The Importance of Web Browser Security and Privacy

Keseana Howard
Department of Computer Science
Hampton University
howard.ksa@gmail.com

Chutima Boonthum-Denecke
Department of Computer Science
Hampton University
chutima.boonthum@hamptonu.edu

ABSTRACT
Web Browsers have storage components and external software that aid in creating an enjoyable and functioning browser experience. Web browser history, cookies, ActiveX controls, and extensions all have vulnerabilities that are exploited by hackers, websites, and the web browsers themselves. Users are putting themselves at risk for an attack on their browser, possibly even their systems if they do not take the proper actions to secure their browser and keep their information private. This paper will discuss the aspects of the web browser named above, their security issues, and what can be done to stay protected.

KEYWORDS
ActiveX controls, cookies, vulnerabilities, exploit, web browser, plug-in, add-on, extension,

1 INTRODUCTION

Sir Timothy Berners-Lee, who is also the creator of the world wide web, wrote the first web browser in 1990, and it was released to the public in August of 1991 [1]. Web browsers were used from the very beginning of the world wide web. As of 2019, it was estimated that over 4 billion people worldwide use web browsers to access the web [2]. You can imagine this number has gone up, even just a little, due to the outbreak of the COVID-19 pandemic.

The use of web browsers comes with a few security and privacy aspects that need to be considered. Web browsers, depending on the setting you choose and what you allow to enhance the browser, could make you vulnerable to hackers. Or you could also be giving permission to websites to access some level of your personal information. There are ways to try to protect yourself against these hackers, but the first step is to understand the settings of the web browser. Then, from there you can decide on what settings and permissions are best for you and the information you want to protect.

Figure 1: Common web browsers [3]

2 WEB BROWSER SETTINGS

Web browser settings can include anything from session history, cookies. autofill (of passwords, addresses, and payment methods), and much more. For the purpose of this research when web browser settings are mentioned we are referring to cookies and site data, browsing history, add-ons (also known as plug-ins, or extensions), and ActiveX controls. In general, the right settings that protect the web browser user are those that allow the browser to be amnesic and provide usability concurrently [4]. Meaning the browser should be able to be used to complete the goals of the user but also does not store the total history.

2.1 Cookies

Cookies are files that are stored on your computer for individual websites and are designed to only be readable by the website that created them [5]. The only interaction most people have with cookies are when they visit a website, if they pay attention enough, to see a pop-up window asking for cookie permissions. In those instances, the website notifies you that it uses cookies, and either lets you choose the cookies you want to allow, or you say okay that you are accepting the use of cookies entirely. The process of how cookies work begins with a session identifier (part of a cookie) being generated when the client contacts the web server [6]. In simpler terms, the web browser is requesting a web page the web server. Next, the session identifier is sent back to the client web browser, stored as a cookie, and the text output of the requested web page is presented to the client [6]. The last part of the process is basically continuous as long as the session is still active. It consists of the web server(s) gradually collecting web page content [6].

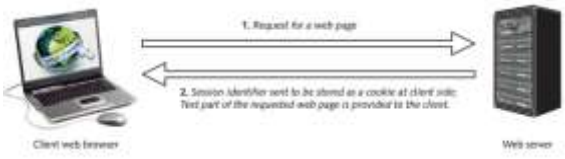


Figure 2. Illustration of how cookie process [6]

2.1.1 Types of Cookies. The first category of cookies has to do with their lifespan. Persistent cookies are "usually stored at the user side in the browser memory, outside of the users' browser control [6]. Meaning that the user does get the ability to access, delete or observe the cookies that were stored. Persistent cookies can last longer than a specified

session, but they also have an expiration date [6]. On the other hand, you have session cookies, also known as temporary or non-persistent cookies. They are subject to the session to which they were generated; they expire when the session expires, or when the web browser is closed. Session cookies are "usually stored in memory (cache) [6]. The second category of cookies have to do with the web server that they are set from. First party cookies are set by the first party server, while third-party cookies are set by third-party servers. Advertising companies are the ones who mainly use third-party cookies. Web pages that contain third-party content, provided by third-party providers, have their cookies received by the browser [6]. The third-party content on web pages mentioned, includes ads and images, which you have no control over. To better understand what third party content on a web page is, think about when you are on a website and you see gaming ads, social media ads, and images on the left and right of the screen. The content has nothing to do with the website that you are on, but in most cases, you cannot stop them from showing up.

