Web Browser Security and Privacy

Keseana Howard
Computer Science
Hampton University
Hampton, VA

Abstract- This report will analyze issues related to web browser security and privacy. The web browser applications that will be looked at are Google Chrome, Bing, Mozilla Firefox, Internet Explorer, Microsoft Edge, Safari, and Opera. In recent months web browsers have increased the number of daily users. With the increase in daily users who may not be as well versed in data security and privacy, comes an increase in attacks. This study will discuss the pros and cons of each web browser, how many have been hacked, how often they have been hacked, why they have been hacked, security flaws, and more. The study utilizes research and a user survey to make a proper analysis and provide recommendations on the topic.

Figure 1: Web Browsers [1]

I. Introduction

Web browsers are one of the few ways to send data over a network and, gain access to the world wide web, or the internet as it is commonly called. As the years go on and efforts are made to make web browsers more secure, there are some areas that are important for the everyday user to know about to protect their personal data. Web browser security and privacy is not only left up to the user, but also the company that provides the web browser itself. The most common web browsers used today include Google's Chrome, Microsoft's Bing, Mozilla's Firefox, Microsoft's Internet Explorer and Edge, Apple's Safari, and Opera. Users of each search engine has a reason they prefer the one that they use from the compatibility of extensions, its speed, its dedication to security and privacy, compatibility on various operating systems (macOS, Windows, Linux, etc.), or if a free VPN is provided with the application.

Extensions, also referred to as plugins, are used to enhance the browser experience. A few of the web browser plugins that are used today are Tweetdeck, Adblock, Adobe Acrobat, Avast Online Security, Cisco Webex, Grammarly, Honey, Skype, and Teleparty (formerly known as Netflix Party). Plugins are used to enhance the browser experience for both business and pleasure purposes. For example, Tweetdeck allows you to track your tweets in real time, which can be used for businesses, big and small, or just for personal reasons. Another example is Teleparty, a plugin that allows you to watch tv shows and movies from various streaming services by synchronizing video playback for everyone in the "party". Like web browsers, the security and privacy of plugins is not just up to the providers of the service but also the user.

Security vulnerabilities are another area of concern when talking about the security and privacy of web browsers. The existing functionality in the web browser is exploited, or abused, by hackers to do numerous things. Hackers use the abuse of that functionality as an entry point to exploit cross-site request forgery flaws and run denial of service attacks. Three methods used to exploit browser security vulnerabilities include UI redress attacks, cursorjacking, and clickjacking. Everything mentioned above regarding security vulnerabilities are considered to be principal threats to the web browser. We also have to mention how malware affects browser security. An example of a malware attack on the web browser itself is the man-in-the browser attack. Malware attacks can also be executed on websites. It is important to note that that website vulnerabilities stand on their own against web browser vulnerabilities. Website vulnerability exploitations are those that might be more common to hear about. An example of an attack on websites are cross site scripting attacks, XSS.

Lastly, when talking about web browser security and privacy you cannot forget to mention browser history and cookies. Cookies are files that are stored on your computer from websites that you have visited. Browser history is the process of previously visited websites being stored in a centralized location in your browser settings. For the most part the user is in control of the privacy and security of their browser when it comes to both topics. Each individual browser gives the user the ability to manage their browser history and cookies in the settings. If the user does not manage their history and cookies well or even at all they are putting themselves more at risk for various hacking techniques. Some of the most popular hacking techniques are history sniffing, cache sniffing, cookie sniffing, and cookie harvesting.

A. Problem Statement

In this era of technology, with increased use during this pandemic, web browsers have been used more than ever. As more and more people are using web browsers, hackers are given more opportunities to attack. The owners of some of the most popular web browsers have had to increase their security and privacy. Owners of web browsers are not the only ones who should be taking actions to protect the user data. It is important for users to understand the threats to their privacy and security and how to manage their web browsers to protect their own data. It is hypothesized that while Google Chrome is one of the most popular browsers, it will not be the browser that upholds security and privacy as well as others.

II. Methodology

This study will use both literature review, documentation exploration, and a user survey to gather results and collect data to gain a better understanding of the content related to the thesis.

A. Literature Review

This paper aims to discuss the security and privacy issues when dealing with web browsers, both generally and specific to seven of the most popular web browsers. Scholarly articles and research reports were referenced to provide us with a foundation to build on research and support findings from the data collection of the web browser user survey.

Web browsers are applications that are used to access the internet [2]. It is imperative that web browser users consider the security and privacy of the web browser(s) that they choose to use. Privacy is how a user chooses to have their personal information used and controlled. Security on the other hand is how the personal information is protected while using the services the web browser provides. Web browsers work hard to protect their users from hackers, businesses, websites, advertisers, internet service providers, and government agencies. You are being tracked by each click that you make, information is being sent to third parties, you are being exposed to malicious or annoying ads, among many other threats [1]. The information that you have stored in your web browser and the personal data that you are passing through websites on the web browsers is what must be protected. In the world that we live in today, 69% of Americans have purchased something online which means they participated in online shopping which requires them to put in credit card information, logging into their banking and insurance portals/websites, which, if hacked while doing so, opens pandora's box [3].

