Usability Characteristics of Security and Privacy Tools: The User's Perspective

Ioanna Topa, Maria Karyda

▶ **To cite this version:**

Ioanna Topa, Maria Karyda. Usability Characteristics of Security and Privacy Tools: The User's Perspective. 33th IFIP International Conference on ICT Systems Security and Privacy Protection (SEC), Sep 2018, Poznan, Poland. pp.231-244, 10.1007/978-3-319-99828-2_17 . hal-02023741

HAL Id: hal-02023741

https://inria.hal.science/hal-02023741

Submitted on 21 Feb 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution 4.0 International License

Usability Characteristics of Security and Privacy Tools: The User's Perspective

Ioanna Topa and Maria Karyda

Department of Information and Communication Systems Engineering,
University of the Aegean, Greece
itopa@aegean.gr, mka@aegean.gr

Abstract. Use of security and privacy tools is still limited for various reasons, including usability issues. This paper analyses usability characteristics of security and privacy tools by drawing on relevant literature and employing scenario-based questionnaires and interviews with 150 users to capture their views. Based on users' feedback, we analyse the role of usability characteristics and identify critical issues such as transparency, control of personal data, design and accessibility and consistency. This paper provides insights into the multifaceted issue of usability of security tools from the users' perspective and a comprehensive picture of users' needs and expectations. Some of the findings of this study show that users regard as important that security and privacy tools incorporate usability characteristics relevant to installation, design and accessibility, control and automation, visible feedback, and locatable security settings. Furthermore, users encounter problems with understanding technical terms and report that the availability of tools among smartphones and operating systems is a usability issue.

Keywords: Usability Characteristics, Security Tools, Privacy Tools.

1 Introduction

While there is a plethora of security and privacy tools available to users, such as antivirus programs, antispyware, VPNs, anti-tracking tools, email authentication tools, etc., users often avoid using them, circumvent them or use them incorrectly. This, however, can have a significant impact such as direct or indirect financial losses, leakage of personal data and failure to comply with legislation or contractual obligations [10]. One explanation for this is that users prefer to avoid the inconvenience caused by the additional security tasks they must perform to use their computer securely [13]. To ease the burden on the user and make tools more user-friendly, researchers have studied usability [5,13], yet despite considerable research on the usability characteristics of various tools [8,15], the issue of incorporating usability characteristics seems to be of low priority for designers and providers of such tools. Furthermore, while several studies analyse different usability characteristics that can influence users towards adopting security tools [1,2,5,6,7,10],

users' perspectives and their expectations are scarcely addressed. Thus, relative research identifies that further research is needed regarding "usable security" and "usable privacy", especially focusing on the user's perspective [4].

This study aims to address this need, by providing an analysis and discussion of users' opinions and expectations, gathered through scenario-based questionnaires and interviews concerning specific usability characteristics, identified through an analysis of relevant literature. Our study offers insights into the different aspects of usability and identifies new factors to consider, highlighting in particular that usability characteristics related to installation(easy installation, avoidance of registration with personal data for ease of use, minor changes upon installations) are regarded as important by users. Other findings posit that users have contradictory preferences regarding control of the tool, with some preferring automated processes, while others not. Design is valued as important by users both for aesthetic reasons and for accessibility reasons supporting disabled people. Availability of security and privacy tools among different platforms was also identified as a usability issue.

2 Background: Usability Characteristics

Several studies in the field of Human Computer Interaction (HCI) exploring the usability of tools and technologies draw on usability characteristics as defined in ISO/IEC 9241-11:1998 [18], namely *effectiveness* (the degree of accuracy and completeness with which the user accomplishes tasks successfully), *efficiency* (resources, often referring to time, required by the user to accomplish tasks) and *satisfaction* (users' positive attitudes towards the use of a tool).