2.1.2 Cookie Security. The three threats to cookies are identified as network threats, end-system threats, and cookie-harvesting threats [6]. Network threats occur because cookies are transmitted in clear-text and modified during transfer [6]. Clear-text is readable text, if someone unauthorized were to access the text they would not have to put in more work to decipher the text. Next, we have end-system threats, which deal with "forgery and impersonation of other users" [6]. Lastly, we have the cookie harvesting threat, which deals with sites specifically. It is the impersonation of a legitimate site to collect user cookies [6]. The confidentiality and integrity of cookies are two vulnerabilities when allowing cookies. When information is revealed to anyone except the web server cookie confidentiality is in play and cookie integrity is an issue when there are no security mechanisms in place to prevent unauthorized modification of cookie content [7].

Attacks that expose cookies themselves include cache sniffing and cross-site scripting (XSS) cookie sniffing. Cache sniffing is generally when an attacker gains access to the browser, therefore they can also access cookie content [6]. Cross-site scripting (XSS) cookie sniffing could cause the most damage of the two. With XSS cookie sniffing a web app is used to collect information from the user, allowing for user settings to be changed, account hijacking, false advertising, or cookie theft [6]. An XSS cookie sniffing attacker would not only gain information about a user but create other issues like open the user up to more vulnerabilities. In a XSS attack the client is not targeted directly, but vulnerabilities in a website that the client visits could be exploited and be used to distribute malicious code to the client's browser [8]. The last vulnerability or security concern is session hijacking. It is a web attack that takes advantage of active sessions, the main principle being computer sessions [8]. A session, in terms of cookies, is the time period when the web server and client web browser communicate. The moment communication is done or expires, the session is over. Prevention against session hacking is recommended to be done on the client side with up-to-date antivirus and anti-malware software [8].

2.2 Browsing History

Browsing history is essentially a list of websites that you have clicked on during your current web session and depending on your browser settings include websites from past sessions.

2.2.1 History Sniffing. History sniffing is a technique used by a website or browser to collect information based on the websites that you have been visiting [9]. History sniffing is more a matter of web browser privacy than security because a website would only need to go through your history for their own benefit. Most web browsers use colors when presenting websites from the search query, those unvisited are blue in color, and purple in color if they have been visited. The history sniffing is more than knowing what URLs are on your history list, it is a series of yes or no questions that are being asked to create a useful profile [9]. "Have you recently visited Amazon.com?", is an example of a question that would be asked. The process of asking possibly thousands of yes or no questions is done by a JavaScript program, so the inefficiency is unimportant also, the web server is unaware of the process happening [9]. Cascading Styling Sheets (CSS) use fonts, colors, backgrounds, etc. to make a web page visually appealing. The unvisited and visited website color variance, done using CSS, are features that were exploited to create the JavaScript programs for history sniffing [10].

2.2.2 History Protection. Two options found to protect browser history privacy, private browser use or clearing browser history. The first of the two, private browser use is a solution that could be problematic to a user because of its amnesic properties. When using a private browser local data like browsing history is not stored, thus making it impossible for websites to collect information using history sniffing [11]. It could be problematic because of the fact that history is never stored, you will never be able to go back and look at what websites you have previously visited if you needed to. Clearing your browser history "removes the data that history sniffing websites tend to query" [11]. With this option you are able to go back and look at previously visited websites before browsing history is deleted (dependent upon browser history settings). But websites will be able to collect information through history sniffing as long as the history has not been cleared. Another solution proposed was tasked to the browser providers themselves. Researchers at the University of California stated that "browsers should set explicit boundaries controlling how users' browsing histories are used to display web pages from different sites" [10]. Clicking on a link on one website has the possibility of changing the color (to purple, for a visited site) of a website link on another website. They are prototyping a fix that would fix this issue. The last option is a solution that browsers have been continuously working on. Updating your web browser to the current version could help protect your privacy; browser vendors have been working to fix the flaws that have been exploited by history sniffing [11].