There are a multitude of web browser security vulnerabilities that can be exploited and interrupt the user's browser experience. The top four common web browser vulnerabilities mentioned by Gergely Kalman, a chief technology officer (CTO) are injection flaws, broken authentication, cross site scripting (XSS), and insecure direct object references. The first vulnerability, injection flaws, is one not many daily users are familiar with. Injection flaws are an effect of a lack of filtering of untrusted input, and even in the case of trusted input you can never be 100% sure [4]. Everything has to be considered untrusted input because if not then you are more at risk of being exploited and it is better to be safe rather than sorry. The next most common web vulnerability is broken authentication. Broken authentication happens when in the process of proving the identity of a user, an interruption occurs. An interruption is when an attacker is able to divert or capture the authentication methods that are put into place. Weaknesses that open the door for interruption could be the use of plain text, encrypted, or weakly hashed passwords, ineffective or missing multi-factor authentication, the allowance of fragile, default, or common passwords, and the allowance of weak credential recovery processes [5]. Multi-factor authentication has taken online security processes by storm. Two-factor authentication is most common and while it does work against hackers trying to gain access to user accounts, if not correctly implemented it then becomes ineffective. In August 2016, the National Institute of Standards and Technology (NIST) withdrew its support of SMS based two-factor authentication because of its risk of SMS interception [6]. Any two-factor authentication process that contains SMS authentication puts users in danger because hackers do not need access to your physical cellular device to intercept the message that is sent. All hackers have to do now is gain access to your carrier account to do all the damage they want to do. An example of a weak credential recovery process is when you forget your password and you have to provide knowledge-based answers. Common knowledge-based questions are "what is your mother's maiden name?", "what was your first pet's name?", or "what was the name of your first elementary school?". Knowledge-based questions are ineffective and can lead to weaknesses due to the fact that there cannot be a guarantee that the person answering the questions are who they say that they are. The next vulnerability is cross site scripting (XSS). Cross site scripting happens when a hacker, or browser user with malicious intent uses a web application to send malicious code to another user's computer, or its the introduction of harmful script while loading a web application [7]. The last of the top four common web browser mistakes is having insecure direct object references (IDOR). Insecure direct object references can lead to vulnerabilities because users are provided with direct access to important items like files and database keys, and hackers can take the reference and cause damage [4]. Authorization is needed because of the direct access that is being provided to web browser users. If the process of authentication is interrupted by a hacker successfully, they now have the access to things that they should not and have the ability to perform actions they would not have been able to without authentication.

For the purpose of this study and using the given definition of security, we are going to look at what makes a browser secure. As a web browser user, you should expect a secure design, security features, regular updates, privacy protection, and usability. The design of a web browser is not just about the convenience, it is also about the security measures that are needed. A secure web browser design weaves security measures into the browser software architecture [8].

Browser architecture is made up of various components that work together to provide us with the complete product that we use every day. The main components that most web browsers have are a user interface, a browser engine and rendering engine, networking subsystems, a JavaScript interpreter, an Extensible Markup Language (XML) parser, a backend display subsystem, and a data persistence subsystem [9].

The user interface is the component that all web browser users see, it allows the user to interact with the browser engine and utilize all features that the browser has to offer. Under the user interface layer is the browser engine subsystem. Its functions include supporting browsing actions (back, forward, and refresh), provides the ability to view browsing session features (i.e. JavaScript alerts and page reload progress), and the ability to manipulate rendering engine settings [9].

The rendering engine can be thought of as a tokenizing system that also contains styling elements and images. It can display Hypertext Markup Language (HTML) and XML documents, includes the HTML parser, and works to continually adjust elements on webpages [9]. Next, we have the networking subsystem, which deals with the transferring of files and information over the network. In addition to that it translates between different character sets, resolves MME media types for files, and can implement a cache of recently retrieved resources [9].

The JavaScript interpreter component does exactly what the name implies that it does. JavaScript is an object-oriented programming language that aids in creating the extra functionality that web pages and browsers use. An example of how JavaScript is used in web browsers and pages are pop-up windows. The JavaScript interpreter "evaluates JavaScript code which may be embedded in web pages" [9].

The XML parser component is another component where the name says exactly what it does. XML documents need to be parsed so the information they contain can be as effective as possible. The documents are parsed into a "Document Object Model (DOM) tree" [9]. Lastly, we have the display backend and data persistence subsystems. The first of the two can be tied in with the operating system and deals with more functionality and styling elements (like fonts and interface widgets) [9]. The data persistence system deals with the "data associated with the browsing session on disk" [9]. The data in this system can be either high- or low-level data, the higher the level of data it does not necessarily contain personal private information, while low level data does. Low level data can be your security certificates, cache, or cookie data [9]. Browser architecture can be broken into two different types, monolithic and modular browser architecture. Monolithic browser architecture is the most common of the two types of browser architectures and all the browser "components are placed in a single operating system process" [10]. The word modular already tells you that some aspect of the architecture is isolated into different modules. The goal of the modular browser architecture is to "isolate web programs but provide compatibility with the current Web" [10].