Nielsen [8] uses the concept of *efficiency*, described as *efficiency to use*, and employs the term *errors* instead of *effectiveness*, *memorability* and *learnability* (the degree to which a user who has never seen the user interface before can learn how to accomplish basic tasks). Nielsen also provides a list of usability heuristics which technologies should integrate [8,15], identifying *visibility of system status* (users being kept aware of the system and its functions by receiving feedback), *match between system and the real world* (the system should use the language, terms and concepts that users are aware of), *user control and freedom* (users should be able to undo their actions), *consistency and standards* (one action should have the same result and format to help users recognise them), *error prevention* (the tool informs users about potential errors and displays a message that asks for users' confirmation before proceeding), *aesthetic and minimalistic design* and *help and documentation.* These heuristics have significantly influenced relevant research, such as Seffah et al. [16], who developed a model for usability measurement which further includes *accessibility, trustfulness* etc. Other researchers also draw on these characteristics, modifying them accordingly. Johnston et al. [1] use some of Nielsen's characteristics to develop their own criteria for developing usable and secure interfaces, including *visibility of system status*, *aesthetic and minimalistic design* and *satisfaction*, and introduce a new usability aspect, namely *convey features*, which is the degree to which the tool helps the user understand the security features the tool supports. They

used the above usability characteristics to evaluate the Internet Connection Firewall (ICF) of Windows XP, suggesting an improved version and concluding that any security interface can be easily improved by applying usability characteristics.

Furnell [2] suggests that usable security tools need to support *visibility*. In contrast to the idea of *aesthetic and minimalistic design*, where the tool displays only the most relevant security related information, Furnell [2] uses the case of an antivirus to show that sometimes additional features are incorporated to show users that "something is going on", e.g. a meter or a chart displayed during the scanning process, as a way of reassuring or attracting users [2]. He also proposes a new usability characteristic called *locatability* (the degree to which security features are evident to users who can easily accomplish security tasks without spending too much time looking for security). Dhillon et al., use locatability with a broader meaning under the term *ease of system navigation* [18].

Analysing usability of privacy tools, Wästlund et al. [3], employed similar terms such as *control*, namely control over users' personal data and *transparency*, which is another term for *visibility*, referring to the degree to which users can see the internal operations of tools and know how their data is being processed. *Feedback* in this case, refers to the information they receive about the handling of their data and whether their privacy is protected or not. Furthermore, a recent report by ENISA [4] introduced new usability characteristics relevant to the installation process including *ease of installation, registration with personal data, changes upon registration,* and *minimum requirements,* as well as referring to *available help and support.*

A limited stream of research studies users' attitudes and perceptions regarding the usability of technologies such as e-banking authentication systems, email authentication services, antispyware and encryption tools. Weir et al., asked users to use three different e-banking authentication mechanisms to measure their *effectiveness*, *efficiency* and *satisfaction* [6], concluding that users have different usability preferences for different mechanisms, e.g. users preferred the more efficient push button token (requiring fewer steps for authentication compared to the other two mechanisms), but regarded chip and PIN-Secured tokens as more secure. Similar findings were reported in the study by Krol et al. [11], where participants preferred authentication mechanisms that were faster and required fewer steps. This study also found that users were confused when authentication in different e-banking systems included different terms (e.g. "password", "passphrase", "user ID") for similar concepts [11].

Whitten and Tygar [5] found that PGP users had difficulties in terms of *efficiency* and *effectiveness of the tool*, as they were unable to complete all tasks successfully in a timely manner. This could be attributed to security limitations of the interface, such as the display of confusing images for the keys, the fact that users might mistakenly delete their key and be unable to retrieve it (irreversible actions). Users also encountered *understandability* problems. In another study where the usability of Tor interfaces was examined, *understandability* was described as *users being aware of the tasks they must perform* [12]. In Weir et al. [6], this usability characteristic was defined as *know what to do next*, with a slightly different meaning, referring in this case to the degree to which users knew how to generate the random number from the

e-banking authentication mechanisms and apply it on the website for authentication. Efficiency problems are also reported by Herath et al. [10], who introduced *responsiveness* as a usability characteristic related to how much time the system takes to respond. In the case of an email authentication service, users form negative views of the tools' ease of use if it takes too long to indicate whether emails were sent from an authenticated entity. Finally, Lee and Kozar [7] studied factors that influence users' adoption of an antispyware tool and identified that *computer capacity* had a significant positive influence.