2.3 Plug-ins, Extensions, and Add-Ons

The terms plug-ins, extensions, and add-ons are used interchangeably throughout most literature. They are third party applications used to enhance web browser capabilities.

2.3.1 Security Concerns. Concerns begin to arise with wanting to enhance the web browser. Some extensions "significantly alter the browsing experience", therefore updates and sometimes the lack of usability test by developers could cause the extension to be an issue [4]. Depending on the extension, updates could alter the browser to the point that it does not work or opens the browser up to more vulnerabilities than there would be without the extension. If a developer does not do a usability test on a product, which is a test to make sure the product is without complication, but instead just deploys the product to the public for use, the developer is not aware of any vulnerabilities, problems, etc. Another issue that comes up with using add-ons is buffer overflow or design flaws, like cross domain violations [5]. A cross domain violation attacker, if successful, would be able to "execute arbitrary commands on the vulnerable system" [5]. The commands that the attacker would be able to execute are commands that were not originally able to be performed on that system or website. The solution to all the concerns listed is to be careful of the type of plug-ins that you are using inside of the web browser. Because they are third party products, they too have their own vulnerabilities, regardless of the normal vulnerabilities of the browser itself.

Figure 3. Microsoft Edge Extensions [12]

2.4 ActiveX Controls

ActiveX Controls are like add-ons, in that they are used to expand the traditional browsing experience but where they are used is different. As far as web browsers go, ActiveX controls only function in Internet Explorer, outside of that they also work in applications like Microsoft Office [13]. Adobe flash is an ActiveX control that most people have interacted with at some point.

2.4.1 Security Concerns. Just like add-ons can cause the browser to be more vulnerable, ActiveX controls are no exception. The design of ActiveX controls themselves are unsecure, therefore not much can be done in moving to secure them [13]. ActiveX controls can already be installed on a Windows system. But it is strongly warned against the downloading of any unnecessary ActiveX controls, especially if the source cannot be trusted. Downloading more and more ActiveX controls "the more websites can take advantage of their problems to damage your computer" [13]. ActiveX controls vulnerabilities could not only affect the browser but the whole system, the security and privacy of more personal information, outside of the browser, could be at risk.

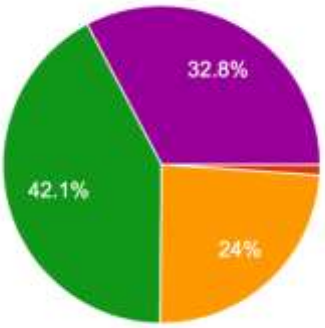
3 METHODOLOGY

A combination of literature and common knowledge were used to conduct a survey to collect data on the web browser use by individuals. The survey was distributed multiple ways, to get a range of answers, not from a specific group of people. It was posted on Facebook to be taken by family and friends, sent in two or three group chats (to immediate family), and sent in two GroupMe school group chats. The purpose of the survey was to understand what people knew about web browser settings (history, extensions, etc.) and if they did what were their settings for each one. Also, a better understanding of what were the web browsers and extensions most people used, and the reason for the latter. The survey was constructed using Google Forms and the responses were neatly organized into graphs and charts for analysis. It contained exactly 10 questions, with 1 optional question about ActiveX controls because of its specificity to Internet Explorer.

4 SURVEY RESULTS

The survey used 10 questions to draw a conclusion about how informed people are about their web browser settings, including cookies, browser history, ActiveX controls, and add-ons. Also, to draw conclusions about how informed they were increased because of the coronavirus pandemic. They were a total of 183 participants who completed the survey. The observation the researcher expected to see was that individuals did not clear their history often because they did not think it was important. The researcher also expected many people to allow the use of ActiveX controls because many people do not even know what they are, and because it is expected that many survey takers do not use Internet Explorer as much as other web browsers. Add-Ons, plug-ins, and extensions were expected to have lots of responses saying that they use them because of how often they are spoken of. There are commercials advertising the use of some extensions. Web browsers are used for pleasure just as much as business, which can be said about extensions also. On social media apps, kids of this generation are telling each other of extensions to add to their browsers that would aid in online schooling and help connect with friends all over the world. If a person said they clear their cookies and browser history often it is expected that they clear it about every month. The researcher used the survey to prove the importance of web browser privacy and security because of the lack of knowledge of the survey takers.

