How do Tor users interact with onion services?

Abstract

Onion services are anonymous TCP services that are exposed over the Tor network. As of November 2017 more than 50,000 onion services make available web sites, chat protocols, and file sharing services. Compared to conventional Internet services, onion services exhibit higher latency, can only be accessed over Tor, are barely indexed by search engines, and employ long, self-authenticating domain names. Our understanding of how users deal with these peculiarities is limited to anecdotal evidence. In this work we fill this gap by studying how people perceive, understand, and use onion services. To that end we employ a mixed-methods approach consisting of semi-structured interviews to explore the problem space, and an online survey to solicit answers to concrete questions. We find that (*i*) users place great trust in The Tor Project but distrust content that is hosted on onion services, (*ii*) users have devised a diverse set of methods to work around the non-memorable domain format, (*iii*) some users have flawed mental models of the underlying technology, and (*iv*) users not only rely on onion services for anonymity but also for their security and NAT-punching properties. Our work enables The Tor Project to focus its efforts on the most pressing usability issues, and improve its documentation by addressing common misconceptions that we identified. Our findings on self-authenticating domain names generalize to other systems such as the Bitcoin network.

1 Introduction

The colloquial meaning behind online anonymity implies *client anonymity*, *i.e.*, a user disguises her IP address, for example by using a VPN. A lesser-known use case is *server anonymity* which allows a web service to disguise its IP address. Service operators have good reasons to employ server anonymity; be it to escape harassment, speak out against power, or voice dissenting opinions. Tor's onion services provide what may be the most popular way of running an anonymous TCP service.[1]

Originally deployed in 2004, onion services have grown substantially over the last years, both in the number of services and users. As of January 2018, The Tor Project's statistics count more than 60,000 onion services each day, relaying an aggregate of more than 750 Mbps of network traffic. Not all of these services host web sites; use cases such as metadata-free instant messaging [4] and file sharing [16] have emerged as well. The Tor Project currently does not have information on the number of onion service users but Facebook reported in 2016 that more than one million users logged into their onion service over a one-month period [20].

Regarding usability, onion services differ from conventional web services in several aspects; (*i*) they can only be accessed over the Tor network; (*ii*) their domain is a hash over their public key, rendering them hard to remember; (*iii*) network latency is noticeable because of the additional hops in between client and onion service; and (*iv*) onion services are private by default, requiring manual dissemination. To date our understanding of how users deal with these idiosyncrasies is anecdotal. We fill this gap by studying how Tor users interact with onion services. In particular, we set out to understand users' mental model of Tor, their expectations of privacy, issues that they experience, and how they adapted their workflows to deal with onion services.

Onion services don't exist in a vacuum. They are tightly coupled to their surrounding software ecosystem—most importantly Tor Browser—which is why an isolated study of onion services is bound to miss important context. While our research question is about onion services, we aim to get as complete a picture as possible by casting a wider net and answering open questions about the use of Tor Browser in particular and privacy expectations in general. To that end we employ a mixed-methods approach involving the creation of an online survey that asked participants to answer an array of questions on Tor Browser, onion service usage and

[1] Onion services used to be known as "hidden services" but were recently renamed to reflect the fact that onion services provide more than just "hiding" a service—most importantly end-to-end security and self-authenticating names.

operation, onion site phishing, and general expectations of privacy. Based on our survey questions, our interviews let us ask follow-up questions and dive deeper into unexpected answers.

Our most salient findings show that (*i*) the flawed mental model some users have of Tor may cause security issues such as a blind reliance on vanity onion domains, (*ii*) the domain format of onion services, while cumbersome, is not among the most pressing usability issues, (*iii*) the content that onion services are perceived to host causes trust issues for non-technical users, and (*iv*) onion service operators seek to foil phishing attacks by having devised a number of strategies, many of which are ineffective.

At the time of this writing, The Tor Project is testing the next generation of onion services, intended to fix security issues and transition to faster and future-proof cryptography. We hope that our results can inform this process. Finally, as many of our findings touch on various aspects of privacy and anonymity, we believe that systems beyond the Tor network can benefit. In summary, we make the following contributions:

- We interviewed seventeen Tor users of diverse backgrounds to understand their habits, assumptions, and expectations related to Tor. Using qualitative data coding, we identified novel themes that underlay our interview data.
- We administered an online survey for Tor users, reaching 621 people. Our survey focused on the most salient issues around onion services, *e.g.*, the domain format, onion service discovery, and phishing attacks.
- Drawing on our two datasets, we identify (*i*) incorrect mental models, (*ii*) key issues that impede the adoption and use of onion services, and (*iii*) ways forward to improve onion services.

The rest of this paper is structured as follows. We begin by discussing related work in Section 2, followed by background on onion services in Section 3. Section 4 then presents the methods we used for our interviews and online survey, followed by Section 5 which discusses our findings from both data sources. Finally, we discuss our results in Section 6 and conclude our work in Section 7.

2 Related work

Tor's user interface has seen numerous substantial changes since its creation in 2003 [29]; from a manually-installed Tor "button," to the Tor Browser Bundle, to the currently-used Tor Browser. Installation hasn't always been as easy as today, which prompted Clark, van Oorschot, and Adams to use cognitive walkthroughs to study how users install, configure, and run Tor [5]. The authors uncovered usability hurdles such as jargon-laden documentation, confusing menus, and insufficient visual feedback. As of January 2018, the study is ten years old—Tor Browser has since seen radical changes.

Much more recently, in 2014, Norcie *et al.* identified stop-points in the installation and use of the Tor Browser Bundle [21].[2] These stop-points represent places in a user interface that require action but are met instead with confusion by users. Having identified these stop-points, the authors then issued interface design recommendations and subsequently tested these recommendations in a user study.

Inspired by Tor's use as anti-censorship system, Fifield *et al.* published a design to study the usability of Tor as a censorship circumvention tool [8]. By drawing on both qualitative and quantitative methods, the authors plan to recruit hundreds of users to study how they use Tor's configuration wizard in an adversarial setting. Lee *et al.* [15] studied the usability of Tor Launcher, the graphical configuration tool that allows users to configure Tor Browser. Their findings paint a bleak picture: 79% of users' connection attempts in a simulated censored environment failed. However, the researchers showed that their proposed interface improvements resulted in less difficulties for users.

Forte *et al.* studied the privacy practices of contributors to open collaboration projects [9]. The authors interviewed 23 contributors to The Tor Project and Wikipedia to learn about how privacy concerns affect their contribution practices. The study found that contributors worry about an array of threats including surveillance, violence, harassment, and loss of opportunity.

Most recently in 2017, Gallagher *et al.* conducted a series of semi-structured interviews to understand both why people use Tor and how they understand the technology [10]. The authors found that experts tend to have a network-centric view of Tor and tend to use it frequently while non-experts have a goal-oriented view and see Tor as a black box that provides a service. Consequently, non-experts don't use Tor if they don't need its service. Furthermore, non-experts tend to consider a single threat while the threat model of experts contains multiple actors.

Several research efforts sought to alleviate the handling of randomly-generated domain names. Sai and Fink proposed a mnemonic system that maps 80-bit onion domains to sentences [25]. Their work is inspired by mnemonicode, a method to map binary data to words [33]. Victors *et al.* proposed a more radical approach by designing the Onion Name System [32] which allows users to reference an onion service by a meaningful and globally-unique identifier. Kadianakis *et al.* designed a modular name system API that allows Tor clients to configure name systems (*e.g.* GNS [27] or OnioNS [32]) on a per-domain basis [13]. Kadianakis summarized the current state of research on onion service naming systems in a blog post [12].

We improve on the existing body of work by studying

[2] The Tor Browser Bundle was later rebranded and is now known as Tor Browser.

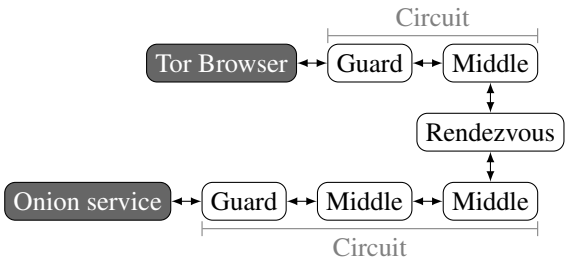


Figure 1: A connection to an onion service typically consists of six Tor relays. Both the client and the onion service create a circuit (consisting of two and three relays, respectively) to the rendezvous relay that serves as a short-lived data exchange point.

unanswered questions about the use of Tor Browser and—the focus of this paper—how users interact with onion services. We believe that many of our findings generalize to other systems, *e.g.*, Freenet [30] and Bitcoin also employ self-authenticating names.

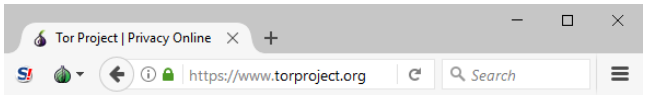
3 Background

Onion services are TCP services that are only accessible over the Tor network. Onion domains take the place of IP addresses, which traditional TCP services use for addressing. These onion domains are resolved and routed inside the Tor network, resulting in a circuit between the client and the onion service which (by default) features six hops (see Figure 1).

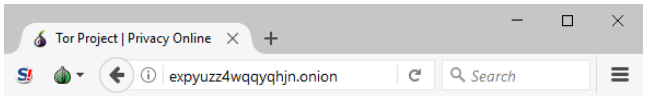
The creation of a new onion domain requires a Tor daemon to generate an RSA key pair. It then computes the SHA-1 hash over the RSA public key, truncates it to 80 bits, and encodes these 80 bits in Base32, resulting in sixteen characters, *e.g.*, expyuzz4wqqyqhjn. As of January 2018, The Tor Project is deploying the next generation of onion services whose domain format will feature 56 instead of sixteen characters [17, § 6]—a Base32 encoding of the onion service's public key, a checksum, and a version number. Because of the next generation using elliptic curve cryptography, the entire public key (instead of just a hash over the public key) is embedded in the domain.

