MacOS versus Microsoft Windows: A Study on the Cybersecurity and Privacy User Perception of Two Popular Operating Systems

Cem Topcuoglu*, Andrea Martinez†, Abbas Acar†, Selcuk Uluagac†, and Engin Kirda*
*Northeastern University, †Florida International University

***Abstract*—Operating Systems (OSs) play a crucial role in shaping user perceptions of security and privacy. Yet, the distinct perception of different OS users received limited attention from security researchers. The two most dominant operating systems today are MacOS and Microsoft Windows. Although both operating systems contain advanced cybersecurity features that have made it more difficult for attackers to launch their attacks and compromise users, the folk wisdom suggests that users regard MacOS as being the more secure operating system among the two. However, this common belief regarding the comparison of these two operating systems, as well as the mental models behind it, have not been studied yet.**

In this paper, by conducting detailed surveys with a large number of MacOS and Windows users ($n = 208$) on Amazon Mechanical Turk, we aim to understand the differences in perception among MacOS and Windows users concerning the cybersecurity and privacy of these operating systems. Our results confirm the folk wisdom and show that many Windows and MacOS users indeed perceive MacOS as a more secure and private operating system compared to Windows, basing their belief on reputation rather than technical decisions. Additionally, we found that MacOS users often take fewer security measures, influenced by a strong confidence in their system's malware protection capabilities. Moreover, our analysis highlights the impact of the operating system's reputation and the primary OS used on users' perceptions of security and privacy. Finally, our qualitative analysis revealed many misconceptions such as being MacOS malware-proof. Overall, our findings suggest the need for more focused security training and OS improvements and show the shreds of evidence that the mental model of users in this regard is a vital process to predict new attack surfaces and propose usable solutions.

I. Introduction

The two most popular desktop operating systems (OSs) today are Microsoft Windows and Apple MacOS, together accounting for approximately 90% of all desktop users globally [27]. Historically, both operating systems have been an attractive attack surface. Ransomware, droppers, and trojan horses have been almost a permanent security problem and have caused much suffering over the years to operating system users. Although Microsoft did not sufficiently secure their systems in the initial versions of the Windows family from the 1990s until mid-2000 (e.g., there was no privilege separation and all operations ran under the administrator account), Windows has evolved to become a significantly more secure and reliable operating system today and is now much more difficult to remotely compromise compared to its earlier versions [4].

Discussions comparing the security and privacy of Windows and MacOS typically focus on two arguments [10], [36]. The first argument is that MacOS has a smaller user base and thus, fewer incentives to attack the OS [10], [36]. While historically, the smaller deployment of MacOS did provide its users a degree of protection against widespread threats, with the increasing popularity of MacOS, attackers started to focus more on this operating system and its users. Indeed, the number of malware instances for MacOS not only rose but even outpaced Windows by detections per endpoint [17]. The second argument is that MacOS, being a UNIX-based OS, is inherently more secure than Windows [36]. While this might have held for earlier versions of Windows, but not necessarily for the modern versions. Many modern and cutting-edge cybersecurity mechanisms have been integrated into Windows that were not contained in the original UNIX OS. Regardless of security architectures and mechanisms inherent to each of these OSs, the attack surface for both OSs is continuously evolving and attackers are increasingly deploying OS-agnostic methods such as web-based and social engineering attacks, targeting users across both platforms. In this shifting threat landscape, user awareness consistently remains a crucial, yet often overlooked, defense point. A recent survey showed that many MacOS users harbor misconceptions and engage in risky behaviors [21]. For instance, a significant portion mistakenly believes malware does not exist for MacOS, while others reuse passwords or skip software updates. Therefore, it's essential to understand the security perceptions of users for each OS.

While prior research has extensively addressed technical security aspects of both Windows and MacOS [14], [38], [11], [22], and some have probed users' mental models concerning security tools and threats [31], [9], [34], a noticeable research gap exists in the comparative study of MacOS and Windows user perceptions. This is surprising given the dominance of these two OSs in today's desktop usage [28]. In this work, we fill this research gap and primarily focus on the user perception of the current security and privacy posture of the two most popular operating systems [28]. We provide an empirical analysis of the determinants of the users' perception and study how users evaluate their operating systems, highlighting the importance of user education with respect to operating systems security. Specifically, we aim to understand which

Symposium on Usable Security and Privacy (USEC) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-5-2
https://dx.doi.org/10.14722/usec.2024.23052
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

OS – MacOS or Windows – is perceived as more secure and private by users and explore the implications of these perceptions in terms of the security and privacy behaviors of the users.

We conducted a series of surveys on Amazon Mechanical Turk, focusing on the 18-49 age group who possessed at least some college-level education. According to existing literature [25], the results of security and privacy surveys conducted on this group have been shown to be representative of the U.S. population within the same group. We recruited 103 MacOS and 105 Windows users and applied rigorous statistical analysis to gain a deeper understanding of how users perceive the cybersecurity and privacy of MacOS and Windows when the operating systems are compared. We asked how they compare these two operating systems in terms of cybersecurity, privacy, and reputation. We also investigated if these different operating systems users demonstrate different behavior patterns (i.e., if there is a statistically significant difference between the security best practices such as antivirus usage). Understanding these differences can shed light on the user mental model and what the users expect from their operating system, which can help us build operating system features that match users' expectations. Furthermore, we can determine trends, predict potential new attack surfaces, and propose actionable recommendations.

In summary, our research confirms that the perception of MacOS as a more secure and private operating system is widespread, although the nature of attacks and operating system security has significantly evolved. Despite all the progress made in the security of the Windows operating system, many users, including Windows users, still believe that MacOS is a much more secure operating system. A large number of users based their choice to the reputation and technology of these OSes and have biased beliefs such as "MacOS is malware proof", and "It is rare to hear about a MacOS device having a virus or malware on it". One of the participants stated that "It has nothing to do with the company, but simply the fact that most hackers design programs to disrupt Windows than Mac", similar to the current Internet discussions. This image of OS security can have an impact on less sophisticated users. That is, these users are left with the illusion that their operating system is responsible for every security and privacy task. This is also reflected in the security behavior of users; we found that users of the two operating systems show statistically significant differences in their antivirus usage, data backup habits, and behaviors related to covering the camera lens. This work also serves to provide insights into the importance of user education and awareness of newer forms of attacks that are agnostic to the type of operating system and can cause irreversible damage to users on almost any platform.

The main contributions of this study are as follows:

- We conducted the first study that analyzes the user perception with respect to the security and privacy of the two most popular desktop operating systems. We analyzed which operating system provides perceived cybersecurity and privacy with a series of surveys on Amazon Mechanical Turk.
- Our quantitative analysis reveals statistically significant differences in two areas: 1) how MacOS and Windows users perceive cybersecurity and privacy; and 2) how these users view the reputations of Apple and Microsoft. Conversely, we determined that demographic features do not have any statistically significant influence on how users perceive the cybersecurity and privacy of their respective OSs.
- We found a statistically significant relationship between being an IT worker and the perceived cybersecurity and privacy comparison of MacOS and Windows, as well as security habits such as performing backups, covering the camera lens of the computer, and using the private mode of the browser.
- We also observed that there is a significant correlation between a user's primary OS and their proactive cybersecurity practices such as utilizing antivirus (AV) software, performing backups, and covering the lens of the computer camera. This perception may lead to a more relaxed assumption about necessary security risks among MacOS users, indicating the need for targeted cybersecurity education.
- Through qualitative analysis, we also uncovered the reasons behind these perceptions and the common misconceptions held by users.

The rest of the paper is organized as follows: Section II describes related work. Section III discusses our methodology. Section IV presents and discusses the results. Section VI discusses the limitations of our work. Section V summarizes our findings and actionable results. Finally, Section VII concludes the paper.

II. Related Work

A. Security and Privacy of Desktop OSs

In the literature, a huge body of research is devoted to Windows computers [15]. Some research papers, though they did not specify the target malware, worked on PE malware that only runs on Windows computers [33], [37] or studied vulnerabilities that exploit Windows computers [24]. On the other hand, researchers also investigated malware targeting MacOS [14], [38], [11], [22]. Lindorfer et al. built a high interaction honeypot capable of automatically downloading OS X binaries [14] while other works targeted the MacOS kernel [38], [11]. Finally, Adam J. O'dOnnell examined why malware attacks might occur on MacOS, and introduced a model on game theory to predict when the malware attacks will increase on MacOS [22]. However, none of these studies investigates the user perception of different OS users.

B. User Perception on Security and Privacy

There has been research that has investigated the perception of users with respect to security and privacy issues from various angles. The first category focuses on the web domain. Turner et al. investigated factors that affect the perception of security and privacy in e-commerce websites [31]. The paper reports that consumers are mainly interested in company reputation, past experiences, and security recommendations from third parties. Moreover, Flinn et al. investigated the security and privacy perception on the web [9]. The second category focused on the security tools such as anti-virus scanners. For

example, Rick Wash presents an analysis of the mental models of users about attackers and security technologies such as anti-virus scanners [34]. The paper reports that every MacOS user believes that their system is immune to viruses and hacking problems and that some users do not use security software because of perceived immunity. The paper only performs a qualitative analysis, and the number of participants is limited to 14. The third category of work is on mobile users. Researchers compared the threats for Android and iOS users [20], [1] while Benenson et al. compared the user behaviors of Android and iOS users concerning security and privacy issues [5]. In another work, Falaki et al. studied application usage in terms of reducing the energy consumption of Android and Windows phone users [8]. In addition, Benenson et al. studied the mental models of smartphone users towards IT security, and found that the users with good security knowledge tend to use additional technical protection means [6]. Finally, Chin et al. studied user confidence in smartphone security and privacy, and looked into the security and privacy perception on smartphones when compared to desktop computers [7]. Interestingly, while this study also recruited MacOS and Windows users, it used computer users as a baseline to discover smartphone-specific issues but did not delve into the issues regarding MacOS and Windows users. However, none of these studies worked on the security and privacy perception of MacOS and Windows users.

To the best of our knowledge, no prior work has attempted to study the differences in cybersecurity and privacy perceptions of users with regard to the popular MacOS and Windows operating systems. A number of works have paid attention to the merits of performing surveys on Amazon Mechanical Turk, and how representative and generalizable the collected data is. Many recent studies, including [12] and [25], have leveraged Amazon Mechanical Turk for survey research. Redmiles et al. highlighted its utility for capturing a U.S. representative demographic in security and privacy contexts [25].

