Understanding Users' Knowledge about the Privacy and Security of Browser Extensions

Ankit Kariryaa, *University of Copehagen & University of Bremen;* Gian-Luca Savino and Carolin Stellmacher, *University of Bremen;* Johannes Schöning, *University of Bremen & University of St. Gallen*

https://www.usenix.org/conference/soups2021/presentation/kariryaa

This paper is included in the Proceedings of the Seventeenth Symposium on Usable Privacy and Security.

August 9–10, 2021

978-1-939133-25-0

Open access to the Proceedings of the Seventeenth Symposium on Usable Privacy and Security is sponsored by

Understanding Users' Knowledge about the Privacy and Security of Browser Extensions

Ankit Kariryaa*
University of Copenhagen & University of Bremen
ak@di.ku.dk

Gian-Luca Savino*
University of Bremen
gsavino@uni-bremen.de

Carolin Stellmacher
University of Bremen
cstellma@uni-bremen.de

Johannes Schöning
University of Bremen & University of St. Gallen
schoening@uni-bremen.de

Abstract

Browser extensions enrich users' browsing experience, e.g., by blocking unwanted advertisements on websites. To perform these functions, users must grant certain permissions during the installation process. These permissions, however, give very limited information about the fact that they allow the extension to access user's personal data and browsing behaviour, posing security and privacy risks. To understand users' awareness of these privileges and the associated threats, we conducted an online survey with 353 participants, focusing on users' attitude, knowledge, and preference towards extensions' permission requests. We found that users report interest in seeking information, trust the developers but do little to protect their data. They have limited knowledge about the technical abilities of browser extensions and prefer permission statements that evoke a clear mental model. Based on our findings we derive recommendations for the improvement of browser extension permission dialogues through clear language, technical improvements and distinct responsibilities.

1 Introduction & Motivation

Web browsers are an important technology in modern daily life. We constantly use them to access online content for news, education, shopping or communication. As a result, browsers have a very large user base as well as a diverse scope of applications. To meet the requirements of such diverse use cases or enhance the browsing experience, browsers' functionalities can be extended through browser extensions.

Browser extensions, also known as browser add-ons, are small software programs that run inside a web browser. They are often developed by third-party companies or independent developers and are typically free of charge. Popular browsers have their web stores offering extensions in various categories ranging from productivity over accessibility to shopping (e.g. over 180k browser extensions are available for Google Chrome as of August 2019 [39]). The ten most popular browser extensions for Google Chrome alone have over 100 million combined downloads. The large number and variety of extensions enable users to customise their browser experience for their personal needs and preferences. Popular extensions block unwanted advertisements on websites or translate web text into the desired language. Others increase the accessibility of the browser through voice interaction [53] or automatically generate image descriptions on Twitter for people with vision impairment [35]. Recently, extensions were also proposed for detecting fake news through automatic fact checking [11], assisting users in the understanding of online privacy policies through spotting opt-out statements [7], or providing personalised password strength estimation [30].

To perform their intended purposes, extensions request permissions to access the content of visited websites and, often, other parts of the browser such as the browser's history. These special privileges enable extensions to read highly sensitive and personal data such as passwords or payment information, which can have serious implications for users' privacy and security. Especially with the nowadays ubiquitous online behaviour, knowledge about users' online browsing habits is highly valuable for revenue generation in the various domains (e.g., targeted advertisement). This illustrates a high commercial interest in users' browsing data which motivates malicious practices to gain access. Many leakage reports over the years [13, 49, 55] explored browser extensions and identified their role in online security and privacy issues.

To install an extension and benefit from its functionality users must grant all requested permissions and allow access to their browsing data. Users, therefore, have to make a trade-off between privacy concerns and convenience.

* denotes equal contribution.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2021.
August 8–10, 2021, Virtual Conference.

These trade-offs are not equally apparent to all users. As cybersecurity expert Schneier states in an interview:

> "In general, security experts aren't paranoid; we just have a better understanding of the trade-offs we're doing. Like everybody else, we regularly give up privacy for convenience. We just do it knowingly and consciously." [38]

It is, therefore, crucial to inform users appropriately about the data collection of browser extensions to enable them to make an informed decision. To do so, most browsers display a permission dialogue that users have to confirm to install browser extensions. However, explanations of these dialogues vary across browsers in regards to the user interface, used language and level of detail, as shown in Figure 1.

While it is easy and fast to install an extension at the click of a button and simultaneously grant the permission requests, it is unknown if the users are aware of the meaning and significance of these permissions and the associated risks. Recent research in the related topic of browsers' private modes has shown that differences in-browser explanations across browsers caused misconceptions about what private browsing mode does and how it protects users' privacy [54]. If such explanations can not convey the necessary knowledge, users are unable to make an informed decision and develop a false sense of security. To ensure their sovereignty over their personal data and to design better technology supporting them in privacy-related decisions, it is crucial to identify these gaps.

To better understand users' attitudes, knowledge, and preference towards browser extension permissions, we conducted an online survey with 353 participants. We investigated the effectiveness of modern browsers to communicate the meaning of permission requests. Our research particularly focuses on users' knowledge of the data that extensions can access and their understanding of the security and privacy risks coming with these privileges. We found that users have limited knowledge about the technical abilities of browser extensions. Their knowledge is mostly restricted to the beneficial features of the extensions they use and does not extend to other possible privacy and security risks. Their inability to apply this knowledge in a broader context shows their lack of technical understanding of the underlying permissions. Furthermore, users' perception of likelihood seems to be driven by the level of intrusion a scenario can potentially have on their privacy. We derive recommendations based upon our results and consider the perspective of users, developers and policymakers. These recommendations focus on improving the extension system, language of permissions and users' attitude. This paper contributes the first large scale survey on understanding users' attitudes, knowledge, and preferences about the privacy and security of browser extensions. Our study identifies a gap in users' perception about the current permission model and calls for long-overdue security improvements inspired by similar domains.

2 Related Work

As relevant prior work, we firstly summarise the background of the current browser extension system. We then present related research in the fields of human-computer interaction (HCI) and usable security about understanding users' knowledge, attitude and behaviour.

2.1 Browser Extensions & Browser Extension Security

With the exception of Safari[1], most modern browsers use the extension system that was first implemented by Google Chrome in 2009. The Chrome extension system stems from the design proposed by Barth et al. [8]. Their design was based upon the assumption that extension developers have good intentions but are, usually, not security experts. They argued that well-intentioned extension developers often write buggy code that can be exploited by malicious website operators to gain control over the extension. These exploits posed significant threats for two main reasons: 1) Under the former Firefox extension system, which was popular at that time, extensions often used unnecessarily powerful APIs and 2) they could have access to full user privileges at par with browsers or other native applications. To overcome these challenges, Barth et al. proposed a new browser extension system that improved the security of extensions by using principles of least privilege, privilege separation, and isolation. Their design separated the extension into three components, namely a content script, an extension core, and a native binary. Only the least privileged part of the extension (i.e. content scripts) was exposed to potentially malicious websites. In an evaluation of this security architecture, Carlini et al. [12] found it was mostly successful at preventing direct web attacks on extensions, but underlined its susceptibility to network attacks and website metadata attacks.

The Chrome extension system was designed to protect buggy-but-benign extensions, however, it provides no protection to users against intentionally malicious extensions. In recent years, a large number of browser extensions were found to be malicious, challenging the buggy-but-benign assumption. In an analysis between 2016 and 2018, Chen and Kapravelos identified over 3000 browser extensions from Chrome and Opera that were potentially leaking privacy-sensitive information [13]. The ten most popular Chrome browser extensions on that list, with confirmed malicious behaviour, affected over 60 million users. Another large-scale study investigated the 10,000 most popular browser extensions of Google Chrome and found that hundreds of extensions leaked sensitive information about users' browsing habits [49]. They found that while most extensions leaked information accidentally, e.g., when third-party content is injected into a website,

[1] Apple announced in WWDC 2020 that Safari will switch to the same extension API in the near future

others abused their access to user data on purpose. In July 2019, Jadali identified eight browser extensions with a total of 4 million downloads that collected browsing histories and exposed them in real time [28]. Similarly, a report from May 2020 identified 111 malicious extensions that were siphoning personal data such as passwords, credential tokens stored in cookies or parameters, screenshots, and tracking users browsing history [25]. Jointly, these 111 extensions had more than 32 million downloads. Another malevolent practice performed through browser extensions is malvertising which includes altering web content and displaying malicious advertisements, leading users to download and install malware. A screening of 18,000 Chrome extensions in 2015 found that extensions practising malvertising had over half a million users [55]. These studies and reports on malicious extensions with millions of downloads strongly challenge the assumption that all extension developers have good intentions.

To protect users from malicious extensions, most web stores use an automated review process [3, 15, 17, 22]. In certain cases, especially when sensitive permissions are involved, a manual review may follow an automated one. However, data leaks and reports of malicious activities underline the limits of these approaches. In response to privacy-breaching browser extensions, various solutions were proposed to protect or inform the users. These solutions include privacy-focused extensions to notify the user if an installed extension was suspected of malicious practices [51] or generating visits to random websites to conceal users' true browsing behaviour [49]. Similarly, to protect users from malvertising, Xing et al. proposed a browser extension that automatically detects extensions that inject ads [55]. These privacy-focused extensions not only increase users' privacy but can also improve users' browsing experience [10]. The proposed solutions and the review process of the web stores can assist users in protecting their online privacy and security. Nonetheless, the decision about extensions' security cannot be left to trusted parties alone [24]. The bulk of potential risks and the responsibility to make an informed choice lies with the user. The current practice of browsers to inform users about their extensions is using dialogues to describe the requested permissions during the installation process. However, there is limited research on users' attitude and knowledge towards browser extensions and the effect that permission dialogues have on them.

2.2 Privacy Knowledge and Data Sharing Behaviours

Next, we discuss related works in associated domains about understanding users' attitude and knowledge towards permissions and data collection.