Taking a step back from browser architecture and design, you should also expect to have a web browser that provides you with the ability to manipulate security and privacy features. As mentioned before, browser users must take actions themselves to increase the privacy and security of their web browser(s). Some advanced settings that browsers should offer to users, include the management of cookies and history, the ability to disable pop-ups and redirections, the power to turn off automatic downloads, and location, camera, and microphone usage restrictions [11]. All those features, if not managed correctly, could lead to vulnerabilities and exploitations which we have talked about earlier in the paper. Every web browser is not made equal, nor can they be made 100% safe and secure. The customization of privacy and security features allows for users to choose what is best for them based on their needs.

While web browser users are working to take actions to meet their needs, developers need to also be working simultaneously to provide software updates for any new security issues and threats that present themselves. Regular updates to the web browser software are the next thing that one should expect from a secure web browser. If regular updates are not happening or being provided, then there will be an increase in the number of security vulnerabilities. An up-to-date browser leads to increased security because due to timely deployment, software stability, and less testing of older versions with new third-party software just to name a few [12]. Hackers are constantly trying to find ways to exploit vulnerabilities, so developers are also working alongside those hackers. They should be working diligently to cut them off before they are successful at any new attack methods.

Privacy protection is just as important to web browsers as regular updates. Incognito mode is one way that users are able to keep their activity private. Incognito mode is advertised as an instance where history, cookies, and really all data is not saved therefore your online activity is private. Virtual Private Networks (VPNs) are another way that web browsers can keep online activity private. Some web browsers actually have built-in VPNs for users. To better understand why VPNs are an important tool to uphold activity privacy, think about when you stay at a hotel. Hotels usually offer complimentary WI-FI service to all guests, but the network is public. A private browser in this instance will not keep your information private from the hotel's service provider, but a VPN will create a virtual tunnel to shield your browsing data, or online activity [13]. VPNs are a tool that provides an extra layer of privacy and security for web browser users.

The last thing that all web browser users should expect from a secure web browser is usability. In the process of looking for a web browser to use, usability is something a user would be able to check off quickly. Usability is a "quality attribute that assesses how easy user interfaces are to use" [14]. Based on the definition of usability, how easy it is for a user to navigate a web browser would include things like speed, if it is visually appealing, practicality, or if it is glitchy. While usability does not necessarily have any direct correlation to web browser security, it is important in the development of software. Software usability involves "efficiency, effectiveness, and satisfaction" [15].

We now know what all web browsers should aim to be and why, but for a better grasp of the information presented we must apply it to seven of the most common browsers used today. We are going to take a look at how the browsers compare as it relates to privacy, speed, the last time the browser was hacked, the last time the browser was updated, etc.

The web browsers advertise to take their privacy seriously, compared to other browsers we are going to see how that holds up. Chrome, Firefox, Explorer, Edge, Safari, Opera, and Bing all have private browsing mode. Disparities begin when looking at if they block third-party tracking cookies by default, if they block crypto mining scripts, and if they block social trackers. Firefox is the only browser that takes precaution and performs all four of those actions. In this comparison Chrome comes out as the worst browser because it only does one of the four things, with Explorer being second worst because it only does two of four [16]. We have to dive deep into the privacy concerns using Google Chrome. Google Chrome is one of those web browsers that people are quick to use, and you would think that it would be the most secure due to the fact that it has so many daily users. Unfortunately, it is not. Google is said to be in the data sharing business, for example when logging into your Gmail account you are automatically syncing information into the browser itself and your browser is being tagged using cookies [17]. Earlier we talked about how web browsers are leaving features up to the user to take action. Chrome is open to all cookies by default and leaving the user in the dark if no research was done prior to use, while the other browsers listed have cookie tracking off by default [17]. Google is aware of how other browsers have handled the cookie problem and still defend their actions. In 2019, Chrome's then director of product management, Ben Galbraith said that "blunt cookie blocking solutions force tracking into more opaque practices" [17]. Saying that something is complicated does not mean taking no action and staying neutral by allowing cookie tracking is a good decision either. This could cause Chrome's reputation to plummet, if it hasn't already. Microsoft explorer as a whole is vulnerable so privacy on that browser will forever be an issue. Microsoft does not support Internet Explorer any longer and has warned current users that there is a critical vulnerability [18]. It does seem as though the web browsers whose parent company has a business that could profit from user data is a browser you can side eye. Bing happens to be one of those browsers, it is getting some of the flack similar to Chrome. Bing is not widely used but because it owns LinkedIn, and because LinkedIn's online ad division brings in so much revenue there can be an issue with trusting your private data in their browser [19].