III. Methodology

Proper sample selection is crucial in online surveys to achieve valid results [3], [29]. We utilized the Amazon Mechanical Turk platform, a crowd-sourcing marketplace [2]. Recent research has determined that Amazon Mechanical Turk is representative of the U.S. population (between the ages 18 and 49 with some degree of college education) with respect to privacy and security topics [25]. Hence, in our survey, we focused on this group. To make sure that our survey data was of high quality, we selected HIT approval rates greater than or equal to 95%. Also, we recruited participants who are located in the United States. For our main survey, we compensated the participants with $1 for well under 10 minutes. We conducted our study between December 2020 and March 2021.

Online surveys have five main advantages: They are easy to prepare, easy to answer, they help avoid desirability bias, they allow to make sure that surveyees are receiving the same set of questions in the same regard, and there is no time constraint for users [3], [29]. At the same time, there is one important disadvantage as well: The lack of an interviewer [3], [29] who can register user reactions and clarify misunderstandings. Hence, we tried to create easy-to-follow text and directives. Furthermore, we kept our survey as simple as possible, and we conducted preliminary experiments to improve our survey quality. To make sure our survey is reliable, we used a two-fold survey structure. In the first survey, we collected demographics and primarily used OS information. By collecting this information from the user, we were able to verify if there were discrepancies between the first and second survey that was focused on cybersecurity and privacy perceptions. We eliminated the surveyee from our analysis if the answers to some questions between the two surveys did not match. Also, we made sure that every Amazon Mechanical Turk user participated in our surveys only once.

IRB approval: Our methodology and survey questions have been submitted to our institution's IRB board, and we obtained IRB approval. Our work was exempted under category #2 by the Human Subject Research Protection department, as we did not collect any sensitive or personally identifiable information from participants and all the participants were anonymous to us. Participants were shown a consent form to inform them about our research. We only accepted participants who were 18 years old or older.

A. Model

We crafted two different regression models before designing our survey. In the first model, we investigated the relationship between the primarily used OS and the perception of which OS (i.e., MacOS or Windows) provides more cybersecurity and privacy. In the second model, we investigated the relationship between primarily used OS and some cybersecurity precautions such as AV software usage. Upon forging the initial regressions, we developed upon it and added independent variables that were likely to be related to the dependent variable. By adding these new independent variables, we aimed to minimize the bias on the primarily used OS variable. Hence, we concluded with two different multiple regression models. Note that all regression models were crafted before we conducted our surveys.

In the first model, the first independent variable is the primarily used OS. The key insight here is that the primarily used OS might be a strong driver for the cybersecurity and privacy perception of that OS. That is, the frequent usage of the OS might create an attachment to that OS (i.e., familiarity). Or, the user might have chosen to use that OS because it has been mandated by work, or because of price reasons. We also added a variable that we call the "desired" OS. This variable is collected by asking users which operating system they would use if they were not constrained by price or their job – that is, we try to capture the "wish" OS of the user. The second and third variables in our model are the perceived reputations of Microsoft and Apple in cybersecurity and privacy. The key insight here is that we believe the perceived reputation represents hearsay information, advertisement power, historical events, and former experiences with the OS. Also, reputation is one of the key factors in the perception of cybersecurity and privacy [31]. The fourth variable, IT, is whether the surveyee works in an Information Technology (IT) or cybersecurity-related job. By using this variable, we aim to measure if the surveyee is knowledgeable in cybersecurity. Clearly, the cybersecurity knowledge a user has can affect her perception and understanding of cybersecurity. The fifth variable in our model is the level of daily computer usage (i.e., experience with computers). We also hypothesize that demographic factors

might affect the security and privacy perception. Previous work also studied the effect of demographics on security perception and found a significant relationship [13]. Hence, finally, we added age, education, and gender variables. To investigate the effect of eight independent variables on the dependent variable that indicates which OS provides more cybersecurity and privacy, we designed the following equation:

$$\begin{aligned} OS\_Comparison = \beta_0 + \beta_1 OS\_or\_Desired\_OS + \\ \beta_2 MS\_Perceived\_Rep. + \\ \beta_3 Apple\_Perceived\_Rep. + \\ \beta_4 IT + \beta_5 Daily\_Computer\_Usage + \\ \beta_6 Age + \beta_7 Education + \beta_8 Gender + \epsilon \end{aligned} \quad (1)$$

In the second model, our independent variable is the primarily used OS. We believe the primarily used OS might be related to cybersecurity behavior. We used four different dependent variables that we dubbed as the cybersecurity behavior variable. Our dependent variables are whether AV software is being used, if data is being backed up regularly, if the user's computer camera lens is covered, and how often the user uses the privacy mode of her browser. By asking for these cybersecurity precautions, we aim to determine behavioral differences between the users of these two OSes. Since we have four different dependent variables, we have four different equations for each precaution. For each dependent variable, we added the IT and daily computer usage variables. Similar to the first equation, we believe, these could be related to cybersecurity behavior. Moreover, we controlled the demographic features such as age, education, and gender as well. Hence, in order to understand whether cybersecurity behavior changes are related to the primarily used OS, we derived the following equation:

$$\begin{aligned} Cybersecurity\_Behavior = \beta_0 + \beta_1 OS + \\ \beta_2 IT + \beta_3 Daily\_Computer\_Usage + \\ \beta_4 Age + \beta_5 Education + \beta_6 Gender + \epsilon \end{aligned} \quad (2)$$

By crafting these regression models, we aim to understand the underlying factors that influence users' perceptions and behaviors concerning cybersecurity and privacy across the two major OS platforms.

B. Survey

Study Design: We conducted our study in two batches: a preliminary and a main survey. In the preliminary survey, our goal was to gather data to identify workers who fit our criteria, as mentioned above. Specifically, we looked at the primarily used OS, the age of the participant, and education information. For the primary OS used, we accepted textual input in the event that a participant's primary OS was not MacOS or Windows. Upon collection of this data, we selected all MacOS and Windows users who were aged between 18 and 49, with at least some college-level education. Then, we assigned these participants qualifications on Amazon Mechanical Turk so that they could participate in our main survey. We set a target number of participants around 100 for both groups.

Preliminary Findings and Modifications: To keep our study simple and understandable, we conducted trials on Amazon Mechanical Turk and among some of our colleagues. The initial results of these trials showed that surveyees were in favor of the MacOS both in terms of providing more cybersecurity and privacy. Note that Apple MacOS users had a stronger opinion about their OS when we compared it with Windows users. After these trials, we decided to make three changes. First, we made operating system names explanatory to avoid confusion such as using 'Apple MacOS' instead of 'MacOS'. Second, we explicitly defined the terms cybersecurity and privacy at the start of our survey.

Survey Content: Our survey starts with background questions about daily computer usage and computer-related job experience. Then, we try to get an idea of backup behavior, physical security behavior, web privacy behavior, and usage of software security programs. Hence, we asked about AV software usage, frequency of performed backups, frequency of the private mode of the browser, and whether the participant covers the webcam with a physical cover to gain a basic understanding of how secure and privacy-aware the participant is. We selected these four questions which are the subset of the recommendations for laptop security [26], [19]. Our aim was to investigate if there is a relationship between the primarily used OS and these behaviors.

Perception Queries: We also asked the participants questions about their perception of the reputation of Apple and Microsoft with respect to cybersecurity and privacy, and which operating system they mainly use. Furthermore, we directly asked the participants which operating system they believe cares more about cybersecurity and privacy in general. We gave the participants a 7-point Likert scale that they could use to evaluate both operating systems. We chose a 7-point Likert scale to give more freedom to evaluate the level of confidence while comparing the operating systems.

Quantitative and Qualitative Analysis: As we described in Section III-A, we crafted detailed regression models. Then, we used R language [23] to conduct the quantitative analysis. Although our analysis was mostly based on quantitative analysis, we also posed some qualitative questions to distill a better understanding of the participants' thoughts and expressions. For example, we asked why the participants believed that the specific operating system they chose offered more cybersecurity or privacy, and collected textual feedback. We used thematic analysis [32], a process that involves reading through a collection of data and searching for patterns in the data to identify themes to process these qualitative questions. We created a spreadsheet from the analysis of the open-ended questions and imported the spreadsheet into Nvivo, a qualitative data analysis software [16], where we analyzed the data and created codes by using inductive coding, an approach where codes are created from the data itself [18]. Then, we proceeded to categorize the codes into themes, again by using an inductive approach, allowing us to derive meaningful patterns from the coded data.

Finally, we collected demographic information at the end of the survey. The full list of the survey questions is in Appendix A.

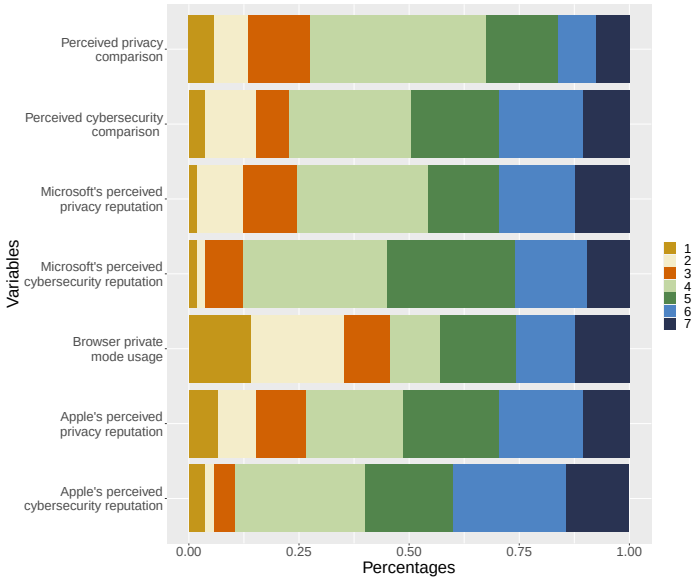

Fig. 1. Only Windows users. Normalized responses to Likert scale survey questions. For rows 1 and 2, the scale ranged from Extremely Windows to Extremely MacOS. For rows 3, 4, 6, and 7, the scale ranged from Poor Cybersecurity or Privacy to Excellent Cybersecurity or Privacy. For row 5, the scale ranged from Never to Always. Only related rows should be compared.