In the domain of mobile applications, researchers found that smartphone users are often unaware of the permission settings and data collection of apps running on their devices [2, 9, 34, 48]. This is partly because users display low attention and comprehension when it comes to reading permission dialogues. In a study, Felt et al. found that 17% of participants paid attention to permissions during installation in a laboratory setting, and only 3% could correctly answer permission comprehension questions in an online survey [19]. When confronted with real app behaviours users felt their personal space had been violated [48]. This insight has led to studies trying to improve users' understanding of certain permissions and the data they give away. Almuhimedi et al. used a custom permission manager to make users aware of the data that applications were accessing and were able to make users reassess and restrict the permissions they were giving to applications [2]. Similar studies have also been conducted in other domains that deal with highly sensitive health data, such as wearable and fitness trackers [23, 40]. Research finds that with wearable technology it is less about the knowledge that data is collected, but about the value of this data [1] and the severity of the consequences of it being collected [47]. Schneegass et al. showed that non-expert users lack an understanding of the relationship between access to sensor data and access to information derived from this sensor data [47]. Furthermore, Aktypi et al. found that users highly underestimate the value of personal fitness data for third parties [1].

These studies across domains have been beneficial in developing systems that support users in making informed and sensible decisions with regards to access permissions. Even though browser extensions have existed for longer than mobile apps and fitness trackers, there is limited research in understanding users' attitude, knowledge or preference towards extension permissions, or making the extension permissions more understandable and usable. To fill this gap in the literature, in this paper, we study the privacy and security attitude of users towards browser extensions. We assess their knowledge about permissions and finally gather their preferences towards existing permission statements.

3 Method

We conducted an online survey to learn about (1) users' attitudes towards privacy and security topics related to browser extensions, (2) their general knowledge about browser extensions, (3) the influence of browser extension permission dialogues on their understanding, and (4) their preference for specific browser extension permission dialogues.

3.1 Browsers and Browser Extensions

In this paper, we study the browser dialogues of the most common browsers and browser extensions. As per Statista, the six largest desktop browsers by market share are Chrome (69.42%), Safari (8.74%), Firefox (8.48%), Edge (3.45%), Internet Explorer (2.88%) and Opera (2.39%) [50]. We excluded Internet Explorer in our study because Microsoft ended development for the browser in 2016 and replaced it with Edge.

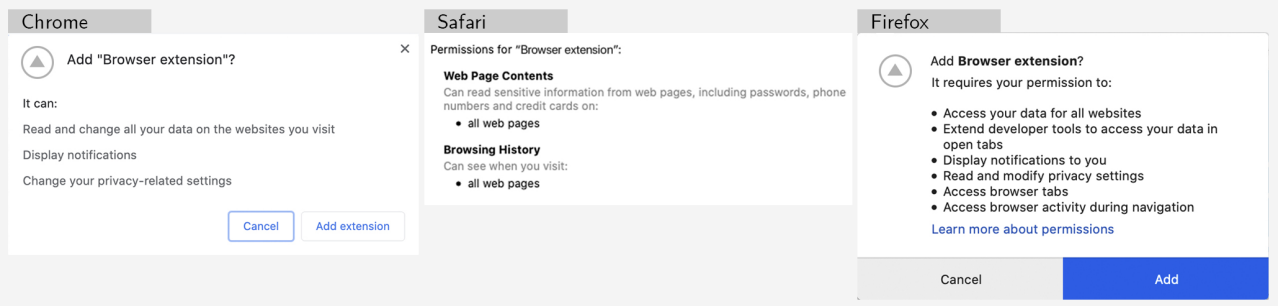

Figure 1: Permission dialogues of our sample extension for Chrome, Safari and Firefox. The sample extension used the super-set of permissions of the selected extensions.

Next, we surveyed the 10 most used extensions for each browser based upon download count if available, otherwise the number of ratings. Table 2 in the appendix (section B) shows these browser extensions for the five browsers. We, then, extracted the extensions with the highest appearance rate (number of browsers they appeared in) and ranked them by downloads across all browsers. Based on our criteria, we identified the following five extensions for our study: (1) Adblock Plus, (2) uBlock Origin, (3) Grammarly, (4) Adblock, and (5) Honey. Since Opera and Edge are both Chromium-based and their permissions are, therefore, almost identical, we decided to eliminate them from our study and focus on the differences between Chrome, Firefox and Safari (having around 86% market share). The permissions requested by the selected browser extensions are shown in Table 1. Next, we implemented a representative extension that used the super-set of permission requested by these five extensions in Chrome, Firefox, and Safari. Our extension used an ambiguous name and logo (see Figure 1). We locally installed the dummy extension on all the browsers and captured the actual permission dialogues.

3.2 Scenarios

To evaluate respondents' knowledge and beliefs about the technical abilities of browser extensions, we created ten scenarios. The scenarios were developed in iterative discussions involving three researchers with backgrounds in usable security and interface design (see section 4.3.2, figure 5 for a complete list of scenarios). Scenarios 1-3, 5, 8 were derived from the existing literature on malicious activities of extensions [13, 25, 28, 32, 37, 49, 55]. Scenarios 4, 6, 7, 9, 10 were added to ensure a broader possibility spectrum. The most common permission required by the browser extensions is to "Access all data on all websites". We found that among the 50 most downloaded browser extensions on the Firefox web store[2], 47 extensions request this permission. Given the ubiquitous need for this permission, five out of ten scenarios were based upon the functionality provided by it. Other scenarios considered access to the device's camera and microphone and the ability to control other extensions. Furthermore, three scenarios were based upon functionality outside the scope of a browser, namely, change the default password of the computer, restart the computer, and install an application on the computer.

We framed the scenarios as neutral statements without any harm being explicitly mentioned in them. We postulate that the neutral statements have a higher ecological validity as they can be considered direct derivatives of the statements of the browser permission dialogues. For example, scenario S_5 "The browser extension reads the user's usernames and passwords and stores them on an external server" is a specific case of the Chrome permission "Read and change all your data on websites you visit". Thus, the scenarios could test the case-specific knowledge of the various permission statements.

The permissions specified under the extension API allow the browser extensions to, among other things, access the web content, and access browsing history. In general, the permissions available under the extension API model are limited to the browsers. However, some extensions work in tandem with desktop applications such as Zotero[3] and Grammarly[4]. This model allows the extensions to leverage the privileges of their tandem applications and perform functions outside the scope of the extension API. Thus, in a broad sense, browser extensions can control any aspect of a computer, even though many functionalities are outside the scope of the extension API. In an absolute sense, all of the scenarios are technically possible but some require additional intervention by the user.

3.3 Survey Structure

Our survey comprised 35 unique questions, including attention checks. However, since it included randomisation and branching logic, the average participant was shown around 28 questions. The survey consisted of "yes/no/don't know",

[2] https://addons.mozilla.org/en-US/firefox/extensions/

[3] https://www.zotero.org/

[4] https://www.grammarly.com/

Extension	Downloads Chrome	Ratings Safari	Downloads Firefox										
				Chrome:	Read and change all your data on the websites you visit	Display notifications	Change your privacy-related settings						
				Safari:	Web Page Content: Can read sensitive information from web pages, including passwords, phone numbers and credit cards on: - all web pages			Browsing History: Can see when you visit: - all web pages					
				Firefox:	Access your data for all web sites	Display notifications to you	Read and modify privacy settings		Access IP address and hostname information	Store unlimited amount of client-side data	Access browser tabs	Access browser activity during navigation	Extend developer tools to access your data in open tabs
Adblock Plus	+10.0M	108	6.8M		C, S, F	C, F		S		F	F	F	F
uBlock Origin	+10.0M	*not available*	3.8M		C, F		C, F		F	F	F	F	
Grammarly	+10.0M	613	1.1M		C, S, F	C, F		S			F		
Adblock	+10.0M	1K	1.0M		C, S, F	C, F		S		F	F	F	F
Honey	+10.0M	4.6K	958K		C, S, F			S					

Table 1: Permissions requested by the selected browser extensions in Chrome (C), Firefox (F) and Safari (S). Download and rating count were retrieved in August 2020 from the respective browser extension stores.

multiple-choice, five-point Likert scale questions and one open-ended question. The complete survey can be found in the appendix (section A). Our survey methodology is adopted from similar studies in the HCI and usable security community that focused on understanding users' knowledge, attitude and behaviour for various digital platforms [23, 27, 44]. The survey consisted of the following sections:

Demographics: Participants' age and education as well as whether they have a professional background in any computer science-related field.

Confidence and attitudes regarding the information on browser extensions: The specific browsers and browser extension participants use. Their confidence about knowing what kind of data browser extensions collect and if developers made sure their data is safe. Their own precautions and attitudes towards privacy policies and terms and conditions.

Knowledge of the capabilities of browser extensions: The plausibility of the ten scenarios and the likelihood of them being used maliciously. Participants had to judge whether the scenarios were technically possible by answering "yes", "no", or "I don't know" and how likely they would deem the scenarios to be used maliciously on a five-point Likert scale from "very unlikely" to "very likely". In a separate question placed before the scenarios, we also asked the participants if an installed ad-blocker can read passwords on various websites.

Comprehension of extension permission dialogues: Comprehension and understanding of existing browser dialogues for Chrome, Firefox, and Safari. Participants were randomly presented with one of the browser extensions permission dialogues. They had to judge the same ten scenarios again on their plausibility and likelihood of being used maliciously, taking the permission dialogue into account. We were interested in whether the dialogues would convey the information to correctly assess the possibility of the scenarios if participants had previously failed to do so.

Preference of permission statements: The three browsers formulate their permission statement differently. Firefox uses all-inclusive words such as *"access"*, Chrome uses distinct keywords such as *"read and change"*, and Safari provides specific examples such as *"read sensitive information on web pages including passwords ..."*. For each of the browsers, we studied information conveyed and participants' preference for four commonly requested permissions. To do so, we created a comprehensive description including an explanation and examples for the four permissions. Our comprehensive description was based upon the reference text provided by the different browsers such as Firefox [20] and Chrome developer documentation [14]. To remove any bias towards a single source, we included the important keywords used by all browsers in our comprehensive description. For example, the following description represents the permission about access to information on all pages:

> "The browser extension can access, meaning read and change, all information including sensitive information such as passwords, phone numbers, credit card numbers, text and images on all websites such as those for online banking, email service, online shopping, and social media."