Opera is another browser that does not have the best record in the category of browser privacy. Opera was sold to a Chinese consortium in 2016 which has led to privacy concerns [20]. It is pretty common knowledge about how China is a communist state and how they do not take privacy as a big issue. With Opera being sold to a Chinese consortium, users can ask how private their information really is when it's owned by country that does not even uphold citizen privacy. In the past, tech companies in China have been in the news for data sharing and privacy policy controversies [20]. In the conversation about browser privacy Safari's Intelligent Tracking Program (ITP) has caused quite the disagreement. Four Google researchers have listed five explicit attacks that have exploited ITP's design; this happened because the list created from ITP's algorithm can be used by websites to discover information about websites Safari users have visited [21]. Of course, Apple is in support of their program because they have built it. Apple and Google cannot agree on how to protect their users from cross site tracking, although ITP is more than what Google Chrome has implemented, which is nothing [21]. To wrap up the topic privacy in general, of the seven web browsers, it seems as though Mozilla's Firefox is the top option.

Security of those web browsers is another issue entirely. The vulnerabilities they possess have led to attacks even up until about two months ago. Again, Google Chrome has been one of the browsers at the forefront of web browser security issues. In an article written by Thomas Brewster, he talks about how Chrome has experienced 12 known zero-day attacks this year alone, and with a new update that rolled out in September of 2021 three vulnerabilities were patched [22]. The vulnerabilities are those that we have not already been mentioned. Two of the vulnerabilities that were mentioned were exploited. One of the weaknesses was an information leakage vulnerability rated medium in severity, while the other was a use after free flaw vulnerability rated high in severity [22]. It is important to note that although the list of zero-day attacks is at 12, it could also mean that researchers are catching the vulnerabilities before they are exploited. Safari has also had some security concerns as of recently. The browser was under attack in the past few months due to two bugs that were causing issues to WebKit, their rendering engine [23]. Safari experienced one of the same exploitations that Chrome experienced, a use after free flaw vulnerability exploitation. The important part, and the only thing that may invalidate the possible zero-day attacks on Safari are that "the bugs affect sixth-generation Apple iPhones, iPads, and iPod touch model hardware..." [23]. Opera's main security issue is different from Safari and Chrome in that it is due to a free service that it offers. Opera offers a built-in VPN service that could has a lower standard of security for various reasons [24].

One of the previous expectations mentioned of a secure web browser was usability. We can use this expectation to compare web browsers to look at speed, compatibility, tools, and conveniences. Michael Muchmore, a lead software analyst for software and web applications compared web browsers by conducting a variety of tests and assessing their usability [25]. He conducted a speed test, a memory use test, a storage use test, and a compatibility test using the HTML5test website, through the JetStream benchmark, and the task manager [25]. From his study, Chrome was found to be the most compatible with a score of 528 out of 555, Opera was close to Chrome, and Firefox and Safari were granted scores of 491 and 471 respectively. When it comes to speed, Chrome again won the race. It received the highest benchmark score on Windows 10, Safari of course won on macOS, and Firefox scored very low on both platforms [25]. For the storage test, Opera actually scored the lowest, which was good for that test. It is the "slimmest on both macOS and Windows 10" [25]. Lastly, for the memory use test Safari scored the highest. Muchmore says that some browsers use sleeping tabs, which are tabs whose content is removed from memory, and this could have skewed results [25]. Tools and conveniences are things that do not really affect the security or privacy of the browser, but they do aid in the usability. Some examples of tools and conveniences that set the browsers apart from each other include voice-reading of webpages, a built-in cryptocurrency wallet, a customizable homepage, and the ability to open a container to log into a site with two different identities just to name a few [25].

Overall, with the given information about web browsers in general and through comparison at least one conclusion can be made. What the research from this review has proven to be true is that Firefox should be a top option when looking for a secure and private web browser, while Chrome, regardless of its popularity should not even be a runner up. Web browser security and privacy is more than just browser history and cookies, you have to dig deeper into the design of the browser, the features, if there are regular updates, privacy protection, and usability. Security and privacy of web browsers should be valued by not only developers but browser users as well. Both have to take action to protect user data from hackers, websites, businesses, and government agencies. Web browser users specifically need to take the time to consider which browser is best for them and while usability is great, their privacy and security should take precedence.

B. *User Survey*

We will collect data from user of web browsers through conducting a survey. The purpose of the survey is to educate users as well as gain a better understanding of what web browsers are used the most among users, how much users of web browsers know about their cookies and history, and their experience with browser hacking. There will be an analysis of the findings from the survey along with the other sources of information to make conclusions and recommend possible solutions to issues mentioned in the thesis.

