



Human-Browser Interaction: Investigating Whether the Current Browser Application's Design Actually Make Sense for Its Users?

Fiona Carroll

To cite this article: Fiona Carroll (2024) Human-Browser Interaction: Investigating Whether the Current Browser Application's Design Actually Make Sense for Its Users?, International Journal of Human-Computer Interaction, 40:22, 7562-7573, DOI: [10.1080/10447318.2023.2266789](https://doi.org/10.1080/10447318.2023.2266789)

To link to this article: <https://doi.org/10.1080/10447318.2023.2266789>



© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 11 Oct 2023.



[Submit your article to this journal](#)



Article views: 2872



[View related articles](#)



[View Crossmark data](#)



Citing articles: 3 [View citing articles](#)

Human-Browser Interaction: Investigating Whether the Current Browser Application's Design Actually Make Sense for Its Users?

Fiona Carroll 

School of Technologies, Cardiff Metropolitan University, Cardiff, UK

ABSTRACT

As a society, we can get so engrossed in using the World Wide Web (WWW) also known as the web. We look for, read about and interact with different people, text, images, videos etc. that we often take for granted how we are doing this. We all use a web browser, we must, to get around the web. Yet, do we ever stop to give much thought to this gateway to the web? The web browser can be fittingly described as a transparent technology. This is in the sense that we don't really stop to think about the browser and its features, we just unconsciously absorb and use it. This paper reports on a study that explores just how effectively we understand and use our web browser applications. The study was focused on people's perceived awareness of desktop web browser functionality, what features they are using/aware of and most importantly what understanding they take from these? The findings show that the majority (69%) of the five hundred and twenty-eight participants studied do not fully understand what the padlock feature on their web browsers represents. In fact, the findings highlight that many of the participants feel that the padlock represents a safe website which it clearly does not. This paper succinctly draws attention to the fact that the current desktop web browser application design is not fit for purpose. In summary, the research pushes for more effective web browser application designs; it provides design recommendations aimed at achieving web browser consistency and creating designs that promote safety, trust, and confidence.

KEYWORDS

Web browser application;
online harm; safety
awareness; user interface
design; usability; human
computer interaction;
consistency



1. Introduction

The internet, especially the World Wide Web (WWW), also known as the web, has become an absolute necessity in our daily lives, especially since Covid-19. It now supports many essential day-to-day activities to the extent that we have become heavily dependent on it. However, as users we tend to get so absorbed in the content on the web to help us with work and school, finding information, and connecting with others, that we often take for granted how we are doing this. We all use a web browser, we must, to get around the web. It has become the mainstream means of retrieving information and displaying it on our desktop and/or mobile devices. Yet, do we ever stop to give much thought to this gateway to the web? The web browser has been described as a transparent technology. This is in the sense that we don't really think about the browser, we just use it. This paper explores just how much notice we take of the desktop web browser applications that we use. In particular it will focus on the features of the desktop web browser to understand what we use but also what we perceive and understand from these? This paper aligns with Human Computer Interaction (HCI) thinking and is

interested in the design of the web browser as the interface between users and the web. In detail, the paper reports on a study that explores people's perceived awareness of the current web browser designs to more fully understand if they make sense for them. Moreover, the paper questions if we should be pushing for more consistency across the web browser applications? The following sections will discuss the role of the web browser application, it covers recent online dangers and whether the current desktop web browser application designs are fit for purpose?

2. The web browser

A web browser is a software program which allows the user to request and retrieve web pages, images, videos, and other multi-media web content from a web server on the web. Today, it is the primary means for accessing information provided on the internet (Asim et al., 2019). As you would expect from a computing sector, there are several browsers (and versions of browsers) available on the market such as Chrome, Edge, Firefox, Safari and Opera etc. From these Chrome is one of the most popular among the internet user community (Rathod, 2017). In detail, the browser market

CONTACT Fiona Carroll  fc Carroll@cardiffmet.ac.uk  School of Technologies, Cardiff Metropolitan University, Llandaff Campus, Western Avenue, Cardiff, CF5 2YB, UK

© 2023 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

share worldwide from December 2021 to December 2022 shows Chrome at 64.68%, Safari at 18.29%, Edge at 4.23%, Samsung Internet at 3.05%, Firefox at 3.01% and finally Opera at 2.25% (Statcounter, 2023a). Google's Chrome, the current leading internet browser, is clearly the browser that the majority of people across the globe are using.

In terms of human computer interaction, the web browser is one of the most used applications on every computational device (Hughes et al., 2021). As Wang et al. (2014, p.575) note a "web browser has become one of the most important applications on a variety of computing devices, including PCs, tablets and mobile phones." Interestingly, it is also an application that we often take for granted, have uncertainties about and/or confuse with other applications such as the search engine. To be clear here, a browser displays websites whilst a search engine is a website itself that allows you to find other web pages by typing a keyword. In fact, both the browser and the search engine need to work together if we want to search for web pages on the web.

In terms of uncertainty, it doesn't help that the Google search engine (January 2015 to December 2022) was also the global market lead at 84.04% (Statcounter, 2023b). As a result of this market dominance, the company Google is widely known and its two applications, Google Chrome and Google (search engine), tend to be referred to interchangeably. To add to this, most browsers nowadays also have a built-in search feature. Setting this aside, people generally tend to use the web browser to perform various activities on the internet such as browsing internet, email, internet banking, social media applications, download files-videos etc. (Rathod, 2017). It is an application to surf the internet, which serves to display and interact with the server (Mustika et al., 2018). Laperdrix et al. (2020, p.8.1) nicely sum it up as "The web is a beautiful platform and browsers give us our entry point into it."

3. Responsibility of a web browser

This "point of entry" comes with a lot of responsibility. In fact, the majority of us now depend on the web browser to access information, web pages, web services etc. And as websites and web applications become more complex, the performance of browsers has become critical for users to have a satisfactory browsing experience (Wang et al., 2014). Jakob Nielsen, often described as the "guru of usability," highlighted that performance and satisfaction scores of web experiences are strongly correlated (Nielsen, 2012). Since the early 1990s, he has spoken extensively on ten heuristics for user interface design including the importance of user control and freedom, consistency and standards and recognition rather than recall, to name a few (Nielsen, 1995). This work along with that of other key human computer interaction (HCI) pioneers such as John Carroll, Ben Shneiderman, Don Norman, Alan Dix, Jenny Preece, David Benyon to name a few, proved to be revolutionary in the design of functioning and satisfying web experiences. This was in parallel with the ISO Usability Standards (ISO 9241-11, ISO/

IEC 9126-1 etc.) which set out the key international standards in the area of usability and user-centred design.

