Exploring the User Experience Design of Commercially Available Cybersecurity Products for Personal Mobile Devices

Sean D. Williams
University of Colorado Colorado Springs

Curtis Blair
University of Colorado Colorado Springs

Jade Stanton
University of Colorado Colorado Springs

Abstract - ***Research shows that when software is difficult to use, the users will either not use it or find ways to shortcut the software. In the case of cybersecurity applications, shortcutting exposes individuals and their organizations to potential threats. While most research in cybersecurity has focused on designing, implementing, and testing enterprise-scale systems, little research exists on cybersecurity for individual devices and especially not the user experience of those applications. Additionally, most literature on cybersecurity systems focuses on the technical aspects of the systems with little regard for the preferences of actual users. The purpose of this study, therefore, was to examine the end user experience of consumer software for securing mobile devices from cyberattacks. Results generated from a three-part method of survey, heuristic analysis, and sentiment analysis suggest that user experience is not a significant obstacle in the adoption of mobile cybersecurity applications. The study, therefore, indicates that individuals' choice not to protect their mobile devices is behavioral and not a user experience problem. Future research should seek to better understand the attitudinal opposition to using mobile cybersecurity applications.***

Index Terms – Cybersecurity, heuristic analysis, mobile applications, sentiment analysis, user experience design

INTRODUCTION

In 2019, attacks on mobile devices increased by more than 50% over 2018, and with the COVID-19 pandemic, the number of attacks in 2020 increased exponentially as individuals worked remotely [1]. According to one industry study [2], the average cost for companies of an individual's password being compromised was $383,365. If mobile devices had been properly secured, the negative impact on these individuals and organizations could have been eliminated or reduced.

However, individuals often don't consider their mobile devices when thinking about cybersecurity, believing that cybersecurity is the domain of organizations and governments, and only 11% of the 275 million mobile devices have protection. This leaves about 245 million devices vulnerable [3]. In short, a weak "cybersecurity culture" exists at the level of individual accountability when compared to the enterprise level, even though our mobile devices are increasingly connected to important enterprise systems. This weak individual cybersecurity culture therefore exposes a critical weakness in the link of systems protecting individual and organizational data [4].

To explore the causes of this weak cybersecurity culture and to recommend potential interventions, this study investigated the individual user experience of commercially available software products to secure personal mobile devices. Research shows that when software is difficult to use, the intended audience will often create workarounds to ease software use [5] or will avoid using the software all together [6, 7]. Given the hundreds of applications for securing personal mobile devices produced by major companies like Norton, McAfee, and Kaspersky and the relatively low adoption rate for these applications, consumers appear to be avoiding use of these applications to secure their devices.

Building on prior work [c.f. 8, 9, 10] this study interrogated the causes of this weak cybersecurity culture by addressing these research questions:

1. *What impact does the user experience design of cybersecurity software have on the adoption of these applications?*
2. *What perceptions do users have about securing their mobile devices?*

Answering these questions helps us to understand the user experience of mobile security software and can help to suggest possible methods for strengthening a culture of cybersecurity by increasing the applications' usability.

METHODS

The methods of this study triangulated users' experiences with mobile security software to better understand the weak culture of individual cybersecurity. The study occurred in three phases: 1) an attitude and behaviors survey; 2) a heuristic analysis prepared by two separate coders using the Nielsen/Molich model 3) a sentiment analysis. The research team chose to evaluate software from Norton, McAfee, and Avast on both Apple iOS and Android platforms (six total installations) because these applications had the most downloads in the Apple Store and Google Play Store at the time of the study (Spring 2021).

I. Attitude and Behaviors Survey

Students are often used as a convenience sample in qualitative research and this part of the method asked students to complete a survey about their cybersecurity attitudes and behaviors. Questions about attitudes (for example, "How concerned are you about your phone being hacked?") interrogated participants' beliefs about mobile cybersecurity while questions about behaviors (for example, "Have you installed a security app on your phone?") demonstrated how those beliefs are/are not enacted. The survey established a baseline of general attitudes and actions among a sample user group (n=97) and framed the results of both the heuristic study and the sentiment analysis.

II. Heursistic Analysis

Two independent raters employed the Nielsen/Molich model to rate each of the six applications on all 10 aspects of the heuristic. After individually scoring the applications, a third rater evaluated the congruence between the two raters and determined a relatively low inter-rater reliability of 48%. Consequently, the two initial raters returned to their independent analyses, discussed their scores, and generated a "normed" score based on the conversation. The normed score formed the basis for the results of the heuristic analysis reported in the results section.