This study draws on the characteristics identified in related research to explore the users' perspective, identifying their needs and expectations as to which usability aspects they consider important and why.

3 Research Method

3.1 Research Design

Drawing on analysis of relevant research we identified a comprehensive set of usability characteristics (described in the following section) and designed three different scenarios that involved using three different, commonly used tools. The tools were chosen from a recent report by ENISA [4] measuring the usability of common privacy tools, and included Ghostery, an anti-tracking tool and Tor, an anonymising network. Furthermore, due to security problems caused by recent malware attacks such as ransomware, we included a popular antimalware tool, Malwarebytes. We had considered several potential tools for this survey, including anti-tracking tools such as Disconnect, uBlock Origin and Privacy Badger. However, we selected the above-mentioned tools based on their popularity and extensive use [4].

Through a cognitive walkthrough of the tools' functionality, we developed suitable scenarios including core security tasks. These scenarios were then given to third year ICT university students, their age ranging from 20 to 25 years old. As experienced ICT users rather than ordinary home users [19], they provided us with their views and feedback to gain in-depth insights regarding the usability of these tools. Participants were asked to install the tools on their personal computers unobserved and follow the required security tasks described in the scenarios. After completing the scenarios, students filled in an online questionnaire of 40 questions, on certain usability characteristics. The questions measured the users' views on the importance of each usability characteristics provided. The users selected their preference from a 5-level Likert scale ranging from 5-"very important" to 1-"unimportant". Prior to providing students with the questionnaires, a pilot study of the first scenario was performed with two individuals. The questionnaires also included open questions to receive more feedback on users' actions when completing the tasks, their understanding of how the tools work and their views regarding the tools' usability. Overall, we gathered completed questionnaires from 150 respondents 65% of whom were male, between March and April 2017.

To address potential biases that can occur from scenario-based questionnaires [19] we carried out follow-up interviews with 112 respondents, lasting approximately 15 minutes each. This step was included to further explore users' views and personal experience regarding the usability of the security and privacy tools, focusing on their effectiveness, their positive/negative aspects, any difficulties encountered, whether they would use the tools again and what changes, if any, they would make if they were to design the tools.

3.2 Description of Scenarios

The first scenario involved downloading and installing the English version of Ghostery, creating a user account, blocking and restricting a defined set of trackers on specific websites, using and configuring certain functionality options and cancelling previous actions. For the second scenario users had to download and install the English version of Malwarebytes, scan for "rootkits", carry out a threat scan and delete any malware that was identified for all available disks and then conduct a custom scan. Finally, in scenario 3 users were asked to download and install the English version of Tor and check the security settings, set security level to high, conduct a search with the appropriate search engine, visit specific websites, change the settings and revoke permissions to view content of the websites, visit a website that does not support SSL encryption and finally create a new identity.

4 Research Findings

In this section, we present the comprehensive findings from our analysis of the questionnaires as well as the interviews, regarding the usability aspects we explored. The usability characteristics of security and privacy tools that were identified in literature are presented under the relevant headings:

4.1 Usability Characteristics Relevant to Installation

Concerning installation, 121 out of 150 respondents find it "important" or "very important" that security tools have an easy installation process. More than three quarters of Ghostery users find it "important" or "very important" to avoid registering for ease of use, with two users finding registration *"unnecessary"* or a *"disadvantage"*. Many Ghostery users had a positive attitude towards the minor change that took place upon installation, namely the add-on on the browser toolbar. Most users reported that the minimum requirements for installation were clearly stated in all three cases.

4.2 Available Information and Support

In total, 137 users reported that it was “important” or “very important” for them to have access to available information to guide them on using the tool. During the interviews, users reported using a variety of different methods, including the manual, videos/tutorials, FAQs, etc. Ghostery users reported using the quick tour, FAQs and videos in this order of preference, suggesting a preference for speedy help.

While 106 users out of 111, who used the available help and support, considered the information they received adequate, some users resorted to the Internet for assistance, especially when using Tor. One user felt that the quick tour in Ghostery *“... didn’t show all the tool’s functionalities”*. Additionally, Ghostery and Tor users mentioned expecting to find a manual and would prefer it to be *“more detailed”*.