However, it is interesting to reflect back on how usability – creating software that people will want to use, will be able to use and will find effective/satisfying when used – took a central role in HCI. In fact, there was a drive in the early days to create interface designs with which users would not need to think too much about how they work (e.g., make it so easy to use that they don't have to think). Since then, HCI has expanded to be being a multi-discipline community encompassing an evolving concept of usability. In detail, it now considers areas such as, aesthetics, accessibility, empathy, security, responsibility, transparency, and trust, to name a few. In many ways, the challenge is now very much centred on how we make people be critically aware and to think before they interact.

Yet despite all this, it seems bizarre that the design of the browser today - this gateway to the world wide web - still remains inconsistent in its design particularly across the different providers. In many ways this might stem from the browser wars of the mid 1990s when the likes of *Netscape* and *Microsoft* tried to outdo each other with faster, better and more unique products. However, these different browser designs seem to go contrary to the usability guidelines and the web design's natural disposition. Especially, when it is now widely known that inconsistency in HCI can breed confusion and from that frustration and lack of use (Wong, 2021). As recent research shows, with options and advantages possessed by each web browser, internet users often do not make the most of the features provided (Mustika et al., 2018).

4. Changing interactions and changing concerns

Observing how end users interact with web applications today, it is certain that users need more from an application and system than merely "ease of use." We are living in a different world today than what we were in during the early 1990s. Users are not only interacting with technology, but they are also interacting with other people through this technology. In terms of the web browser and its usability, we now also need to take the security, safety and privacy of our end-users into consideration. As ethically aligned design has become more a part of the computing and HCI culture, security and privacy are being seen as vital attributes of IT systems and services (Carroll, 2021). Indeed, within the competitive landscape of browsers, it has now become more about providing users with an ever growing number of security, privacy and performance enhancements and also new and novel browser extensions/tools. However, as mentioned previously, internet users often do not make the most of these features.

Therefore, people – for their own well being – need to be more supported to think about the interface, content, and who they are interacting with as they interact. For example, in their study, Macaulay et al. (2020) found that while children (8–11 years old) generally reported feeling safe online and perceived that they had a good awareness of online

dangers and how to avoid them, they tended to be poor at articulating for themselves exactly what those dangers were and how they personally could elude them. Also, studies of parents' online safety concerns typically centre on information privacy and on worries over unknown third parties preying on children... (Greyson et al., 2023). Without a doubt, the opportunity for online engagement increases possible exposure to potentially risky behaviours, which may have significant negative consequences (Rutkowski et al., 2021).

Presented via the web browser, harmful effects for society are increasing such as heightened exposure to harm, social isolation, depression and cyber-bullying (Best et al., 2014). For many these include privacy violations and unwanted solicitation (Moreno et al., 2013). Research on internet safety for adolescents, in particular, has identified several important issues including unwanted exposure to sexual material and sexual solicitation (Buijs et al., 2017). Fairbrother and Langford (2020, p.1) go as far as saying: "If you were a paedophile and you were looking to invent a system for abusing children, identifying them, grooming them, being able to meet them where your safety was guaranteed to carry out ads for your sexual gratification, you'd invent the internet." The reality is that young people and their families may not know how to stay safe online or how to respond following unsafe internet experiences (Loneragan et al., 2023). Equally, they may not fully appreciate the role of the browser application in all of these online experiences. In line with McLuhan (1964) "the medium is the message," they might not recognise the communication medium itself, not solely the messages it carries, as being an important focus of study.

5. Being safe online

From a HCI perspective, we need to further examine the design of these web browser applications to ensure that they afford appropriate and responsible interactions. It is well known that people say and do things in cyberspace (online) that they wouldn't naturally say and/or do in the face-to-face world. Some people feel more uninhibited online (Aiken, 2016). The author asks the question "why?," "what is it about the design of these virtual spaces that affords these feelings and behaviours?." What is it about the design of these online spaces that make us feel more callous, anxious, insecure, or even too secure (e.g., invisible)? When we design our physical environments, careful consideration is drawn from many fields to plan and design environments that affect, and are affected by, human behaviour appropriately (i.e., fair, sustainable, safe etc.). Through its design, the physical environment can facilitate and/or discourage certain interactions amongst people, to a certain extent, it can influence peoples' behaviour and motivation to act etc. For example, an inviting space with comfortable surroundings, security and privacy can encourage certain feelings of safeguarding and avoiding harm. The question is how do we do we design this integrally for our online spaces? And where do we start?

The browser is the gateway to all of this but also it can be the gateway to stopping all of this. There are many researchers already working on this. For example, recent research (Gowda et al., 2020) have developed a novel technique to identify phishing websites effortlessly on the client side by proposing a novel browser architecture named as "Embedded Phishing Detection Browser" (EPDB). However, it is unfortunate to say that the overall drive of browsers to outdo one another is still producing inconsistencies in design and the end-user browser experience. For instance, unlike the other browsers, Chrome's official extension repository has more than 63,000 extensions, with some of them having more than ten million users (Picazo-Sanchez et al., 2020). This opens up the potential for the Chrome browser to provide a completely different user experience/impression when compared to the other browsers. This also has the scope to create confusion and lack of motivation amongst the end-users. For example, end-users might unfairly categorise one browser as the same as the other browsers and as we have seen misunderstand the features and/or not use them.

To elaborate further, in their study, Leith (2021) show that the different browser designs afford different risks for the end-users. They show that browsers such as Chrome, Firefox, Safari and Edge all share details of web pages visited with back end servers but Chrome, Firefox and Edge have also been found to share long-lived identifiers (Leith, 2021). Unknown to the end-user, these can be used to link connections together and so potentially allow the tracking of a person's usage of the web over time (Leith, 2021). More so, in their study, Hughes et al. (2021) highlight that private browsing does not mean absolute anonymity on the browsers (Google Chrome, Microsoft Edge, Mozilla Firefox and Brave) and someone with the appropriate skills and tools can recover different amounts of artefacts (depending on what browser is being used) related to the activity carried out through the web browser. Looking at the positive side of things, browsers can play a pivotal role in any forensic investigation and help determine if nefarious or suspicious activity has occurred on a device (Hughes et al., 2021). In fact, the basics of web browser forensics revolve around the artifacts such as web sites visited, malicious URLs, time stamps, counts of access, search histories, cookies, downloaded activities etc. (Asim et al., 2019). However, with the positive comes the negative, and the "inconsistently designed" web browser application seems to be opening up more vulnerabilities and enabling more harm to the end user than many of us fully realise.