Total of responses (n = 186)

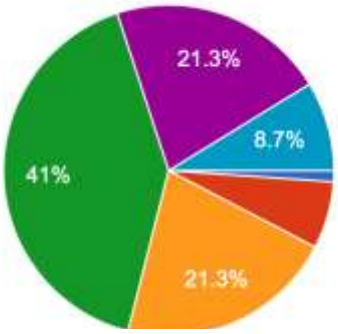


1. How old are you?

Under 12 years old	0	0%
12-17 years old	2	1.1%
18-24 years old	44	24%
25-49 years old	77	42.1%
50 years or older	60	32.8

Figure 4: Gauging survey taker age range

2. What would you say is your level of computer literacy?



Below level 1	2	1.1%
Fundamental Skills (level 1) - identify parts of a computer, turn computer on…	12	6.6%
Beginner (level 2) - recognize and save files in multiple formats, select the cor…	39	21.3%
Intermediate/Average (level 3) - locate and use accessibility features (ex: sti…	75	41%
Proficient (level 4) - technical User	39	21.3%
Advanced (level 5) - computing, applications, programming	16	8.7%

Figure 5: Level of computer literacy

3. What web browsers do you use?

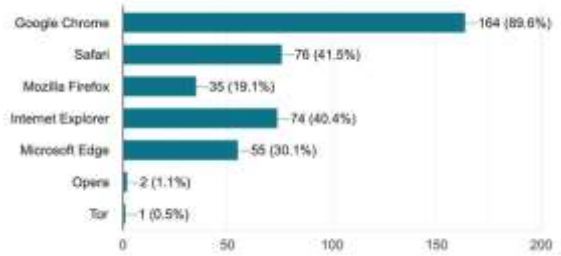
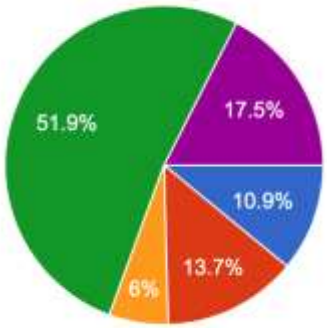


Figure 6: Use of particular web browsers. *Outside answers allowed*

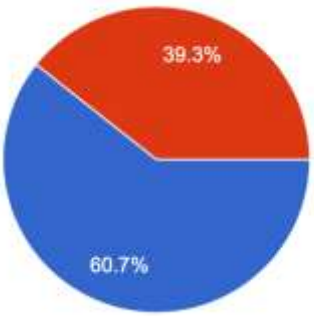
4. What are your cookie settings?



Allow all cookies	20	10.9%
Block third party cookies	25	13.7%
Block all cookies	11	6%
Allow cookies for certain websites	95	51.9%
I don't know	32	17.5%

Figure 7: Cookie Settings

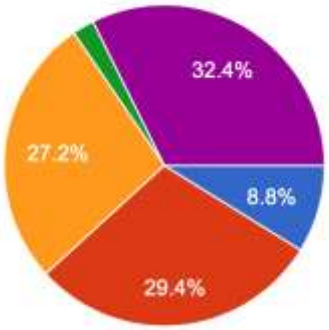
5. Do you clear your history and cookies often?



Yes	111	60.7%
No	72	39.3%

Figure 8: Clearing of cookie and browser history

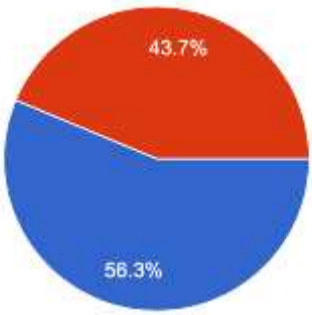
6. If so, how often?