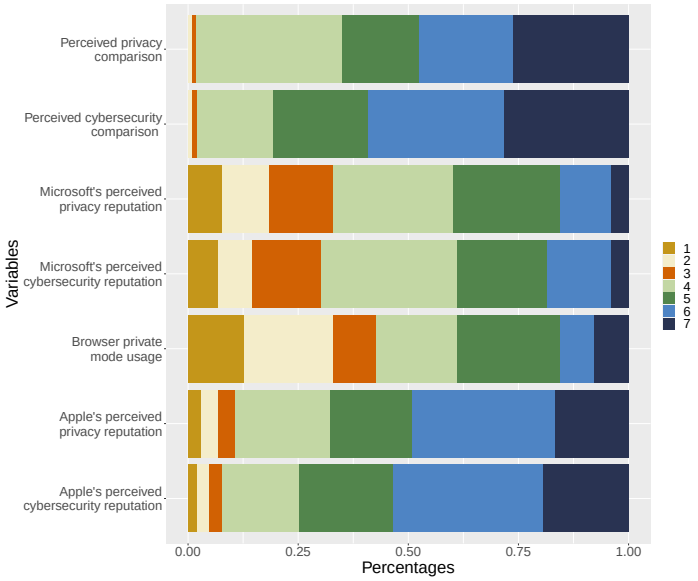

Fig. 2. Only MacOS users. Normalized responses to Likert scale survey questions. For rows 1 and 2, the scale ranged from Extremely Windows to Extremely MacOS. For rows 3, 4, 6, and 7, the scale ranged from Poor Cybersecurity or Privacy to Excellent Cybersecurity or Privacy. For row 5, the scale ranged from Never to Always. Only related rows should be compared.

C. Participant Data

Preliminary Survey: In total, we recruited 1,974 participants in the preliminary survey. The distribution of primarily-used operating system information for these participants is as follows: 70% of the participants were using Microsoft Windows, 16% were using Chrome OS, 13% were using Apple MacOS, and 1% were using Linux. After collecting this information, we selected the Amazon Mechanical Turk workers for our main survey as we described in Section III-B.

Main Survey: At the end of our main survey, we had 211 participants who met our selection criteria. However, we eliminated some of the surveyees since they had discrepancies in their responses to the first and second surveys. By excluding these data points, we collected survey data for 103 unique MacOS and 105 unique Windows users. In Section IV, we statistically investigate the collected data.

Gender, Education, and Age: Our population is almost balanced based on gender. That is, there are 114 female (55%) and 90 male (43%) participants. Most of our surveyees had a bachelor's degree (50%). Also, most of the participants were in between of 30 and 39. 91 of the participants were between the ages of 30 and 39 (44%). Detailed demographics statistics presented in Table I.

Computer Usage: Table I also presents the results for computer usage. The majority of our participants are heavy computer users which aligns with our expectations since we conducted our survey on Amazon Mechanical Turk. Also, 35 surveyees (17%) reported that they work in an IT or cybersecurity-related job. Among those 35, 21 were Windows, and 14 were MacOS users.

Reputation Perceptions: Figures 1 and 2 present the normalized results to reputation perception questions for each

TABLE I. DETAILED DEMOGRAPHIC STATISTICS

Age	MacOS	Windows	Total
18-24	12	7	19
25-29	30	27	57
30-39	44	47	91
40-49	17	24	41
Gender			
Female	62	52	114
Male	39	51	90
Prefer not to say	2	2	4
Education			
Associate degree	7	11	18
Bachelor's degree	52	53	105
Master's degree	29	22	51
Ph.D. degree or higher	3	2	5
Some college education	12	17	29
Computer Usage			
Less than 1 hour	2	0	2
From 1 up to 4 hours	15	19	34
From 4 up to 8 hours	55	31	86
From 8 up to 12 hours	26	44	70
12 hours or more	5	11	16

OS users. As depicted, for Microsoft's perceived privacy and cybersecurity reputation variables, Windows users tend to give higher scores compared to MacOS users. MacOS users tend to believe that Windows provides neither perfect nor poor cybersecurity – with a slight tendency towards thinking more positively about this issue. The situation is reversed for Apple's perceived privacy and cybersecurity reputation variables, where MacOS user responses concentrated more on higher scores. Almost half of the MacOS users score Apple's reputation as 6 or 7 on the Likert scale. Overall, MacOS users tend to be neutral on the privacy reputation of Microsoft, while Windows users have a positive opinion about Apple's privacy reputation.

Private Mode Usage: Figures 1 and 2 present the normalized results to browser private mode usage question. MacOS users tend to accumulate around the middle, while Windows users' scores to be either higher or lower. Also, 33% of the MacOS users reported that they are not using AV software, 15% reported they do not back up their data at all, and 64% stated that they do not cover the lens of their computer camera. Among Windows users, 12% reported that they are not using AV, 24% stated that they do not back up their data, and 45% stated that they are not covering the lens of their computer camera. Perhaps unsurprisingly, Windows users tended to be more cautious when it came to malware protection, and attacks that malware could launch such as recording video from the camera of the computer.

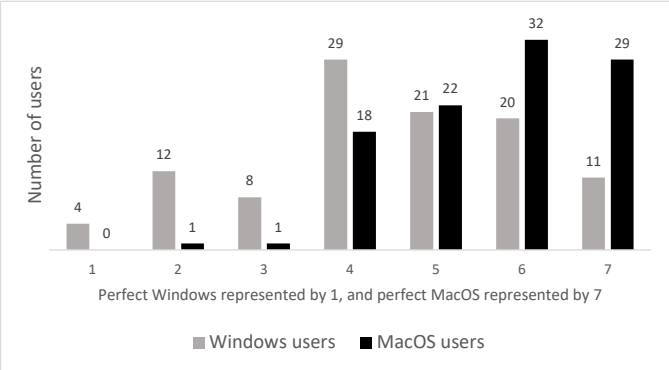

Fig. 3. Results to the question of which OS offers more cybersecurity.

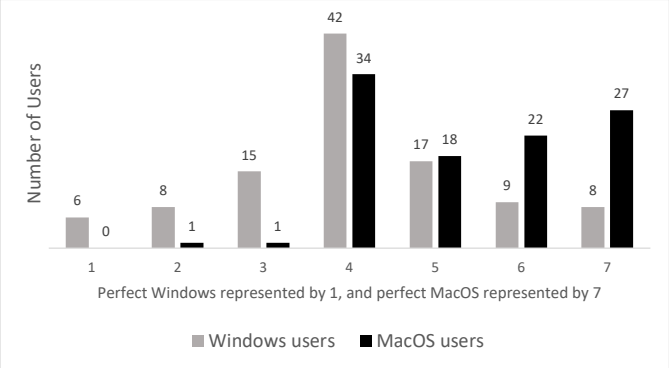

Fig. 4. Results to the question of which OS cares more about privacy.

IV. Results and Discussion

In this section, we describe the statistical analysis of our results. Figure 3 shows the surveyee responses to whether Windows or MacOS provides more cybersecurity. Perhaps unsurprisingly and confirming the folk wisdom, the majority of the MacOS users (i.e., more than 80%) believed that MacOS offers more cybersecurity than Windows. For Windows users, the majority of the users perceived MacOS to be better than or equal to Windows (i.e., 77%). In fact, almost half (i.e., 49%) of the users tend to believe that MacOS is better than Windows when it comes to cybersecurity. Our results suggest that, as perhaps many people would expect, MacOS users seem to have more sympathy and appreciation for their OS. MacOS users were more enthusiastic when it came to ranking their OS as being extremely better than Windows in contrast to the Windows users who were judging their own OS.

Figure 4 depicts the surveyee responses to whether Windows or MacOS cares more about user privacy. The majority of the MacOS users (i.e., 65%) believed that MacOS doing a better job in securing user privacy than Windows. In contrast, 28% of the Windows users did not believe that MacOS was doing a better job in securing user privacy when compared to Windows. Many Windows users were neutral, and tend to believe that there is not a major difference in privacy between MacOS and Windows (i.e., 40%). 32% of the Windows users in our study had the belief that MacOS was doing a better job in privacy when compared to Windows – a significant number.

Figures 1 and 2 present normalized results for MacOS and Windows with respect to what users perceive about their cybersecurity and privacy. The results show that both MacOS and Windows users tend to believe that MacOS is provides more than Windows when it comes to cybersecurity and privacy. Almost all of the MacOS users perceive their OS at least as good as Windows – most of them think MacOS is better. Windows users also share this sentiment, although not as strongly as MacOS users.

We also looked into what the desired OS was among our surveyees. The desired OS parameter in our model represents the answer to which OS the surveyee would use if she was not constrained by price or employment. 7 MacOS and 21 Windows users stated that they would switch their OS. The results suggest that overall, MacOS users are very confident about using their OS and do not wish to migrate to Windows. Also, users who desire Windows as an OS seem to believe that Windows is better than MacOS when it comes to privacy.

A. Cybersecurity Regression Analysis

In this section, we used R language [23] to analyze the data and to apply the regression models we described in Section III-A. We decided to use ordinal logistic regression since our dependent variable is ordinal. Table II presents the simplified cybersecurity regression results and we present the detailed regression results in Appendix B1.

OS Perception: We started by regressing the primarily used operating system as an independent variable with the perceived cybersecurity comparison of MacOS and Windows as a dependent variable where 7 represents MacOS offers more cybersecurity than Windows and 1 represents the opposite. The primarily used OS parameter is a dummy variable where 1 represents being a Windows user, and 0 represents being a MacOS user. We determined that there is a statistically significant relationship between these variables. We also calculated the odds ratio, which is 0.246. That is, the odds of a MacOS user having a higher security comparison score are approximately 4.07 times the odds of a Windows user having a higher security comparison score.

Influence of Company Reputation: In the second regression, we added MacOS' and Windows' perceived cybersecurity reputation variables. We determined that there is a statistically significant relationship between the perceived reputations of the companies and the dependent variable. Also, when we added the reputation of the companies to the equation, the

TABLE II. CYBERSECURITY REGRESSION TABLE. ONLY SIGNIFICANT LOG ODDS VALUES, ROUNDED TO THE THIRD DECIMAL, ARE REPORTED. SIGNIFICANCE LEVELS ARE INDICATED WITH STARS (* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$). ALL ESTIMATES ARE BASED ON STANDARDIZED REGRESSION MODELS. A DETAILED VERSION OF THIS TABLE IS AVAILABLE IN THE APPENDIX.