6. Web browsers and warnings

Despite the internet playing a big role in our lives, we don't always notice what the web browser warnings are telling us about our online threats. As Reeder et al. (2018) describe "when someone encounters a browser security warning, they need to make a security-critical decision should they adhere to the advice in the warning or proceed to the website despite the risk of an attack?." In reality, there are many people

at risk who may not see or hear a warning, or they may not understand it (Laughery & Wogalter, 2010). Often users habituate to warnings and feel *warning fatigue* and as a result they ignore them completely, they don't believe the potential threat is really a risk and as a result click through them (Agrawal et al., 2020). The safety hierarchy - often referred to as the design, guard and warn sequence - shows warnings are third in the sequence because even the best warnings are not likely to be 100% effective (Laughery & Wogalter, 2010).

To overcome these negative outcomes, the effective design of the warning is crucial. As (Wogalter, 2019, p.42) points out "the warning needs to be highly salient and persuasive to attract and maintain attention despite the person's tendency to ignore." Indeed, the purpose of a warning is to show the user why they should be cautious, it needs to provide enough information so users can make informed decisions about safe usage, including the choice on whether to use it at all (Laughery & Wogalter, 2010). "Warnings are a type of risk communication intended to give people information about potential hazards and instructions to promote safe behaviour" (Wogalter & Mayhorn, 2017, p.331). In conjunction with protecting people from harm, "warnings are also intended to modify behavior to comply with existing safety regulations; to decrease the likelihood of health problems, accidents, or property damage; and to serve as reminders" (Bravo-Lillo et al., 2011, p.18). However, unfortunately, many conventional projects, don't consider security and usability as primary goals, making them likely candidates for sacrifice in the rush to meet project deadlines (Faily et al., 2015).

In order for a warning to be effective, it must contain and afford certain things. Firstly, it needs to capture the users attention and then afford enough motivation from the user to encode it. As Laughery and Wogalter (2006) emphasise warnings must be sufficiently conspicuous, and they must have characteristics that encourage encoding the content... they must also provide the information needed for recipients to make informed decisions regarding compliance. Interestingly in their study, (Bravo-Lillo et al., 2011, p.25) found that participants often didn't thoroughly read warnings; "giving them more text to read might worsen the problem." It is important that users don't become desensitized to warnings, that warnings are presented only when necessary, and then with only the necessary information. Interestingly, one of the main elements that contributes to the attention of users towards warnings is the signal icons and signal words (Samsudin et al., 2016). Furthermore, (Akhawe & Felt, 2013, p.270) found that users "rarely click on the explanatory links such as "More Information" or "Learn More" and designers who utilize such links should ensure that they do not hide a detail that is important to the decision-making process."

Historically, web browser warnings generally focus on helping protect people from malware, phishing, and network attacks (Reeder et al., 2018). However, when we look at things like disinformation, the question lies on if the browser can help? To be sure, there are several browser

extensions that can help users figure out how to detect misleading articles and untrustworthy websites. For example, tools like fact checkers can help to overcome the potential harmful consequences of disinformation (Hameleers et al., 2020). However, researchers have argued that fact checkers can only be successful if they win the trust of the audience - by making their practices transparent (Humprecht, 2020). When interacting with the web, end users generally want the experience to be as seamless as possible. In practice, end-users do not like to be interrupted - by additional tools or pop up windows - from their flow of interaction (Kaley, 2019). For example, Microsoft's office assistant called Clippy was often hated during its lifespan in product (1996-2006) (Baym et al., 2019). Interestingly, in their research, (Kim et al., 2016) explore why consumers enjoy a computer game less when they receive assistance from a computerized helper imbued with humanlike features than from a helper construed as a mindless entity. Moreover, it has to be said that the digital assistant has greatly evolved from the Microsoft's Clippy to now experiences like Amazon's Alexa. However, regardless of this and despite increased interests in the study of fake news, how to effectively aid users' decision in handling suspicious or false information has not been well understood (Seo et al., 2019). The author asks: "Could the web browser play a bigger role in supporting the end-user with these challenges?"

7. Study

This study investigates the effectiveness of the desktop web browser application design. It aims to give some initial insight into how individuals feel about their web browser application. In particular their understanding of the features on the web browser application and if there is a need for more effective designs and more targeted support. The study took place at Cardiff Metropolitan University in Autumn 2023.

7.1. Participants

Five hundred and twenty-eight participants (P.1 to P.528) between the ages of eighteen and eighty-six years old took part in this study. These included two hundred and eighty-two females and two hundred and thirty-nine males, seven participants preferred not to say. In terms of educational background, 53% of these participants have a bachelor's degree and/or above, 22% of participants have a college certificate (non-degree) and the remaining have a secondary school certificate or less.

7.2. Methods

A survey research method was used here to collect data from participants. Using the Qualtrics online survey software, participants were presented with a series of twenty-five questions. The questionnaire was designed to take approximately ten-fifteen minutes in duration to complete. In terms of data analysis, descriptive statistics was used to

Table 1. Question: How confident are you with browsing the world wide web (www)?

Age Group	Extremely Confident	Extremely Unconfident
17–25 years	30	5
26–35 years	72	2
36–45 years	67	0
46–55 years	57	2
56–65 years	51	0
66–75 years	0	0
76–85 years	1	0
86+ years	0	3
TOTAL	278 participants	12 participants

describe the relationship between variables in the sample of participants. This was in the form of measures of frequency (i.e., count and percent) and measures of tendency (i.e., mean). Moreover, a thematic analysis was used to examine themes or patterns of meaning within the qualitative data collected. The experimental procedure was approved by the ethics board of Cardiff Met University and subjects provided consent for study participation and the academic use of de-identified data.

7.3. Findings

The demographic information was firstly analysed to better understand the background characteristics of the participants. In particular, we can see that from a total of five hundred and twenty-eight participants, more than half (53%) are extremely confident with using web browsers. As Table 1 shows the age groups that are the most confident with browsing the web are those from the 26–35 and 36–45 years age ranges. The overall results also show that males appeared more extremely confident than females in browsing the web (see Table 2). Though specifically for the 26–35 and 36–45 years old age groups more women were extremely confident than men. Moreover, Google Chrome is the most popular browser (see Figure 1). In detail, three hundred and ninety-four participants said they use Google Chrome when compared to Apple Safari (e.g., one hundred and seventy-one participants), Microsoft edge (e.g., one hundred and eleven participants), Mozilla Firefox (one hundred and three participants), Opera (e.g., fifty-one participants), Vivaldi (e.g., twenty-three participants) and fifteen participants who said they use other browsers. In terms of length of time spent using the web browser, 45% of participants from the age groups 26–45 years old showed a higher overall usage of the web browser. 10% of the women, as opposed to 7% of the men, indicated that they usually spend 6 hours or more per week on the web (see Figure 2). 31% of participants who took part in the study stated that they use their web browsers for between 2–4 hours a day.