Due to an onion domain being a function of its public key, onion domains are self-authenticating, *i.e.*, as long as a client has the correct domain, it knows what public key to expect. The downside is that sixteen random characters are impractical to remember, let alone 56 characters.

We can make onion domains at least partially meaningful by repeatedly creating RSA keys until the resulting domain contains a desired string. We call these *vanity onion domains*. A vanity prefix of length n takes on average $0.5 \cdot 32^n$ key creations given Base32's alphabet size of 32 characters. After having created a set of domains featuring a vanity prefix, one can search this set for the domain that is the easiest



(a) The Tor Project's web site when accessed over its conventional domain.



(b) The Tor Project's web site when accessed over its onion service.

Figure 2: Tor Browser 7.0.10's user interface on Windows 10 when opening a conventional domain (top) and when opening the corresponding onion service (bottom). Note that the onion version lacks a padlock icon—an issue that's currently being worked on [2].

to remember, *e.g.*, by using a Markov model to filter domains that resemble words in the English language. While this method will not produce fully-meaningful domains, it can facilitate memorization as evidenced by the vanity domains of Facebook (facebookcorewwwi.onion), ProPublica (propub3r6espa33w.onion), and the New York Times (nytimes3xbfgragh.onion). In practice, many onion service operators use the tool scallion [28] to find vanity domains in parallel.

Onion services are private by default. Once an onion service is created, it is its operator's task to disseminate the domain, *e.g.*, by adding it to onion site search engines such as Ahmia [22]. The lack of a go-to service such as Google for onion service discovery prompted the community to devise various ways to disseminate onion services, most importantly an array of search engines and curated lists.

On the usability front, Tor Browser's user interface when accessing onion services is designed to be seamless. Figure 2a shows the UI when accessing The Tor Project's web site while Figure 2b shows a connection to the corresponding onion site.

4 Method

We will now elaborate on how we designed our interviews (Section 4.1) and our online survey (Section 4.2). For both we will discuss participant recruitment, how we structured the interview or survey process, and research ethics.

4.1 Interviews

We developed a question set that served as the basis for each interview.[3] The semi-structured nature of our interviews allowed us to deviate from this question set, *e.g.*, by asking follow-up questions. We began by asking demographic information (gender, age range, occupation, country of res-

[3]The question set is available online at https://nymity.ch/onion-services/pdf/interview-checklist.pdf.

idence, and level of education), followed by information about online behavior, and finally questions specific to Tor Browser and onion services.

4.1.1 Procedure

Princeton University's institutional review board (IRB) deemed our study exempt from further review.[4] We conducted thirteen interviews in person and four interviews remotely; over Skype, Signal, WhatsApp, and Jitsi—depending on what our interviewees felt the most comfortable with. For in-person interviews we asked our interviewees to sign a consent form. This was not practical for remote interviews, so we sent the consent form in advance, over email, and, after seeking permission from our IRB, asked for verbal consent before the interview. In all cases we explicitly asked for permission to record the conversation. All except two participants agreed to have their interview recorded. In the remaining two interviews we took notes instead. We made it clear to our participants that they could withdraw their consent at any time. Each interview ended with a debriefing phase in which we asked if our participants had any remaining questions. After that we offered our participants a gift card worth twenty dollars as a token of appreciation. We conducted our first interview on July 13, 2017 and the last on October 20, 2017.

We had our recordings transcribed by a company that offered transcription services and a non-disclosure agreement protected the confidentiality of our data. Once our interview recordings were transcribed, we deleted the original recordings and employed qualitative data coding to analyze the transcripts. Each interview transcript was coded by two members of our team. This process identified twenty-seven themes that are all listed in Appendix D.

4.1.2 Recruitment

To select eligible interview subjects, we created a short pre-interview survey (see Appendix A), which was advertised by The Tor Project both in a blog post [35] and on its Twitter account. Our selection process favored laypeople and sought to maximize cultural, gender, location, education, and age diversity. In addition to our online screening, we recruited participants in person at an Internet freedom event. We found it difficult to draw a uniform sample of Tor users to interview. We believe that The Tor Project's blog and Twitter account are mainly followed by disproportionately technical users while many non-technical users may install Tor Browser in a one-off process and then cease to follow the project. To make matters worse, many Tor users value their privacy significantly more than the average Internet user, making it challenging to evoke enough trust to have users open up to us about their browsing habits.

[4] Our IRB protocol number is 8251.

We ended up interviewing seventeen subjects whose demographic information is shown in Table 1. Given the sensitive nature of our interviews, we only present aggregate information to protect the identity of our participants. We believe that our sample is biased towards educated and technical users (almost 60% of our participants have a postgraduate degree) but it also shows the diversity among Tor's user base: Our participants comprised human rights activists, legal professionals, writers, artists, and journalists, just to name a few.

4.2 Online survey

Shortly after we conducted our first batch of interviews, we launched an online survey to complement our interview data.

4.2.1 Procedure

We created our survey in Qualtrics because our institution had a subscription, it had all the features we deemed necessary, and an out-of-the-box Tor Browser could display its interface correctly. Qualtrics however requires JavaScript which is deactivated if Tor Browser is set to its highest security setting. A number of users complained about our reliance on JavaScript in the recruitment blog post comments [35].

Respondents had to agree to a consent form before starting the survey. The consent form informed the respondents about the procedure of our experiment and required that all respondents were at least eighteen years of age. Our survey was only available in English but we targeted an international audience because Sawaya *et al.* showed that there are cultural differences in security behavior [26]. Ignoring these differences would tailor Tor Browser to the needs of a predominantly Western audience which runs counter to The Tor Project's global mission.

We used cognitive pretesting (sometimes also called cognitive interviewing) to improve the wording of our survey questions [6]. Pretesting reveals if respondents (*i*) understand questions, (*ii*) understand questions consistently, and (*iii*) understand questions the way we intended. A pretest entailed administering our survey and asking our respondents to fill out the survey while verbalizing their thought process. We occasionally asked follow-up questions to make sure that our pretesters understood all questions as intended. However, not all cognitive processes can be verbalized and cognitive pretesting may change the way respondents answer questions. We had five pretesters whose input helped us improved our survey iteratively. Two pretesters were native English speakers while the remaining three were fluent but spoke English as a second language.

To weed out low-quality responses we incorporated four attention checks into our survey [3]. Having four attention checks instead of just one allows us to measure a respondent's *degree* of attention, meaning that we only discard responses that failed more than two attention checks.

Age	#	%	Gender	#	%	Continent of residence	#	%	Education	#	%
18–25	2	11.8	Female	5	29.4	Asia	3	17.6	No degree	1	5.9
26–35	10	58.8	Male	12	70.6	Australia	1	5.9	High school	3	17.7
36–45	4	23.5				Europe	4	23.5	Graduate	3	17.7
46–55	1	5.9				North America	8	47.1	Postgraduate	10	58.8
						South America	1	5.9			

Table 1: The distribution over gender, age, country of residence, and education for our seventeen interview subjects. We chose not to display per-person demographic information to protect the identity of our interview subjects.

Topic	# of questions
Consent and demographic information	1
Tor usage	4
Onion site usage	20
Onion site operation	5
Onion site phishing and impersonation	9
Expectations of privacy	9
End of survey	1
Total	49

Table 2: The topical question blocks in our survey and the number of questions they contain.

The majority of our survey focused on onion services, but we also added some questions about Tor in general. Table 2 shows that our survey consists of six blocks that are ordered by topic. It takes about fifteen minutes to answer all questions. The full survey is listed in Appendix B.

4.2.2 Recruitment

Similar to our interviews, we advertised our survey (*i*) in a blog post on The Tor Project's blog [35], (*ii*) on its corresponding Twitter account, and (*iii*) on three Reddit subforums.[5] Unlike our interviews participants, our survey respondents are self-selected. Again, we expect this recruitment strategy to bias our sample towards engaged users because casual Tor users are unlikely to follow The Tor Project's social media accounts.

To incentivize participation, we originally planned to give respondents the option to participate in a gift card lottery but we abandoned the idea because it was difficult to reconcile anonymous participation with a lottery because we would have to collect our respondents' email addresses to notify them in case they won. Despite the lack of incentives, we collected a satisfactory number of responses. In fact, we believe that many respondents were only motivated by improving Tor—some of our interview participants even turned down the gift card we offered them.

We launched our survey on August 16, 2017 and ended it on September 11, 2017, so it was active for twenty-seven days and was taken 828 times. However, not all responses are necessarily of high quality; people may have rushed their answers, aborted our survey prematurely, or given deliberately wrong answers. We therefore weed out low-quality responses that either did not finish the survey or that failed more than two out of our four attention checks. We collected a total of 828 responses but only 604 (73%) completed the survey and 527 (64%) passed at least two attention checks. The remainder of this work focuses on these 527 responses.

Table 3 shows the demographics of our survey. Not surprisingly, our respondents were *young and educated*: more than sixty percent are younger than thirty-six, and another sixty percent have at least a graduate degree. Finally, another sixty percent consider themselves at least highly knowledgeable in matters of Internet privacy and security.

5 Results

We organize the presentation of our findings by topic, starting with Tor Browser, and then onion service-specific topics such as service discovery and the operation of onion services. We interweave the results from our online survey and from our interviews, focusing primarily on our survey data but bringing up anecdotes and findings from our interviews as appropriate.

5.1 The Tor Project

Our work focuses on the usability of onion services but our interviews and parts of our survey data also provided some insight into how our respondents perceive The Tor Project and its work. We will now briefly summarize these findings.

5.1.1 Documentation and localization

The Tor Project's documentation covers an array of topics including installation, the use on Android, the operation of Tor relays, several FAQs, and a wiki. Having worked with this documentation, some of our interview and survey participants lamented its scope:

> Tor does a good job on their web site of telling you to modify your [configuration] file, and then

[5] The forums are https://reddit.com/r/tor/, https://reddit.com/r/onions/, and https://reddit.com/r/samplesize/.