Participants were asked to rate the similarity and preference of browsers' original permission statements compared to the

comprehensive descriptions. The complete list of comprehensive descriptions that we developed for the study can be found in the survey (appendix section A, Q 6.1-4, page 17-18).

3.4 Participants

The recruitment of participants was done through the online platform Prolific [41]. The survey was hosted on Qualtrics [43]. 408 participants completed the survey, and on average it took them 11 minutes to finish it. The study participants had an average Prolific approval rating of 98.9% and they resided in more than 20 countries (mostly EU). Participants were paid £1.2 at a rate of £6.5 per hour. We excluded 12 participants due to failed attention checks and ended up with a total of 396 valid survey responses. Since we were interested in users of browser extensions, we excluded 43 participants from the main analysis who do not use browser extensions. We will, however, discuss their answers separately in our insights. Consequently, we analysed a data set of 353 responses of participants using browser extensions.

Of the 353 respondents, 219 (62%) identify as male, 134 (38%) as female. Their age ranged from 18 to 63 with a mean age of 28 ($SD = 9.6$). Regarding education, six (2%) had no formal education, 130 (37%) had a high school diploma or equivalent, 209 (59%) had a university degree and eight (2%) a doctoral degree.

3.5 Limitations and Ethical Considerations

While our study is based upon a relatively large and diverse sample, it may not be representative of the entire population. Our sample is relatively young, well educated and has a high proportion of people with a background in computer science. We also recorded 12 invalid responses from participants who left the survey early as well as 10 participants who did not finish the survey in the maximum allocated time of 49 minutes. This might have been due to a stereotype bias caused by the leading demographic questions, however, given the relatively small number of invalid responses the bias is unlikely to be pronounced. As it is sometimes the case with surveys in the domain of usable privacy and security, we would like to underline that some of our findings may have been impacted by social desirability and response bias where participants tend to present an inflated view of their privacy concerns, believing this is how the researchers want them to respond. Besides these, in our survey, most questions were based upon a rating scale and we had limited free text questions. For example, to study the appropriateness of extension browser permission statements, we asked the participants to evaluate their similarity and preference as compared to their comprehensive descriptions on a three-point scale (see section 4.3.5 and 5.2.4 for more information). While this approach allows us to determine the appropriateness of browser permission statements, it is not suitable to determine specific shortcomings in a given statement. A future work looking to elicit these specific shortcomings may find other approaches such as surveys focused on open response questions followed by qualitative coding more useful. It should also be noted that our study is based upon a frequently used, but limited, set of permissions, which only covers a part of the many permissions that are available to browser extensions.

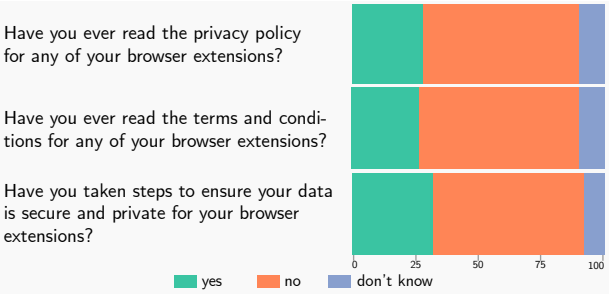

Figure 2: Participants' response to having read the privacy policy or terms and conditions of their installed extensions.

The survey was conducted within the ethical research guidelines of our university and did not require separate approval from the ethics board. Besides the Prolific IDs, which were necessary for compensating the participants, we did not collect any personally identifiable information in the survey.

4 Results

The following results were extracted from the survey and present users' usage of browsers and browser extensions, as well as our three main focal points on users' attitude, knowledge, and preference. Since our survey is exploratory, we primarily used descriptive statistics supported by graphic representations and complemented with significance testing where applicable.

4.1 Browsers and Browser Extensions

Most participants report Chrome (66%) as their default browser. This is followed by Firefox (18%), Opera (6%), Brave (4%), Edge (3%), and Safari (3%). Vivaldi, Yandex and Opera GX were also mentioned by one participant each.

85% of the participants use ad-blockers (e.g. Ad-block Plus, uBlock Origin), 30% use language tools (e.g. Oxford Dictionary, Grammarly), 29% use video or music downloaders (e.g. YouTube Downloader, Video DownloadHelper), 26% use password managers (e.g. LastPass, 1Password), 25% use shopping assistants (e.g. Honey, Piggy), and 19% use productivity tools (e.g. Todoist, Evernote).

Of the 43 respondents who do not use browser extensions, 44% didn't know they existed, 42% said that they do not need them, 7% find them too difficult to install, and 5% do not

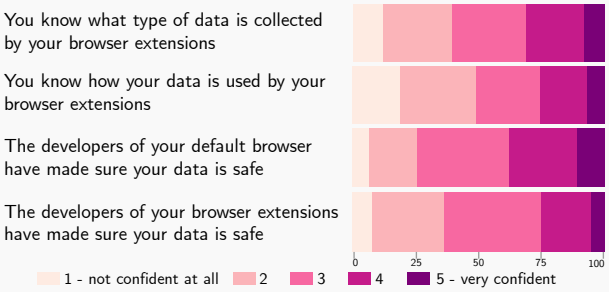

Figure 3: Participants' confidence in their own knowledge about the data collection, data usage and developers of their installed browser extensions.

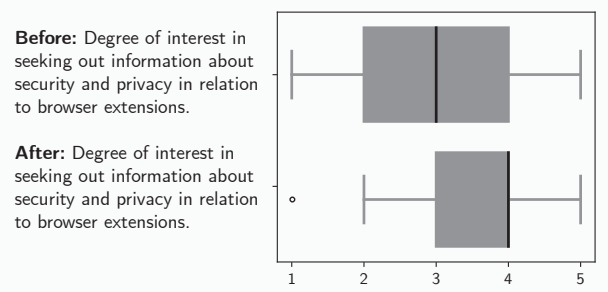

Figure 4: Interest in seeking information in the beginning and end of the survey.

use them because of concerns about data privacy. 2% were uncertain if they were using browser extensions.

4.2 Attitude

This section presents users' attitudes towards reading terms and conditions, their confidence in developers of web browsers and browser extensions, the impact of the permission dialogue and their interest in seeking information on security and privacy concerning browser extensions.

4.2.1 Terms and Conditions

More than 60% of the participants in our survey reported that they have not read the privacy policy or the terms and conditions of their installed browser extensions. Furthermore, 59% reported that they did not take any steps to ensure their data is safe with the browser extensions. Figure 2 shows the response of the participants.

4.2.2 Confidence in Developers

Figure 3 shows the participants' confidence in developers of their default browser and installed browser extensions, that they have ensured user data is not being tampered with or shared without explicit consent. Participants showed slightly higher confidence in the developers of their default browser ($median = 3.0, mean = 3.17, SD = 1.07$) compared to the developers of their browser extensions ($median = 3.0, mean = 2.87, SD = 1.00$). A Wilcoxon signed-rank test showed that the differences were statistically significant ($p < 0.001$). Only a small number of participants had either very high or no confidence in the developers of both browsers and browser extensions, with three out of five being the most frequent choice.

4.2.3 Awareness of Permission Dialogues

To study users' awareness of permission dialogues, we showed participants the Chrome dialogue as a representative of browser extension dialogues. 123 (34.8%) of the participants reported that they had seen the provided example or a similar permission dialogue before. 28.3% reported that they had not seen a permission dialogue, and the rest could not remember. Out of the 123 who had seen a permission dialogue, 68% reported that it influenced their decision about installing the browser extension.

4.2.4 Interest in Seeking Information

We asked the participants about their interest in seeking out information on security and privacy concerning browser extensions in the beginning as well as at the end of the survey. At the end of the survey, participants were more interested in seeking out information and the median interest increased from three to four. The results are shown in figure 4. A Wilcoxon signed-rank test showed a statistically significant difference between the interest in the beginning and the end of the survey ($p < 0.001$). Furthermore, most participants are not comfortable in having browsing history or personal data being collected and stored by a browser extension. On a scale from 1 - Not at all comfortable to 5 - Extremely comfortable, they gave a median score of two.

4.3 Knowledge

In this section, we report our findings in regards to participants' knowledge about browser extensions, the practices of data collection and the impact permission dialogues have on users' knowledge.

4.3.1 Data Collection And Use

We asked participants to rate their confidence in their knowledge of what data is collected, and how the collected data is used by browser extensions. Participants rated their confidence on a five-point unipolar Likert scale from 1 - Not at all confident to 5 - very confident. Figure 3 shows a mostly uniform distribution of the responses. However, participants were less confident in how the data is used than what type of data is collected.