Despite the inconsistency across the design of the main web browser applications (Calzavara et al., 2020) (Amrutkar et al., 2015), the findings show that 84% of females and 83% of males who partook in the study were satisfied with their web browser experience. Furthermore, when asked about the features on a Google Chrome web browser address bar (see Figure 3), the participants clearly said “yes” that they recognise the features.

Table 2. Question: How confident are you with browsing the world wide web (www)?

Age Group	Extremely Confident	Extremely Unconfident
Female	134	6
Male	142	3
Rather not say	2	3
TOTAL	278 participants	12 participants

However, Table 3 shows that the number of participants perceiving/recognising the web browser features varies. In detail, the “back button” is recognised by more participants when compared to the “padlock” and “profile” features. When participants are asked if they think it is important that the features/buttons are consistent across all the browsers, the majority of participants (75%) said “yes.” As we can see from Figure 4, consistency is important for participants in terms of ease of use and easier use.

- So people always understand what certain icons mean (P.11)
- It just helps people seamlessly move from one to the next (P.16)
- It makes sense, as radically different features just confuse users (P.22)
- I think it's a good idea to be as why would you want to make things complicated for users (P.27)
- to simplify the experience for those who struggle with computers (P.158)
- then if i change browser i know exactly when i am safe and not (P.267)

In contrast, 17% of participants said “no,” it is not important that the features/buttons are consistent across all the browsers.

- I just use Chrome so dont need to have consistency with other browsers (P.18)
- People have different ways of looking at things and ways of working. It should be customisable, The P in PC stands for Personal after all (P.24)
- different companies can do things their way (P.86)
- Their differences make each of them unique in their way (P.100)
- They are different brands, so they have to be unique (P.108)
- People tend to stick to 1, as long as they can use it's ok (P.277)

Examining the padlock feature in more depth, the author focuses on the data collected from the question: “On this Google Chrome browser bar ... do you know what the padlock icon represents/means? Please elaborate here.” A thematic analysis was applied. The first stage of this data analysis was to become familiarised with the qualitative data, this was done by reading through the data and becoming acquainted with participants thoughts, feelings and actions around the padlock. It involved the identification of several preliminary codes and then themes that were created from the data in order to describe and understand the content.

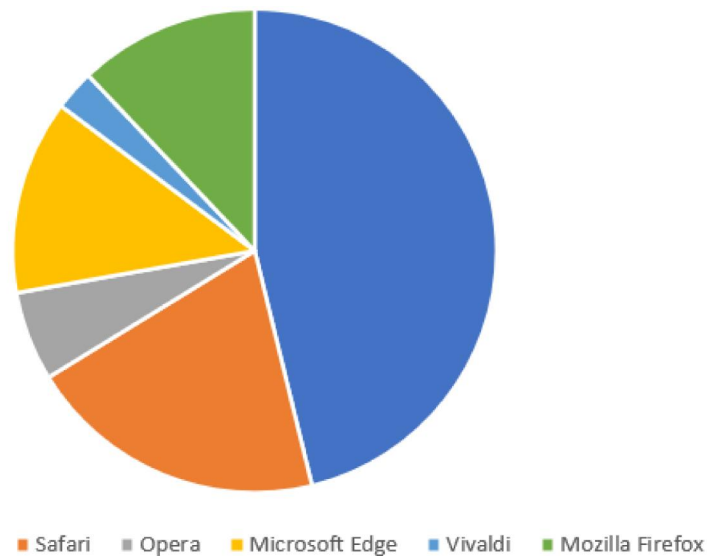


Figure 1. Question: Which of the following browsers do you tend to use?.

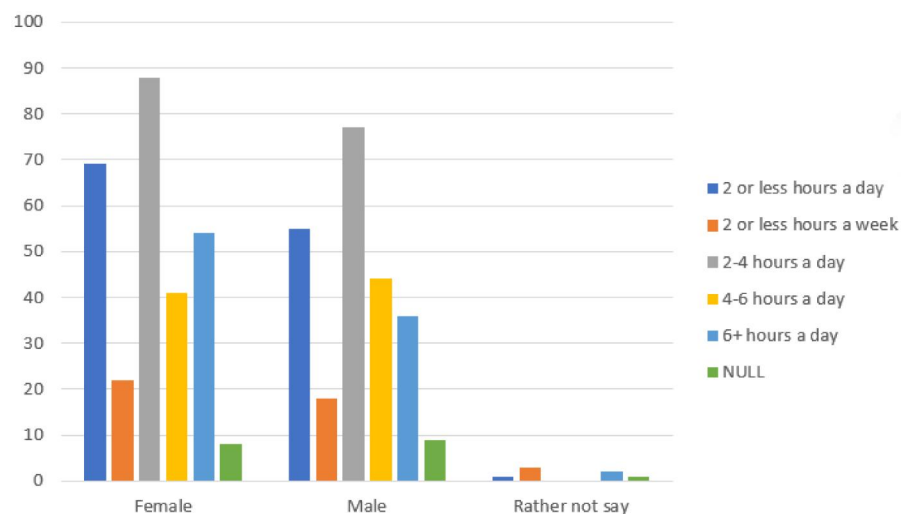


Figure 2. Question: How long do you typically spend on the world wide web (www) per day?.



Figure 3. Google browser address bar (desktop).

Table 3. Question: What web browser features are used the most?

Web Browser Features	Number of Participants
Back Button	337
Refresh Button	328
Address Bar	306
Forward Button	287
Home Button	269
Share this page Button	125
Padlock Button	124
Profile Button	104

The following codes were identified: yes; no; uncertain; safe/secure website; safe connection; secure page; private; feature; encryption; locked; secure web address; nonsense; vague; trustworthy; not harmful; genuine; and not used.

In detail, one hundred and eight participants clearly replied with a “No” or a variation of “No” (e.g., nope, nil, none,

nothing, I don’t know etc.) that they don’t know what the padlock means and/or represents. Nineteen participants stated that they were unsure. Fourteen participants simply said “Yes” with twelve more participants saying “Yes” they know what it meant with a little further elaboration. One participant stated they do not use the padlock. Moreover, one hundred and four participants stated that they felt that the padlock meant that the website was secure and/or safe. Fifteen participants felt that the padlock represented a safe webpage. Five participants talk about the padlock affording privacy. Thirty participants talk about the concept of the website being “locked.” Three participants felt that the padlock meant that the website was more trustworthy. Two participants equated the padlock to meaning that the website was more genuine. Only sixteen participants stated that the padlock represented the safe connection, and three participants talk about it involving encryption.