4.3 Language Used

82 users out of 150 reported that they were not concerned about the language and terms used by the tools, despite using the English version, not their native language. However, during the interviews some users had difficulty distinguishing between certain terms, e.g. “block” and “restrict” (scenario 1), “threat scan” and “custom scan” (scenario 2) and “temporarily allow scripts” and “globally allow scripts” (scenario 3). In all three scenarios, many users who had previously claimed to understand the differences failed to explain them correctly.

Thus, it seems that even experienced users may find the terminology confusing. Though one user commented that the *“complexity of the terms block and restrict might confuse novice users”,* in fact several respondents found the differences hard to explain, with one user attributing this to *“the lack of a concise and exact description”.* Users may therefore struggle to fully comprehend specific terms, especially in a non-native language*”. We also found that* the lack of consistency in similar terms used by different tools can confuse users (e.g. Malwarebytes uses “threat scan” and “custom scan”, with one respondent suggesting they should be named *“fastscan”* and *“fullscan”* respectively*)*.

4.4 Locatability

In total, 144 students replied that it is “important” or “very important” to find what they were looking for easily. During the interviews users described difficulties in finding some options. More specifically, most Ghostery users were unable to locate a specific functionality to perform a certain task (clear tracker settings). To overcome this, most resorted to alternative solutions such as visiting every website separately to undo the restricted trackers. While eventually managing to accomplish the task, they did so through a slower, cumbersome process. *“We were looking for an option to undo the restricted trackers collectively, but we didn’t find such an option”*. Furthermore, Tor users reported needing a lot of time to find the security slider, suggesting that security settings should be *“more visible (for a novice user)”*.

According to many comments, having all settings *"gathered together"* in one location is preferable. Moreover, regarding Ghostery, which is an add-on, users feel *"all procedures should be conducted from the Ghostery window rather than from different websites"*.

4.5 Understandability

125 users out of 150, considered knowing what to do next "important" or "very important. However, interview responses indicated that difficulties were encountered.

When using Ghostery, one user reported difficulty in identifying slow trackers as *"there wasn't an "indicative" picture"*. Another preferred the previous version of Ghostery because *"it was easier to understand and use"*. One user felt *"lost"* in performing the last 2 tasks and was under the false impression that he had completed the last task successfully, though he had not found the "clear tracker settings" button.

Tor users reported finding it hard to apply advanced settings such as "set security to high level*",* "test security settings*"*, "temporarily change settings to view the content of the specific website". One user was unsure what might happen after creating a new identity.

Conversely, all users using Malwarebytes reported that they knew what to do next with no difficulties cited. Malwarebytes was intuitive for users, guiding the user through the process, step by step. After selecting the category of scan and the drives and types of malware to be scanned, the scanning process started automatically.

4.6 Feedback

A total of 120 users considered receiving feedback as "important" or "very important". However, most users' responses in all scenarios indicated that they did not notice feedback from the tools. One Ghostery user commented that *"a notification that the restriction or blocking of trackers was successful"* would be useful, despite the tool displaying a similar pop-up message, while some users wanted more feedback *"about each tracker"*, and more specifically *"what it is and what it does"*.

Tor users would prefer more and visible feedback *"when the user changes security settings and detailed explanation about their impact"*. Users were not satisfied with the *"small banner"* that appeared on maximising the window to warn them that this practice is dangerous. Another user would prefer feedback when his browsing *"is not secure"*. On being asked to perform a search, more than half of the users chose Google Chrome instead of Duck Duck Go, despite the message "Search securely with Duck Duck Go" displayed on the first page of Tor.

Interestingly, concerning Malwarebytes, all respondents reported that feedback was noticeable, though a few would prefer more feedback after the scanning process, feeling that the tool did not *"adequately explain what kind of malware is identified"*. However, most interviewees did not read the reports provided by the tools.