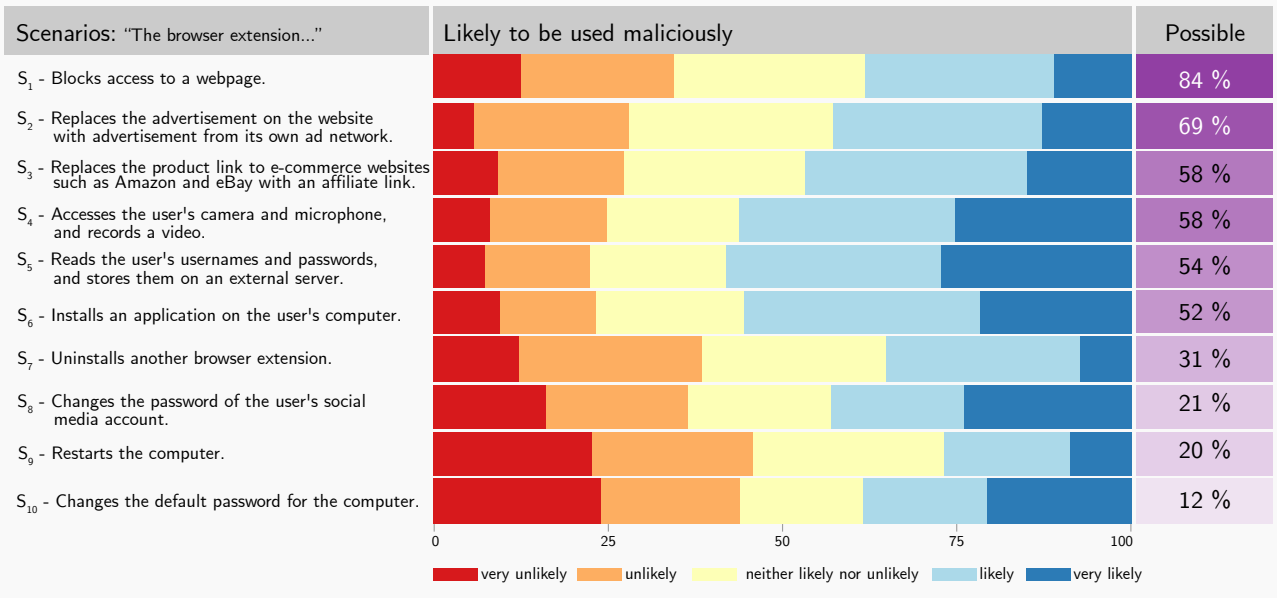

Figure 5: Participants' perception of the plausibility of scenarios and likelihood of them being used maliciously.

4.3.2 Users' Knowledge of Browser Extensions

For each of the ten scenarios (see figure 5), we asked participants to select "yes", "no", "don't know" to indicate whether they thought a scenario was technically possible to occur (which all of them were as explained in section 3.2). We found that most users thought S_1: "Blocks access to a web page" (84%) and S_2: "Replaces advertisements" (69%) was possible. Roughly half of all participants thought S_3: "Replaces product links" (58%), S_4: "Accesses the camera and microphone" (58%), S_5: "Reads the user's password" (54%), and S_6: "Installs an application on the user's computer" (52%) were possible to occur. Less than a third of the participants thought S_7, S_8, S_9, S_{10} were possible. Figure 6 shows the reported plausibility of selected scenarios across the conditions.

Furthermore, participants rated the likelihood of the scenarios being used maliciously. On a bipolar five-point Likert scale, the median response was "likely" for scenarios S_4, S_5, and S_6, and "neither likely nor unlikely" for the rest. The impact of the different permission dialogues on participants' perceptions is further illustrated in a graph in the appendix (figure 8).

4.3.3 Knowledge of Ad-Blockers

To the separate question on "Assuming that you have an ad-blocker installed as a browser extension, can it read passwords that you use on various websites?", 41 (9%) participants selected "yes", 142 (40%) selected "no" and rest of the participants (51%) did not know.

4.3.4 Effectiveness of The Browser Extension Dialogues

To test how effective the browser dialogues were in communicating the abilities of the browser extension, we scored participants' knowledge before and after they saw the dialogue. To calculate the score, one point was added for a correct assessment of a scenario to be possible, one point was subtracted for a wrong answer, and no point was added for answering "I don't know". For this comparison, we only took scenarios S_1, S_2, S_3, S_5, and S_8 into account which were explicitly permissible by the permissions (i.e. without the need of a tandem application). Thus, the maximum score was $+5$ and the minimum score was -5. Without seeing a dialogue, respondents had a median score of two ($mean = 1.69, SD = 2.48$). After seeing a dialogue the median score increased significantly ($p = 0.015$) to three ($mean = 2.05, SD = 2.68$) across all browser dialogues. Regarding individual browsers, participants who saw the Firefox dialogue had a median score of three ($mean = 2.16, SD = 2.54$), those who saw the Chrome dialogue had a median score of three ($mean = 2.6, SD = 2.41$), and the ones who saw the Safari dialogue had a median score of two ($mean = 1.29, SD = 2.96$). A Kruskal-Wallis test found a significant difference between the browsers ($p < .001$). Post-hoc Wilcoxon rank-sum tests found that there is a statistically significant difference between Firefox and without dialogue ($p = .045, r = .09$), Chrome and without dialogue ($p < .001, r = .17$), Firefox and Safari ($p = .038, r = .14$), and Chrome and Safari ($p < .001, r = .22$). Effect sizes were calculated according to Robertson and Kaptein [45]. To summarise, Chrome and Firefox significantly improved the score as compared to the baseline (i.e. without-dialogue) and Safari with a small effect.

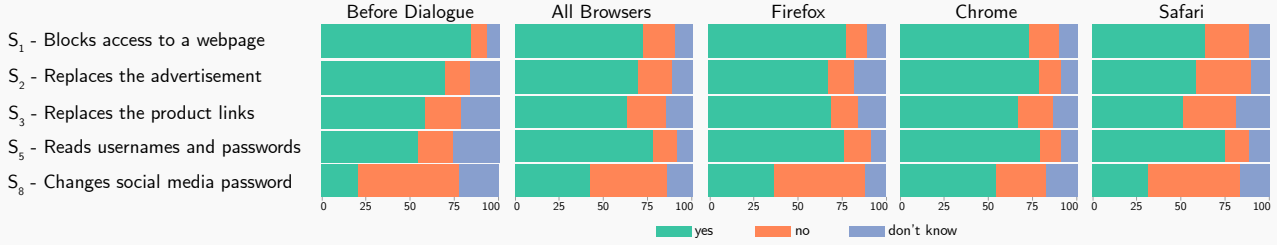

Figure 6: Participants' evaluation of the plausibility of selected scenarios. Each participant first evaluated the plausibility without seeing a permission dialogue, and then again after seeing a permission dialogue of either Firefox, Chrome, or Safari (randomly chosen). The permission dialogues for the three browsers are shown in figure 1.

4.3.5 Similarity and Preference of Existing Permission Dialogues

Participants rated all permission statements as similar to our comprehensive descriptions. Figure 7 shows that for different statements, the majority of participants rated them "Extremely similar", and less than 13% rated them to be "Not at all similar". However, participants did not prefer most of the original browser permission statements to be used instead of our description. For all statements except two, the majority of the participants rated them as "Not at all preferred", and less than 12% rated them to be "Extremely preferred". The only two statements for which participants reported slightly higher preference were "display notification" and "display notification to you" (see figure 7).

5 Findings

We draw the following main insights from the findings of our survey results.

5.1 Attitude

We found that the majority of users are interested in seeking out information about security and privacy in relation to browser extensions. They feel somewhat confident about what data is collected by their browser extensions and how the data is used. However, less than a third have ever read the terms and conditions or the privacy policy of their browser extensions or have taken any steps to ensure their private data is secure. Here our findings are in line with existing literature that the majority of the users do not read privacy policies [5, 23] and further highlight the low utility of terms and conditions and privacy policies in conveying to the user what information online services collect and how it is used [26, 29, 36].

5.1.1 Trust in Developers

With regards to the access and storage of users' data, the majority of the participants reported moderate to high trust in developers. They put slightly higher trust in developers of the browsers as compared to the trust in the developers of extensions. Here the results vary from our initial hypothesis that the trust in developers of browsers would be notably higher as compared to the trust in the extension developers since, in contrast to browser extensions, browsers are universally adapted applications and developed by selected organisations. Given the findings, we speculate that the trust in browsers is extended to the trust in the browser extensions since browser extensions are distributed through the browsers' webstore.

5.1.2 Users Seek More Information

Our results show that after having completed our survey, participants' interest in seeking more information about security and privacy in regards to browser extensions increased significantly. In the text field at the end of the survey P54 commented "I'm more aware of the risks now". P311 wrote: "It made me more aware of the vulnerabilities of all the extensions I use". For some participants, the survey even made them reiterate their past and future decisions (P85): "I will re-read all my extensions and read the terms every time I install a new one".

5.2 Knowledge

5.2.1 Users' General Knowledge about Technical Abilities of Browser Extensions is Limited

Participants gave higher possibility ratings to scenarios that are closely related to specific types of browser extensions. The two scenarios where participants were most sure of their plausibility are: S_1: "Blocks access to a web page" (84%) and S_2: "Replaces advertisements" (69%). Both scenarios are strongly connected to ad-blockers which the majority of participants use (85%). Scenario S_3: "Replaces the product link" is most likely associated with shopping assistants and scenario S_5: "Reads user names and passwords" with Password managers, which both a quarter of all participants use.

Regarding the likelihood, scenarios were rated more likely to be used maliciously when they included an invasion of privacy. S_4: "Accesses the camera and microphone", S_5: "Reads

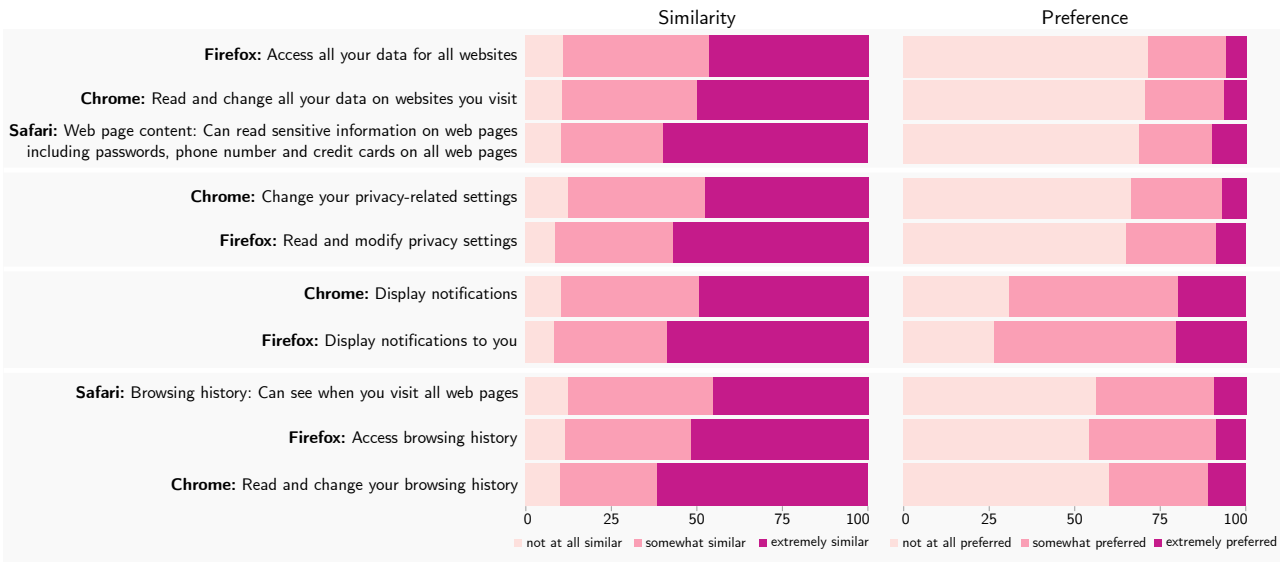

Figure 7: Participants' rating of similarity and preference of existing permission statements in comparison to our comprehensive descriptions. The majority of the participants rated existing permission statements to be similar but did not prefer them in place of our description.

the user's password", and S_6: "Installs an application on the user's computer", had the highest ratings in this regard.