It seems that the padlock icon is giving the wrong message to the participants. The padlock is affording the idea that the entire page is locked and no one can use it only those with the key (password) rather than the connection is secure.

- It means it is locked so needs a password to open (P.18)
- It's enable locking of a particular page of the website (P.70)
- To lock the site, or bookmark it (P.129)
- I am not too sure - does it keep that page locked so you can't move away from it or have updates/changes made to it? (P.147)
- privacy lock so no one can use kf (P.151)
- To lock a page so that the page can remain there (P.336)
- the padlock icon represents a website that is deemed secure. (P.361)

To sum up, the presence of the padlock only means that the data transmitted between the participant and the website site is encrypted and secure. Drawing a parallel with the physical world, it is the gate and pathway to the house that is locked. It doesn't mean that everything inside the house is locked as well. A padlocked website (e.g., HTTPS site) can still be malicious and harmful. When we explore the "correct understanding of what the padlock represents" theme, there are much less participants who understand that the padlock is about the connection, that the subtheme "safe connection" is more aligned with what the padlock represents:

- It brings up further information on the site you're on i.e., if its a secure connection and gives you a chance to alter your settings (P.9)
- that the site connection is secure (P.73)
- A padlock (or lock) icon displayed in a web browser indicates a secure communication channel between the browser and the server on which the website is hosted. It signifies that the connection to the website is encrypted using HTTPS and has an SSL/TLS (P.166)
- padlock mean page uses more secure HTTPS rather than older less secure method to send the data (P.167)
- I think the padlock means it is a secure site so anything you enter cannot be seen by anyone else. (P.298)
- It means it's a secure connection (P.323).

Interestingly, when we look back through the data collected from all the different browser experiences, particularly in relation to this question on the padlock feature (do you know what the padlock icon represents/means?). The single word responses of "Yes" or "No" clearly presents a pattern across all the four web browser experiences studied (see Figure 5). For the Google Chrome web browser, sixty-five participants stated "No" they didnt know what the padlock represented and fourteen stated "Yes," they did. Similarly, the Safari browser found one hundred and two participants said "No" and six participants said "Yes." Moreover, for the Opera web browser ninety-one

participants were recorded as saying "No" and nine said "Yes" and finally for Microsoft Edge web browser ninety-two participants said "No" and ten said "Yes."

It is important to note here that a user's experience of the browser can be highly subjective and can indeed vary based on their exposure, usage experience, and personal preferences. For example, a participant familiar with Google Chrome might find it less challenging and/or more satisfying to use when compared to another browser application etc. However, in this instance, the focus was solely on how the participants perceived and understood the padlock icon. Despite the inconsistencies in the padlock design, there are also certain similarities in how it has been designed across different web browsers. In detail, its general recognition is prominent across all the browsers tested. The author's intention was for this universality (its widespread design recognition) to mitigate any past usage experiences that participants might have had across the various browser applications.

To probe the data gathered from this question more deeply, the author examines the broader narrative provided for each browser tested and then categorises participants' indirectly expressed responses into "Yes" or "No" clusters. Firstly, she cleans the data set (e.g., discards the nonsensical and incomplete/vague answers). Then, she organises the broader narrative-type responses into a "Yes" or "No" category. This new data set with a count of three hundred and ninety-three responses consisted of "No" for all participants who clearly stated "No," they don't know, they don't use etc. And "Yes" for all participants who provided a confident explanation of the padlock whether it was correct or not correct. For example, statements such as "it means its a secure page," "page is secured," "it locks the page" etc. would be placed into the "Yes" category. A key point to emphasise here is that a greater number of participants feel confident in their comprehension of the padlock icon (see Figure 6) when compared to the data presented in Figure 5.

The rationale for this extra analysis is to highlight the capacity of the padlock design to shape participants' ability to confidently explain the significance of the padlock icon. As we have seen in the thematic analysis, the padlock icon, despite not being accurately understood by all participants, effectively communicates a sense of security and instills confidence through its presence and positive associations. In detail, we are interested in the concept of perceived security and how a design can afford confidence (e.g., elicit a notably confident/positive response) despite participant's limited understanding of the padlock icon's meaning. Perceived security refers to how safe people believe they are, regardless of their actual understanding of the underlying mechanisms. As (Chang & Chen, 2009, p. 412) note perceived security is "a personal perception rather than any objective measurement, and assumes a customer's intuitive ability to assess risk."

Using a 2-tailed, paired t-test on each pair of browsers a set of p values were calculated (e.g., using the average of the "Yes" and "No" responses for each browser). As we can see from Table 4, there is significant difference between people's understanding of the padlock feature on the Chrome

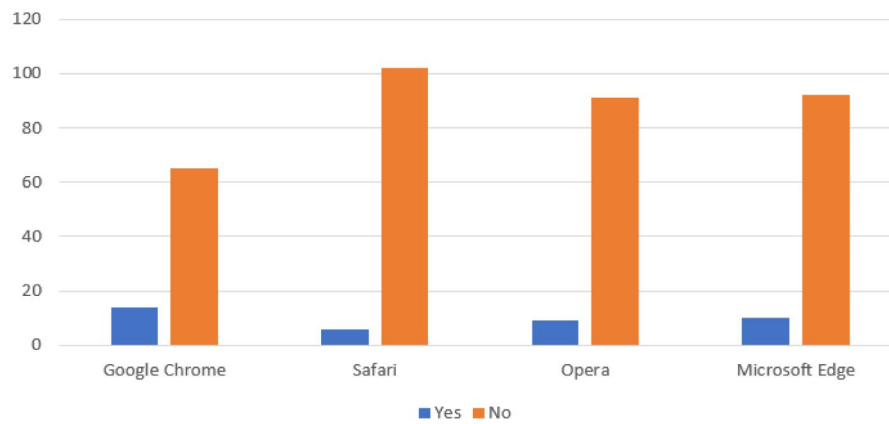


Figure 5. Question: Do you know what the padlock icon represents? YES and NO answers.