Gender	#	%	Age	#	%	Education	#	%	Domain knowledge	#	%
Male	444	85.7	18–25	186	35.7	No degree	26	5.0	No knowledge	1	0.2
Female	49	9.5	26–35	184	35.3	High school	173	33.3	Mildly knowledgeable	37	7.1
Other	25	4.8	36–45	88	16.9	Graduate	215	41.4	Moderately knowledgeable	178	34.1
N/A	9	1.7	46–55	43	8.3	Post graduate	105	20.2	Highly knowledgeable	230	44.1
			56–65	16	3.0	N/A	8	1.5	Expert	76	14.6
			> 65	4	0.8				N/A	5	1.0
			N/A	6	1.2						

Table 3: The distribution over gender, age, education, and domain knowledge for our 527 survey respondents. It was optional to provide demographic information which is why we lack data for a small number of respondents.

> getting the onion set up. But it's just very basic. I have to go [to] other people's blog post to find out. (P14)

Another participant struggled with the lack of localization. While Tor Browser's user interface is available in Spanish, the documentation is not:

> Think more [about] the Spanish community…because in my case I'm trying to train people to use Tor but I work in the indigenous communities and there are some things that [are] hard for me to explain in terms of how you use Tor… (P11)

5.1.2 Public perception

The Tor Project goes to great lengths to minimize the trust its users have to place in it by publishing design documents, source code, and coordinating development in public. Laypeople however lack the skill while experts typically lack the time to audit source code, which is why trust and reputation matter. The Tor Project enjoyed a lot of trust among our interview participants, which, admittedly, comes as no surprise because we recruited our interviewees from Tor-friendly social media and an Internet freedom event.

> Because, you guys…have the sort of…not a monopoly on trust, but you have like a really great brand name when it comes to this stuff… (P08)

While the work of Tor developers is often held in high esteem, the content that is hosted on onion services is perceived very differently. Upon being told what an onion service is, one participant sought clarification:

> So it's like the Hidden Wiki and stuff like that, where you can buy drugs and…or supposedly. (P03)

Several interviewees voiced concern that their mere use of Tor may draw unwanted attention. Tor Browser comes with modules that disguise the fact that one is using Tor but a standard Tor connection does not use these modules, making it easy to identify for Internet service providers [31]. One participant worried:

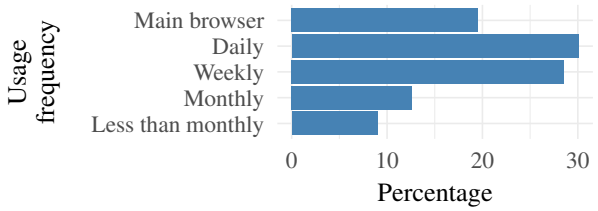


Figure 3: The usage frequency of Tor Browser among our respondents, almost half of whom use Tor Browser either daily or as their main browser.

> I guess you could put yourself on some kind of watch lists, that you are a person of interest, just because you're using [Tor]. (P03)

5.2 Tor Browser usage

Our survey started with two questions about how often our respondents use Tor Browser. The results are illustrated in Figure 3. Almost half of our participants use Tor Browser either daily or even as their main browser. Both Gallagher *et al.* [10, § 4.3.2] and our interview data suggests that non-experts frequently use Tor for specific tasks but don't embed it in their daily workflow:

> Right now, I use it very little, just because I don't have a lot of reasons to, because of the fact that I have other security practices that do the trick for the kind of work that I do. (P07)

Figure 4 illustrates what entities our respondents seek to protect themselves from when using Tor Browser. The majority considers ad companies, governments, and—most prominently—their ISP. More tangible entities such as family, employers, and schools are less prevalent. People who selected "Other" gave a variety of responses. A number of respondents specifically pointed out Google and Facebook. ISPs, backbone ISPs, and web sites were another common

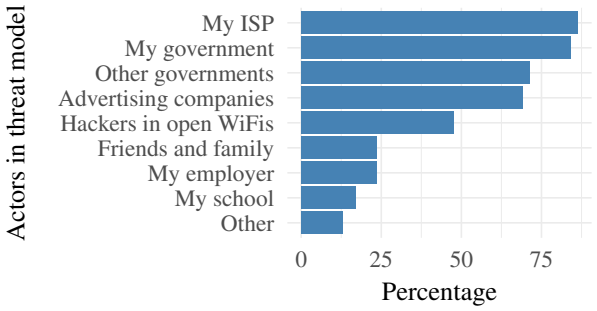


Figure 4: The threat actors that our respondents seek to protect themselves from by using Tor Browser.

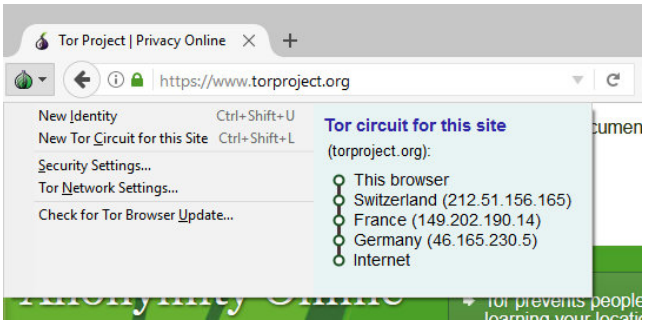


Figure 5: A click on the onion icon reveals the Tor relays that constitute the circuit that was used to fetch the current page.

theme. A number of respondents are struggling with personal threats that include identity theft, targeted harassment, and stalking. Research is another common theme: Several respondents want to learn about a topic without revealing their interest in it. Some respondents use Tor for search engine optimization, computer security research, and to research medical conditions. Finally, Tor has use cases that don't involve a threat actor. Some respondents want IPv6 connectivity, evasion of geographical content restrictions, and access to onion services. One respondent stated that they don't need anonymity themselves but use Tor to provide cover traffic for "people who need protection."

5.2.1 Users enjoy a look "under the hood"

By clicking on the onion icon in the top left corner of Tor Browser (see Figure 5), one can see the circuit that is used for the current web site. Some of our interviewees appreciated this visual feedback:

> I love how I can monitor the network through this little kind of bar that comes up. (P08)

Not satisfied with seeing only the current circuit, some participants wished it were easier to learn what else is happening behind the scenes:

> [It] would be nice to have some kind of application, something on that browser, that gives you an impression of... what the Tor Browser's actually doing. (P02)

Finding the right balance between what information to show and what to hide is challenging in itself, and only exacerbated by Tor's heterogeneous user base. While technical users may appreciate a look "under the hood," non-technical users, who often use Tor as a tool to get a specific job done, can easily feel bewildered and overwhelmed. One aspect however in which more transparency could benefit Tor's entire user base is when web sites don't load, as suggested by one participant:

> ... maybe some sort of graphical representation of is the circuit still being built, or is the circuit built, and the site isn't responding at all to the third relay? (P05)

5.2.2 Quantifying anonymity is hard

The degree of anonymity that protects a Tor user in a given situation depends on a number of variables including her guard relay, intermediate autonomous systems on the network path, and other people that are using Tor at the same time, just to name a few. Unlike the JAP anonymity tool [11], Tor Browser makes no attempt to display the degree of anonymity it believes it can provide. Asked about how well Tor works for them, one of our participants explained:

> In terms of the anonymity, you can't really tell... That's fairly opaque, so I can't even tell how effective that's working, or whether it is... (P12)

Quantifying anonymity in a real-world setting is complex, error-prone, and often misleading. What's more, Tor Browser does not have available all the data it needs to quantify its user's anonymity—an "anonymity meter" may therefore create more problems than it solves.

5.2.3 UI, speed, and CAPTCHAs remain frustrating

Perhaps the most prevalent usability issue is, still, browsing speed. An interviewee provided the following anecdote:

> The speed of it is problematic; sometimes I have a path that allows me to watch full HD YouTube videos, and the next time, five minutes later, I'm barely getting kilobytes through. (P01)

Occasionally, Tor is preceded by its reputation, preparing users for what to expect, as another interview participant reported:

> I didn't think it was as slow as people say it was. People said it would be a much slower experience but... a little bit slower, but it didn't matter for the things that I was doing. (P03)

In addition to the perceived slowness, several participants lamented the old-fashioned user interface, describing Tor Browser's looks as "it felt like it was about five years outdated," "it looked like I was in 1982," and "I think the colors look a bit old fashioned and in the former Soviet Union." To our surprise, one participant expressed that the antiquated user interface also evoked trust:

> At the same time I thought... it gave them a certain amount of credibility, like they weren't building this for the looks, but they were building it for functionality... At the same time, as I thought it was outdated in terms of how it looked, I also thought it was sort of genuine in a way. (P02)

Orthogonal to Tor's speed and user interface, the browsing experience occasionally suffers. Relying on naive, IP address-based metrics of "maliciousness," some content delivery networks such as Cloudflare label Tor exit relays as malicious which results in Tor users having to solve (sometimes multiple) CAPTCHAs before being granted access to a web site. In 2016, Khattak *et al.* documented the issue for a number of content providers [14]. Both survey and interview participants brought up the topic and one person managed to depict the issue without the use of profanity:

> It is still sometimes challenging using some everyday services because of CAPTCHAs and those things, but I also understand that's not so much to do with Tor, but to do with the creators of those web sites. (P06)

5.2.4 Empowerment through security and privacy

It comes as no surprise that our data reveals that the main benefit of Tor Browser is the increase in privacy and security, brought up by practically all of our interview participants. One of our more technical interviewees (and several of our survey respondents) further distinguished between security and privacy. Asked about if they feel safer when using Tor, they responded:

> In a privacy sense, I do. In a security sense... I don't assume that Tor is protecting me from all of the vulnerabilities or exploits that I might encounter... (P06)

Besides the obvious improvement in security and privacy, a defining aspect of Tor is that it puts users back in control, or, as one of our participants eloquently phrased it:

> I feel like I'm more in control of my internet experience that way, I'm not sort of like a will-less victim of what other people want to do with me, so I feel I'm more empowered and have more agency when I use the Tor Browser. (P02)

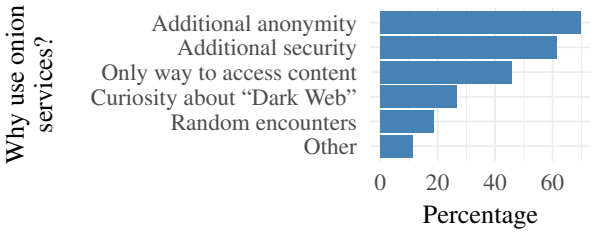


Figure 6: Our respondents' (multiple choice) reasons for using onion services.