III. Sentiment analysis of user comments

On both Google Play and the Apple Store, users leave comments about their opinions. To uncover patterns in user responses, we scraped user comments from the software download pages and then selected a random sample of 100 responses from the thousands of comments available for each of the six applications. The comments were first coded as positive or negative where ratings of 3, 4 and 5 stars were "positive" and ratings of 1 and 2 stars were "negative." The responses were then grouped according to their major category, positive or negative. The narrative responses were then evaluated by two separate coders according to the Nielsen/Molich usability categories to uncover common complaints (and compliments) about the applications. Finally, the team counted the frequency of responses in each of the Nielsen/Molich categories.

RESULTS

The results that follow appear according to each of the three methods: the survey of attitudes and behaviors; the heuristic analysis; and the sentiment analysis. Additionally, the results include one unintended finding presented below about the incongruence between expert evaluators and actual users.

I. Attitude and Behavior Survey Results

The survey demonstrated that while the majority (55%) of respondents doubt the security of applications they download and 47% doubt the security of their phone generally, only 21% have installed a security application on their devices. Stated another way, 79% of the survey respondents have no protection on their mobile devices although most distrust the cybersecurity of their phones and the applications they use. See figures 1 and 2.

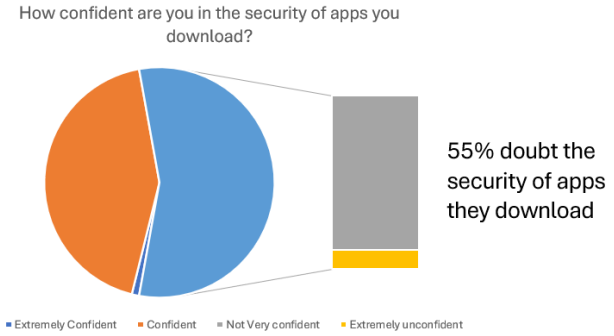

FIGURE 1. PERCENTAGE OF SURVEY RESPONDENTS WHO DOUBT THE SECURITY OF APPLICATIONS ON THEIR PHONES.

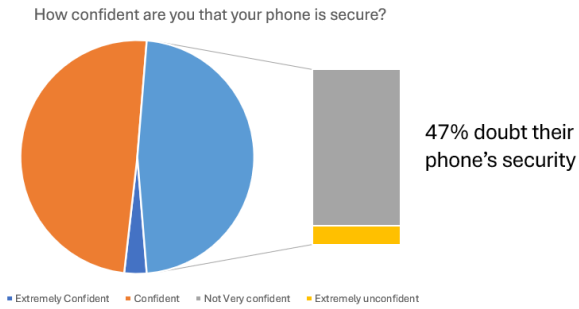

FIGURE 2. PERCENTAGE OF SURVEY RESPONDENTS WHO DOUBT THE SECURITY OF THEIR PHONE GENERALLY.

II. Heuristic Analysis Results

The heuristic analysis showed that three different categories, *Help and Documentation*, *Aesthetic and*

Minimalist Design, and *Recognition Rather than Recall* accounted for 65% of all negative comments, and that another three categories had virtually no errors: *Visibility of System Status* (2.4%); *Consistency and Standards* (0%); *Match Between System and Real World* (0%). Finally, the issues as a percentage of all comments across the three platforms was relatively consistent: Avast (25%); McAfee (23%); Norton (19%). See figures 3 and 4.

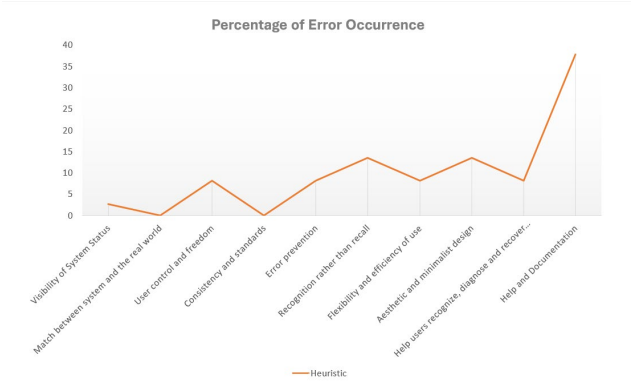

FIGURE 3. PERCENTAGE OF ERROR OCCURRENCE ACROSS CATEGORIES OF THE NIELSEN/MOLICH MODEL.

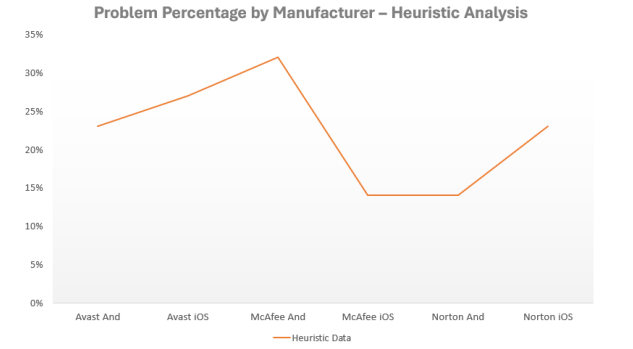

FIGURE 4. ERRORS REPORTED IN HEURISTIC ANALYSIS AS A PERCENTAGE OF ALL COMMENTS FOR EACH APPLICATION.