Generally, we observe that users' understanding relies on individual experiences with specific extensions. While users seem to be aware that browser extensions such as password managers can read and store passwords, they do not consider that similar permissions are enabling ad-blockers to do the same.

5.2.2 Permission Dialogues Have Limited Effectiveness

We found significant differences between the browsers and observed that the framing of the permission statements matters just as much as having permission statements in the first place. The dialogues of Chrome and Firefox significantly improved participants' scores as compared to Safaris' dialogue and the baseline. Overall, the browser permission dialogues improved participants' scores significantly. While the median score improved from two to three across all browsers, 30% of all participants still scored 0 and lower. Even with the permission dialogues, participants were still not entirely informed about the technical implications of all the permissions.

5.2.3 Specific Statements Restrict Peoples' Ability to See Implications

Both Chrome and Firefox's permission dialogues improved user scores as compared to the baseline and Safari. Scenario S_5 "Reads usernames and passwords" was the only scenario where the Safari condition shows similar plausibility scores to Chrome and Firefox. This was also the only scenario explicitly mentioned in Safari's permission dialogue (see figure 1). The same permission, however, also enables the other four scenarios, which users, seeing the Safari permission dialogue, did not consider to be possible. Contrary to our initial hypothesis, that permission statements with examples would improve users' overall understanding, we find that Safari's dialogue statements are too specific and limit users' ability to see its implications for other scenarios.

5.2.4 Users do Not Prefer Existing Permission Statements

In the survey questions Q6.1-4, we had asked participants about the similarity in the information conveyed by four existing permission statements, as well as their preference for these browser permission statements compared to the comprehensive descriptions. When analysing the response of the participants we consider the four cases by dividing the score into low and high for similarity and preference. Firstly we consider the case when most participants give high similarity and high preference scores to the browser permission statement compared to its comprehensive description. We argue that this implies that the two statements have the same meaning and that the comprehensive description is a natural elaboration of the browser permission statement. In this case, the browser permission statement is better (and thus more preferred) since the users do not gain new information from the comprehensive description. We observe this case in response to question Q6.3 for the "send notifications" statement.

In the second case, most participants give a high similarity but low preference score to the browser permission statement.

This would imply that the comprehensive description can be compacted to the browser permission statement but with loss of information. In this case, the comprehensive description is better since the user gains new and relevant information from it (and thus the browser permission statement is less preferred). We observe this case in response to question Q6.1, Q6.2 and Q6.4 for "access all data for all websites", "change privacy related settings" and "access browsing history" related statements for the three browsers. Our results suggest that existing permission dialogues for these three permissions are too limited to be regarded as a suitable representative of their underlying meaning. The other two cases with a low similarity score would imply that the statements are disjoint. These cases are not observed in the responses.

5.3 Summary

Our findings show that users have a conflicting attitude towards privacy and security topics when it comes to browser extensions. Although users indicate interest in the topic, the majority of them have not read privacy policies, terms and conditions or taken steps to ensure the safety of their personal data. They trust developers to securely handle their data but often lack the knowledge to see the potential threats. Users' knowledge in regards to browser extensions is highly connected to individual experiences. While most users know extensions can read passwords, probably because of their experience with password managers, they don't consider that similar permissions enable ad-blockers to do the same. Permission dialogues help users, but unfortunately, their effectiveness is limited in building this understanding. We find that they alone are not sufficient to impart the knowledge needed for making informed decisions. Finally, we see preference as an important lever to make information accessible to users. The improved knowledge can change peoples' attitude towards topics such as security and privacy of browser extensions.

Overall we conclude that people's attitudes can be positively affected through knowledge as our evaluation about users' interest in the topic, before and after the survey, suggests (see figure 4). Participants were not only more interested but also more concerned about the topic. P288 even commented: "I am now scared of browser extensions", which highlights the scale of the problem and the large gap that is there to close in users' understanding of browser extensions.

6 Discussion

Browser extensions use extensive permissions, such as one single permission to access a whole website. This coarse model allows a range of extensions to access all kinds of user data. For example, under this model, both ad-blockers and dictionary extensions can technically access the same sensitive user information such as passwords, tokens, page URL, and payment information. To inform about these possibilities, browsers present the requested permissions during the installation process to assess the technical abilities of the extensions before (re-)confirming users' decision of installing an extension. These permissions aim to assist users to fill the knowledge gap between the technical abilities and functionalities of an extension.

In this paper, we explored the effectiveness of browser permissions in informing users about the plausibility of the technical abilities of the extensions. We find that the current model leaves a gap between the conveyed information and the user's understanding. In many cases, users have a misconception about the technical abilities of the extensions and the majority does not think that these abilities are likely to be used maliciously. More importantly, the permission statements have limited success in conveying the technical abilities of the extensions or changing users' perception of the likelihood. The problems are further exacerbated because the majority of the users do not read the privacy policy or the terms and conditions, and they have moderate to high trust in the browsers and browser extensions.

The results of our study are in line with trends in the related domain of mobile applications. We find that the majority of the users have a considerable understanding of the scenario related to popular features, such as the ability of an ad-blocker to replace advertisement or block access. However, they lack understanding about other scenarios feasible under the same permissions. Similarly, studies in the fields of mobile applications and wearables have shown that users have a limited understanding of the permissions and data collection [1, 2, 6, 19, 23]. In our study, only 34% of participants recall seeing the permission dialogue. This is similar to the results of Felt et al. on users' behaviour towards mobile app permission dialogues, where they found that the majority of the people just skip over or accept them without reading [19].

Even though in many ways, browser extensions are more powerful than and equally popular as mobile applications, limited research has looked into users' understanding of their abilities and users' attitude towards them, while numerous studies have been conducted for mobile applications [4, 18, 19, 33, 56]. With this study, we take a step towards filling this gap in the usable privacy and security literature for browser extensions.

Over the years, various measures for data security have been proposed, such as the *right of informational self-determination* introduced by German Federal Constitutional Court, which states the users should be able to decide what parts of their personal data can be accessed by whom, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) [42] and EU's General Data Protection Regulation (GDPR) [52]. In this paper, we present evidence that, with respect to browser extensions, users cannot make use of these rights, because they do not know that data is made accessible, let alone what kind of data is given away.

Users seem unaware of the trade-off between privacy and convenience and they are unable to make an informed choice in relation to browser extensions.

6.1 Recommendations

Based on our findings, we provide recommendations for further developing the extension model to empower the users and to safeguard them from malicious extensions.

1. Users' perspective: Improve understanding

The overall goal of the permission dialogues should be to increase informational self-determination by users. We find that existing permission statements are not a suitable representative of their underlying meaning in case of three out of the four permissions that we studied. Considering these aspects, we recommend that the browser should not assume that users are aware of the meaning of various permissions, and instead encourage the user in gaining information about the extent of the permissions. Here we suggest the use of "Human in the loop" framework [16] while designing the permission dialogues to ensure that the users comprehend the meaning of the statements. As Cranor [16] points out, similarity to related symbols, complexity and vocabulary all impact comprehension. Using familiar and unambiguous statements can aid these shortcomings and offer help in building understanding for terms that do not yet have a stable mental model. Similarly, for conveying which information is collected and how it is processed, an approach based upon the "nutrition label for privacy" may be better suited [31].

Building on existing experiences, we also recommend *parity with similar systems:* Recently, iOS 14 and Android 10 introduced a new fine-grained permission system that allows for time-limited permissions, permission reminders and confirmation on first-use, among others. Browsers already have runtime notifications for some permissions such as camera and microphone. While this may not be possible for all extension permissions as they are required for the basic functioning of the extension, the browser may still benefit from displaying permissions on runtime (i.e. when users first open a webpage) instead of only during the installation as it would allow the user to see the permission in the context of the webpage. Browsers can further call attention to the extent of the permission by highlighting the parts of the web page and browser settings accessible under it.

2. Browser's perspective: Limit access To improve the existing permission system, browsers should assume that deliberately or otherwise the extensions are prone to be malicious. Following the principle of least privilege [46], we recommend that browser extensions should be provided access only to the relevant part of the DOM. The sensitive information should be redacted from the extensions that do not need it (*Redacted DOM*). Most browsers already identify sensitive fields (such as password or credit-card fields) and, thus, they can be encapsulated with separate permissions.

Furthermore, as proposed in Chrome Manifest V3[5] and Apple WWDC 2020[6] browsers should provide the possibility to limit the scope of the extensions to certain categories of websites (*Restricted website access*). This feature could be especially helpful in preventing malicious extensions from gaining access to sensitive information on corporate websites or financial web services.

3. Policy perspective: Convey responsibility We recommend that browsers should make users aware of their responsibilities as well as the responsibilities browsers take on themselves. Browsers should convey to the users that they are responsible to only allow access to the extension APIs specified in the permission statements, and the users' responsibility lies in making an informed choice after knowing the upper bounds from the permission statements and understanding the actual behaviour through terms and conditions. If the browser takes additional responsibility they should explicitly specify it. A similar technique is adopted by the Firefox Recommended Extensions program to promote the safest and highest quality extensions [21]. We hypothesise that making users aware of their responsibility can improve their attitude towards online security in the long term. Further studies are required to establish the effectiveness of our recommendation on clearer language, parity with similar systems, redacted DOM, restricted website access, and responsibility conveying.

