 2020.
[18] Disable Plaintext HTTP Clearnet Connections (#19850) · Issues · The Tor Project / Applications / Tor Browser · GitLab, August 2016.
[19] Duncan Russell. New Release: Tor Browser 11.5 | Tor Project, July 2022.
[20] {Isabela} . Tor security advisory: exit relays running sslstrip in May and June 2020 | Tor Project, August 2020.
[21] Nate Nelson and Dark Reading September 29. Spyware Vendor Targets Egyptian Orgs With Rare iOS Exploit Chain, September 2023. Section: dr-global.
[22] Christoph Kerschbaumer, Frederik Braun, Simon Friedberger, and Malte Jurgens. The State of https Adoption on the Web. In *Network and Distributed System Security (NDSS) Symposium 2025*, 2025.
[23] W3Techs. Usage Statistics of Default protocol https for Websites, October 2023, October 2023.
[24] HTTPS encryption on the web – Google Transparency Report.
[25] Adrienne Porter Felt, Richard Barnes, April King, Chris Palmer, Chris Bentzel, and Parisa Tabriz. Measuring HTTPS Adoption on the Web. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1323–1338, Vancouver, BC, Canada, 2017. USENIX Association.
[26] G. Harry Mc Laughlin. SMOG Grading-a New Readability Formula. *Journal of Reading*, 12(8):639–646, 1969. Publisher: [Wiley, International Reading Association].
[27] Brave: Secure, Fast, & Private Web Browser with Adblocker.
[28] Strict HTTPS Upgrade Mode in Brave Browser, May 2023.
[29] 1644146 - Change HTTPS Only Mode error copy to give the sense of "protection", 2020.
[30] Tor Project. NoScript | Tor Project | Support.
[31] Tor Project. JavaScript enabled by default in Tor Browser.
[32] Iacovos Kirlappos and M. Angela Sasse. Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security & Privacy Magazine*, 10(2):24–32, March 2012.
[33] Adrienne Porter Felt, Robert W. Reeder, Hazim Almuhimedi, and Sunny Consolvo. Experimenting at scale with google chrome's SSL warning. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, pages 2667–2670, Toronto, Canada, April 2014. Association for Computing Machinery.
[34] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. Improving SSL Warnings: Comprehension and Adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2893–2902, Seoul Republic of Korea, April 2015. ACM.
[35] Lujo Bauer, Cristian Bravo-Lillo, Lorrie Cranor, and Elli Fragkaki. Warning Design Guidelines. Technical report, Carnegie Mellon University, 2013.
[36] Joe DeBlasio. Towards HTTPS by default.
[37] Joe DeBlasio. Protecting users from insecure downloads in Google Chrome, 2020.
[38] Devdatta Akhawe and Adrienne Porter Felt. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 257–272, Boston, MA, 2013. USENIX Association.
[39] Rainer Böhme and Stefan Köpsell. Trained to accept? a field experiment on consent dialogs. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, pages 2403–2406, New York, NY, USA, April 2010. Association for Computing Machinery.
[40] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, CHI '18, pages 1–13, New York, NY, USA, April 2018. Association for Computing Machinery.
[41] Serge Egelman and Stuart Schechter. The Importance of Being Earnest [In Security Warnings]. In David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell, Moni Naor, Oscar Nierstrasz, C. Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Doug Tygar, Moshe Y. Vardi, Gerhard Weikum, and Ahmad-Reza Sadeghi, editors, *Financial Cryptography and Data Security*, volume 7859, pages 52–59. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013. Series Title: Lecture Notes in Computer Science.
[42] Hazim Almuhimedi, Adrienne Porter Felt, Robert W. Reeder, and Sunny Consolvo. Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 113–128, Menlo Park, CA, 2014. USENIX Association.
[43] Holly E. Hancock, C. Travis Bowles, Wendy A. Rogers, and Arthur D. Fisk. Comprehension and Retention of Warning Information. In *Handbook of warnings*, Human factors and ergonomics, pages 267–277. Lawrence Erlbaum Associates Publishers, Mahwah, NJ, US, 2006.
[44] Kenneth R. Laughery and Julie A. Stanush. Effects of Warning Explicitness on Product Perceptions. *Proceedings of the Human Factors Society Annual Meeting*, 33(6):431–435, October 1989. Publisher: SAGE Publications.
[45] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *18th USENIX Security Symposium*, page 18, Montreal, Canada, August 2009. USENIX Association.
[46] Jackson Stokes, Tal August, Robert A Marver, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, and Katharina Reinecke. How Language Formality in Security and Privacy Interfaces Impacts Intended Compliance. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23, pages 1–12, New York, NY, USA, April 2023. Association for Computing Machinery.
[47] Joel Weinberger and Adrienne Porter Felt. A Week to Remember: The Impact of Browser Warning Storage Policies. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 15–25, Denver, CO, 2016. USENIX Association.

## APPENDIX

### A. Survey Intstrument

This project is investigating the risks associated with users of Tor browser visiting non-HTTPS websites. In particular we are interested in recent developments in browser warning pages, e.g. Firefox's new HTTPS-Only mode which warns users when visiting non-TLS websites. The goal of this survey is to seek broad guidance on what kinds of issues should be discussed if such a mode was to be integrated into Tor

Browser. We are not considering Tor Onion Services in this survey, only websites that can be accessed with or without using Tor.

An invitation to partake in this survey has been extended to members of the tor community in thehopes that their expert advice can inform future work regarding the design of tor browser http warning pages.

All aspects of this survey are completely optional, you can choose to fill out as much or as little as you wish. You may also withdraw your consent at any time by not submitting the survey or by contacting the researchers and asking for your data to be deleted.

1) While browsing the web, what broad risks do you think occur for a user visiting non-HTTPS websites?
2) Does the level of risk vary depending on the activity being performed? Why do you believe this is the case?
3) Is this level of risk greater for users of Tor Browser, compared to those connecting directly to the site? Or are there new additional risks to visiting non-HTTPS sites when using Tor Browser? What if any, are these risks?
4) Can you identify specific criteria which makes visiting a non-HTTPS website more or less risky? In what scenarios are visiting non-HTTPS sites safe?
5) For you personally, when faced with a non-HTTPS website, what factors affect whether you will continue to the website, or abandon it?
6) Can you comment on what technical factors a user must understand in order to make an informed decision regarding non-HTTPS sites being 'safe' or less risky, and why do you think these are important?
7) TLS provides confidentiality of communications, as well as authenticity and integrity. Do you think these concepts, and how they are provided by TLS is well understood by typical Tor Browser users?
8) Do you believe it is necessary to understand confidentiality, authenticity and integrity of HTTP communications in order to make informed decisions about visiting non-HTTPS websites over Tor Browser? Why do you think this is the case?