III. Sentiment Analysis Results

The sentiment analysis showed that three categories, *Visibility of System Status*, *User Control and Feedback*, and *Flexibility and Ease of Use* accounted for more than 50% of all negative comments while interface design issues (*Aesthetic and Minimalist Design*, *Recognition and Recall*, and *Consistency and Standards*) accounted for just 11% of all problems reported.

Commenting on the first major concern, *Visibility of System Status,* one response stated, for example:

> [I] don't know why the app is going into a different mode again and again. It gets into the default mode and keeps on displaying a message on the screen that it is updating the virus database and never ends. It does not get back to normal until I uninstall and again reinstall it.

Similarly, another respondent commenting within the category of *User Control and Feedback* wrote:

> Why doesn't the app provide the user with some way of switching the protection off for certain unsecured connections? Don't make us uninstall then reinstall the app when we've completed dealing with an unsecured network that we control.

Finally, another sample response that exemplifies the category, *Flexibility and Ease of Use,* notes:

> I always have to go through the process of giving the app access in order to scan. It is easily turned off after I give the permission or after a scan. And I have to scan 3 or 4 times in a row to achieve desired results.

Importantly, Avast (26.5%) and McAfee (30.5%) have far fewer reported problems than does Norton (62%) when considering negative comments as a percentage of the total number of comments. See figure 5.

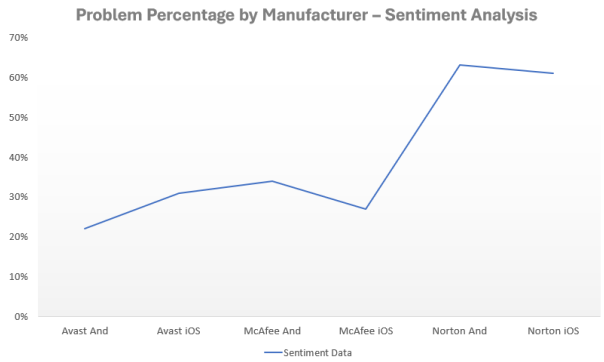

FIGURE 5. ERRORS REPORTED IN SENTIMENT ANALYSIS AS A PERCENTAGE OF ALL COMMENTS FOR EACH APPLICATION.

IV. An Unintended Finding

Finally, an unintended result was that experts conducting a heuristic analysis of the applications differed quite remarkably from actual users in problems that they identified. Both groups—user and experts—found a relatively similar number of problems, but the distribution of where those problems arose varied. As Table 1 shows, the only agreement between users (Sentiment) and experts (Heuristic) on the 10 areas of the Nielsen/Molich model occurred on the topic of "Error Prevention." This suggests that collecting more data from actual users and from more

applications could generate better results to guide user experience design of mobile cybersecurity applications.

TABLE 1. COMPARISON OF ACTUAL USER AND EXPERT ANALYSIS.

Nielsen/Molich Category	Sentiment	Heuristic
Visibility of System Status	18.8%	2.7%
Match between system and the real world	10.4%	0.0%
User control and freedom	16.2%	8.1%
Consistency and standards	6.4%	0.0%
Error prevention	*8.5%*	*8.1%*
Recognition rather than recall	2.8%	13.5%
Flexibility and efficiency of use	15.5%	8.1%
Aesthetic and minimalist design	1.7%	13.5%
Help users recognize, diagnose, and recover from errors	12.0%	8.1%
Help and Documentation	7.8%	37.8%

The result, while an unintended outcome of the study, shouldn't surprise us since other studies have uncovered a similar result [c.f. 11, 12, 13].

CONCLUSIONS

The results of this study lead to mixed conclusions for the two questions that guided this study.

First, in response to the study's major question—What impact does the user experience design of cybersecurity software have on the adoption of these applications—the results suggest that user experience does ***not*** play a significant obstacle in the adoption of mobile cybersecurity applications. Both users and experts reported greater than 70% satisfaction with the apps when the results from both the heuristic analysis and the sentiment analysis are aggregated. Recall from Figure 4 that the heuristic analysis showed low numbers of usability issues—less than 30% of all reported problems. While the sentiment analysis (Figure 5) found a greater number of issues in the Norton application, the percentage of issues was relatively low across the applications taken as a whole.