	Ordinal Logistic Regression:							
	Perceived cybersecurity comparison of MacOS and Windows							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
OS (Windows = 1)	-1.403^{***}	-0.963^{***}	-0.989^{***}	-0.941^{***}	-0.937^{***}	-0.897^{***}	-0.971^{***}	
Apple's cybersecurity reputation		0.948^{***}	0.962^{***}	0.986^{***}	1.017^{***}	1.028^{***}	1.048^{***}	0.983^{***}
Microsoft's cybersecurity reputation		-0.666^{***}	-0.701^{***}	-0.726^{***}	-0.746^{***}	-0.746^{***}	-0.773^{***}	-0.798^{***}
IT			0.816^{**}	0.747^{**}	0.794^{**}	0.695^{*}	0.723^{*}	0.677^{*}
Computer usage				...	...	...	...	...
Age					...	...	...	...
Education						...	...	...
Gender							...	...
Desired OS								-1.340^{***}
Observations	208	207	205	205	205	205	205	205

Note: *p<0.1; **p<0.05; ***p<0.01

log odds value of the primarily used OS decreased from -1.403 to -0.963 while remaining statistically significant. This decrease demonstrates that by controlling the reputations, we captured some of the bias on the primarily used OS. The odds ratio value for the reputation of MacOS is 2.579, which means that the odds of having a higher dependent variable value (i.e., towards MacOS offers excellent security) are approximately 2.579 times greater for each unit increase in Apple's perceived cybersecurity reputation. For Microsoft, the odds ratio value is 0.513, which represents a negative relationship between the dependent and independent variables.

Influence of IT Background: In the third regression, we added the IT variable. Interestingly, we found a statistically significant relationship between the dependent and IT variable. The log odds of the IT variable was 0.816 and the odds ratio was 2.262 (i.e., the odds of having a higher dependent variable value are approximately 2.262 times larger, when we switched from a non-IT worker to an IT worker.) Note that apart from small coefficient changes, there was no change in the significance of the previous variables. In the sequential regressions, we added the daily usage of the computers, the age of the participants, the education level of the participants, and their gender. However, we could not find any statistically significant relationship in any of these categories.

In the complete model, the log odds for primarily used OS, Apple's cybersecurity reputation, Microsoft's cybersecurity reputation, and IT variables are -0.971, 1.048, -0.773, and 0.723, respectively, all of which are statistically significant.

Influence of Desired OS: In a final step, we added the desired OS variable to understand if a surveyee's preference for an OS makes a difference in their judgment of the cybersecurity capabilities of that OS. We did indeed find a statistically significant relationship between the desired OS and the dependent variable. The log odds of the desired OS variable is -1.340 and the odds ratio is 0.262. This demonstrates that individuals who are using their desired OS in practice tend to perceive their OS as being more secure than users on a platform that is not their favorite.

B. Privacy Regression Analysis

In this section, we discuss the regression results on the OS privacy questions. Table III presents the privacy regression results.

OS Perception: In the first regression, we used the perceived privacy comparison of the Windows and MacOS variables as the dependent variable. The first independent variable was the primarily used OS. There is a negative relationship between these two variables. The log odds value of the independent variable is -1.609 (odds ratio is 0.200), and there is a statistically significant relationship. That is, if we switch from a Windows user to a MacOS user, the odds of having a higher value for the privacy comparison (towards MacOS) are approximately 5 times of a Windows user. Hence, a MacOS user, relative to a Windows user, finds that MacOS cares more about privacy than Windows.

Influence of Company Reputation: In the second regression, we added Apple's and Microsoft's perceived privacy reputation to the equation. We found that Apple's perceived privacy reputation has a positive coefficient, and Microsoft's has a negative coefficient. The odds ratio for Apple's and Microsoft's perceived privacy reputation are 3.113 and 0.452. Similar to cybersecurity analysis, we found a positive relationship between the dependent variable and Apple's perceived privacy reputation, and a negative relationship with Microsoft's perceived privacy reputation. Note that both of the variables have a statistically significant relationship with the dependent variable.

When we added Apple's and Microsoft's reputation to the equation, similarly to our analysis of cybersecurity perception, the log odds value of the primarily-used OS decreased from -1.609 to -0.951 while keeping its statistical significance. This decrease demonstrates that by controlling the reputations for privacy, we again captured some of the bias on the primarily used OS.

Influence of IT Background: In the third regression, we added the IT variable. We found a positive relationship and statistical significance between the IT and the dependent variable. Furthermore, we controlled the computer usage, age, education level, and gender variables. However, once again,

TABLE III. PRIVACY REGRESSION TABLE. ONLY SIGNIFICANT LOG ODDS VALUES, ROUNDED TO THE THIRD DECIMAL, ARE REPORTED. SIGNIFICANCE LEVELS ARE INDICATED WITH STARS (* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$). ALL ESTIMATES ARE BASED ON STANDARDIZED REGRESSION MODELS. A DETAILED VERSION OF THIS TABLE IS AVAILABLE IN THE APPENDIX.

	Ordinal Logistic Regression:							
	Perceived privacy comparison of MacOS and Windows							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
OS (Windows = 1)	-1.609^{***}	-0.951^{***}	-0.969^{***}	-0.931^{***}	-1.006^{***}	-1.044^{***}	-1.099^{***}	
Apple's privacy reputation		1.136^{***}	1.165^{***}	1.175^{***}	1.172^{***}	1.161^{***}	1.240^{***}	1.200^{***}
Microsoft's privacy reputation		-0.793^{***}	-0.837^{***}	-0.844^{***}	-0.855^{***}	-0.835^{***}	-0.917^{***}	-0.945^{***}
IT			0.869^{**}	0.774^{**}	0.850^{**}	0.852^{**}	0.760^{*}	0.718^{*}
Computer usage				...	...	...	...	...
Age					...	...	...	...
Education						...	...	...
Gender							...	...
Desired OS								-1.569^{***}
Observations	208	207	205	205	205	205	205	205

Note: *p<0.1; **p<0.05; ***p<0.01

we could not find any significant relationship between these variables and the dependent variable. In the equation where we added all the variables in our model, we can summarize the log odds variables of primarily-used OS, Apple's reputation, Microsoft's reputation, and IT as -1.099, 1.240, -0.917, and 0.760. These four variables have a statistical significance with the dependent variable.

Influence of Desired OS: As a final step, we switched the primarily used OS variable with the desired OS variable. We found that the log odds of the desired OS is -1.569, and statistically significant. That is, individuals who are using their desired OS are predicted to perceive their OS as caring more about privacy than other users. Finally, Apple's and Microsoft's perceived privacy reputation variables and IT are still significant, and their coefficients are 1.200, -0.945, and 0.718.

C. User Behavior Regression Analysis

In this section, we investigated the relationship between the primarily used OS and the four cybersecurity and privacy behaviors (i.e., backing up files, covering the lens of the computer camera, using AV software, and using the browser in private mode). Table IV presents the behavioral regression results. For this analysis, AV software usage, performing backups, and covering the lens of the computer camera are binary variables where 0 represents a 'no' and 1 represents a 'yes'. The usage of browsers in private mode variables is on a Likert scale (1-7). To investigate this relationship, we formed a multiple regression model that we previously described in Section III-A. As AV software usage, performing backups, and covering the lens of the computer camera are binary variables, we use binomial logistic regression for those dependent variables. For the usage of browsers in private mode variable, we use ordinal logistic regression.

AV Usage Behavior: In the first model, we analyzed AV usage. In this regression, we found that there is a statistically significant relationship between primarily used OS and AV usage. The coefficient of the primarily used OS is 1.293. This positive correlation between the two variables means that when we switched from a MacOS user to a Windows user, the log odds of the usage of the AV increases by 1.293. Afterward, we introduced the IT, daily computer usage, and demographic variables to our regression. The coefficient was 1.314 and the significance is preserved.

Backup Behavior: In the second model, we investigated the performing backup behavior. The coefficient of the first equation is -0.715, and we found a statistically significant relationship between primarily used OS and backup behavior. In the complete model, the coefficient of the primarily used OS for performing backups became -1.157, and there was again a statistically significant relationship. That is, when we switched from a MacOS user to a Windows user, the log odds of backup behavior decreases by -1.157. Interestingly, we also found a statistical significant relationship between working in IT job and backup behavior. When we switched from a non-IT worker to an IT worker, the log odds of backup behavior increases by 1.450. Another statistical significant relationship was in computer usage. When we switched from a computer user who uses its computer less than 1 hour to 1 to 4 hours or 8 to 12 hours, the log odds of backup behavior increases by 3.778 and 3.970.

Covering of the Lens of the Computer Camera Behavior: In the third model, we checked the covering of the lens of the computer camera behavior. We found that the coefficient of the first model is 0.751 with a statistically significant relationship. In the full model, the coefficient of the primarily used OS was 0.717, and its significance persisted. That is, when we switched from a MacOS user to a Windows user, the log odds of covering the lens of the computer camera behavior increases by 0.717. Again, the relationship between being an IT worker and covering the camera was statistically significant and positive.

Browsing in Private Mode: In the fourth model, we regressed the usage of the private mode with the primarily used OS. The coefficient of the initial model is 0.108, and the full model is -0.078. However, we could not find any significant relationship for the usage of the private mode variable. We only found a statistically significant relationship between being an IT employee and private mode usage.

Overall, this analysis showed that there are some distinct cybersecurity behavioral differences between MacOS and Windows users. Specifically, we observed significant variations in

TABLE IV. BEHAVIORAL REGRESSION TABLE. ONLY SIGNIFICANT LOG ODDS VALUES, ROUNDED TO THE THIRD DECIMAL, ARE REPORTED. SIGNIFICANCE LEVELS ARE INDICATED WITH STARS (* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$). ALL ESTIMATES ARE BASED ON STANDARDIZED REGRESSION MODELS. A DETAILED VERSION OF THIS TABLE IS AVAILABLE IN THE APPENDIX.