III. Results

The findings of the survey came out as predicted and had a total of 70 participants. Google Chrome was the most commonly used web browser with 78.6% of people saying they currently used it as their web browser, Safari followed up with 55.7%. As far as care for web browser security and privacy goes, 64.3% of the participants said that they cared a lot about their web browser security and privacy. When asked about downloading extensions and plug-ins, 58.6% of participants said that they have downloaded extensions and/or plug-ins before. While the majority of participants said that they have downloaded extensions and/or plug-ins before, a low majority of participants, 34.3%, said that they did not know that their extensions and plug-ins must be updated. Opposite of this, 31.4% stated that they have automatic updates enabled for their browsers with the second majority, 24.3%, stating that they did not know it must be updated. Of 34 out of 70 participants that said their browser had been hacked before, 21 reported using Google Chrome as their browser at the time that they were hacked.
When asked about cookies, 40% of participants stated that their cookie settings were set to allow all cookies. Half of the participants answered "whenever I feel like it" when asked how often they delete their browser history. To end the survey participants were asked what steps they take to secure their browser and 55.7% of participants answered saying that they block pop-ups with the next majority of 32.9% of people answering saying that they managed cookies and history.

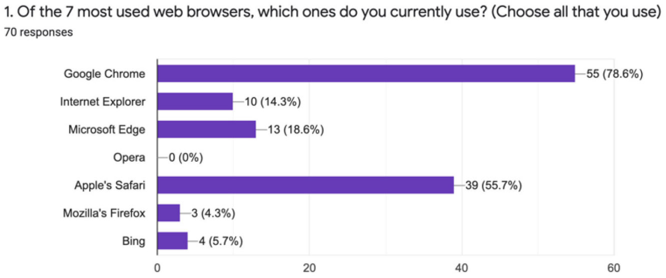


Figure 2: Web Browser Usage

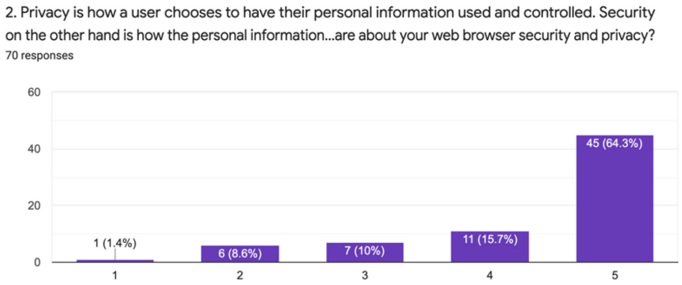
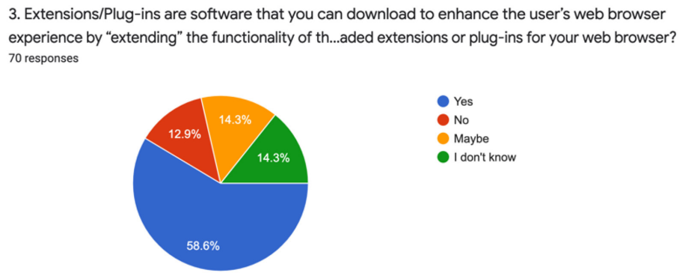
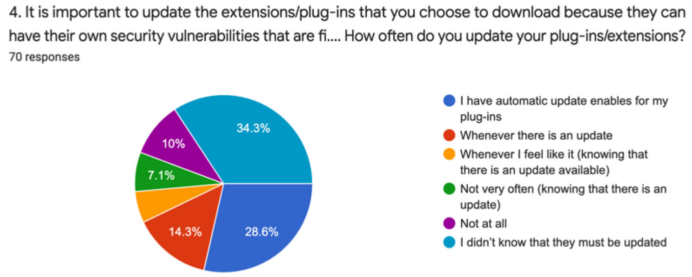


Figure 3: Privacy and Security


3. Extensions/Plug-ins are software that you can download to enhance the user's web browser experience by "extending" the functionality of th...aded extensions or plug-ins for your web browser?

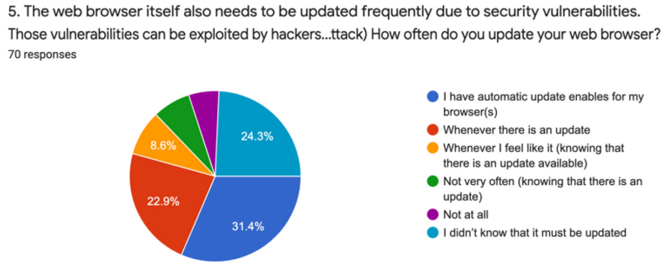
70 responses

Figure 4: Use of Extensions/Plug-ins


4. It is important to update the extensions/plug-ins that you choose to download because they can have their own security vulnerabilities that are fi.... How often do you update your plug-ins/extensions?

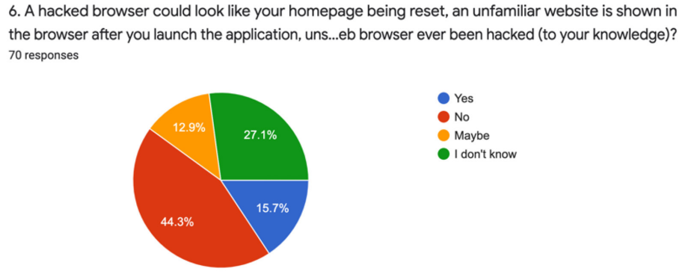
70 responses

Figure 5: Extensions/Plug-in Updates


5. The web browser itself also needs to be updated frequently due to security vulnerabilities. Those vulnerabilities can be exploited by hackers...ttack) How often do you update your web browser?