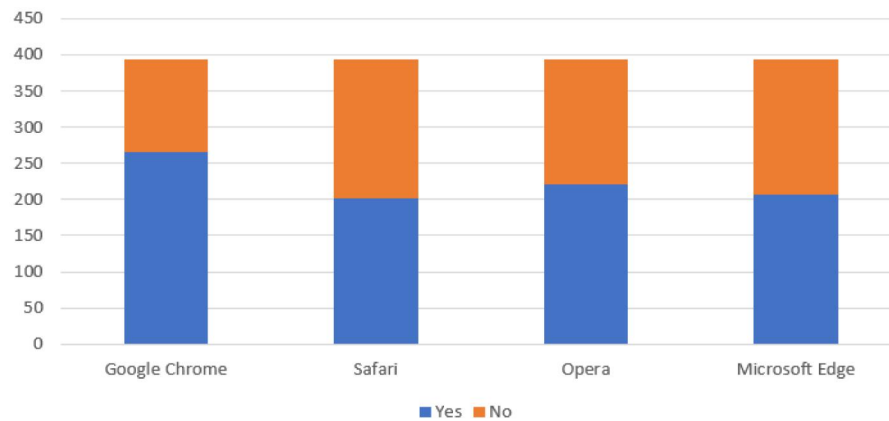


Figure 6. Question: Do you know what the padlock icon represents? Variants of YES and NO answers.

Table 4. 2-tailed, paired t-test on each pair of browsers.

Web Browsers	Chrome	Opera	Edge	Safari
Chrome	X	0.0001	0.0001	0.0001
Opera	0.0001	X	0.0050	0.5723
Edge	0.0001	0.0050	X	0.0320
Safari	0.0001	0.5723	0.0320	X

browser when compared to the other browsers (p value = 0.0001). In fact, the proportion of people saying “Yes, I know” or “No, I don’t know” or feeling they know what the padlock represents on the Chrome browser is higher than the other browsers. These figures could be influenced by usage experience and the fact that more people tend to use the Chrome browser. For future studies, it would be interesting to involve participants with no or little prior usage experience and/or exposure to the padlock icon. Saying that, the difference between the Opera and the Edge Browser is also significantly different ($p = 0.0050$), though the remaining cases are less noticeable. Indeed, different browsers have different ways of presenting the padlock feature. The padlock icon is usually displayed in the address bar, and its visual appearance can vary between browsers. For example, some browsers may display a green padlock, while others might use a black, grey or no colour. For this study the Opera padlock icon was black whilst the Microsoft padlock icon was white. Also, the position of the padlock can vary as well. In the web browser designs used in this study, the padlock is shown at the beginning of the address bar (Chrome,

Microsoft edge and Opera), while in others (e.g., Safari), it may appear at the end or even inside the address bar. Regardless of this, as we have seen from the earlier qualitative data, many participants feel satisfied with their browser experience and confident that it is keeping them safe from malicious websites. They generally think that the padlock feature on the browser application and in particular the chrome browser application affords security and safe web pages. The scary reality is that it does afford security but not in the way they perceive/understand.

8. Discussion

Focusing on the issues discussed or at least, the reasons why these issues are still emerging, the author is very much centred on the design. In particular, how the padlock icon needs to be more intuitively designed and developed to afford the correct meaning. Also, how the front-end framework of the browser application needs to include considerations for aesthetics, accessibility, inclusivity, empathy, security, responsibility, transparency, and trust. Interestingly, sixty-two percent of participants said they think it would be useful to have a feature on the browser bar that would allow them to check if the content on the web page is accurate. It took participants an average of 40.82 seconds to answer this question. This contrasts to the 65.15 seconds average time taken to respond to the online profile-type (e.g., digital

footprint) question. In detail, fifty-six percent of participants thought it would be useful to have a feature on the browser that would give people more information on the data that is being collected on them whilst they are browsing. Twenty-seven percent of participants thought it would not be useful. Finally, thinking, more generally, about online activity, many participants (fifty-five percent) did not think that it would be useful to have a feature on the browser bar that checked their own behaviour/monitored the content that they shared online. This question was answered promptly with an average of 42.25 seconds.

Overall, the study highlights significant web safety vulnerabilities in the browser application. Particularly, where many participants feel that the browser affords trust and a website with safe content when it clearly does not. In addition, it should be noted that many participants do not fully understand what the role of the browser entails. When asked: In your opinion, what is the role of a web browser?. Words like information (146 hits), find (86 hits), search (86 hits), help (56) were featuring heavily in the responses. This is compared to words like internet (54 hits), access (49 hits), web (45 hits), browse (13 hits) and connect (11 hits). There still seems to be an uncertainty between the role of the browser and that of the search engine. More crucially, there is a clear mismatch between what the current browser design affords and what the end-user understands.

8.1. Limitations of the study

As discussed, we have performed an in-depth study of people's perceptions of the desktop browser application design as opposed to the mobile browser application design. It was decided to focus solely on the desktop browser application design because of the differences in the design due to smaller screen sizes of the mobile devices. In detail, these different designs with many unique features can have an impact on how users interact with them. They can afford different behaviours when it comes to perceiving and browsing the web. However, in hindsight, there are several limitations to only studying the desktop browser application and neglecting the mobile browser application. Firstly, there has been a recent shift in internet usage from desktop to mobile devices. In fact, mobile browsing has become increasingly more popular than the desktop, with many users now primarily accessing the web through their smartphones. Moreover, users tend to interact with the desktop and mobile browser applications in different ways and in distinct contexts. For example, desktop browsing tends to often occur in a more controlled and focused environment, such as a workplace or home. Whilst, mobile browsing, tends to take place on-the-go and in more social situations.

Furthermore, the fact that the mobile browser application sits on a smaller screen and affords different interactions, is important to note. This can impact how users perceive the browser application but also it can constrain how they perform tasks. Mobile browsers also offer unique features which can enhance user experiences and engagement in different ways to the desktop browsers. In summary, studying only

desktop browser applications comes with limitations, as it neglects the more dominant mobile browsing trend and the unique user perceptions, behaviours, contexts, and constraints associated with mobile devices. Saying that, despite these limitations, the results generated through this study has provided us with an important first step in understanding how people perceive the desktop browser application design. Future research is needed to help us gain a more comprehensive understanding of the complete browser application design environment (e.g., desktop and mobile and also perception as well as interaction with these). Ultimately, understanding the differences between desktop and mobile browser application design is crucial for improving the overall perception and experience for end-users.

9. Conclusion

It has become more important than ever for end-users to be more aware of their online safety whilst browsing the web. This thinking is the result of many harms suffered online. As the UK's communications regulator (Ofcom) highlighted through their online harms survey (2021), a high percentage of people are now suffering online harms, with content harms being the most prevalent (Yonder, 2021). Unfortunately, as Price (2021) has noted current regulatory approaches are totally outpaced by web technology and do not protect users from online harms transmitted over online platforms. Therefore, the author feels that we need to push for higher standards and solutions from the design side. Focusing on the gateway to the web, the browser application inconsistencies need to be addressed. People need a uniform and effective browser application to counter and fully protect against harms as they browse online. For example, it is no longer acceptable to have features like the padlock that people don't fully understand. This paper was specifically focused on people's perceptions of desktop browser applications, e.g., the features they use and importantly, their perceptions and understanding of these features. The findings clearly show that some features are used more than others and that people's understanding of these features varied, with many having an incorrect interpretation. Also, when probed, the participants confirmed possibilities of how to extend the browser application design with further useful yet integrated and effectively designed features.