	Logistic (Binomial) Regression:						*Ordinal Logistic Regression:*	
	AV		Backup		Cover		Private	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
OS (Windows = 1)	1.293^{***}	1.314^{***}	-0.715^{*}	-1.157^{***}	0.751^{***}	0.717^{**}	0.108	-0.078
IT		0.628		1.450^{**}		0.770^{*}		1.062^{***}
Computer usage		...		...		...		...
Age		...		...		...		...
Education		...		...		...		...
Gender		...		...		...		...
Constant	0.664^{***}	15.171	1.827^{***}	0.379	-0.579^{***}	1.099		
Observations	208	206	206	204	208	206	208	206
Log Likelihood	-105.330	-99.515	-99.415	-86.973	-139.650	-130.500	NA	NA
Akaike Inf. Crit.	214.661	231.031	202.831	205.945	283.300	293.000	NA	NA

Note: *p<0.1; **p<0.05; ***p<0.01

TABLE V. PARTICIPANT COMMENTS ON WHY THEY CHOSE ONE OS OVER ANOTHER FOR CYBERSECURITY (W: WINDOWS USERS, M: MACOS USERS)

User Opinion	**W**	**M**
MacOS is malware proof	8	27
The positive reputation of MacOS	12	15
The positive reputation of Windows	5	-
The "bad" reputation of Windows	1	-
Better technology on MacOS	4	14
Better technology on Windows	4	-
The enclosed ecosystem and better monitoring of MacOS (i.e., difficult to break)	5	2
Relatively small user base of MacOS provides better cybersecurity	6	8
Wide usage of Windows provides cybersecurity advantages (e.g., more people audit the system)	3	-
The financial power of Apple provides better cybersecurity	3	-
The financial power of Microsoft provides better cybersecurity	1	-
MacOS is a UNIX-based system, hence, making it automatically more secure	-	5
Total	52	71

the use of AV software, the practice of performing backups, and the habit of covering the lens of the computer camera. These behavioral differences might stem from a belief held by MacOS users that their platform is less susceptible to malware. Additionally, the behaviors might be influenced by the perception that MacOS offers superior cybersecurity and ensures greater privacy, as discussed in previous sections. Another interesting result was that, all else being equal, IT workers are more likely to perform backups, cover the lens of the computer camera, use the private mode of the browser. We hypothesize that these differences originate from the result of better awareness of the security and privacy issues.

It's worth noting that during the analysis of the cybersecurity, privacy, and behavior regressions, we added interaction variables into our models. However, these interaction variables did not demonstrate any significant relationships.

D. Qualitative Analysis

In this section, we present our analysis of cybersecurity and privacy-related open-ended questions. We used NVivo qualitative analysis software [16], and created a codebook with categories, themes, and codes from our qualitative data, as we previously described in Section III-B. The complete codebook can be found in the Appendix. We also categorized the participant responses to why they think that Windows or MacOS might offer more cybersecurity or privacy into different subject areas to acquire a feeling for how the surveyees perceive the cybersecurity of an OS.

1) Cybersecurity: We identified ten themes corresponding to users' operating system perception on cybersecurity, by looking at the responses on why the participants chose one OS over another for cybersecurity comparison. In summary, those ten themes are: a) Same Security Outlook, b) Cybersecurity Investment, c) Ecosystem Control, d) Low Vulnerability and Virus Incidence, e) Mac-specific Security, f) Reputation and User Safety, g) Strong Security Measures, h) Achieve Cybersecurity Excellence, i) Ease of Use and Familiarity, and j) User-Centric Approach.

Table V also presents the categorized responses, which are malware resistance, reputation, better technology, a closed ecosystem, user base size, wide usage, financial backing, and OS's foundation (i.e., UNIX-based). Interestingly, 27 MacOS and 8 Windows users commented that MacOS is malware-proof or less vulnerable to malware. For instance, a participant said:

> **P118:** *"I think MacOS is less vulnerable as it is not widely used as windows so hackers don't target it".*

Another participant stated:

> **P119:** *"I feel like MacOS is less susceptible to viruses and I have never had a virus on my mac compared to my old windows computer".*

Additionally, reputation was also one of the common topics – 15 MacOS and 12 Windows users mentioned the positive reputation of MacOS whereas only 5 Windows users mentioned the positive reputation of Windows. Also, a higher number of MacOS users believed that MacOS has better technology. For example, a MacOS participant mentioned:

> **P144:** *"Their reputation shows that they have internalized cyber security and make it a priority in their products"*.

It is also worth noting that although 38 Windows users were positive for MacOS cybersecurity, none of the MacOS users were positive for Windows. This observation aligns with our findings from the quantitative analysis section, where we highlighted that the majority of the MacOS users believe that MacOS is at least as good as Windows in cybersecurity.

2) Privacy: We identified eight themes corresponding to user operating system perception on privacy, by analyzing the responses on why the participants chose one OS over the other for privacy. In summary, those eight themes include a) Same Privacy Outlook, b) Customer Trust and Satisfaction, c) Security and Protection, d) User Data Protection and Enhancement Efforts, e) Customer-Centric Focus, f) Privacy-Centric Business, g) Product Improvement and Quality, and h) Reputation and Media.

Table VI also presents the categorization of user opinions. Just as with cybersecurity, these opinions are organized into reputation, privacy-centric technology, and the foundational type of OS (i.e., UNIX-based). Additionally, we identified new themes, including personal sentiments and experiences, company-consumer relationships, the potential for data sales, and the extent to which privacy is wielded as a marketing strategy.

Reputation was again one of the common subjects – 23 MacOS and 8 Windows users mentioned the positive privacy reputation of MacOS. Interestingly, 13 MacOS and 4 Windows users thought that Apple cares about the privacy of their users and does not sell data. For instance, a participant expressed:

> **P207:** *"They want to keep updating their systems so that they can keep protecting their customers"*.

Another participant stated:

> **P140:** *"Apple wants to offer a high quality product so they are consistent in making sure that consumers' products are safe to use through free updates of their OS"*.

In contrast, only one Windows user noted that Microsoft cares about the privacy of its users. We also observed that 9 Windows users reported that MacOS has privacy-supporting technology and that it is automatically better than Windows because it is a UNIX-based system. For example, a participant said:

> **P205:** *"Given that MacOS is Unix based it has better security measures built in"*.

Similar to the cybersecurity analysis, none of the MacOS users mentioned positively for Windows. Also, fewer Windows users mentioned positively for MacOS in the privacy comparison, compared to the responses for cybersecurity.

V. Main Findings and Actionable Results

In this section, we present the main findings and actionable results.

Confirming the folk wisdom: Many computer scientists and users are aware of the folk wisdom that MacOS is superior to Windows in terms of security (i.e., often referred to as the "religious OS wars"). In this work, we studied the perception of users with respect to the security and privacy of these operating systems. The main finding of our work is that many MacOS users appear to be convinced that their operating system is better than Windows with respect to cybersecurity and privacy. Notably, this sentiment also seems to be shared by many Windows users as well. This finding, perhaps, is to be expected, but we were able to verify it empirically and were able to confirm the folk wisdom that MacOS is indeed perceived to be more "secure" by many users.

Differences in cybersecurity habits: Our work also found that there is a statistically significant difference between cybersecurity habits such as covering the camera lens of the computer, performing backups regularly, and using AV software between MacOS and Windows users. In fact, MacOS users seem to be taking some of these actions less seriously. The reasoning can be identified by our qualitative analysis that showed that MacOS users are confident that their system is malware-proof, and has better technology and prestige. IT workers also seem to take cybersecurity habits more seriously. We found a statistically significant relationship between being an IT worker and backup, covering the lens of the camera, and using the private mode behaviors. We can hypothesize that IT workers are more aware of the possible security and privacy issues.

Reputation and primary OS matter: Our analysis showed that the primarily used OS and the reputation of the vendor are the main determinants of the perception of more cybersecurity and privacy. The difference between the perception of MacOS and Windows users is, as we determined, statistically significant. In this manner, OS developer companies, especially Microsoft, could benefit from trust-building campaigns that highlight security enhancements to reposition their brand.

Caution for organizations: Our empirical results suggest that the mental models of users do not match reality in this space. We have shown that many MacOS users have the perception that their OS will protect them against attacks and that the risk of being compromised is less when compared to Windows users. This perception may lead to a more relaxed assumption about necessary security risks among MacOS users. We also showed that IT workers favor MacOS more than non-IT workers in the perceived cybersecurity and privacy comparison between the two operating systems. IT workers play an important role in the security and privacy posture of organizations. If this favoritism towards MacOS relaxes some assumptions about risks among IT workers, it could have tremendous effects on organizations. As a result, organizations that have users on MacOS need to be especially prudent about the behaviors of their users and their inclination to be more relaxed about necessary cybersecurity precautions.

Security training and OS improvements: We believe there are two main determinants of improving the security and privacy of OS users. First, security training needs to focus

TABLE VI. PARTICIPANT COMMENTS ON WHY THEY CHOSE ONE OS OVER ANOTHER FOR PRIVACY (W: WINDOWS USERS, M: MACOS USERS)

User Opinion	W	M
The positive reputation of MacOS	8	23
The positive reputation of Windows	9	-
Privacy-supporting technology on MacOS	6	-
MacOS is a UNIX-based system, hence, making it automatically more secure	3	-
Good feelings and experience with MacOS	1	6
Privacy is a marketing strategy for MacOS	3	4
Apple cares more about their clients	4	5
Microsoft cares about their clients	1	-
MacOS does not share or sell user info with third parties	-	8
More people use Windows so it is more likely to sell/leak our data	-	2
Total	35	48

more on the role of users in maintaining their security posture. Individuals should become aware of emerging trends and learn what cannot be offered or guaranteed by operating systems. Second, regardless of any misconceptions or flawed mental models users may have, operating system vendors should incorporate as many built-in cutting-edge features as possible to compensate the errors in the user mental models. For example, operating system vendors should add as much built-in features as they can into operating systems (e.g., enhanced built-in AV programs, password managers, and a physical button for the microphone). Although some of the companies have already implemented or currently implementing some of the suggested precautions, they are not generally implemented (e.g., many companies do not insert a physical cover for the computer camera.) A recent example of a computer camera vulnerability [35] underscores that, although rare in advanced operating systems, vulnerabilities are always possible. Also, since the reputation of the companies is one of the main determinants, the extent of the advertisements about cyber-security and privacy capabilities could be narrowed down (e.g., each advertisement could contain a piece of advice to improve cybersecurity awareness). Known techniques in other domains such as behavioral economics and psychology could be helpful in this domain as well. For instance, the concept of nudging [30] can be used more systematically by operating system vendors to modify a user's perceptions when it is not very realistic.

VI. LIMITATIONS AND FUTURE WORK

Crowdsourcing platform: We performed experiments on Amazon Mechanical Turk. One potential limitation is the inherent bias that might come with this choice. Participants on this platform are likely to be more tech-savvy and familiar with the intricacies of operating systems. One way to overcome this issue is to directly engage with the participants. The additional ability to interview participants face-to-face might have been useful, and we might have had the opportunity to ask follow-up questions. However, according to [25], our work on Amazon Mechanical Turk should be representative of the U.S. population on the 18-49 age group who possessed at least some college-level education, with some skew towards more technology-inclined individuals. This skew, in our case, is not a problem as we were interested in recruiting participants who were computer users.