5.3 Onion service usage

We now move on to results specific to onion services, the focus of our online survey. The usage frequency of onion services is almost uniformly distributed among our respondents; 24% use onion sites less than once a month, 22% use them about monthly, 25% weekly, and 23% daily. The remaining 6% has never used an onion service before.

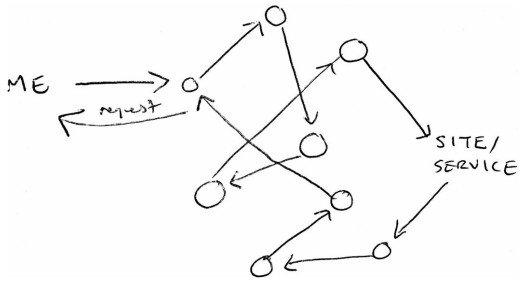
The majority of our respondents (61.8%) has used onion services for purposes other than web browsing before. Several protocols such as the chat application Ricochet [4] and the file sharing application OnionShare [16] were purpose-built on top of onion services while existing TCP-based tools such as SSH can transparently use onion addresses instead of traditional IP addresses. Almost one third (29.7%) of our participants use onion services for non-browsing activities at least once a week.

But why do Tor users browse onion services in the first place? Figure 6 provides some insight. The majority uses onion services because of the additional anonymity (70%) and the additional security (61%). For 46% it is the only way to access content they enjoy, making the use of onion services a necessity. 27% of our respondents found themselves eager to learn more about the "Dark Web" and set out to satisfy their curiosity while 19% occasionally stumble upon links to onion services in their day-to-day browsing activity. Respondents who selected "Other" gave a variety of reasons, the most predominant being the ability to set up a TCP service behind a NAT device. That makes it possible to run an SSH server in a home network that has neither a permanent IP address nor port forwarding. Others use onion services to reduce the load on exit relays, to do technical research, and to access sites that are otherwise unavailable.

5.3.1 Mental models are often patchy

We asked our interview participants to draw sketches of how they believe Tor and onion services work.[6] Everybody drew a sketch of Tor but some didn't draw onion services because they had no mental model of it. Interestingly, all participants understood that key to Tor's anonymity is the bounc-

[6] All sketches are available online at https://nymity.ch/onion-services/mental-models/.



(a) A non-technical interview subject's sketch of how they believe Tor works. The participant correctly understands the concept of bouncing network traffic over several hops.

(b) A non-technical interview subject's sketch of their mental model of an onion service. Instead of a web site, the final hop is another Tor hop.

Figure 7: Sketches of two different, non-technical interview participants of how Tor works (top) and how onion services work (bottom).

ing of network traffic across several relays, as evidenced by Figure 7a, drawn by a participant with no technical background.[7] Analogously, most of our participants understood that network traffic does not leave the Tor network when connecting to onion services. Figure 7b illustrates an example, again drawn by a non-technical participant. The last hop in the circuit is an onion, correctly suggesting that network traffic does not leave the Tor network.

Some of our interviewees did not distinguish disguising their IP address from disguising their real-world identity, and instead used the umbrella term of "anonymity" to refer to both concepts. This conflation of concepts paints an incomplete picture of the security and privacy guarantees that Tor provides, further illustrated by one participant's question:

> What's the point of going to Facebook using onion services when their business model is still about collecting your data? (P07)

There is merit in using Facebook's onion service. While the company indeed knows who is logging in, it does not know Tor users' IP address (and hence location) or operating system. On top of that, onion services provide end-to-end security and self-authenticating names. These benefits are difficult to convey to non-technical users and even experts sometimes advocate an "all or nothing" approach to online anonymity, overlooking important nuances.

An unrelated yet hardly unexpected flawed mental model is the domain format of onion services. Some users have come to believe that the seemingly-random characters in onion domains are the reason why onion services are anonymous. Accordingly, these users also believe that vanity domains are "less anonymous" because part of their domains is clearly not random.

[7] The however sketch got two details wrong: the number of hops in a Tor circuit is three and the circuit's forward and reverse path are identical.

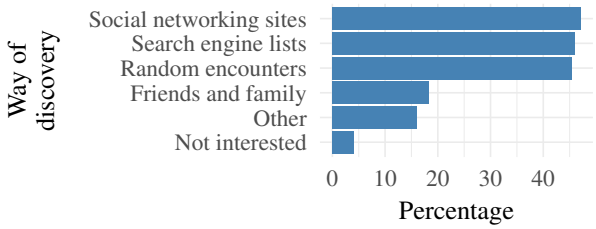


Figure 8: Our respondents' (multiple choice) methods of discovering onion services.

5.3.2 Makeshift solutions ease onion service discovery

Recall that a freshly set up onion service is private by default, leaving it up to its operator to disseminate the domain. Established search engines such as Google are therefore inadequate to find content on onion services. We wanted to find out how our respondents discover onion services. Figure 8 illustrates the results. The three most popular ways of discovering new onion sites, all approximating 50%, are (*i*) social networking sites such as Twitter and Reddit, (*ii*) the list of search engines such as Ahmia[8], and (*iii*) randomly encountering links when browsing the web.

While significantly less popular, discovering onion domains through friends and family has the advantage that domains come from a trusted source—and aspect that mattered to some of our survey and interview participants. Finally, a mere 4% indicated that they are not interested in learning about new onion services.

Respondents who selected "Other" predominantly brought up independently-maintained lists of onion services and aggregators. A noteworthy example is the Hidden Wiki, a community-curated and frequently-forked wiki that contains categorized links to onion services.

The next question in our survey asked if our respondents are satisfied with the way they discover onion services. 60% selected "Yes" while 40% selected "No." Some respondents who selected "Yes" brought up that they have no interest in learning about new onion services, in part because they only use a small set of onion services. Among the people who are not satisfied, the most prominent complaint was about broken links on onion site lists. There is non-trivial churn among onion sites and our respondents were frustrated that existing lists are typically not curated and link to numerous dead domains. The lack of curation also leads to these lists containing the occasional scam and phishing site. The dif-

[8] Ahmia.fi is an onion site search engine that crawls user-submitted onion domains. It publishes the list of all indexed onion services at https://ahmia.fi/onions/.

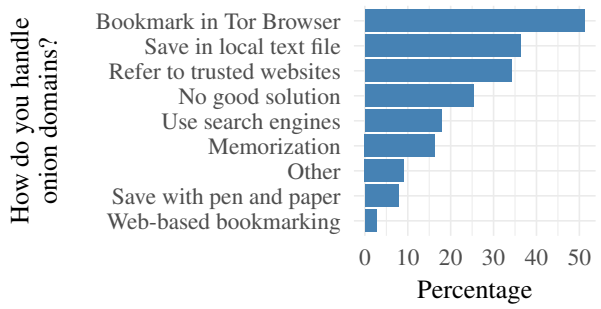


Figure 9: The strategies that our respondents use to handle onion domains. More than half use bookmarks inside of Tor Browser and a quarter thinks that there's no good solution.

ficulty of telling apart two given onion domain names exacerbates this issue for users. Another common wish for aggregators was for them to be more verbose in their description of onion sites. In particular, some respondents want to avoid illegal and pornographic content, which is often difficult if the description is vague and the onion domain reveals nothing about its content. Many respondents were not aware of search engines such as Ahmia. Among those that were, many were dissatisfied with both the search results and the number of indexed onion sites. Unsurprisingly, a "Google for onion sites" was a frequent wish.

Many respondents expressed frustration about the difficulty of finding out if example.com has a corresponding onion service. A common wish was to have example.com list its onion service prominently in a footer. Ironically, some respondents were surprised that torproject.org has a corresponding onion site—they couldn't find it on the web site. Interestingly, some respondents voiced frustration about various usability issues, but mentioned in the same sentence that this is an inherent trade-off of privacy technology, suggesting that there is nothing that can be done about it.

5.3.3 Onion domain management is problematic

Conventional domains are designed to be easy to remember and recognize. But how do users handle randomly-generated onion domains? Our survey question 3.8 sought an answer and the results are illustrated in Figure 9.

Most respondents use Tor Browser's bookmarks to save onion domains. While convenient, it leaves a trace of (presumably) visited sites on somebody's computer. One of Tor Browser's security requirements is "disk avoidance," *i.e.*, the browser must not write anything to disk that would reveal the user's browsing history [24, § 2.1]. Bookmarking links is a violation of this security requirement albeit requested by the user. Many of our respondents were aware of this issue and about a dozen respondents who selected "Other" stated that they store onion domains in an encrypted manner—either in a text file or in their password manager. Somewhat less popular is saving onion domains in local text files (36%), getting them from trusted web sites (34%), using search engines (18%), memorizing domains (16%), using some other techniques (9%), or employing pen and paper (8%). Notably, one quarter of our respondents does not have a good solution to the problem. Given the alarming number of (possibly insecure) home-baked solutions, a Tor Browser extension that solves this problem may be warranted.