Moreover, it is the authors opinion that more pressure needs to be placed on the key web browser developers to ensure that there is consistency across all browser applications. The world of usability and HCI has done years of work in this field and the browser application should not ignore these valuable efforts. In 2002, research highlighted the inconsistencies across browsers and the need for value sensitive design (Friedman et al., 2002) but over twenty years on, the need still exists. The fact that people are interpreting features such as the padlock incorrectly, should be sufficient a sign to take action. The internet, at the best of times, is not a very safe place, the least we can do is make sure that we get the design of its gateway consistent and effective.

9.1. Recommendations

While it is hoped that web browser applications would adhere to web standards such as the World Wide Web Consortium (W3C), there still exists variations in their designs. As we have seen in this study, the web browser application consistency is a complex challenge. In terms of the padlock feature, the lack of consistency across the design means that the users don't have a uniform understanding and experience while using different web browser applications. This is particularly challenging as users usually expect applications like this to provide a familiar browsing experience. Yet even more challenging is the fact that they are not even noticing the differences. As evident from this study, some people haven't even notice the padlock feature, and many don't have a clear understanding of what the padlock represents. For others, it is almost like they have accepted it being there without fully understanding what its role is on the browser application. To improve this, there would need to be: (1) a clear and universal understanding of what the padlock feature entails (e.g., should the padlock feature appear only on a HTTPS connection and not on a HTTP connection?) (2) a consistency in the location of the padlock icon on the address bar (e.g., should it be on the left of the address bar, visible whilst typing in the URL?) (3) a standard padlock design across all browsers to maintain consistency and avoid confusion (e.g., should we consider a design/icon that affords more of a connection) (4) a colour or sound to differentiate the padlock's states (e.g., should we use a green padlock to indicate a secure connection and a red padlock to represent an insecure connection?). It is only through thinking about the design of the padlock feature and then the overall web browser application consistency, can we hope to effectively communicate this secure connection to users. It is only through effective user interface design that we can foster "real" trust and confidence in people's web browser application interactions.

Acknowledgments

Thank you to Dr. Rhyd Lewis and Ms. Diep Linh Nguyen for their support whilst writing this paper.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Fiona Carroll  <http://orcid.org/0000-0002-9967-2207>

References

- Agrawal, N., Zhu, F., Carpenter, S. (2020). Do you see the warning?: Cybersecurity warnings via nonconscious processing. *ACMSE 2020 - Proceedings of the 2020 ACM Southeast Conference*.
- Aiken, M. (2016). *The cyber effect; an expert in cyberpsychology explains how technology is shaping our children, our behavior, and our values—and what we can do about it*. Spiegel & Grau. (23 Aug. 2016).

- Akhawe, D., Felt, A. P. (2013). Alice in warningland: A large-scale field study of browser security warning effectiveness. *Proceedings of the 22nd USENIX Security Symposium*.
- Amrutkar, C., Traynor, P., & Oorschot, P. C. V. (2015). An empirical evaluation of security indicators in mobile web browsers. *IEEE Transactions on Mobile Computing*, 14(5), 889–903. <https://doi.org/10.1109/TMC.2013.90>
- Asim, M., Amjad, M. F., Iqbal, W., Afzal, H., Abbas, H., & Zhang, Y. (2019). Androkit: A toolkit for forensics analysis of web browsers on android platform. *Future Generation Computer Systems*, 94, 781–794. <https://doi.org/10.1016/j.future.2018.08.020>
- Baym, N., Shifman, L., Persaud, C., & Wagman, K. (2019). Intelligent failures: Clippy memes and the limits of digital assistants. *AoIR Selected Papers of Internet Research*, 2019. <https://doi.org/10.5210/spir.v2019i0.10923>
- Best, P., Manktelow, R., & Taylor, B. (2014). Online communication, social media and adolescent wellbeing: A systematic narrative review. *Children and Youth Services Review*, 41, 27–36. <https://doi.org/10.1016/j.childyouth.2014.03.001>
- Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security and Privacy*, 9, 18–26. <https://doi.org/10.1109/MSP.2010.198>
- Buijs, P. C., Boot, E., Shugar, A., Fung, W. L. A., & Bassett, A. S. (2017). Internet safety issues for adolescents and adults with intellectual disabilities. *Journal of Applied Research in Intellectual Disabilities*, 30(2), 416–418. <https://doi.org/10.1111/jar.12250>
- Calzavara, S., Roth, S., Rabitti, A., Backes, M., Stock, B. (2020). A tale of two headers: A formal analysis of inconsistent click-jacking protection on the web. *Proceedings of the 29th USENIX Security Symposium*.
- Carroll, F. (2021). *Usable security and aesthetics: Designing for engaging online security warnings and cautions to optimise user security whilst affording ease of use* [Paper presentation]. ACM International Conference Proceeding Series. <https://doi.org/10.1145/3481357.3481376>
- Chang, H. H., & Chen, S. W. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information & Management*, 46(7), 411–417. <https://doi.org/10.1016/j.im.2009.08.002>
- Faily, S., Lyle, J., Flechais, I., & Simpson, A. (2015). Usability and security by design: A case study in research and development.
- Fairbrother, N., & Langford, F. (2020). Internet safety. *Journal of the Institute of Telecommunications Professionals*, 14, 37–43. <https://safetynetfoundation.org/2020/10/01/internet-safety-2/>
- Friedman, B., Hurley, D., Howe, D. C., Felten, E., & Nissenbaum, H. (2002). Users' conceptions of web security: A comparative study. *Conference on Human Factors in Computing Systems - Proceedings* (pp. 746–747). <https://doi.org/10.1145/506443.506577>
- Gowda, H. M., Adithya, M., Prasad, S. G., & Vinay, S. (2020). Development of anti-phishing browser based on random forest and rule of extraction framework. *Cybersecurity*, 3. <https://doi.org/10.1186/s42400-020-00059-1>
- Greyson, D., Chabot, C., Mniszak, C., & Shoveller, J. A. (2023). Social media and online safety practices of young parents. *Journal of Information Science*, 49(5), 1344–1357. <https://doi.org/10.1177/01655515211053808>
- Hameleers, M., Powell, T. E., Meer, T. G. V. D., & Bos, L. (2020). A picture paints a thousand lies? the effects and mechanisms of multi-modal disinformation and rebuttals disseminated via social media. *Political Communication*, 37(2), 281–301. <https://doi.org/10.1080/10584609.2019.1674979>
- Hughes, K., Papadopoulos, P., Pitropakis, N., Smales, A., Ahmad, J., & Buchanan, W. J. (2021). Browsers' private mode: Is it what we were promised? *Computers*, 10(12), 165. <https://doi.org/10.3390/computers10120165>
- Humprecht, E. (2020). How do they debunk "fake news"? a cross-national comparison of transparency in fact checks. *Digital Journalism*, 8(3), 310–327. <https://doi.org/10.1080/21670811.2019.1691031>