7 Conclusion

To conclude, our survey results have provided insight into the attitude, understanding and preferences towards security and privacy practices of browser extension users. Users expressed confidence in their knowledge of what data is collected and trust developers to securely handle their data but they have limited understanding to assess the potential risks. Users' knowledge in regards to browser extensions seems to be connected to individual experiences. For example, while most users know extensions can read passwords, probably due to their experience with password managers, they don't consider that similar permissions enable ad-blockers to do the same. Overall, our findings lead us to believe that browser extension users require a greater awareness of the risks associated with browser extensions and future work should look into making extension permissions understandable and fine-grained.

Acknowledgments

We would like to thank the anonymous reviewers for their constructive feedback that greatly improved the paper, Jasmin Niess for her help in designing the study, and Nadine Wagener for the help with the figures. This research was supported by

[5] https://developer.chrome.com/docs/extensions/mv3/intro/
[6] https://developer.apple.com/wwdc20/

the Volkswagen Foundation through a Lichtenberg Professorship and by the Federal Ministry of Education and Research of Germany (BMBF) through the Wintermute project (award number 16KIS1127).

References

[1] Angeliki Aktypi, Jason R.C. Nurse, and Michael Goldsmith. Unwinding ariadne's identity thread: Privacy risks with fitness trackers and online social networks. In *Proceedings of the 2017 on Multimedia Privacy and Security*, MPS '17, page 1–11, New York, NY, USA, 2017. Association for Computing Machinery.

[2] Hazim Almuhimedi, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. Your location has been shared 5,398 times! a field study on mobile app privacy nudging. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15, page 787–796, New York, NY, USA, 2015. Association for Computing Machinery.

[3] Opera Software AS. Publishing Guidelines. Retrieved June 11, 2020 from https://dev.opera.com/extensions/publishing-guidelines/.

[4] Kathy Wain Yee Au, Yi Fan Zhou, Zhen Huang, and David Lie. Pscout: analyzing the android permission specification. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 217–228, 2012.

[5] Brooke Auxier, Monica Anderson Lee Raine, Andrew Perrin, Madhu Kumar, and Erica Turner. Americans' attitudes and experiences with privacy policies and laws, 2019. Retrieved May 20, 2021, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.

[6] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. " little brothers watching you" raising awareness of data leaks on smartphones. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–11, 2013.

[7] Vinayshekhar Bannihatti Kumar, Roger Iyengar, Namita Nisal, Yuanyuan Feng, Hana Habib, Peter Story, Sushain Cherivirala, Margaret Hagan, Lorrie Cranor, Shomir Wilson, Florian Schaub, and Norman Sadeh. Finding a Choice in a Haystack: Automatic Extraction of Opt-Out Statements from Privacy Policy Text. In *Proceedings of The Web Conference 2020*, WWW '20, pages 1943–1954, New York, NY, USA, 2020. Association for Computing Machinery.

[8] Adam Barth, Adrienne Porter Felt, Prateek Saxena, and Aaron Boodman. Protecting browsers from extension vulnerabilities. In *Network and Distributed System Security Symposium*, 2010.

[9] Matthias Böhmer, Brent Hecht, Johannes Schöning, Antonio Krüger, and Gernot Bauer. Falling asleep with angry birds, facebook and kindle: a large scale study on mobile application usage. In *Proceedings of the 13th international conference on Human computer interaction with mobile devices and services*, pages 47–56, 2011.

[10] Kevin Borgolte and Nick Feamster. Understanding the Performance Costs and Benefits of Privacy-focused Browser Extensions. In *The Web Conference 2020 - Proceedings of the World Wide Web Conference, WWW 2020*, WWW '20, pages 2275–2286, New York, NY, USA, 2020. Association for Computing Machinery.

[11] Bjarte Botnevik, Eirik Sakariassen, and Vinay Setty. BRENDA: Browser Extension for Fake News Detection. In *Proceedings of the 43rd International ACM SIGIR Conference on Research and Development in Information Retrieval*, SIGIR '20, pages 2117–2120, New York, NY, USA, 2020. Association for Computing Machinery.

[12] Nicholas Carlini, Adrienne Porter Felt, and David Wagner. An evaluation of the google chrome extension security architecture. In *Presented as part of the 21st {USENIX} Security Symposium ({USENIX} Security 12)*, pages 97–111, 2012.

[13] Alexandros Chen, Quan and Kapravelos. Mystique: Uncovering Information Leakage from Browser Extensions. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 1687–1700, New York, NY, USA, 2018. Association for Computing Machinery.

[14] Google Chrome. Declare Permissions. Retrieved June 20, 2020 from https://developer.chrome.com/extensions/declare_permissions.

[15] Google Chrome. Publish in the Chrome Web Store. Retrieved June 11, 2020 from https://developer.chrome.com/webstore/publish.

[16] Lorrie Faith Cranor. A framework for reasoning about the human in the loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security*, UPSEC'08, USA, 2008. USENIX Association.

[17] Microsoft Edge. Publish Your Extension. Retrieved June 11, 2020 from https://docs.microsoft.com/en-us/microsoft-edge/extensions-chromium/publish/publish-extension.

[18] Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, and David Wagner. Android permissions demystified. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 627–638, 2011.

[19] Adrienne Porter Felt, Elizabeth Ha, Serge Egelman, Ariel Haney, Erika Chin, and David Wagner. Android permissions: User attention, comprehension, and behavior. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, New York, NY, USA, 2012. Association for Computing Machinery.

[20] Mozilla Firefox. Permission Request Messages for Firefox Extensions. Retrieved September 11, 2020, https://support.mozilla.org/en-US/kb/permission-request-messages-firefox-extensions.

[21] Mozilla Firefox. Recommended Extensions program. Retrieved June 11, 2020 from https://blog.mozilla.org/firefox/firefox-recommended-extensions/.

[22] Mozilla Firefox. Submitting an Add-on. Retrieved June 11, 2020 from https://extensionworkshop.com/documentation/publish/submitting-an-add-on/.

[23] Sandra Gabriele and Sonia Chiasson. Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, page 1–12, New York, NY, USA, 2020. Association for Computing Machinery.

[24] Cristiano Giuffrida, Stefano Ortolani, and Bruno Crispo. Memoirs of a Browser: A Cross-Browser Detection Model for Privacy-Breaching Extensions. In *ASIACCS 2012 - 7th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '12, pages 10–11, New York, NY, USA, 2012. Association for Computing Machinery.

[25] Gary Golomb. The Internet's New Arms Dealers: Malicious Domain Registrars. Retrieved June 11, 2020 from https://awakesecurity.com/blog/the-internets-new-arms-dealers-malicious-domain-registrars/.

[26] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, pages 133–144, 2009.

[27] Chris Jay Hoofnagle, Jennifer King, Su Li, and Joseph Turow. How different are young adults from older adults when it comes to information privacy attitudes and policies? *Available at SSRN 1589864*, 2010.

[28] Sam Jadali. DataSpii: The Catastrophic Data Leak via Browser Extensions. Retrieved July 7, 2020 from https://securitywithsam.com/2019/07/dataspii-leak-via-browser-extensions/.

[29] Carlos Jensen and Colin Potts. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 471–478, 2004.

[30] Ankit Kariryaa and Johannes Schöning. Moiprivacy: Design and evaluation of a personal password meter. In *19th International Conference on Mobile and Ubiquitous Multimedia*, MUM 2020, page 201–211, New York, NY, USA, 2020. Association for Computing Machinery.

[31] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W Reeder. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[32] Swati Khandelwal. 8 More Chrome Extensions Hijacked to Target 4.8 Million Users. Retrieved May 25, 2021 from https://thehackernews.com/2017/08/chrome-extension-hacking.html.

[33] Jialiu Lin, Shahriyar Amini, Jason I Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM conference on ubiquitous computing*, pages 501–510, 2012.

[34] Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhimedi, Shikun (Aerin) Zhang, Norman Sadeh, Yuvraj Agarwal, and Alessandro Acquisti. Follow my recommendations: A personalized privacy assistant for mobile app permissions. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 27–41, Denver, CO, June 2016. USENIX Association.

[35] Christina Low, Emma McCamey, Cole Gleason, Patrick Carrington, Jeffrey P. Bigham, and Amy Pavel. Twitter A11y: A Browser Extension to Make Twitter Images Accessible. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pages 1–12, New York, NY, USA, 2020. Association for Computing Machinery.

[36] Aleecia M McDonald and Lorrie Faith Cranor. The cost of reading privacy policies. *Isjlp*, 4:543, 2008.

[37] Andrey Meshkov. "Big Star Labs" Spyware Campaign Affects Over 11,000,000 People. Retrieved May 25, 2021 from https://adguard.com/en/blog/big-star-labs-spyware.html.

[38] Liz Mineo. On internet privacy, be very afraid. *Harvard Gazette*, 2017.

[39] Extension Monitor. Breaking Down the Chrome Web Store. Retrieved September 3, 2020 from https://extensionmonitor.com/blog/breaking-down-the-chrome-web-store-part-1.

[40] Vivian Genaro Motti and Kelly Caine. Users' privacy concerns about wearables. In Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff, editors, *Financial Cryptography and Data Security*, pages 231–244, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[41] Stefan Palan and Christian Schitter. Prolific. ac—a subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, 17:22–27, 2018.

[42] Stephanie E Perrin. *The personal information protection and electronic documents act: An annotated guide*. Irwin Law, 2001.

[43] Qualtrics. Qualtrics, 2020. Retrieved September 4, 2020 from https://www.qualtrics.com.

[44] Marshall David Rice and Ekaterina Bogdanov. Privacy in doubt: An empirical investigation of canadians' knowledge of corporate data collection and usage practices. *Canadian Journal of Administrative Sciences / Revue Canadienne des Sciences de l'Administration*, 36(2):163–176, 2019.