Of the respondents that memorize onion domains, we found that most respondents memorize either one onion domain (15% of total respondents) or four onion domains (11% of total respondents); significantly fewer respondents memorize two domains (5%), three domains (4%), and more than four domains (1%). As mentioned in the previous paragraph, bookmarking onion domains can leave a trace of visited sites, and about 28% of respondents said they memorize onion domains to prevent this digital trace. On the other hand, more respondents memorize domains to allow them to open the site more quickly (51%), ensure that they are visiting the correct site and not a phishing site (44%), and automatically start to memorize it based on typing it many times (60%).

Our survey also asked respondents about whether or not they memorize vanity domains — specifically facebookcorewwwi.onion — and how difficult they find it to memorize onion domains of differing levels of vanity. 59% of respondents replied that facebookcorewwwi.onion is among the sites that they have memorized. This is because it is "easy to memorize" and "after seeing [it] many times, I automatically start to memorize it." When asked about different levels of vanity domains, the respondents expressed differing levels of ease in which to memorize them; these results are shown in Figure **??**. URLs such as expyuzz4wqqyqhjn.onion and torproz4wqqyqhjn.onion are harder for respondents to remember because they mention that "numbers make the names harder to remember." Other respondents stated that domains are easier to remember when they are speakable and can be pronounced. One respondent described it saying "phonetic pronunciation plays a large part in how I remember onions." Many other resondents stated that onion domains that are supported by a mneumonic are also easier to remember.

The next question in our survey asked if our respondents expect the next-generation domain format to change their browsing habits. Interestingly, only 17% expect their browsing habits to change while 83% don't. Among the respondents who selected "Yes," many expressed that they memorize a small number of onion domains (such as Facebook's), which will no longer be possible. People who selected "No" mostly brought up that they treat onion domains as opaque identifiers and handle via tools such as bookmarks. These results suggest that the current state is dire, yet not expected to worsen with the new domain format.

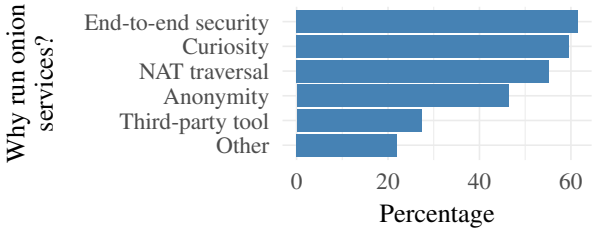


Figure 10: The (multiple-choice) reasons our respondents have for running onion services.

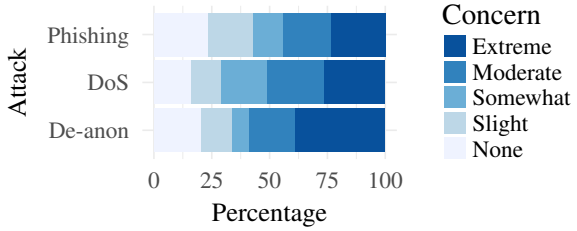


Figure 11: The level of concern onion service operators have with respect to a phishing clone of their service, denial-of-service attacks, and deanonymization.

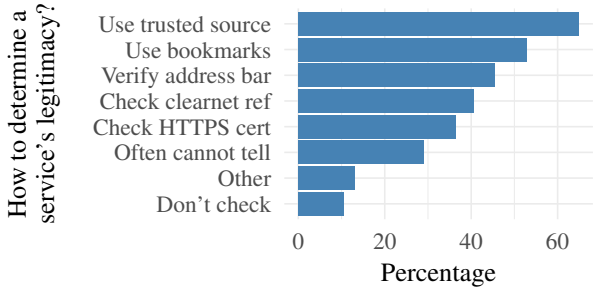


Figure 12: How our respondents determine an onion service's legitimacy.

5.3.4 Onion services have many use cases

A question block on onion service operation inquired about the motivation for running an onion service and what sort of issues operators encounter in the process. 40% of our respondents once set up an onion service. Among the respondents who never have, 31% have considered doing so while 30% have never considered it. Interestingly, 79% of operators have run an onion service for private use while 53% have run them for the public.

Figure 10 gives an overview of the reasons our respondents have for running onion services. Interestingly, the extra security properties outweigh the anonymity properties of onion services. Another popular motivation is NAT traversal—many respondents noted that onion services allow them to expose a TCP service in their home network despite being behind a NAT device. Finally, some people run onion services indirectly because third-party tools such as OnionShare [16] or Ricochet [4] are built on top of them. A survey respondent gave the following reason for running onion services:

> We use it for delivering updates to our router to customers securely and without leaking metadata. (Survey respondent)

Figure 11 illustrates the concerns that onion service operators experience. We consider three attacks; (*i*) somebody setting up a phishing site for the operator's site, (*ii*) a denial-of-service attack, and (*iii*) a deanonymization attack. More than half of our respondents are at least somewhat concerned about all of these attacks. Almost 40% claim to be extremely concerned about somebody deanonymizing their onion service. Indeed, many respondents lamented the difficulty of protecting onion services from application-layer deanonymization attacks. Matic *et al.* demonstrated some of these issues in 2015 [18].

5.3.5 Susceptibility to phishing attacks

Phishing remains an issue despite onion services' extra anonymity and security properties. Past work has uncovered an attack that transparently rewrote Bitcoin addresses to hijack Bitcoin transactions [36, 23, 19]. Key to this attack is the difficulty of telling apart an authentic from an impersonation domain. For conventional domains we rely on (EV) certificates, browser protections, search results, and long-lived reputation, but none of these methods work well for onion services. Does the nature of onion services facilitate phishing attacks? If so, what can we do to mitigate the issue?

We asked our respondents if they ever thought about the authenticity of an onion site. With 80%, the majority of our respondents did while 20% didn't. Clearly, there is a need for verification but how does one verify that an onion service is authentic? Figure 12 gives an overview of the strategies that our respondents employ.

More than half either consult trusted sources (*e.g.* friends or another web site) or use bookmarks when revisiting onion services. Many respondents also verify the domain in the browser's address bar (46%), check if the corresponding web site has a link to its onion site (41%), or hope that the onion service has an HTTPS certificate (36%).[9] Alarmingly, almost 30% of respondents stated that they sometimes cannot tell the difference between an authentic service and an impersonation, and 11% never check a service's legitimacy in the first place. People who selected "Other" provided a wide variety of ad-hoc phishing protections—some clearly misguided, which reinforces the scope of the problem.

Originally meant to improve usability, vanity onion do-

[9] DigiCert is issuing EV-certificates for onion sites [7] but adoption has been slow—presumably in part because EV certificates require the CA to verify the applicant's identity and they are not for free.

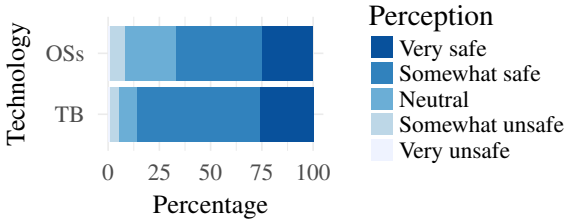


Figure 13: The level of security our respondents perceive when using Tor Browser (TB) and onion services (OSs).

mains also play a role in the context of phishing. There is concern that the short and recognizable prefixes tempt users to only verify the prefix and ignore subsequent characters [34]. This oversight may allow attackers to create impersonation domains that feature the prefix but differ in subsequent characters. Nurmi [23] and Monteiro [19] have both documented such an attack but its effectiveness is not known.

The majority of our respondents appreciates vanity domains because they are easy to remember (64%), easy to recognize (64%), and they provide a unique "branding" (34%). Some responses indicate that a vanity prefix conveniently informs about an onion service's topic, letting visitors know what to expect. Only 8% dislike vanity onion domains and 15% don't have an opinion. Interestingly, some respondents consider vanity domains unfair because wealthy entities can afford to generate longer prefixes. Several respondents voiced their concern that vanity domains create a false sense of security and facilitate phishing attacks. In a separate question we inquired how many characters our respondents verify in onion domains. 43% verify 13–16 digits, *i.e.* (almost) the full domain, while 46% verify up to nine digits, which is within the realm of brute force attacks. Finally, a handful number of respondents cited misguided reasons why they dislike vanity domains, *e.g.* some believe that vanity domains are a sign of weak hash functions while others believe that vanity domains make the onion service "less hidden" or allow somebody to create "the same private key."

5.3.6 Perceived security

Questions 6.4 and 6.6 asked how safe our respondents feel when using Tor Browser and onion services, respectively. Figure 13 shows the results. Using Tor Browser makes 86% of our respondents feel at least somewhat safe. The same is true for 67% when using onion services—clearly not as many as for Tor Browser.

Asked about why our respondents feel that way about Tor Browser, our results reveal that non-experts lack the ability to evaluate (or even understand) Tor's design which is why they defer to expert opinion, their gut feeling, or the trust they have in Tor developers. The Tor Project is perceived to take security and privacy more seriously than any other browser vendor, which is appreciated among our respondents. Most of our respondents' criticism focused not on Tor Browser but on the underlying Firefox code base. Many participants were unhappy with the exploit mitigation techniques, the lack of sandboxing, and the complex code base. Chrome was sometimes brought up as the golden standard for browser security.[10] Malicious exit relays were a concern for a handful of participants while another couple of participants are concerned that their use of Tor makes them stick out and turn into a target for government agencies. Some participants weren't sure if their Tor setup works properly—a common theme that we also noticed in our interviews: Non-technical users desire visual feedback confirming that their network traffic comes out "somewhere else."

With respect to onion services, the majority expressed that the added security and anonymity makes them feel safe. Another factor contributing to the perceived security is that onion services make use of far fewer advertising companies. Orthogonal to the technology, many participants voiced concern about illegal and questionable content on onion services, described by some as a "Wild West." Phishing sites, honeypots, and compromised onion sites further contribute to this perception.