- Kaley, A. (2019). *Popups: 10 problematic trends and alternatives*. Nielsen Norman Group (NN/g).
- Kim, S., Chen, R. P., & Zhang, K. (2016). Anthropomorphized helpers undermine autonomy and enjoyment in computer games. *Journal of Consumer Research*, 43(2), 282–302. <https://doi.org/10.1093/jcr/ucw016>
- Laperdrix, P., Bielova, N., Baudry, B., & Avoine, G. (2020). Browser fingerprinting: A survey. *ACM Transactions on the Web*, 14(2), 1–33. <https://doi.org/10.1145/3386040>
- Laughery, K. R., & Wogalter, M. S. (2006). Designing effective warnings. *Reviews of Human Factors and Ergonomics*, 2(1), 241–271. <https://doi.org/10.1177/1557234X0600200109>
- Laughery, K. R., & Wogalter, M. S. (2010). The safety hierarchy and its role in safety decisions. 1010–1016.
- Leith, D. J. (2021). Web browser privacy: What do browsers say when they phone home? *IEEE Access*, 9, 41615–41627. <https://doi.org/10.1109/ACCESS.2021.3065243>
- Loneragan, A., Moriarty, A., McNicholas, F., & Byrne, T. (2023). Cyberbullying and internet safety: A survey of child and adolescent mental health practitioners. *Irish Journal of Psychological Medicine*, 40(1), 43–50. <https://doi.org/10.1017/ipm.2021.63>
- Macaulay, P. J. R., Boulton, M. J., Betts, L. R., Boulton, L., Camerone, E., Down, J., Hughes, J., Kirkbride, C., & Kirkham, R. (2020). Subjective versus objective knowledge of online safety/dangers as predictors of children's perceived online safety and attitudes towards e-safety education in the united kingdom. *Journal of Children and Media*, 14(3), 376–395. <https://doi.org/10.1080/17482798.2019.1697716>
- McCluhan, M. (1964). *Understanding media: The extension of man*. McGraw-Hill.
- Moreno, M. A., Egan, K. G., Bare, K., Young, H. N., & Cox, E. D. (2013). Internet safety education for youth: Stakeholder perspectives. *BMC Public Health*, 13(1), 543. <https://doi.org/10.1186/1471-2458-13-543>
- Mustika, W. P., Mardian, M., & Rinawati, R. (2018). Analitical hierarchy process untuk menganalisa faktor pemilihan web browser pada desktop. *J-SAKTI (Jurnal Sains Komputer Dan Informatika)*, 2(1), 83. <https://doi.org/10.30645/j-sakti.v2i1.57>
- Nielsen, J. (1995). *Jakob Nielsen's ten usability heuristics*. Nielsen Norman Group.
- Nielsen, J. (2012). User satisfaction vs. performance metrics. Retrieved from <https://www.nngroup.com/articles/satisfaction-vs-performance-metrics/>
- Picazo-Sanchez, P., Tapiador, J., & Schneider, G. (2020). After you, please: Browser extensions order attacks and countermeasures. *International Journal of Information Security*, 19(6), 623–638. <https://doi.org/10.1007/s10207-019-00481-8>
- Price, L. (2021). Platform responsibility for online harms: Towards a duty of care for online hazards. *Journal of Media Law*, 13(2), 238–261. <https://doi.org/10.1080/17577632.2021.2022331>
- Rathod, D. M. (2017). Web browser forensics: Google chrome. *International Journal of Advanced Research in Computer Science*, 8, 896. <https://doi.org/10.26483/ijarcs.v8i7.4433>
- Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., & Egelman, S. (2018, April). *An experience sampling study of user reactions to browser warnings in the field* [Paper presentation]. Conference on Human Factors in Computing Systems - Proceedings, <https://doi.org/10.1145/3173574.3174086>
- Rutkowski, T. L., Hartikainen, H., Richards, K. E., & Wisniewski, P. J. (2021). Family communication: Examining the differing perceptions of parents and teens regarding online safety communication. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 1–23. <https://doi.org/10.1145/3479517>
- Samsudin, N. F., Zaaba, Z. F., Singh, M. K., & Samsudin, A. (2016). Symbolism in computer security warnings: Signal icons & signal words. *International Journal of Advanced Computer Science and Applications*, 7(10). <https://doi.org/10.14569/IJACSA.2016.071020>
- Seo, H., Xiong, A., Lee, D. (2019). Trust it or not: Effects of machine-learningwarnings in helping individuals mitigate misinformation. *WebSci 2019 - Proceedings of the 11th ACM Conference on Web Science*.
- Statcounter (2023a). Browser market share worldwide dec 2021 - dec 2022. Retrieved from <https://gs.statcounter.com/>
- Statcounter (2023b). Worldwide desktop market share of leading search engines from january 2015 to december 2022. Retrieved from <https://gs.statcounter.com/>
- Wang, H., Liu, M., Guo, Y., & Chen, X. (2014). *Similarity-based web browser optimization* [Paper presentation]. WWW 2014 - Proceedings of the 23rd International Conference on World Wide Web. <https://doi.org/10.1145/2566486.2567971>
- Wogalter, M. S. (2019). *Communication-human information processing (c-hip) model*.
- Wogalter, M. S., & Mayhorn, C. B. (2017). *Warning design*. (pp (P. Luna, O. Lund, & S. Walker, Eds.). *Information design*. : 331–348). In A. Black.
- Wong, E. (2021). Principle of consistency and standards in user interface design. Retrieved from <https://www.interaction-design.org/literature/article/principleof-consistency-and-standards-in-user-interface-design>
- Yonder (2021). Ofcom pilot online harms survey 2020/21. Retrieved from https://www.ofcom.org.uk/_data/assets/pdf_file/0014/220622/online-harms-survey-waves-1-4-2021.pdf

About the author

Fiona Carroll has a proven track record of Human Computer Interaction (HCI) teaching and research excellence spanning over twenty years. She is committed to improving 'human wellbeing' through HCI and advocates for diversity and equality in the education of computing subjects.