[45] Judy Robertson and Maurits Kaptein. *Modern Statistical Methods for HCI*. Springer Publishing Company, Incorporated, Switzerland, 1st edition, 2016.

[46] Jerome H Saltzer and Michael D Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, 1975.

[47] Stefan Schneegass, Romina Poguntke, and Tonja Machulla. Understanding the impact of information representation on willingness to share information. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–6, New York, NY, USA, 2019. Association for Computing Machinery.

[48] Irina Shklovski, Scott D. Mainwaring, Halla Hrund Skúladóttir, and Höskuldur Borgthorsson. Leakiness and creepiness in app space: Perceptions of privacy and mobile app use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '14, page 2347–2356, New York, NY, USA, 2014. Association for Computing Machinery.

[49] Oleksii Starov and Nick Nikiforakis. Extended Tracking Powers: Measuring the Privacy Diffusion Enabled by Browser Extensions. In *Proceedings of the 26th International Conference on World Wide Web*, WWW '17, pages 1481–1490, Republic and Canton of Geneva, CHE, 2017. International World Wide Web Conferences Steering Committee.

[50] StatCounter. Global market share held by leading desktop internet browsers from january 2015 to june 2020 [graph]. *Statista*, 2020.

[51] Gaurav Varshney, Manoj Misra, and Pradeep K. Atrey. Detecting Spying and Fraud Browser Extensions: Short Paper. In *Proceedings of the 2017 on Multimedia Privacy and Security*, MPS '17, pages 45–52, New York, NY, USA, 2017. Association for Computing Machinery.

[52] Paul Voigt and Axel Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[53] Jofish Williams, Alex C. and Cambre, Julia and Bicking, Ian and Wallin, Abraham and Tsai, Janice and Kaye. Toward Voice-Assisted Browsers : A Preliminary Study with Firefox Voice. In *Proceedings of the 2nd Conference on Conversational User Interfaces*, CUI '20, New York, NY, USA, 2020. Association for Computing Machinery.

[54] Yuxi Wu, Panya Gupta, Miranda Wei, Yasemin Acar, Sascha Fahl, and Blase Ur. Your Secrets Are Safe: How Browsers' Explanations Impact Misconceptions About Private Browsing Mode. In *Proceedings of the 2018 World Wide Web Conference*, WWW '18, pages 217–226, Republic and Canton of Geneva, CHE, 2018. International World Wide Web Conferences Steering Committee.

[55] Xinyu Xing, Wei Meng, Byoungyoung Lee, Udi Weinsberg, Anmol Sheth, Roberto Perdisci, and Wenke Lee. Understanding Malvertising Through Ad-Injecting Browser Extensions. In *Proceedings of the 24th International Conference on World Wide Web*, WWW '15, pages 1286–1295, Republic and Canton of Geneva, CHE, 2015. International World Wide Web Conferences Steering Committee.

[56] Liu Yang, Nader Boushehrinejadmoradi, Pallab Roy, Vinod Ganapathy, and Liviu Iftode. Short paper: enhancing users' comprehension of android permissions. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices*, pages 21–26, 2012.

A Survey

Demographics

Q1.1 Please enter your Prolific ID here

Q1.2 What is your age?

Q1.3 What is your gender?

Options: Male; Female; Diverse; Other; Prefer not to say

Q1.4 What is your highest level of education?

Options: No formal education; High school diploma or equivalent; Bachelor's degree or equivalent; Master's degree or equivalent; Doctoral degree or equivalent

Q1.5 Are you majoring in or have a degree or job in computer science, computer engineering, information technology, or a related field?

Options: Yes; No

Behaviour and knowledge

Q3.1 Which is your default desktop browser?

Options: Chrome; Firefox; Safari; Edge; Opera; Other (Please specify)

Q3.2 Please select all the desktop browsers that you use to some extent.

Options: Chrome; Firefox; Safari; Edge; Opera; Other (Please specify)

Q3.3 Do you use browser extensions?

Options: Yes; No

Q3.4 (Shown if Q3.3 = Yes) Which type of browser extension do you use? (Select all that apply)

Options:

Advertisement, cookies, or tracker blocker (e.g. Ad-block plus, uBlock origin);

Password manager (e.g. Lastpass, 1Password); Shopping assistant (e.g. Honey, Piggy);

Language tool (e.g. Oxford dictionary, Grammarly);

Productivity (e.g. Todoist, Evernote);

Video or music downloader (e.g. Youtube Downloader, Video DownloadHelper);

I don't use any browser extension;

Other (Please specify)

Q3.5 (Shown if Q3.3 = Yes) Please indicate on the scale; how confident you are that:

Columns: 1 - Not at all confident; 2; 3; 4; 5 - Very confident

Rows:

R1 You know what type of data is collected by your browser extensions;

R2 You know how your data is used by your browser extensions;

R3 Please choose the fourth option;

R4 The developers of your default browser have made sure your data is safe from being tampered with or shared without your consent;

R5 The developers of your browser extensions have made sure your data is safe from being tampered with or shared without your consent

Q3.6 (Shown if Q3.3 = Yes) Please respond to the following questions, in relation to your browser extension:

Columns: Yes; No; I don't remember

Rows:

R1 Have you ever read the privacy policy for any of your browser extensions?;

R2 Have you ever read the terms and conditions for any of your browser extensions?;

R3 Have you taken steps to ensure your data is secure and private for your browser extensions?

Q3.7 (Shown if Q3.3 = No) Please indicate on the scale; how confident you are that:

Columns: 1 - Not at all confident; 2; 3; 4; 5 - Very confident

Rows:

R1 You know what type of data is collected by browser extensions;

R2 You know how user data is used by browser extensions;

R3 Please choose the fourth option;

R4 The developers of browsers have made sure user data is safe from being tampered with or shared without user's consent;

R5 The developers of browser extensions have made sure user data is safe from being tampered with or shared without user's consent.

Q3.8 (Shown if Q3.3 = No) Please respond to the following questions, in relation to browser extensions:

Columns: Yes; No; I don't remember

Rows:

R1 Have you ever read the privacy policy of any browser extension?;

R2 Have you ever read the terms and conditions of any browser extension?;

R3 Have you taken steps to ensure your data is secure and private for any browser extension?

Q3.9 Please indicate on the scale:

Columns: 1- Not at all interested; 2; 3; 4; 5 - Extremely interested

Rows:

R1 Your degree of interest in seeking out information about security and privacy in relation to browser extensions.

Q3.10 Please indicate on the scale; how comfortable you are with:

Columns: 1 - Not at all comfortable; 2; 3; 4; 5 - Extremely comfortable

Rows:

R1 Having everything you do in the browser collected and stored by a browser extension.

Q3.11 (Shown if Q3.3 = No) Why don't you use browser extensions?

Options (randomised):

I don't need them;

I didn't know they exist;

Due to concerns about data privacy;

It's too difficult to install them;

Other:

Q3.12 Assuming that you have an Ad-blocker installed as a browser extension; can it read passwords that you use on various websites?

Options: Yes; No; I don't know

General Scenarios

Q4.1 Please indicate if you think it is technically possible for a browser extension to cause the following scenarios. Also indicate how likely you think the scenario will be used in a malicious way. An installed browser extension:

Columns: G1 Possible (SG1 Yes; SG2 No; SG3 I don't know); G2 Likely to be used in a malicious way (SG4 Very unlikely; SG5 Unlikely; SG6 Neither likely nor unlikely; SG7 Likely; SG8 Very likely)

Rows (randomised):

R1 Reads the user's usernames and passwords and stores them on an external server;

R2 Replaces the product link to e-commerce websites such as Amazon and eBay with an affiliate link;

R3 Replaces the advertisement on the website with advertisement from its own ad network;

R4 Accesses the user's camera and microphone and records a video;

R5 Uninstalls another browser extension;

R6 Installs an application on the user's computer;

R7 Blocks access to a webpage;

R8 Changes the password of the user's social media account;

R9 Restarts the computer;

R10 Changes the default password for the computer.

Specific Scenarios

(Each participants is shown one question out of Q5.1-3 at random)

Q5.1 (Chrome permission dialogue) Given the dialogue below; please indicate if you think it is technically possible for a browser extension, asking for these permissions, to cause the following scenarios. Also indicate how likely you think the scenario will be used in a malicious way. The browser extension:

Columns: G1 Possible (SG1 Yes; SG2 No; SG3 I don't know); G2 Likely to be used in a malicious way (SG4 Very unlikely; SG5 Unlikely; SG6 Neither likely nor unlikely; SG7 Likely; SG8 Very likely)

Rows - Same as in Q4.1 with the randomised order maintained

Q5.2 (Safari permission dialogue) - Same as Q5.1 in other aspects and the randomised order maintained from Q4.1 in rows

Q5.3 (Firefox permission dialogue) - Same as Q5.1 in other aspects and the randomised order maintained from Q4.1 in rows

Analysis of permission statements

Q6.1 Statement A: "The browser extension can access; meaning read and change; all information including sensitive information such as passwords, phone numbers, credit card numbers, text and images on all websites such as those for online banking, email service, online shopping, and social media." Compared to Statement A; please indicate ...

... how similar is the information conveyed by the following permissions.

... your preference for the following permissions in place of Statement A.

Columns: G1 Similarity (SG1 Not at all similar; SG2 Somewhat similar; SG3 Extremely similar); G2 Preference (SG4 Not at all preferred; SG5 Somewhat preferred; SG6 Extremely preferred)

Rows (randomised):

R1 Access all your data for all websites;

R2 Read and change all your data on websites you visit;

R3 Web page content: Can read sensitive information on web pages including passwords, phone number and credit cards on all web pages.

Q6.2 Statement B: "The browser extension can read and modify the privacy settings of your browser. These settings control the information the browser makes available to websites, manage the browser's inbuilt password manager, and control the network connections." Compared to Statement B; please indicate ...

... how similar is the information conveyed by the following permissions.

... your preference for the following permissions in place of Statement B.