4.7 Visibility

A total of 110 users regard as "important" or "very important" the existence of status indicators showing them what is happening inside the tool in terms of security (Malwarebytes) and privacy (Tor and Ghostery). In Ghostery, most users identify images of the padlock, the "tick" and the "shield" and their different colours (e.g. red for the padlock and "tick", green for the shield) as status indicators. One user preferred text to pictures suggesting that *"I would change the buttons block/restrict/trust so that they contain text"*. Some Malwarebytes users wanted more practical information e.g. *"to see a percentage of scan completion and what has been scanned so far and what is left to be scanned"*.

Most Tor users noticed pictures indicating the tool's security and privacy status (e.g. the pictures of Noscript, the padlock depicting a secure SSL connection, the warnings). Surprisingly, few users referred to the security slider as a status indicator, and only two cited the image of the Tor circuit (depicting the path of Tor computers used to hide the user's IP). Users' responses indicate that some status indicators in Tor are not easily noticeable, especially those crucial for ensuring users' privacy.

4.8 Undo

Although in all three scenarios almost all users found it "important" or "very important" to undo their actions, more than half of Ghostery users could not find the button "clear tracker settings" to undo the restricted trackers collectively and easily.

4.9 Error Prevention

The majority of Tor users reported that it is "important" or very "important" to receive error messages, displayed as warnings when users apply specific settings, such as maximising the window and allowing scripts globally.

4.10 Control

Although most respondents (142 out of 150) found it "important" or "very important" to be in control of the tool, some would prefer Ghostery to provide automated procedures and apply certain settings by default. One user *"would prefer it if some procedures were carried out automatically, if the tool blocks some suspicious trackers after installation (by default)"*. Another suggested *"algorithms should be used to block trackers automatically"*.

Malwarebytes users would also prefer some automated procedures. One user reported *"I would automate some updates and threat scans in case users have forgotten"*. While custom scan offers users control by selecting which drives they

want to scan, one user would prefer an option to scan everything, *"Threat scan didn't find one Trojan inside a file in disk "C". It was found only during custom scan. I would add one option for scanning all files, like fullscan".* Another user was not satisfied with the default settings of Malwarebytes, e.g. "Treat as malware" for PUP (Potential Unwanted Program) "*is selected by default […]. This is something that users might not want".* He also reported that as "Scan for rootkits" is deactivated by default *"users might miss this important option".*

Tor users controlled the security level, though they did recognise the trade-off between security and usability, *"When the tool is set to the highest level of security, it hides content from the websites […], the appearance of the website is unattractive".*

4.11 Learnability

The majority of users reported that it was easy to learn how to use the tools.

4.12 Satisfaction

While most users were satisfied with all the tools, some were dissatisfied with Tor, reporting *"high security settings result in a poorer browsing experience"*, *"being unable to read websites"* or "*having to verify that you are not a robot".*

4.13 Effectiveness

While most users found the tools usable and easy to use, they failed to perform some tasks successfully. For example, in Ghostery some users could not block some of the specified trackers, and many had trouble finding the option "clear tracker settings". In Tor, errors occurred, with some users not knowing how to test the settings, nor understanding which settings to configure to view all the website's contents. Many users did not select Duck Duck Go as a search engine.

4.14 Efficiency

In Ghostery some users reported *"a considerable delay on the loading of the website when using the tool".* With Malwarebytes, most users felt custom scan took many hours, which can be attributed to low computer capacity. Users also cited *"a negative impact on the speed"* of their computers during malware scanning. Tor users reported delays when browsing online, describing it as *"a slow tool, compared to other browsers. It protects users' privacy, but it sacrifices browsing speed, which is important for most internet users"*. Users thus want to use security and privacy tools without time delays and report that the more computer capacity the better their performance.

4.15 Design and Accessibility

One Ghostery user found the purple box (a feature showing all trackers of every website the user visits) *"unattractive"*. He further commented that he found it annoying as *"if there are many trackers on one website it covers the screen and the user has less visibility of the website's content. The purple box should be deactivated by default"*. Users want security and privacy tools to display the appropriate information in a clutter-free way.

Three Tor users were not satisfied with the design of the interface, describing it as outdated. As one said, *"the design components (images, layout of the websites) are not aligned with the modern design trends"*. Another user, however, commented favourably that *"Tors' settings are convenient for colour blind people like me"*.