Daily	12	8.8%
Weekly	40	29.4%
Monthly	37	27.3%
Yearly	3	2.2%
Whenever I feel like it	44	32.4%

Figure 9: How often cookie and browser history are cleared

7. Have you become more conscious of your web browser settings since being at home? (due to the Covid-19 pandemic)



Yes	103	56.3%
No	80	43.7%

Figure 9: Browser setting consciousness due to COVID-19 pandemic

8. What add-ons/extensions do you have installed for your web browser?

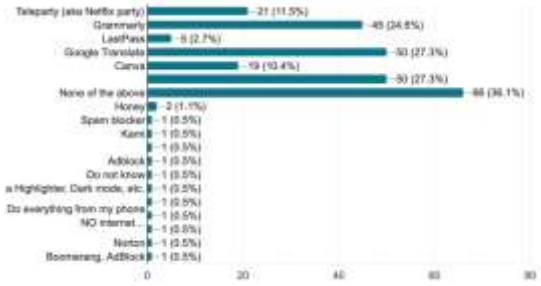
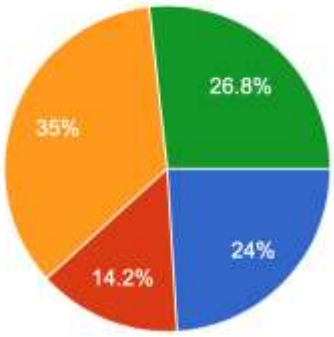


Figure 10: Most commonly used web browser extensions. *Outside answers allowed*

9. What classification would you say most of the add-ons/extensions you have fall under?



Business	44	24%
Pleasure	26	14.2%
It is half and half	64	35%
I don't have any	49	26.8%

Figure 11: Classification of web browser add-on

10. If you use Internet Explorer, do you allow the use of ActiveX controls (Internet Explorer specific add-ons)? (OPTIONAL)

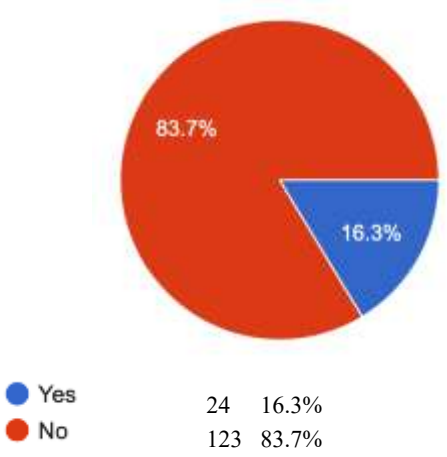


Figure 12: Permission to use ActiveX controls (if a user of Internet Explorer).

5 ANALYSIS OF RESULTS

Based on the results of question 1, it shows that the survey was taken mainly by people in the 25-49 age group. This is most likely due to the fact that it was sent out on Facebook (a social media app used for the most part by people 25 and older). I was not surprised to see that most people considered their level of computer literacy to be intermediate or average. This level included the ability to locate and use accessibility features (ex: sticky keys), save a compressed file, attach and use peripheral devices (ex: scanners, projection devices, memory storage devices), and view file properties. An everyday user of a computer, for work or school, would probably need to know how to do those things to be successful. Basic computer literacy and proficient computer literacy were the next largest groups, equaling 39 survey takers each.

Overall, questions besides those about computer literacy and age I was a little surprised at the results. It was expected that Google Chrome would have the highest percentage of users. 164 survey takers out of 183 said that they use Google Chrome (89.6%). Survey takers were able to type any other web browsers that they used, results showed that 1 person used a browser that was not listed, Tor. Results showed that people cleared their history and cookies often. I was surprised to see that 60.7% of the survey takers cleared their browser history and cookies often, that was way more than I had expected. The questions grouped both together so those that clear their history often but not their cookies could have said yes to the whole question and vice versa. I expected the history to be cleared often but not cookies, neither can be proven because of the way the question was asked. My expectation that browser history and cookies are cleared monthly was almost correct. Results show that most people clear their history and cookies whenever they feel like it, which is not the best decision supported by literature. Monthly clearance was the third largest percentage at 27.3%, behind weekly at 29.4%. I did not expect to see that most people did not use any of the extensions asked about because of how much I personally have seen them used and shared about. The people who did not use any of them accounted for only 66 of the 183 survey takers. Of the 117 left, the results show that many used more than one extension, either listed or one that they typed in themselves. The results of question 9 show that everyone who said they do use add-ons; half were for business and half were for pleasure. This was expected because of how the world has had to transition to virtual learning and working from home. When survey takers were asked did, they think that they were more conscious of their browser settings due to the pandemic, 56.3% said they were. This was not surprising due to the fact that people are on their computers more now than ever. The last question asked about the use of ActiveX controls. 83.7% said that they did not use ActiveX controls which supports what I expected. I can conclude that this means they are not downloading more ActiveX controls, which can be dangerous, neither are they using the ones that were preinstalled on their systems.