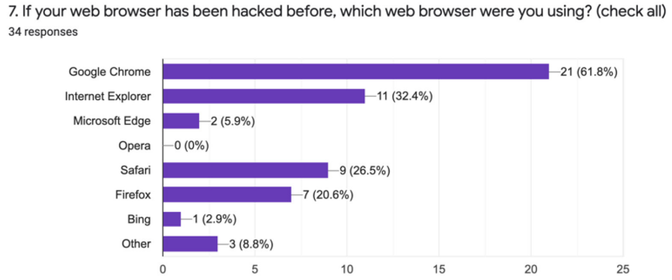
70 responses

Figure 6: Web Browser Updates


6. A hacked browser could look like your homepage being reset, an unfamiliar website is shown in the browser after you launch the application, uns...eb browser ever been hacked (to your knowledge)?

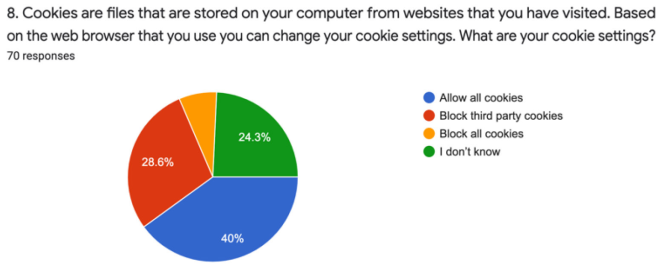
70 responses

Figure 7: Web Browser Hacking


7. If your web browser has been hacked before, which web browser were you using? (check all)

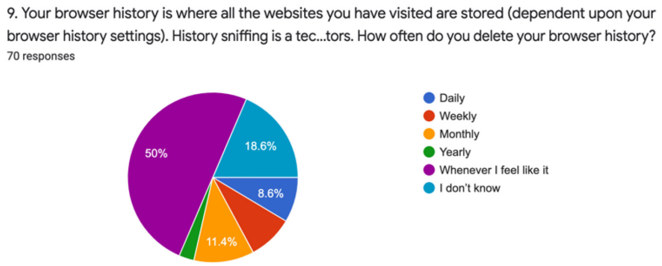
34 responses

Figure 8: Web Browsers Hacked


8. Cookies are files that are stored on your computer from websites that you have visited. Based on the web browser that you use you can change your cookie settings. What are your cookie settings?

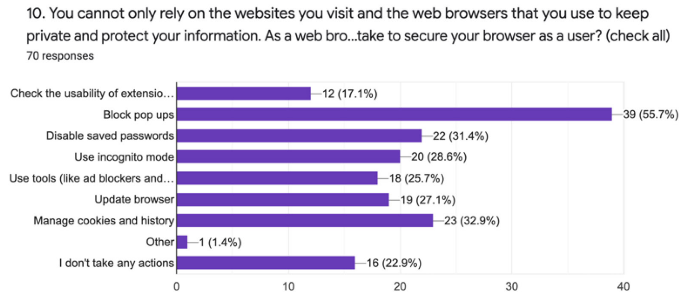
70 responses

Figure 9: Cookie Settings


9. Your browser history is where all the websites you have visited are stored (dependent upon your browser history settings). History sniffing is a tec...tors. How often do you delete your browser history?

70 responses

Figure 10: Browser History Management


10. You cannot only rely on the websites you visit and the web browsers that you use to keep private and protect your information. As a web bro...take to secure your browser as a user? (check all)

70 responses

Figure 11: User Actions

IV. Analysis

Most of the results came out as expected. Google Chrome and Safari being the highest web browsers was a prediction that could have been made, with Apple being the largest tech company and, as the literature review of this article stated, Google Chrome being the most used web browser. What came as a shock was that, even though an overwhelmingly large majority stated that they care about their web browser security and privacy, a majority also did not know that plug-ins and extensions needed to be updated which puts their browser at higher risk for being attacked. It would have been assumed that if a user cares about their browser security and privacy they would be more prone to updating their plug-ins and extensions.

Web browser users should download security browser extensions. Security browser extensions is a tool that has is recommended in most literature that talks about how to make a web browser more secure. On the other hand, though, users should make the decision to either disable extensions all together or do a little research into the extensions they use before using them. Extensions can possibly open the door to exploitations. Google at one point “removed dozens of extensions from its stores involved in information theft” [26]. Extensions expand on web browser functionalities so it is not necessarily logical to say extensions should be banned all together, but again users have to look into what they are choosing to use.