The choice of operating systems: By focusing predominantly on two operating systems, MacOS and Windows, our study might inherently favor or overlook nuances present in other systems. Our intent, however, was strategic, as we aimed to capture the majority of market share and user perceptions associated with these leading platforms.

Survey questions and actionable results: To make sure that our survey is easily understandable for average users and to ensure participant engagement, we kept the number of questions limited. However, this choice has the disadvantage of having limited depth and consequently, a limited range of actionable insights we could derive. While we aimed for a balance, there is always a trade-off between the length of the survey and the participant's attention span. While inherent biases such as brand reputation and personal OS preferences play a significant role in shaping cybersecurity perceptions, the underlying beliefs are multifaceted. Self-report and recall biases were also inevitable in our case since the participants self-reported from their past experiences. Further studies might consider exploring other factors, such as personal experiences with malware or cyberattacks, exposure to advertising, or peer opinions, to gain a more comprehensive understanding of what drives these perceptions. We used having an IT or cybersecurity-related job as an indicator for cybersecurity knowledge to shorten our survey. To improve the reliability of the results, future studies might use a better scale to measure cybersecurity knowledge.

Future work-1: An interesting future research direction would be conducting interviews about personal experiences with malware and cyber attacks. Subsequent studies can also focus on the effect of educating users, try to gain more insights into why individuals do or do not take some security precautions, and how we can make these users feel more secure while they are using their OS, by asking more detailed questions. For example, researchers can inform the surveyees about the detailed capabilities of each operating system, and then, ask them to compare the operating systems.

Future work-2: Given the ubiquity of mobile devices, exploring user perceptions about mobile operating system security could offer invaluable insights. Comparing these findings with desktop OS perceptions might also highlight unique challenges or beliefs specific to mobile platforms.

Our purpose is to provide a secure, private, and stress-free environment for users while helping them take some security-privacy precautions. This work was one of the steps toward this goal. By understanding these, we will gain more insights into the perception and, hence, will develop usable and secure solutions.

VII. Conclusion

In this work, we conducted surveys with a large number of MacOS and Windows users on Amazon Mechanical Turk. We aimed to understand what the differences in perception are among MacOS and Windows users with respect to the cybersecurity and privacy of these operating systems. Our results confirm the folk wisdom and show that many Windows and MacOS users indeed have the perception that MacOS is a more secure and private operating system when compared to Windows. At the same time, our results suggest that Windows is overall considered by users not to be an insecure operating system and that the reputation of the operating system has indeed improved over the last decade through the investments made by Microsoft in its cybersecurity. We hope that understanding the perception of users in this regard will pave the way for determining new trends, predicting potential new attack surfaces, and proposing usable solutions.

Acknowledgment

This work was partially supported by the U.S. National Science Foundation (Awards: NSF-EAGER-2219920 and NSF-1663051), Cyber Florida, and Microsoft. The views expressed by the authors in this paper are their own, not those of the funding entities.

References

[1] F. Al-Qershi, M. Al-Qurishi, S. Md Mizanur Rahman, and A. Al-Amri, "Android vs. ios: The security battle," in *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 2014, pp. 1–8.

[2] Amazon, "Amazon mechanical turk," Oct. 2023. [Online]. Available: https://www.mturk.com

[3] H. L. Ball, "Conducting Online Surveys," *Journal of human lactation*, vol. 35, no. 3, pp. 413–417, 2019.

[4] G. Belding, "Windows OS Security Brief History," Oct. 2019. [Online]. Available: https://resources.infosecinstitute.com/topic/windows-os-security-brief-history/

[5] Z. Benenson, F. Gassmann, and L. Reinfelder, "Android and ios users' differences concerning security and privacy," in *CHI'13 Extended Abstracts on Human Factors in Computing Systems*, 2013, pp. 817–822.

[6] Z. Benenson, O. Kroll-Peters, and M. Krupp, "Attitudes to it security when using a smartphone," in *2012 Federated Conference on Computer Science and Information Systems (FedCSIS)*, 2012, pp. 1179–1183.

[7] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," in *Proceedings of the eighth symposium on usable privacy and security*, 2012.

[8] H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin, "Diversity in smartphone usage," in *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010, pp. 179–194.

[9] S. Flinn and J. Lumsden, "User perceptions of privacy and security on the web," in *PST*. Citeseer, 2005.

[10] Intel, "PC vs. Mac: The Big Debate," Mar. 2021. [Online]. Available: https://www.intel.com/content/www/us/en/tech-tips-and-tricks/pc-vs-mac-the-big-debate.html

[11] Y. Jin, J. Lim, I. Yun, and T. Kim, "Compromising the macos kernel through safari by chaining six vulnerabilities," in *Black Hat 2020*. Black Hat, 2020.

[12] P. G. Kelley, "Conducting usable privacy & security studies with Amazon's Mechanical Turk," in *Symposium on Usable Privacy and Security (SOUPS)(Redmond, WA*. Citeseer, 2010.

[13] J. E. Klobas, T. McGill, and X. Wang, "How perceived security risk affects intention to use smart home devices: A reasoned action explanation," *Computers & Security*, vol. 87, p. 101571, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404819301348

[14] M. Lindorfer, B. Miller, M. Neugschwandtner, and C. Platzer, "Take a bite-finding the worm in the apple," in *2013 9th International Conference on Information, Communications & Signal Processing*. IEEE, 2013, pp. 1–5.

[15] S. Lipner and M. Howard, "Inside the windows security push: A twenty-year retrospective," *IEEE Security & Privacy*, 2023.

[16] Lumivero, "NVivo - Lumivero," (2023), https://lumivero.com/products/nvivo/.

[17] Malwarebytes, "State of Malware Report," Feb. 2020. [Online]. Available: https://resources.malwarebytes.com/files/2020/02/2020_State-of-Malware-Report.pdf

[18] P. Medelyan, A., "Coding Qualitative Data: How To Code Qualitative Research (2023) — Thematic." (2023), https://getthematic.com/insights/coding-qualitative-data/.

[19] Microsoft, "Keep your computer secure at home," 2023, https://support.microsoft.com/en-us/windows/keep-your-computer-secure-at-home-c348f24f-a4f0-de5d-9e4a-e0fc156ab221.

[20] I. Mohamed and D. Patel, "Android vs ios security: A comparative study," in *2015 12th International Conference on Information Technology - New Generations*, 2015, pp. 725–730.

[21] Moonlock, "Mac Security Survey 2023," 2023, https://moonlock.com/2023/06/Mac_Security_Survey_2023.pdf.

[22] A. J. O'Donnell, "When Malware Attacks (Anything but Windows)," *IEEE Security Privacy*, vol. 6, no. 3, pp. 68–70, 2008.

[23] R Core Team, *R: A Language and Environment for Statistical Computing*, R Foundation for Statistical Computing, Vienna, Austria, 2023. [Online]. Available: https://www.R-project.org/

[24] C. Ravi and R. Manoharan, "Malware detection using windows api sequence and machine learning," *International Journal of Computer Applications*, vol. 43, no. 17, pp. 12–16, 2012.

[25] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1326–1343.

[26] S. Sham, "6 steps to practice strong laptop security," 2020, https://www.okta.com/blog/2020/09/6-steps-to-practice-strong-laptop-security/.

[27] Statista, "Global market share held by operating systems for desktop PCs, from January 2013 to July 2023," (2023), https://www.statista.com/statistics/218089/global-market-share-of-windows-7/.

[28] S. G. Stats, "Desktop operating system market share worldwide," Oct. 2023. [Online]. Available: https://gs.statcounter.com/os-market-share/desktop/worldwide

[29] V. M. Sue and L. A. Ritter, *Conducting online surveys*. Sage, 2012.

[30] R. Thaler and C. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, ser. A Caravan book. Yale University Press, 2008. [Online]. Available: https://books.google.com/books?id=cYdYngEACAAJ

[31] C. W. Turner, M. Zavod, and W. Yurcik, "Factors that affect the perception of security and privacy of e-commerce web sites," in *Fourth International Conference on Electronic Commerce Research, Dallas TX*. Citeseer, 2001, pp. 628–636.

[32] F. Villegas, "Thematic Analysis: What it is and How to Do It. QuestionPro." (2023), https://www.questionpro.com/blog/thematic-analysis.

[33] P. Vinod, R. Jaipur, V. Laxmi, and M. Gaur, "Survey on malware detection methods," in *Proceedings of the 3rd Hackers' Workshop on computer and internet security (IITKHACK'09)*, 2009, pp. 74–79.

[34] R. Wash, "Folk models of home computer security," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010, pp. 1–16.

[35] William Gallagher, "Apple pays record $100,500 to student who found Mac webcam hack," 2022, https://appleinsider.com/articles/22/01/25/apple-pays-record-100500-to-student-who-found-mac-webcam-hack.

[36] M. Williams, "Are Macs more secure than PCs? Not always. Here's why," Jan. 2021. [Online]. Available: https://www.pensar.co.uk/blog/are-macs-more-secure-than-pcs

[37] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar, "A survey on malware detection using data mining techniques," *ACM Computing Surveys (CSUR)*, vol. 50, no. 3, pp. 1–40, 2017.

[38] T. Yin, Z. Gao, Z. Xiao, Z. Ma, M. Zheng, and C. Zhang, "{KextFuzz}: Fuzzing {macOS} kernel {EXTensions} on apple silicon via exploiting mitigations," in *32nd USENIX Security Symposium (USENIX Security 23)*, 2023, pp. 5039–5054.