Second, in response to the second major question about users' attitudes toward cybersecurity for mobile devices, the conclusion seems to be quite clear: people are aware of the risks, but generally do not utilize the protections of third-party software. Recall that 79% of people have no protection. In other words, users seem complacent about actively protecting their mobile devices. Unfortunately, the survey questions can't answer the logic behind this thinking.

RECOMMENDATIONS

Because the findings for the study suggest that user experience issues are not a source of low adoption of mobile cybersecurity applications, additional research could help explore this conundrum in more depth. At least four questions could help add nuance to the findings of this study.

First, university students were a convenience sample used for this study, and that group might not sufficiently represent the larger population of mobile phone users and their beliefs about personal safety on their devices. What if the study investigated the attitudes and behaviors of different user groups? How might the survey results be different based upon age, for example? A future study might engage a more diverse sample of users.

Second, this study focused on only three software companies (although in both iOS and Android) so examining more applications might help to determine if the same patterns of user experience issues (and successes) occur generally across this class of software. Perhaps the findings in this study are peculiar to these three platforms rather than a characteristic of mobile cybersecurity software in general.

Additionally, the methods of evaluating the software didn't include observational data from detailed and formal usability studies. Usability studies of these platforms (and potentially others) might better explain users' experiences—both positive and negative—and would certainly add nuance to the findings. In turn, a more nuanced analysis might detect patterns of actual use that led to the findings reported in this study. In other words, a limitation of this study was explaining why users rated the software as they did in the comments reported in the sentiment analysis.

Finally—and importantly—we must better understand why users don't install security software on their mobile devices since the user experience seems not to be a significant issue in adoption. Constructing and delivering a comprehensive behavioral survey might help us learn the reasons behind this general pattern of behavior and could suggest ways that cybersecurity companies could position their products to more effectively persuade consumers to adopt their software.

This study only begins a dialogue that user experience professionals need to have about mobile cybersecurity software. Our mobile devices are increasingly essential in our everyday lives, both for work and for personal uses, so

their security warrants the same scrutiny that enterprise systems have received. Unfortunately, little work exists that examines mobile cybersecurity platforms from the user's perspective, and hopefully these initial results will inspire more research into this important topic. We all would benefit from such research because it would help to address this critical weakness in the link of systems protecting individuals and organizations.

ACKNOWLEDGEMENTS

This study was funded by a grant from the University of Colorado – Colorado Springs Cybersecurity Seed Grant program.

REFERENCES

[1] Cyberattack Trends: 2020 mid-year report. [Online]. Available: https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.

[2] 2018 State of cybersecurity in small and medium size businesses. [Online]. Available: https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf.

[3] Consumer view on mobile security: Allot mobile trends report H1/2017. [Online]. Available: https://www.allot.com/resources/MobileTrends_Consumer-View-on-Mobile-Security.pdf.

[4] M.A. Harris and K.P. Patten. "Mobile device security considerations for small-and medium-sized enterprise business mobility." *Information Management & Computer Security*, vol. 22, no 1, pp. 97-114, 2014.

[5] N. Micallef, M. Just, L. Baillie, M. Halvey, and H.G. Kayacik. "Why aren't users using protection? investigating the usability of smartphone locking." In *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services,* 2015*,* pp. 284-294.

[6] F. Wolf, R. Kuber, and A.J. Aviv. "Pretty Close to a Must-Have: Balancing Usability Desire and Security Concern in Biometric Adoption." In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019,* pp. 1-12.

[7] M.A. Sasse, M. Smith, C. Herley, H. Lipford, and K. Vaniea. (2016. Debunking security-usability tradeoff myths. *IEEE Security & Privacy*, vol. 14, no. 5, pp. 33-39, 2016

[8] S. Kurkovsky, and E. Syta. "Digital natives and mobile phones: A survey of practices and attitudes about privacy and security." In *2010 IEEE International Symposium on Technology and Society, 2010,* pp. 441-449.

[9] H. Chen, H, and W. Li. "Mobile device users' privacy security assurance behavior." *Information and Computer Security*, vol. 25, no. 3, pp. 330-344, 2017.

[10] N. Thompson, T.J. McGill, and X. Wang. "Security begins at home: Determinants of home computer and mobile device security behavior." *Computers & Security*, vol 70, pp. 376-391, 2017.

[11] R. Khajouei, A. Ameri, and Y. Jahani. "Evaluating the agreement of users with usability problems identified by heuristic evaluation." *International Journal of Medical Informatics*, vol 117, pp.13-18, 2018.

[12] Usability Testing vs. Expert Reviews [Online]. Available: https://www.uxmatters.com/mt/archives/2009/10/usability-testing-versus-expert-reviews.php.

[13] R. Jeffries, and H. Desurvire. "Usability testing vs. heuristic evaluation: was there a contest?" *ACM SIGCHI Bulletin*, vol. 24, no.4, pp. 39-41, 1992.