Following a similar narrative, Chrome being the most commonly hacked browser while also being the most used by participants is also a shocking statistic. This statistic shows that speed and popularity do not equal security as previous research has shown. The data also tells us that most chrome users secure their browser by blocking pop-ups and the majority of these same participants deleted their browser history whenever they felt like it. This statistic may tell us that lack of knowledge as to how to make your browser more secure and private leads to a more vulnerable browser with, in terms, leads to the browser getting hacked. With this statistic, the question is raised as to whether it is the user’s responsibility to make their browser more private and secure or if the responsibility relies solely on the web browser company.

Majority of the participants did say that they have automatic updates turned on for their web browsers. Although automatic updates make sure that the browser is being updated at the time a new update is released, sometime web browsers need to be restarted to make sure that it is updated fully. If the web browser is not updated often, bugs that could lead to vulnerabilities can lead to full blown exploitations, or functionality could be affected for better or worse. It is recommended that browser users check for updates frequently and as soon as you see that an update is available go ahead and start the process. Also, it is important to manually check because they might have to force an update.

When the participants of the survey were asked about their cookie settings. A little less than half of them said that they allow all cookies, which is not a good thing at all. Cookies can lead to vulnerability exploitations because not only are businesses using web browser users’ personal data, but also websites, and possibly hackers. Although browser users do not have to block all cookies, they can become a problem if the wrong person gets a hold of them, even if they are not trying to cause damage. It is all about privacy. When cookies are infected by malware, that malware stealing the cookie information is where the threat comes from [26]. Some websites do need cookies to provide the best services so it’s okay to allow some. It is recommended that users should take the time to manage their cookies to better protect themselves. Understand what cookies are, why they are needed, and make the executive decision for what is best for what you need in the situation.

One action that a user can take to further increase their web browser’s security and privacy is to use a sandbox. A sandbox is an application that “blocks software applications from accessing the hard disk” [26]. They are similar to virtual disks. A few sandbox environments, or software are VirtualBox, Sandboxie, and VMware Workstation Pro.

The main recommendation that there is from the research and survey results is that web browser users should try to look outside of the most popular options available. What I would consider a second tier of web browser options are Tor and Chromium. There are also private browsing options. In an article by Brian Chen, he tested out 3 different private browsers, DuckDuckGo, Brave, and Firefox Focus. Firefox Focus is a browser that is only available on mobile devices, which after you close the app the history is gone, and a database is relied on to know which websites to block [13]. The only con to this web browser is that it is only available on mobile devices, but it can also be a pro because of how much information is on most people’s mobile devices. The DuckDuckGo browser is the second private browser that was tested out, it is also only available on mobile devices, and it is more like a traditional browser [13]. It is very similar to Firefox Focus in that it also allows users the ability to erase the browsing session with the click of a button. The last private browser that was reviewed that people should consider is Brave. Brave is also like a traditional browser in that it has private mode and anti-tracking technology, it also almost blocks all ads [13]. The only thing with using private or less common web browsers are that some functionalities and website elements may not look or behave the same. Chen personally recommended that even if you do not make any of the private browsers your default browser, they can still be useful for things like sensitive web searches [13].

V. Conclusion

Security and privacy are amongst the main issues that are looked at when studying web browsers. The surveys and research of this article showed that while Google Chrome is the fastest and most popular web browser, it is not the most private and secure. While the results of the survey did not directly show a causation for FireFox being the most dependable browser, the outside research done within the literature review shows evidence for FireFox being the most dependable and secure web browser. Users who transition from Chrome to Firefox should see a change in increased privacy and trust in a web browser. For mobile app users, private browsers such as DuckDuckGo, Brave, or FireFox Focus are recommended for the most secure and private options. The survey results also help make an inference that the lack of knowledge of web browser users may lead to a likelihood of their browser getting hacked. Users do not have to switch web browsers if they are okay with the security and privacy of the browser they have chosen. It is recommended for web browser users to at least take the time to read up on the web browser(s) that they to choose to use. If they do that they will at least be aware of what happens every time they are using the web browser, as well as what they can do if they do not want to switch browsers. This does not exempt the browsers from doing their part in making sure that their browsers are as secure as possible for their users.

ACKNOWLEDGEMENTS

This work is partly supported by the National Science Foundation CyberCorps: Scholarship for Service program under grant award# 1754054.

References

[1] "Most Popular Web Browsers between 1995 and 2019 via Data is Beautiful," 4 September 2020. [Online]. Available: https://igguru.net/2020/09/04/most-popular-web-browsers-between-1995-and-2019-via-data-is-beautiful/. [Accessed December 2021].

[2] D. Bodnar, "What Is a Web Browser?," 28 January 2021. [Online]. Available: https://www.avast.com/c-what-is-a-web-browser#gref. [Accessed December 2021].

[3] M. Djordjevic, "26 Useful Statistics on Online Shopping vs in Store Shopping [The 2021 Edition]," 19 November 2021. [Online]. Available: https://savemycent.com/statistics-on-online-shopping-vs-in-store-shopping/. [Accessed December 2021].