APPENDIX

A. Demographic Survey Questions

- Q1: Which operating system are you primarily using?
  - Chrome OS
  - Fedora
  - Microsoft Windows
  - Solaris
  - Apple MacOS
  - Free BSD
  - Debian
  - Other
- Q2: Which option best describes your age group?
  - Under 18
  - 18 - 24
  - 25 - 29
  - 30 - 39
  - 40 - 49
  - 50 - 59
  - 60 - 69
  - 70 or older
- Q3: What is the highest level of education you have completed?
  - Some High School
  - High School Diploma
  - Some College
  - Associate Degree
  - Bachelor's Degree
  - Master's Degree
  - Ph.D. degree or Higher
- Q4: Worker ID
  - short answer text

B. Main Survey Questions

- Q1: How much time do you spend on your computer each day?
  - Less than 1 hour
  - From 1 hour up to 4 hours
  - From 4 hours up to 8 hours
  - From 8 hours up to 12 hours
  - 12 hours or more
- Q2: Are you working in an Information Technology (IT) or Cybersecurity-related job?
  - Yes
  - No
- Q3: How do you feel about Apple's reputation in cybersecurity? (1 to 7 Likert scale)
  - 1 - Poor Cybersecurity
  - 7 - Excellent Cybersecurity
- Q4: How do you feel about Apple's reputation in privacy? (1 to 7 Likert scale)
  - 1 - Poor Privacy
  - 7 - Excellent Privacy
- Q5: How do you feel about Microsoft's reputation in cybersecurity? (1 to 7 Likert scale)
  - 1 - Poor Cybersecurity
  - 7 - Excellent Cybersecurity
- Q6: How do you feel about Microsoft's reputation in privacy? (1 to 7 Likert scale)
  - 1 - Poor Privacy
  - 7 - Excellent Privacy
- Q7: Which operating system are you primarily using?
  - Apple MacOS
  - Microsoft Windows
- Q8: Which operating system would you use if you were not constrained by price or your job?
  - Apple MacOS
  - Microsoft Windows
- Q9: Which operating system do you think offers more cybersecurity? (1 to 7 Likert scale)
  - 1 - Extremely Windows
  - 7 - Extremely MacOS
- Q10: Which operating system do you think cares more about privacy? (1 to 7 Likert scale)
  - 1 - Extremely Windows
  - 7 - Extremely MacOS
- Q11: Why do you think this operating system offers more cybersecurity?
  - short answer text
- Q12: Why do you think this operating system cares more about privacy?
  - short answer text

1) Behavior Questions:

- Q1: Are you using an antivirus program?
  - Yes
  - No
- Q2: Do you back up your data?
  - Yes
  - No
- Q3: Do you cover your webcam with a physical cover?
  - Yes
  - No
- Q4: In a typical week, how often do you use the private mode of your browser? (1 to 7 Likert scale)
  - 1 - Never
  - 7 - Always

TABLE VII. DETAILED CYBERSECURITY REGRESSION TABLE

	Ordinal Logistic Regression:							
	Perceived cybersecurity comparison of MacOS and Windows							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
OS (Windows = 1)	−1.403***	−0.963***	−0.989***	−0.941***	−0.937***	−0.897***	−0.971***	
	(0.262)	(0.271)	(0.275)	(0.287)	(0.291)	(0.293)	(0.298)	
Apple's cybersecurity reputation		0.948***	0.962***	0.986***	1.017***	1.028***	1.048***	0.983***
		(0.122)	(0.124)	(0.126)	(0.129)	(0.130)	(0.131)	(0.132)
Microsoft's cybersecurity reputation		−0.666***	−0.701***	−0.726***	−0.746***	−0.746***	−0.773***	−0.798***
		(0.114)	(0.117)	(0.119)	(0.120)	(0.121)	(0.123)	(0.124)
IT			0.816**	0.747**	0.794**	0.695*	0.723*	0.677*
			(0.369)	(0.375)	(0.374)	(0.381)	(0.385)	(0.388)
From 1 hour up to 4 hours				−1.483	−1.272	−1.244	−0.455	−0.757
				(1.233)	(1.228)	(1.238)	(1.427)	(1.389)
From 4 hours up to 8 hours				−1.252	−1.042	−0.997	−0.309	−0.661
				(1.192)	(1.187)	(1.202)	(1.376)	(1.345)
From 8 hours up to 12 hours				−1.300	−1.141	−1.134	−0.469	−0.825
				(1.206)	(1.198)	(1.209)	(1.376)	(1.345)
12 hours or more				−1.009	−0.837	−0.709	−0.037	−0.377
				(1.273)	(1.266)	(1.275)	(1.450)	(1.410)
Age 25-29					0.004	−0.020	−0.068	−0.315
					(0.492)	(0.504)	(0.508)	(0.514)
Age 30-39					−0.248	−0.374	−0.485	−0.505
					(0.472)	(0.484)	(0.490)	(0.498)
Age 40-49					0.311	0.151	0.134	−0.041
					(0.525)	(0.540)	(0.542)	(0.541)
Associate degree						−0.223	−0.229	−0.374
						(0.558)	(0.560)	(0.565)
Bachelor's degree						−0.137	−0.128	−0.079
						(0.401)	(0.403)	(0.409)
Master's degree						0.422	0.469	0.412
						(0.460)	(0.463)	(0.466)
Ph.D. degree or higher						−0.217	−0.009	0.144
						(0.907)	(0.918)	(0.933)
Female							−1.286	−1.023
							(1.099)	(1.102)
Male							−0.859	−0.511
							(1.092)	(1.097)
Desired OS								−1.340***
								(0.307)
Observations	208	207	205	205	205	205	205	205

Note: *p<0.1; **p<0.05; ***p<0.01

TABLE VIII. DETAILED PRIVACY REGRESSION TABLE

	Ordinal Logistic Regression:							
	Perceived privacy comparison of MacOS and Windows							
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
OS (Windows = 1)	−1.609***	−0.951***	−0.969***	−0.931***	−1.006***	−1.044***	−1.099***	
	(0.271)	(0.283)	(0.287)	(0.294)	(0.300)	(0.308)	(0.310)	
Apple's privacy reputation		1.136***	1.165***	1.175***	1.172***	1.161***	1.240***	1.200***
		(0.127)	(0.129)	(0.131)	(0.132)	(0.133)	(0.138)	(0.139)
Microsoft's privacy reputation		−0.793***	−0.837***	−0.844***	−0.855***	−0.835***	−0.917***	−0.945***
		(0.117)	(0.120)	(0.121)	(0.121)	(0.122)	(0.127)	(0.127)
IT			0.869**	0.774**	0.850**	0.852**	0.760*	0.718*
			(0.378)	(0.385)	(0.392)	(0.394)	(0.395)	(0.395)
From 1 hour up to 4 hours				−0.332	−0.139	−0.100	−0.350	−0.939
				(1.418)	(1.464)	(1.497)	(1.853)	(1.990)
From 4 hours up to 8 hours				0.220	0.388	0.471	0.123	−0.406
				(1.382)	(1.426)	(1.472)	(1.829)	(1.982)
From 8 hours up to 12 hours				0.192	0.364	0.478	0.069	−0.529
				(1.392)	(1.435)	(1.478)	(1.835)	(1.983)
12 hours or more				0.204	0.325	0.517	0.096	−0.390
				(1.453)	(1.493)	(1.531)	(1.884)	(2.024)
Age 25-29					0.252	0.302	0.228	0.022
					(0.532)	(0.545)	(0.550)	(0.552)
Age 30-39					0.322	0.267	0.094	0.121
					(0.504)	(0.514)	(0.522)	(0.526)
Age 40-49					0.909*	0.814	0.708	0.626
					(0.552)	(0.573)	(0.575)	(0.571)
Associate degree						−0.477	−0.487	−0.766
						(0.572)	(0.592)	(0.593)
Bachelor's degree						−0.664	−0.634	−0.598
						(0.417)	(0.418)	(0.420)
Master's degree						−0.181	−0.087	−0.101
						(0.463)	(0.466)	(0.464)
Ph.D. degree						0.001	0.364	0.476
						(1.013)	(1.034)	(1.055)
Female							0.464	0.877
							(1.139)	(1.270)
Male							1.370	1.842
							(1.138)	(1.275)
Desired OS								−1.569***
								(0.322)
Observations	208	207	205	205	205	205	205	205

Note: *p<0.1; **p<0.05; ***p<0.01

TABLE IX. DETAILED BEHAVIORAL REGRESSION TABLE

	Logistic (Binomial) Regression:						*Ordinal Logistic Regression:*	
	AV		Backup		Cover		Private	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
OS (Windows = 1)	1.293***	1.314***	−0.715*	−1.157***	0.751***	0.717**	0.108	−0.078
	(0.362)	(0.402)	(0.366)	(0.441)	(0.284)	(0.318)	(0.244)	(0.267)
IT		0.628		1.450**		0.770*		1.062***
		(0.563)		(0.701)		(0.414)		(0.360)
From 1 hour up to 4 hours		−15.484		3.778**		0.773		1.155
		(942.637)		(1.927)		(1.688)		(1.726)
From 4 hours up to 8 hours		−15.803		2.558		−0.027		0.953
		(942.637)		(1.819)		(1.656)		(1.700)
From 8 hours up to 12 hours		−15.449		3.970**		0.044		1.411
		(942.637)		(1.871)		(1.657)		(1.706)
12 hours or more		−16.323		2.621		−0.381		0.878
		(942.637)		(1.904)		(1.730)		(1.744)
Age 25-29		0.784		−0.699		−0.143		0.539
		(0.625)		(0.868)		(0.570)		(0.459)
Age 30-39		0.732		−0.661		0.001		0.388
		(0.595)		(0.847)		(0.551)		(0.446)
Age 40-49		0.822		−0.455		0.601		0.498
		(0.688)		(0.908)		(0.610)		(0.499)
Associate degree		−1.149		−0.229		−1.025		0.116
		(0.829)		(0.770)		(0.669)		(0.554)
Bachelor's degree		−0.775		−0.060		−0.211		0.184
		(0.642)		(0.573)		(0.460)		(0.391)
Master's degree		−0.623		0.292		−0.787		0.320
		(0.712)		(0.684)		(0.526)		(0.443)
Ph.D. degree or higher		−1.542		15.413		−0.054		1.258
		(1.188)		(1,014.996)		(1.058)		(0.997)
Female		1.198		−0.988		−1.634		−0.292
		(1.288)		(1.643)		(1.416)		(1.024)
Male		0.975		−1.117		−1.614		−0.526
		(1.291)		(1.627)		(1.411)		(1.026)
Constant	0.664***	15.171	1.827***	0.379	−0.579***	1.099		
	(0.208)	(942.636)	(0.288)	(1.973)	(0.205)	(1.732)		
Observations	208	206	206	204	208	206	208	206
Log Likelihood	−105.330	−99.515	−99.415	−86.973	−139.650	−130.500	NA	NA
Akaike Inf. Crit.	214.661	231.031	202.831	205.945	283.300	293.000	NA	NA