6 Discussion

6.1 Biases

It is difficult to draw a truly uniform sample of Tor users. The only way to reach all Tor users uniformly would be to modify Tor Browser's landing page that is displayed on start—an approach that we considered prohibitively invasive. Instead, we decided to ask The Tor Project to disseminate our survey on its blog and social media accounts. We believe that this recruitment strategy was subject to the following biases.

Non-response bias. People who noticed our call for volunteers and decided against participating may exhibit traits that are fundamentally different from those who did participate. These non-respondents may have valued their privacy too much, falsely believed that their experience is irrelevant, lacked the time, or had other reasons not to participate.

Survivor bias. We predominantly heard from people who can tolerate Tor's usability issues, which is why they are still around to tell their tale. We likely did not hear from many—if any—people who gave up on Tor and were thus unable to tell us what drove them away. The danger of survivor bias lies in optimizing the user experience for the subset of people who can tolerate a non-optimal user experience.

Self-selection bias. Due to the nature of our online survey, participants could voluntarily select themselves into the

[10] Note that our survey was run before Mozilla released Firefox Quantum on Nov 14, 2017, which brought substantial improvements in both security and usability.

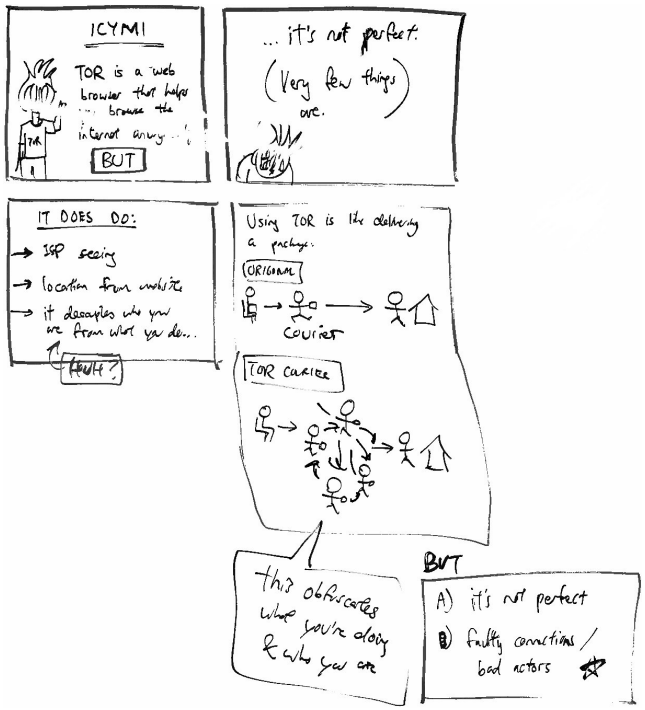


Figure 14: A comic draft that illustrates what Tor can and cannot provide for non-technical users. The comic was drawn by artist Jason Li while working with one of the authors.

group of respondents. This set of people may be unusually engaged and technical, which is why they have formed opinions that they consider worth sharing.

6.2 Take-aways for Tor developers

Several of our interview participants pointed out Tor Browser's antiquated user interface. Past work has shown that users interpret unrelated aspects such as voice quality as a proxy signal for security, which raises the question if the same holds true for user interface design [1, § IV.A]. If so, it is important to equip Tor Browser with a modern user interface.

6.3 Take-aways for Tor users

The strong security properties of onion services are futile if users cannot tell apart a genuine domain from its impersonation. Awareness of this issue is the first step and several onion services have long begun to alert their users.

6.4 Take-aways for Tor researchers

We found it challenging, yet rewarding and illuminating to study the Tor community. Tor users obviously value their privacy which reduces their willingness to participate in research projects. Past academic research projects that involved questionable methods turned this care into distrust for many users. Showing willingness to directly interact with the community and taking seriously their concerns signals respect and transparent methods. For our online survey, we recommend to use software that works in Tor Browser[11] and does not fetch tracking scripts such as Google Analytics. For the survey design, one likely has to forego asking questions that are best practice such as income level and country of residence. We made even the basic information we asked optional so our respondents had the chance to answer the survey without providing any personal information at all. In our interviews we tried to accomodate the needs of our participants by using software of their choice.

7 Conclusion

Acknowledgements

We want to thank George Kadianakis for helpful feedback on our survey questions, Katherine Haenschen for helping us improve our method, and Mark Martinez for helping us conduct some of our interviews. We are also grateful to Roya Ensafi, Will Scott, Jens Kubiziel, and Vasilis Ververis for pre-testing our survey. We want to thank Stephanie Whited for helping us disseminate our survey and greatly increasing our reach. Finally, we want to thank the broader Tor community for helpful feedback, for volunteering for our interviews, and for taking our survey.

This research was supported in part by the Center for Information Technology Policy at Princeton University. This project was further supported in part by National Science Foundation Awards CNS-1540055 and CNS-1602399.

References

[1] Ruba Abu-Salma, Anastasia Danilova, M. Angela Sasse, Alena Naiakshina, Joseph Bonneau, and Matthew Smith. "Obstacles to the Adoption of Secure Communication Tools". In: *Security & Privacy*. IEEE, 2017. URL: https://www.ieee-security.org/TC/SP2017/papers/84.pdf (cit. on p. 13).

[2] Isabela Bagueros. *Communicating security expectations for .onion: what to say about different padlock states for .onion services*. URL: https://bugs.torproject.org/23247 (visited on Jan. 9, 2018) (cit. on p. 3).

[3] Adam J. Berinsky, Michele F. Margolis, and Michael W. Sances. "Separating the Shirkers from the Workers? Making Sure Respondents Pay Attention on Self-Administered Surveys". In: *American Journal of Political Science* 58.3 (2014). URL: http://web.mit.edu/berinsky/www/files/shirkers1.pdf (cit. on p. 4).

[11] Note that Tor Browser supports three security levels; the default of "low," "medium," and "high." Some users brought to our attention that our survey did not work when the security level is set to "high" because it disables JavaScript, which our survey required—an oversight on our end.

[4] John Brooks. *Ricochet*. URL: https://ricochet.im (visited on May 15, 2017) (cit. on pp. 1, 8, 11).

[5] Jeremy Clark, Paul C. Van Oorschot, and Carlisle Adams. "Usability of Anonymous Web Browsing: An Examination of Tor Interfaces and Deployability". In: *SOUPS*. ACM, 2007. URL: https://www.freehaven.net/anonbib/cache/tor-soups07.pdf (cit. on p. 2).

[6] Debbie Collins. "Pretesting Survey Instruments: An Overview of Cognitive Methods". In: *Quality of Life Research* 12.3 (2003). URL: https://link.springer.com/content/pdf/10.1023%2FA%3A1023254226592.pdf (cit. on p. 4).

[7] DigiCert. *Ordering a .Onion Certificate from DigiCert*. Dec. 2015. URL: https://www.digicert.com/blog/ordering-a-onion-certificate-from-digicert/ (visited on Dec. 5, 2017) (cit. on p. 11).

[8] David Fifield, Linda N. Lee, Serge Egelman, and David Wagner. "Tor's Usability for Censorship Circumvention". In: *HotPETS*. URL: https://petsymposium.org/2015/papers/fifield-tor-censorship-usability-hotpets2015.pdf (cit. on p. 2).

[9] Andrea Forte, Nazanin Andalibi, and Rachel Greenstadt. "Privacy, Anonymity, and Perceived Risk in Open Collaboration: A Study of Tor Users and Wikipedians". In: *CSCW*. ACM, 2017. URL: http://andreaforte.net/ForteCSCW17-Anonymity.pdf (cit. on p. 2).

[10] Kevin Gallagher, Sameer Patil, and Nasir Memon. "New Me: Understanding Expert and Non-Expert Perceptions and Usage of the Tor Anonymity Network". In: *SOUPS*. ACM, 2017. URL: https://www.usenix.org/system/files/conference/soups2017/soups2017-gallagher.pdf (cit. on pp. 2, 6).

[11] JAP Team. *JAP – Anonymity & Privacy*. URL: https://anon.inf.tu-dresden.de/screenshot_en.html (visited on Jan. 12, 2018) (cit. on p. 7).

[12] George Kadianakis. *Cooking With Onions: Names for your onions*. Apr. 2017. URL: https://blog.torproject.org/blog/cooking-onions-names-your-onions (visited on May 4, 2017) (cit. on p. 2).

[13] George Kadianakis, Yawning Angel, and David Goulet. *A Name System API for Tor Onion Services*. 2016. URL: https://gitweb.torproject.org/torspec.git/tree/proposals/279-naming-layer-api.txt (visited on Nov. 7, 2017) (cit. on p. 2).

[14] Sheharbano Khattak, David Fifield, Sadia Afroz, Mobin Javed, Srikanth Sundaresan, Vern Paxson, Steven J. Murdoch, and Damon McCoy. "Do You See What I See? Differential Treatment of Anonymous Users". In: *NDSS*. Internet Society, 2016. URL: http://www.icir.org/vern/papers/tor-differential.NDSS16.pdf (cit. on p. 8).

[15] Linda Lee, David Fifield, Nathan Malkin, Ganesh Iyer, Serge Egelman, and David Wagner. "A Usability Evaluation of Tor Launcher". In: *PoPETS* 2017.3 (2017). URL: https://petsymposium.org/2017/papers/issue3/paper2-2017-3-source.pdf (cit. on p. 2).

[16] Micah Lee. *OnionShare*. URL: https://onionshare.org (visited on May 15, 2017) (cit. on pp. 1, 8, 11).

[17] Nick Mathewson. *Next-Generation Hidden Services in Tor*. 2013. URL: https://gitweb.torproject.org/torspec.git/tree/proposals/224-rend-spec-ng.txt (visited on Apr. 27, 2017) (cit. on p. 3).

[18] Srdjan Matic, Platon Kotzias, and Juan Caballero. "CARONTE: Detecting Location Leaks for Deanonymizing Tor Hidden Services". In: *CCS*. ACM, 2015. URL: https://software.imdea.org/~juanca/papers/caronte_ccs15.pdf (cit. on p. 11).