[4] G. Kalman, "10 Most Common Web Security Vulnerabilities," 29 May 2014. [Online]. Available: https://www.toptal.com/security/10-most-common-web-security-vulnerabilities. [Accessed December 2021].

[5] D. Blazquez, "Broken Authentication," 9 October 2021. [Online]. Available: https://hdivsecurity.com/owasp-broken-authentication. [Accessed December 2021].

[6] R. Brandom, "Two-Factor Authentication Is A Mess," 10 July 2017. [Online]. Available: https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess. [Accessed December 2021].

[7] G. E. Rodriguez, J. G. Torres, P. Flores and D. E. Benavides, "Cross-site scripting (XSS) attacks and mitigation: A survey," *Computer Networks,* vol. 166, 15 January 2020.

[8] A. Grant, "Most Secure Web Browsers - 2021," 2021. [Online]. Available: https://bestvpn.org/best-secure-web-browsers/. [Accessed December 2021].

[9] A. Grosskurth and M. W. Godfrey, "A reference architecture for web browsers," in *Proceedings of the 21st IEEE International Conference on Software Maintenance*, 2005.

[10] M. Šilić,, J. Krolo and G. Delač, "Security Vulnerabilities in Modern Web Browser Architecture," in *33rd International Convention on Information and Communication Technology, Electronics and Microelectronics*, Rijeka, 2010.

[11] K. Aoki, "How to Increase Web Browser Security," 10 January 2020. [Online]. Available: https://www.lifewire.com/increase-web-browser-security-4767673. [Accessed December 2021].

[12] T. Duebendorder and S. Frei, "Why Silent Updates Boost Security," Zürich, 2009.

[13] B. X. Chen, "If You Care About Privacy, It's Time to Try a New Web Browser," 31 March 2021. [Online]. Available: https://www.nytimes.com/2021/03/31/technology/personaltech/online-privacy-private-browsers.html. [Accessed December 2021].

[14] J. Nielsen, "Usability 101: Introduction to Usability," 3 January 2012. [Online]. Available: https://www.nngroup.com/articles/usability-101-introduction-to-usability/. [Accessed December 2021].

[15] P. Martinez, "What is Software Usability and How to Do it Successfully," 25 September 202. [Online]. Available: https://mockitt.wondershare.com/ui-ux-design/software-usability.html. [Accessed December 2021].

[16] Mozilla, "Seven of the best browsers in direct comparison," 2020. [Online]. Available: https://www.mozilla.org/en-US/firefox/browsers/compare/. [Accessed December 2021].

[17] G. A. Fowler, "Goodbye, Chrome: Google's Web browser has become spy software," 21 June 2019. [Online]. Available: https://www.washingtonpost.com/technology/2019/06/21/google-chrome-has-become-surveillance-software-its-time-switch/. [Accessed December 2021].

[18] Komando Staff, "Still using Internet Explorer? Here's another reason to stop," 17 June 2021. [Online]. Available: https://www.komando.com/technology/stop-using-internet-explorer/793533/. [Accessed December 2021].

[19] L. Tung, "Best browser for privacy 2021: Secure web browsing," 25 May 2021. [Online]. Available: https://www.zdnet.com/article/best-browser-for-privacy/. [Accessed December 2021].

[20] M. Bizzaco, "Opera browser review," 5 July 2021. [Online]. Available: https://www.techradar.com/reviews/opera-browser. [Accessed December 2021].

[21] L. Tung, "Google to Apple: Safari's privacy feature actually opens iPhone users to tracking," 23 January 2020. [Online]. Available: https://www.zdnet.com/article/google-to-apple-safaris-privacy-feature-actually-opens-iphone-users-to-tracking/. [Accessed December 2021].

[22] T. Brewster, "Update Chrome Again: Google Confirms 12th Zero-Day Attack," 1 October 2021. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2021/10/01/google-chrome-updated-after-2-more-zero-day-hacks/?sh=bc0490cf4b31. [Accessed December 2021].

[23] T. Spring, "Apple Hurries Patches for Safari Bugs Under Active Attack," 15 June 2021. [Online]. Available: https://threatpost.com/apple-patch-safari-active-attack/166922/. [Accessed December 2021].

[24] P. Black, "Best browser for privacy," 27 September 2021. [Online]. Available: https://nordvpn.com/blog/best-privacy-browser/. [Accessed December 2021].

[25] M. Muchmore, "Chrome, Edge, Firefox, Opera, or Safari: Which Browser Is Best?," 20 May 2021. [Online]. Available: https://www.pcmag.com/picks/chrome-edge-firefox-opera-or-safari-which-browser-is-best. [Accessed December 2021].

[26] A. Patrizio, "10 tips for a secure browsing experience," 12 May 2020. [Online]. Available: idginsiderpro.com/article/3539828/10-tips-for-a-secure-browsing-experience.html. [Accessed December 2021].