Columns: G1 Similarity (SG1 Not at all similar; SG2 Somewhat similar; SG3 Extremely similar); G2 Preference (SG4 Not at all preferred; SG5 Somewhat preferred; SG6 Extremely preferred)

Rows (randomised):

R1 Change your privacy-related settings;

R2 Read and modify privacy settings.

Q6.3 Statement C: "The browser extension can display notifications to you. Notifications can be used to inform you about background processes such as a summary of network requests blocked by an Ad-blocker or combine messages from one or more web services." Compared to Statement C; please indicate ...

... how similar is the information conveyed by the following permissions.

... your preference for the following permissions in place of Statement C.

Columns: G1 Similarity (SG1 Not at all similar; SG2 Somewhat similar; SG3 Extremely similar); G2 Preference (SG4 Not at all preferred; SG5 Somewhat preferred; SG6 Extremely preferred)

Rows (randomised):

R1 Display notifications;

R2 Display notifications to you.

Q6.4 Statement D: "The browser extension can access; meaning read and change; your browsing history. Your browsing history contains information including timestamps and number of visits about the websites that you have opened in the past." Compared to Statement D; please indicate ...

... how similar is the information conveyed by the following permissions.

... your preference for the following permissions in place of Statement D.

Columns: G1 Similarity (SG1 Not at all similar; SG2 Somewhat similar; SG3 Extremely similar); G2 Preference (SG4 Not at all preferred; SG5 Somewhat preferred; SG6 Extremely preferred)

Rows (randomised):

R1 Browsing history: Can see when you visit all web pages;

R2 Access browsing history

R3 Read and change your browsing history.

Privacy policy and terms of use

Q7.1 Please indicate on the scale; the likelihood that you will now:

Columns: 1 - Not at all likely; 2; 3; 4; 5 - Extremely likely

Rows (randomised):

R1 Read the privacy policy for your browser extensions;

R2 Read the terms and conditions for your browser extensions;

R3 Take steps to ensure your data is secure and private for your browser extensions

Q7.2 Please indicate on the scale; the likelihood that you will now:

Columns: 1 - Not at all likely; 2; 3; 4; 5 - Extremely likely

Rows (randomised):

R1 Read the privacy policy if you will install a browser extension;

R2 Read the terms and conditions if you will install a browser extension;

R3 Take steps to ensure your data is secure and private if you will install a browser extension.

Q7.3 Please indicate on the scale:

Columns: 1 - Not at all interested; 2; 3; 4; 5 - Extremely interested

Rows:

R1 Your degree of interest in seeking out more information about security and privacy in relation to browser extensions.

Q7.4 Have you ever seen this or a similar permission dialogue?

Options: Yes; No; I don't remember

Q7.5 (Shown if Q7.4 = Yes) Did the permission dialogue influence your decision about installing the browser extension?

Options: Yes; No

Q7.6 (Shown if Q7.4 = Yes) Please explain your answer to the last question.

B Additional Graphs and Tables

as of September 2020 | Selected five extensions for our study

Extension	In Firefox top 10?	In Chrome top 10?	In Edge top 10?	In Opera top 10?	In Safari top 10?	Appears on x top lists across browsers	Number of users/ downloads	Ratings/ Reviews	Number of requested permissions
Chrome									
Adblock - best ad blocker	X	X		x	x	4	+10.0M	295K	2
Adblock Plus	X	X		x		3	+10.0M	171K	2
Honey		X	x			2	+10.0M	158K	1
Adblock for Youtube		X				1	+10.0M	113K	
Google Translate		X				1	+10.0M	43K	
Grammarly for Chrome	X	X			x	3	+10.0M	38K	2
Avast Online Security		X				1	+10.0M	24K	
uBlock Origin	X	X	x	x		4	+10.0M	22K	2
Adobe Acrobat		X				1	+10.0M	11K	
Avast SafePrice		X				1	+10.0M	11K	
Safari									
Magic Lasso Adblock for Safari					x	1		928	
Adblock for Safari	x	x		x	x	4		902	2
Rakuten Ebates Cash Back					x	1		718	
Grammarly for Safari	x	x			x	3		613	2
Unicorn Blocker:Adblock					x	1		346	
Notebook - Take Notes, Sync					x	1		245	
StopTheMadness					x	1		194	
Mate: Universal Tab Translator					x	1		159	
Ka-Block!					x	1		152	
Ecosia					x	1		146	
Firefox									
Adblock Plus	X	x		x		3	6.8M		6
uBlock Origin	X	x	x	x		4	3.8M		6
Easy Screenshot	X					1	3.0M		
Video DownloadHelper	X					1	2.3M		
Cisco Webex Extension	X					1	2.2M		
Facebook Container	X					1	1.5M		
Grammarly for Firefox	X	x			x	3	1.1M		3
DuckDuckGo Privacy Essentials	X					1	1.0M		
Ghostery - Privacy Ad Blocker	X			x		2	1.0M		
Adblock for Firefox	X	x		x	x	4	1.0M		6
Excluded browsers in our study									
Edge									
WindmillVPN - Fast,Safe,Best VPN & Proxy			X			1		708	
G-Translate			X			1		650	
Norton Safe Web			X			1		619	
Honey		x	X			2		530	
uBlock Origin	X	x	X	x		4		522	
AdGuard AdBlocker			X	x		2		514	
Tampermonkey			X			1		428	
Video Downloader professional			X			1		387	
YouTube Video Downloader and MP3 converter			X			1		309	
Hola Free VPN proxy Unblocker - Best VPN			X			1		307	
Opera									
SaveFrom.net helper				x		1	87.2M	3467	
Adblock Plus	x	x		x		3	40,7M	2625	
Adblock	x	x		x	x	4	14.2M	1212	
Install Chrome Extensions				x		1	13.6M	2611	
360 Internet Protection				x		1	8.8M	687	
Adguard			x	x		2	7.9M	2303	
uBlock Origin	x	x	x	x		4	7.1M	1580	
Translator				x		1	5.8M	2063	
Ghostery	x			x		2	5.6M	946	
Amazon for Opera				x		1	5.5M	307	

Table 2: Table of the top 50 most used browser extensions across Chrome, Safari, Firefox, Edge and Opera as of September 2020. In addition, the number of requested permissions are listed for the five browser extensions we selected for our survey study.

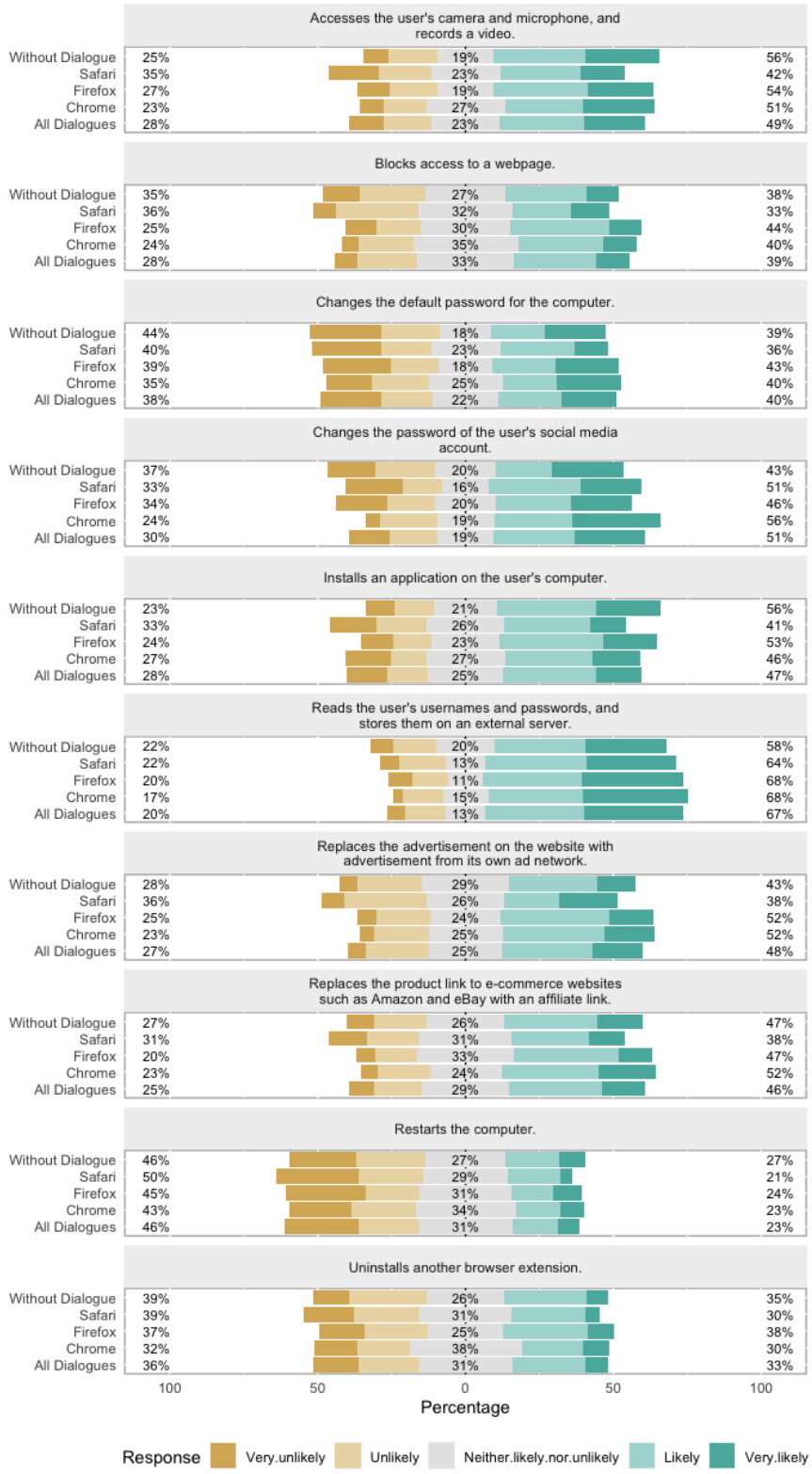

Figure 8: Impact of permission dialogues on participants' perception of the likelihood of scenarios being used maliciously.