[19] Chris Monteiro. *Intercepting drug deals, charity and onionland*. Oct. 2016. URL: https://pirate.london/intercepting-drug-deals-charity-and-onionland-a2f9bb306b04 (visited on Oct. 23, 2017) (cit. on pp. 11, 12).

[20] Alec Muffett. *1 Million People use Facebook over Tor*. Apr. 2016. URL: https://www.facebook.com/notes/facebook-over-tor/1-million-people-use-facebook-over-tor/865624066877648/ (visited on May 15, 2017) (cit. on p. 1).

[21] Greg Norcie, Jim Blythe, Kelly Caine, and L. Jean Camp. "Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems". In: *USEC*. Internet Society, 2014. URL: https://www.freehaven.net/anonbib/cache/usableTor.pdf (cit. on p. 2).

[22] Juha Nurmi. *Ahmia – Search Tor Hidden Services*. URL: https://ahmia.fi (visited on Jan. 8, 2018) (cit. on p. 3).

[23] Juha Nurmi. *Warning: 255 fake and booby trapped onion sites*. June 2015. URL: https://lists.torproject.org/pipermail/tor-talk/2015-June/038295.html (visited on Dec. 5, 2017) (cit. on pp. 11, 12).

[24] Mike Perry, Erinn Clark, Steven Murdoch, and Georg Koppen. *The Design and Implementation of the Tor Browser*. Draft document. Mar. 2017. URL: https://www.torproject.org/projects/torbrowser/design/ (cit. on p. 10).

[25] Sai and Alex Fink. *Mnemonic .onion URLs*. Feb. 2012. URL: https://gitweb.torproject.org/torspec.git/tree/proposals/194-mnemonic-urls.txt (visited on May 4, 2017) (cit. on p. 2).

[26] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. "Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior". In: *CHI*. ACM, 2017. URL: https://users.ece.cmu.edu/~mahmoods/publications/chi17-cross-cultural-study.pdf (cit. on p. 4).

[27] Martin Schanzenbach. *The GNU Name System*. 2012. URL: https://gnunet.org/gns (visited on Nov. 7, 2017) (cit. on p. 2).

[28] Eric Swanson. *Scallion: GPU-based Onion Hash generator*. URL: https://github.com/lachesis/scallion (visited on May 5, 2017) (cit. on p. 3).

[29] Paul Syverson. *Onion Routing: Brief Selected History*. 2005. URL: https://www.onion-router.net/History.html (visited on Oct. 30, 2017) (cit. on p. 2).

[30] The Freenet Project. *Documentation*. URL: https://freenetproject.org/pages/documentation.html (visited on Apr. 28, 2017) (cit. on p. 3).

[31] The Tor Project. *Tor: Pluggable Transports*. URL: https://www.torproject.org/docs/pluggable-transports (visited on Jan. 11, 2018) (cit. on p. 6).

[32] Jesse Victors, Ming Li, and Xinwen Fu. "The Onion Name System". In: *PoPETS* 2017.1 (2017). URL: https://www.degruyter.com/downloadpdf/j/popets.2017.2017.issue-1/popets-2017-0003/popets-2017-0003.pdf (cit. on p. 2).

[33] Stephen Paul Weber. *mnemonicode*. 2017. URL: https://github.com/singpolyma/mnemonicode (visited on Apr. 27, 2017) (cit. on p. 2).

[34] Philipp Winter. *Are vanity onion domains a good idea?* Oct. 2015. URL: https://moderncrypto.org/mail-archive/messaging/2015/001928.html (visited on Dec. 5, 2017) (cit. on p. 12).

[35] Philipp Winter. *Take Part in a Study to Help Improve Onion Services*. URL: https://blog.torproject.org/take-part-study-help-improve-onion-services (visited on Oct. 25, 2017) (cit. on pp. 4, 5).

[36] Philipp Winter, Roya Ensafi, Karsten Loesing, and Nick Feamster. "Identifying and characterizing Sybils in the Tor network". In: *USENIX Security*. USENIX, 2016. URL: https://nymity.ch/sybilhunting/pdf/sybilhunting-sec16.pdf (cit. on p. 11).

A Pre-interview survey

We asked potential interview subjects to fill out a short survey (see below) before we proceeded with selecting our subjects. This survey allowed us to select for subjects with the most interesting background.

1. What is your name?
2. What is your email address?
3. Are you 18 years or older?
   - ○ Yes
   - ○ No
4. Have you used Tor Browser in the past?
   - ○ Yes
   - ○ No
5. Have you used onion services in the past?
   - ○ Yes
   - ○ No
6. How do you rate your knowledge about Internet privacy and security?
   - ○ Not at all knowledgeable
   - ○ Slightly knowledgeable
   - ○ Somewhat knowledgeable
   - ○ Moderately knowledgeable
   - ○ Extremely knowledgeable

B Interview questions

We started the interview by handing our interviewees the consent form and explained the purpose of our research to them.

Introductory questions

1. Tell us how often and why you use Tor?
2. Do you remember the first time you used Tor?

Expectations of privacy

1. What would make you use onion services more? (speed, quality/quantity of content, better domain format, popular web sites having onion sites)
2. Who or what are you trying to protect yourself against when using Tor?
3. The domain format of onion sites is weird. How do you deal with that?
4. Would you like it if Tor Browser automatically redirected you to onion sites? Even if that were the case for all onion sites?
5. How do you learn about new onion sites?
6. Do you think phishing is a concern with onion sites? How do you know if an onion site is legitimate?
7. Assume you use Tor to open `example.com`. Who can see what? What if you open the corresponding onion site instead?
8. What are you concerned about when using Tor?
9. Certain things are hidden from certain entities when you are using Tor. Please explain your beliefs.
10. Some web sites use "vanity onion domains." Whare are your thoughts on that?
11. Explain in your own words how you believe Tor works.
12. Is there anything else about the usability of onion services that you wish to share?

C Survey questions

This section contains our online survey, consisting of seven sections. Each section holds a number of questions and their respective responses. In the responses, circles indicate that only one response can be selected while squares indicate the possibility to select multiple responses.

C.1 Demographic information

1. What is your gender?
   - ○ Female
   - ○ Male
   - ○ Other
2. What is your age?
   - ○ 18–25 years
   - ○ 26–35 years
   - ○ 36–45 years
   - ○ 46–55 years
   - ○ 56–65 years
   - ○ Older than 65 years
3. What is the highest level of education that you completed?
   - ○ Some education, but no high school diploma or equivalent
   - ○ High school diploma or equivalent
   - ○ College or university degree (for example a bachelor's degree)
   - ○ Post-graduate education (for example a master's or a doctorate degree)
4. How would you rate your knowledge about Internet privacy and security?
   - ○ No knowledge
   - ○ Mildly knowledgeable
   - ○ Moderately knowledgeable
   - ○ Highly knowledgeable
   - ○ Expert

C.2 Tor usage

1. Tor Browser is a web browser—similar to Firefox—that allows you to browse the web anonymously. Have you ever used Tor Browser?
   - ○ Yes
   - ○ No
2. How frequently do you use Tor Browser?
   (Please select the answer that applies the most.)
   - ○ Never
   - ○ On average less than once a month
   - ○ On average about once a month
   - ○ On average about once a week
   - ○ On average about once a day
   - ○ Tor Browser is my main browser
3. When using Tor Browser, who do you want to protect your browsing activity from?
   (Check all that apply.)
   - □ My government
   - □ Other governments
   - □ My Internet service provider (ISP)
   - □ My school
   - □ My employer
   - □ Friends and family
   - □ Advertising companies
   - □ Hackers in open WiFis (for example in coffee shops)
   - □ Other (Please elaborate below.)
4. For quality purposes, please select only "iPhone" and "Android" in the options below.
   - □ PC
   - □ Mac
   - □ iPhone
   - □ Android
   - □ Other (Please elaborate below.)

C.3 Onion site usage

1. The Tor Browser allows you to browse "onion sites." Onion sites are web sites that can only be accessed over the Tor network. The domains of onion sites end with `.onion` instead of `.com`, `.net`, etc.; they are of constant length; and they tend to "look random." For example, The Tor Project's web site, `torproject.org`, is also available at `expyuzz4wqqyqhjn.onion` as an onion site.
2. How frequently do you use Tor Browser to browse onion sites?
   (Please select the answer that applies the most.)
   - ○ I have never used onion sites
   - ○ On average less than once a month
   - ○ On average about once a month
   - ○ On average about once a week
   - ○ On average about once a day
3. How frequently do you use onion sites for purposes other than web browsing? For example for remote login (SSH) or chat (IRC, or XMPP)?
   - ○ Never
   - ○ On average less than once a month
   - ○ On average about once a month