Note: *p<0.1; **p<0.05; ***p<0.01

Category	Sub-Category	Theme	Code	Description	Ref.
OS Cybersecurity Perception	Both OS	Same security Outlook	Neither offers more security	I don't think any operating system offers more cyber security.	4
			Roughly equal	I think they're roughly equal	27
	Mac OS	Cybersecurity Investment	Money to spend on cyber security	It has more money to spend on it	2
			More advanced and proactive	I feel that they are more advanced and prepared to be proactive instead of reactive.	3
			Not impacted by viruses or other threats	Apple has a history of not being impacted by viruses or other threats. They are known in the industry as being one of the most secure systems.	7
			Put more money and work into their security	They have put more money and work into their security system.	2
		Ecosystem Control	Better designed	Better designed	2
			Enclosed ecosystem	a more enclosed ecosystem	1
			Feels secure with simplistic layout	It just feels more secure with a simplistic layout.	1
			Inability to customize or download third party apps	The inability to customize or download third party apps	1
			Less enticing to hackers	Mac is less enticing to hackers.	1
			Less modifiable which provides more security	It's less accessible, less modifiable which means it's more secure.	1
			Limits what can be installed	I think MacOS does a good job about limiting what can be installed on their devices	1
			Not open-sourced or require anti-virus software	MacOS is not open-sourced and generally does not require anti-virus software.	1
			Safer due to apps being vetted	Heard something about it being safer since apps are vetted	1
		Low Vulnerability and Virus Incidence	Harder creating viruses	harder to make viruses for	3
			Less issues with viruses	I have had way less issues with viruses since switching to a MAC	6
			Less prevalent	Less prevalent, so less of a target.	3
			Less prone to viruses	Apple systems are not prone to viruses like Windows based operating systems are.	15
			Less report of viruses	People report fewer viruses	1
			Less vulnerable due to not being widely used	I think MacOS is less vulnerable as it is not widely used as windows so hackers don't target it	3
		Mac-specific Security	Have not experience slowness	I have never experienced slowness on my Mac	2
			Have not heard issue with Mac system	I hardly ever hear of any issues with this system	1
			MacOS rarely having virus or malware	It is rare to hear about a MacOS device having a virus or malware on it.	4
			Not much hacking due to lower market share	MacOS is more secure just because people aren't trying to hack it as much because it has lower market share	3
		Reputation and User Safety	Good reputation of being secure	I feel that MacOS has a good reputation as being very secure.	18
			Greater transparency	There are just less viruses written for OSX. Also, it's built on a Linux kernel, there's greater transparency as to what's going on under the hood. You can always issue a "top" command and "kill -9" any rouge processes.	1
			Known for privacy and innovation	Apple is known for their privacy and innovation in addition to their focus on the customer.	2
			Offers superior security	Apple products in general offer superior security.	2
			Protect user's information	I have heard explicitly that Apple protects users' info, while Microsoft profits off of it	1
			Reputation shows internalized cyber security	Their reputation shows that they have internalized cyber security and make it a priority in their products	1
			Their reputation	Just the reputation	1
			User safety	To keep the users safe	2
		Strong Security Measures	Attack resistant and less exploitable	I feel as if Apple is more attack-resistant and less exploitable than Windows.	5
			Better security measures built in	Given that MacOS is Unix based it has better security measures built in.	1
			Browser add-ons	Free add-ons for the browser	1
			Built in anti-virus software	It has built in anti-virus software	1
			Good security features by providing fingerprint authentication and blockage of unwanted activities	In MacOS speed, security features are good compared to windows. It provides fingerprint authentication; it blocks the lot of unwanted activities.	2
			Good security measures like encryption	Apple is known for their security measures, including their encryption, so it feels more safe	2
			High priorities on security	I think the company places higher priorities on security	1
			Higher security level	They simply have a higher level of security which is very hard to breach	5
			Offers fingerprint authentication and drive encryption	It offers fingerprint authentication and drive encryption with the T2 Security Chip, and will generally be safer running a non-Windows operating system	1
			Provides Mitigation Strategies	Provide Mitigation Strategy Guidance	1
			Secures personal information	for securing personal information and preventing attack	2
			Superior in cyber security	I have read about how superior it is in cyber security	1
			TouchID security	They secure everything with touchID which can't be replicated	1
			Virus proof	I've heard MacOS is almost virus proof.	2
			Vocal about privacy	Apple is very vocal about privacy when other companies aren't.	2
	Windows OS	Achieve Cybersecurity Excellence	Been around longer with more cybersecurity improvements	I think they have been around longer and have had more work with cyber security	3
			Built-in antivirus that scan and remove malware	Windows has a great built in antivirus that scans and removes malware automatically.	1
			Built-in safeguards and firewalls	Windows has more built in safeguards and firewalls as compared to Mac.	1
			Heavily invested on security and privacy	Microsoft are a big company that is heavily invested on security and privacy	1
			More defence and better encryption	More line of defence and better encryption codes	1
			More software developed	There's just more software developed for Windows, so there are more options for security.	2
			Not many reports of attacks	less reports of attacks.	1
			Prevent attacks	I think they both offer it to prevent attacks.	2
			Protects identities, device and information	Protects identities, device and information.	1
			Removes malware automatically	Windows has a great built in antivirus that scans and removes malware automatically.	1
			Tested and developed necessary tools for robust cybersecurity	I believe that because this operating system has been around longer and is more widely used in business and government, that they have tested and developed the necessary tools to provide more robust cyber security.	1
		Ease of Use and Familiarity	Don't have issue	I have always used Windows and have never had an issue.	2
			Familiarity with system	I am more familiar with it.	3
			Feel safer to use	Safer to use	1
			Harder to install programs on MacOS	Because it's harder to install programs on MacOS	1
			Less concerned gathering and selling user data	Windows isn't as concerned with gathering and selling personal data to advertisers	1
			No keylogger	it doesn't have a keylogger	1
			Widely used OS	Because I think that it is the operating system that is used more worldwide.	1
		User-Centric Approach	Broader user base	Broader user base	3
			Built-in programs for user protection	It has built in programs so even the most stupid and non-techsavvy consumers get some protection.	3
			Cares about customers	Microsoft cares more about its customers. Apple just wants money.	1
			More advanced	Because they are more advanced compared to others.	1
			User trust	It is the one I have always used and trust.	3

Category	Sub-Category	Theme	Code	Description	Ref.
OS Caring About Privacy Perception	Both OS	Same Privacy Outlook	Both OS care due to money	I think they both care because they both care about money	1
			Equally comparable with privacy	I feel that both systems are comparable when it comes to privacy.	25
			Neither are better than the other in privacy	I don't think either brand is really better than the other in the privacy department. They both have their faults.	14
			No good privacy policies	They both do not have good privacy policies.	1
	Mac OS	Customer Trust and Satisfaction	Better reputation	To maintain a better reputation	6
			Consumer trust	It wants people to trust them.	2
			Create products for consumers that are safe	Apple wants to offer a high-quality product so they are consistent in making sure that consumers' products are safe to use through free updates of their OS.	1
			Customer centric product	They have always had a customer-centric product and are known for their superior privacy.	1
			Does not care about its customers	Apple doesn't care about its customers	1
			For the public image	Public image more than anything else.	1
			Goes the extra mile to satisfy their customers	Apple goes the extra mile for their customers	1
			Maintain good security with updates	They make a focused effort to maintaining great security with updates	1
			Marketing purposes	Marketing purposes	1
			More consumers and wants to keep good image	I think because it has more consumers and wants to keep its good name it tries to take care of them	1
			Provide better products for their customers	It wants to provide the best privacy for their customers for them to purchase their wide variety of apple products	1
			Reputation for being invasive	Apple has a reputation for being incredibly invasive.	1
			To emphasize they prioritize privacy	Tends to emphasize that they prioritize privacy	1
			Value their clients	They value their clients more as compared to others.	1
		Security and Protection	Continues to create more privacy updates	they keep creating more privacy updates	1
			Crucial for modern day	It is a crucial aspect in modern day	1
			Devices are used widely	They have to care more because their devices are used more widely	1
			Does not allow anyone to decrypt devices easily	Apple as a whole seems to care more than others. See law enforcement anger at their refusal to decrypt devices of the accused.	2
			Keep user information safe	I think that their operating system has more security features to keep your information safe.	2
			Keeps updating system to protect customers	They want to keep updating their systems so that they can keep protecting their customers	1
			Protect consumers	They want to protect their consumers.	1
			To prevent hacking or surveillance	it has improved its data security by preventing hardware that leads to hacking or surveillance	1
		User Data Protection and Enhancement Efforts	Allow users to browser privately	I feel like I can use private browsing modes and shut off my information from being shared. For example, private browsing.	1
			Allow users to encrypt files	I feel it is a bit more secure and my files are encrypted better, ensuring more privacy	1
			Cares about user privacy	I believe that Apple as a company strongly cares about its users privacy	5
			Corrected privacy flaws	Apple has acknowledged and corrected their privacy flaws in the past	1
			Creating a secure place	Because they choose to put money and effort into creating a secure place.	4
			Protect privacy to cover up their actions	I think Apples reputation for wanting to protect privacy has more to do with covering up their own actions and not consumer privacy	2
			Recognize the need for privacy and embrace it	I feel that they have recognized the need for privacy and embraced it.	1
			Transparency in privacy policies	You are always shown privacy policies and asked if you want to share your data	1
			Upfront controls after installation	Upfront controls immediately after OS installation	1
	Windows OS	Customer-Centric Focus	Cares about their customers	Because I believe it has more customers, and would like to do the best possible to keep them satisfied.	3
			Keep customer satisfied	Because I believe it has more customers, and would like to do the best possible to keep them satisfied.	1
			Users trust	Because they want users to trust them and use their products	2
		Privacy-Centric Business	Bad for business if privacy is not integrated	its bad business for them if they don't	1
			Privacy controls	Upfront controls immediately after OS installation	2
			Privacy is part of innovation	Windows cares more about privacy because it comes from a smarter company. Apple has only made slight tweaks to an iPhone while Microsoft continues to innovate. Privacy is part of that innovation.	1
			Protect personal life	Want to make sure you protect as much of personal life	2
			Protecting user	More geared toward protecting the user	1
			Provide user flexibility over settings	It offers more user flexibility, and control over security settings.	1
			Provides opt out option to protect user privacy	They give you the option to opt out of this and that, so you can think that they take your privacy safety.	1
			Use privacy as a selling point for their product	They use it as a selling point for their product.	1
			Value transparency and honesty on keeping user safe	I feel that Windows cares more because they are more open and honest about their operating system and how they keep users safe.	2
		Product Improvement and Quality	Improve products	They want their products to be top notch	1
			To keep bad stuff out	They work harder to keep the bad stuff out.	1
		Reputation and Media	Keep collecting user's data	To keep collecting your data	1
			Less worried about media	They are less worried about being in the media and integrating with social media	1
			Not concerned with data gathering	They are not as concerned with data gathering so their privacy policy is more geared toward protecting the user	1
			Protects reputation	Because it protects their reputation	3