6 CONCLUSION

In summary, we have learned about browser history, ActiveX controls, cookies, and the use of plug-ins and conducted a survey to collect data. Having the knowledge about each aspect of the web browser makes all the difference in keeping your personal information private and your browser secure. Each item is used to create a better browser experience for the user, but in doing so vulnerabilities are liable to be exploited by hackers or information is not kept private. Web browser users should be aware of the problems or vulnerabilities that come with using each feature of a web browser that we have talked about. This is the first step to keeping your browser secure and private. Being informed about each feature allows the user to get a chance at making the right choice to protect their browser, information, and sometimes their system. Just telling web browser users what they should not do is not enough, it is best to also explain why that is. Based on the survey it was shown that a fair amount of people is taking some action to protect their browser and information, whatever the reason is. But a fair amount is not enough, the numbers should be higher. I believe that begins with staying informed.

Acknowledgements

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

REFERENCES

[1] "History of the Web," [Online]. Available: https://webfoundation.org/about/vision/history-of-the-web/. [Accessed 8 February 2021].

[2] I. Stevanovic, "22 Interesting Browser Statistics for 2020," 4 December 2019. [Online]. Available: https://kommandotech.com/statistics/browser-statistics/. [Accessed February 2021].

[3] "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 February 2021].

[4] K. M. Kern and E. Phetteplace, "Hardening the Browser," *Reference & User Service Quaterly,* vol. 51, no. 3, pp. 210-214, 2012.

[5] CyberSecurity & Infrastructure Security Agency, "Securing Your Web Browser," 8 September 2015. [Online]. Available: https://us-cert.cisa.gov/publications/securing-your-web-browser. [Accessed December 2020].

[6] R. Tirtea, C. Castelluccia and D. Ikonomou, "Bittersweet Cookies. Some security and privacy considerations," 2 February 2011. [Online]. Available: https://www.enisa.europa.eu/publications/copy_of_cookies. [Accessed February 2021].

[7] L. Wei-Bin, H.-B. Chen, S.-S. Chang and T.-H. Chen, "Secure and Efficient Protection for HTTP Cookies with Self-Verification," *International Journal of Communication Systems,* vol. 32, no. 2, pp. 1-10, 24 October 2018.

[8] Jithin, "What is Session Hijacking and how to prevent it?," 14 October 2016. [Online]. Available: https://www.interserver.net/tips/kb/session-hijacking%20prevent/. [Accessed February 2021].

[9] B. Hayes, "Computing Science: Uniquely Me!," *American Scientist,* vol. 102, no. 2, pp. 106-109, March 2014.

[10] University of California, "These new techniques expose your browsin history to attackers," 30 October 2018. [Online]. Available: https://techxplore.com/news/2018-10-techniques-expose-browsing-history.html. [Accessed February 2021].

[11] J. Zimmerman, "Snuffing Undisclosed History Sniffingq," 5 December 2012. [Online]. Available: https://www.consumer.ftc.gov/blog/2012/12/snuffing-undisclosed-history-sniffing. [Accessed February 2021].

[12] DevProblems, "Best Microsoft Edge extensions 2020 - Must-have browser add ons," 22 March 2020. [Online]. Available: https://www.devproblems.com/best-edge-extensions/. [Accessed February 2021].

[13] C. Hoffman, "What ActiveX Controls Are and Why They're Dangerous," 5 May 2013. [Online]. Available: https://www.howtogeek.com/162282/what-activex-controls-are-and-why-theyre-dangerous/. [Accessed February 2021].