- ○ On average about once a week
- ○ On average about once a day

4. Why do you browse onion sites?
(Check all that apply.)
   - □ Because of the additional anonymity – traffic to onion sites never leaves the Tor network
   - □ Because of the additional security – onion sites provide end-to-end security
   - □ Some sites I like are only available as onion sites and not as normal web sites
   - □ No particular reason; I occasionally just click on links to onion sites
   - □ I read about the "dark web" and wanted to form my own opinion
   - □ Other (Please elaborate below.)
5. How do you discover new onion sites?
(Check all that apply.)
   - □ I browse the list of onion site search engines such as `ahmia.fi`
   - □ From social networking sites such as Reddit or Twitter
   - □ Recommendations from friends and family
   - □ I randomly encounter them while browsing the web
   - □ I am not interested in learning about new onion sites
   - □ Other (Please elaborate below.)
6. Are you satisfied with the way you discover new onion sites?
(Check all that apply.)
   - ○ Yes
   - ○ No (Please elaborate below.)
7. Many people memorize popular domains such as `youtube.com` and `wikipedia.com` for quick access. How do you deal with the domain of onion sites such as `expyuzz4wqqyqhjn.onion`?
(Check all that apply.)
   - □ I save a list of onion domains in a file on my computer
   - □ I write onion domains down using pen and paper
   - □ I bookmark onion domains in Tor Browser
   - □ I use a web-based bookmarking service such as Firefox Sync or Google Bookmarks
   - □ I use a search engine each time (for example, to search for "facebook onion site")
   - □ I go to web pages I trust that have links to onion sites
   - □ I memorize some onion domains
   - □ I don't have a good solution
   - □ Other (Please elaborate below.)
8. The Tor Project is currently working on the next generation of onion services. The new onion domain format will consist of 52 characters, for example: `a1uik0w1gmfq3i5ievxdm9ceu27e88g6o7pe0rffdw9jmntwkdsd.onion` Do you expect this to change your browsing habits?
   - ○ Yes (Please elaborate below.)
   - ○ No (Please elaborate below.)
9. Do you have a Facebook account?
   - ○ Yes
   - ○ No
10. Have you ever logged in to Facebook over its onion site `facebookcorewwwi.onion`?
   - ○ Yes, that is the only way I log in to Facebook
   - ○ Yes, occasionally
   - ○ No, never
   - ○ I didn't know about this onion site until now
11. For quality purposes, please select "Yes, more than once" in the options below.
   - ○ Yes, once
   - ○ Yes, more than once
   - ○ No
12. How many onion domains do you have fully memorized?
   - ○ None
   - ○ One
   - ○ Two
   - ○ Three
   - ○ Four
   - ○ More than four
13. Is `facebookcorewwwi.onion` among the sites that you have memorized?
   - ○ Yes
   - ○ No
14. Why do you memorize onion domains?
(Check all that apply.)
   - □ It allows me to open the site more quickly

- □ I don't want to leave any digital traces of the onion sites I visit
- □ That way I can be sure that I end up at the right onion site and not a phishing site
- □ After typing a domain many times, I automatically start to memorize it
- □ Other (Please elaborate below.)

15. Imagine you had to memorize onion domains. Please rate the difficulty of memorizing the following domains.

    - `facebookcorewwwi.onion`
    - `expyuzz4wqqyqhjn.onion`
    - `torproz4wqqyqhjn.onion`
    - `torprojectqyqhjn.onion`

    For each answer, we provided the following Likert scale:

    - Very easy
    - Somewhat easy
    - Neither easy nor difficult
    - Somewhat difficult
    - Very difficult

16. Please explain the reason for the rating you gave above.

17. If popular web sites such as YouTube, Twitter, or Amazon offered onion sites in parallel to their normal web sites, which one would you prefer?

    - ○ Always the normal web site
    - ○ Always the onion site
    - ○ Other (Please elaborate below.)

18. Please explain the reason for the choice you made above.

19. If Tor Browser could automatically redirect you from a web site to its corresponding onion site (for example from `facebook.com` to `facebookcorewwwi.onion`), would you use this feature?

    - ○ No, never
    - ○ Yes, for some sites
    - ○ Yes, always
    - ○ Other (Please elaborate below.)

20. Please explain the reason for the choice you made above.

21. Please rate how important the following criteria are for the usability of onion sites.
    (Check all that apply.)

    - Page load time
    - Quality of content (e.g., up-to-date, interesting sites)
    - Diversity of content (e.g., sites about politics, technology, social media, etc.)
    - Easy-to-remember domain format
    - Having an onion service version of popular services such as Facebook
    - Existence of a search engine (like Google) for onion services

    For each answer, we provided the following Likert scale:

    - Very unimportant
    - Somewhat unimportant
    - Neutral
    - Somewhat important
    - Very important

C.4 Onion site operation

1. Have you ever set up your own onion site?

    - ○ Yes
    - ○ No, but I have considered doing it
    - ○ No, and I have not considered it

2. Did you experience any issues while setting up your onion site?

    - ○ No
    - ○ Yes (Please elaborate below.)

3. Why did you set up your own onion site?
    (Check all that apply.)

    - □ I wanted my site to be anonymous
    - □ I wanted my site to have end-to-end security
    - □ I used a tool that automatically creates onion sites (for example OnionShare or Ricochet)
    - □ To make my site accessible behind a NAT device
    - □ Out of curiosity
    - □ Other (Please elaborate below.)

4. Were the onion site(s) you set up intended for the general public, or only for private use?
    (Check all that apply.)

    - □ For public use (for example, a public blog)
    - □ For private use (for example, sharing pictures with a friend)

5. Please rate the level of concern you would have for the following scenarios.

   - Somebody deanonymizing my onion service
   - Somebody taking my onion service offline
   - Somebody setting up a phishing site targeting my onion service

   For each answer, we provided the following Likert scale:

   - Not at all concerned
   - Slightly concerned
   - Somewhat concerned
   - Moderately concerned
   - Extremely concerned

C.5 Onion site phishing and impersonation

1. Did you ever type an onion domain manually?

   ○ Yes
   ○ No

2. Please elaborate on why you typed an onion domain manually?

3. How do you realize that you made a typo when typing an onion URL?
   (Check all that apply.)

   □ When the page won't load
   □ When a wrong page shows up
   □ I don't know
   □ Other (Please elaborate below.)

4. Have you ever thought about whether the onion site you are browsing is the authentic site you are trying to reach?

   ○ Yes
   ○ No

5. How do you know an onion site is the legitimate site you are trying to reach, and not an impersonation?
   (Check all that apply.)

   □ I verify (part of) the onion domain in Tor Browser's address bar
   □ I use bookmarks when accessing onion sites
   □ I go to the corresponding web site and look for the link to its onion site
   □ Sometimes I cannot tell the difference between the legitimate and the impersonation site
   □ I copy&paste onion domains from a trusted source
   □ I check if the onion site's HTTPS certificate is valid (if it has one)
   □ I don't check
   □ Other (Please elaborate below.)

6. How many characters of a domain do you verify? Recall that an onion domain has 16 characters.

   ○ 1–3
   ○ 4–6
   ○ 7–9
   ○ 10–12
   ○ 13–16

7. For quality purposes, please select "Less than once a month" in the options below.

   ○ Less than once a month
   ○ About once a month
   ○ About once a week
   ○ About once a day

8. Have you ever sent Bitcoins to a Bitcoin address that you got from an onion site?

   ○ Yes
   ○ No

9. Some onion site owners use tools to have a short word at the beginning of their onion domain. This is why Facebook's domain (`facebookcorewwwi.onion`) looks the way it does. We call these customized domains "vanity onion domains."

10. What is your overall opinion on vanity onion domains?
    (Check all that apply.)

    □ I find them useful because they are easier to memorize
    □ I find them useful because they are easier to recognize
    □ I like them because they make an onion site look "unique"
    □ I dislike them because onion sites shouldn't contain their name in their domain
    □ I don't see a benefit
    □ I don't have an opinion
    □ Other (Please elaborate below.)

C.6 Expectations of privacy

1. Let us move away from onion services and turn to expectations of privacy. If you use Tor Browser to open `http://example.com`, who do you believe can see your connection to `http://example.com`?
(Check all that apply.)

   - ☐ Your Internet service provider (ISP)
   - ☐ The ISP of `example.com`
   - ☐ Your Tor "exit relay"
   - ☐ Your Tor "guard relay"
   - ☐ Nobody
   - ☐ I don't know
   - ☐ Other (Please elaborate below.)

2. Now imagine that you are instead using Tor Browser to open the *onion site* of `http://example.com`. Who do you believe can see your connection to this onion site?
(Check all that apply.)

   - ☐ Your Internet service provider (ISP)
   - ☐ The ISP of the onion site
   - ☐ Your Tor "exit relay"
   - ☐ Your Tor "guard relay"
   - ☐ The "guard relay" of the onion site
   - ☐ Nobody
   - ☐ I don't know
   - ☐ Other (Please elaborate below.)

3. How safe do you feel when using Tor Browser compared to another browser?

   - ○ Very unsafe
   - ○ Somewhat unsafe
   - ○ Neutral
   - ○ Somewhat safe
   - ○ Very safe

4. Please elaborate on why you feel that way when using Tor Browser.

5. Please tell us about how safe you feel when browing onion sites as compared to normal web sites?

   - ○ Very unsafe
   - ○ Somewhat unsafe
   - ○ Neutral
   - ○ Somewhat safe
   - ○ Very safe

6. Please elaborate on why you feel that way when using onion sites.

7. For quality purposes, please select only "Very unsafe" in the options below.

   - ○ Very unsafe
   - ○ Somewhat unsafe
   - ○ Neutral
   - ○ Somewhat safe
   - ○ Very safe

8. Assume you just set up your own onion site. Who do you believe can see that this onion site was set up?
(Check all that apply.)

   - ☐ The onion site's ISP
   - ☐ The developers of The Tor Project
   - ☐ (Some) Tor relays
   - ☐ Nobody
   - ☐ I don't know
   - ☐ Other (Please elaborate below.)

9. Facebook already runs the onion site `facebookcorewwwi.onion`. How difficult or easy do you believe is it for someone to create domains that begin with the following characters? Note that the `X` symbols below are just placeholders. What matters is the first characters.

   - `facebookcoreXXXX.onion`
   - `facebookXXXXXXXX.onion`
   - `faceXXXXXXXXXXXX.onion`

   For each answer, we provided the following Likert scale:

   - Very easy
   - Moderately easy
   - Neither easy nor difficult
   - Moderately difficult
   - Very difficult
   - I don't know

C.7 End of survey

1. Finally, is there anything else about the usability of Tor or onion services that you wish to share with us?

D Coding themes

Table 4: The codewords we developed while coding our interviews, together with their respective explanations, and the number of interviewees who brought them up.

Category	Codeword	Explanation	Occurences
	90s-experience	Tor provides a browsing experience akin to the 90s.	N
	slow-browsing	Browsing the web over Tor feels slow.	N
	empowerment	Tor equips users with control over their browsing.	N