4.16 Consistency

Users who are accustomed to using tools do not seem to welcome new features easily, with one regular Ghostery user preferring the previous version without the purple box, which in his opinion is not usable. This implies that users want consistency among different versions of security and privacy tools; otherwise they might not use them.

4.17 Control of user's personal data and transparency

Some users chose not to share their data with Ghostery. Although not in the scenario, this indicates users' concern about their privacy and their reluctance to share personal data with the privacy tool company. Respondents expressed their concern about the lack of *"transparency in the processing of data"* and the possibility that Ghostery might profit from *"selling anonymised data"*. Users might therefore be sceptical towards trusting a tool.

4.18 Availability of tools among various platforms

Availability of security and privacy tools among different platforms is a usability aspect. One user wanted to install Ghostery on his smartphone, but *"it was not available"*, while in the second scenario, a user reported that he could not install Malwarebytes because he is a *"Linux user"*.

Table 1. Users' views about usability characteristics

Usability Characteristics	**Studies**	**Users' views about security and privacy tools identified in this study**
Easy installation	[4]	Users find easy installation important.
Avoid registering	[4]	Users prefer not to register for ease of use.
Changes upon installation	[4]	Users find it important that tools have only minor changes upon installation.

Minimum requirements	[4]	Users want tools to indicate the minimum requirements for installation.
Available information and support	[4], [15]	Access to available information and support is valued.
Language	[15]	Users seem unconcerned about the number of technical terms used but may have difficulty in understanding some.
Locatability	[2], [6]	Users want to find the tools' security settings easily and in one place.
Understandability	[2], [5], [6], [12]	Users find it important to know how to perform security tasks.
Feedback	[15]	Users want detailed and visible feedback.
Visibility	[1], [2], [15]	Users find it important that tools show them what is happening in terms of security.
Undo	[15]	The ability to undo actions is important.
Error Prevention	[15]	Users find it important that tools inform them how to avoid potential errors.
Control	[15]	Most user value having control, though some prefer automated procedures.
Learnability	[8]	Users find it important that they can learn how to use the tools easily.
Satisfaction	[6], [18]	Users dislike tools which create inconvenience to ensure security.
Effectiveness	[6], [18]	Users found tools usable but failed to complete certain tasks.
Efficiency	[6], [18]	Users prefer not to experience time delays.
Aesthetic and minimalistic design	[15]	Users want tools to have minimalistic design and follow modern design standards.
Accessibility	[16]	Access for users with disabilities is valued.
Consistency	[15]	Users want consistency and may not welcome new features.
Control of user's personal data	[3]	Users want privacy tools to offer them control over their personal data.
Availability among platforms	This study	Users want to use tools among various platforms.

5 Discussion

This study has drawn on recent literature to identify characteristics of security and privacy tools considered important by users. We identified from questionnaires the following factors as valued by users: *easy installation, avoid registering with personal data, changes upon installation, available information and support,*

locatability, understandability, feedback, visibility, undo, error prevention, control, learnability and *satisfaction.*

Through interviews, we identified further issues that users consider important, such as *efficiency*, *design*, both in terms of aesthetics as well as functionality for users with special needs (accessibility), *consistency*, *transparency*, *control of personal data*, *minimum requirements* and *availability of tools among different platforms*.

We found that users clearly valued specific characteristics differently depending on the scope of each tool. For instance, Ghostery users highlighted characteristics such as *transparency, control of personal data, avoid registration with personal data, and control*, while Tor users focused on *efficiency*, *satisfaction*, *locatability, and understandability.* We also identified that relevant literature contains many overlapping or similar characteristics using different terms such as *visibility* and *feedback.*

This study focused on different factors regarding usability and special attention was given to the installation process, as identified in [4]. Findings show that users prefer security and privacy tools which have an easy installation process, do not require them to register with their personal data for ease of use, have only minor changes after installation and show users the minimum installation requirements.

As shown in the analysis, we identified that users have mixed preferences regarding the degree of control and tool automation. While many users preferred to be in control of the tools, some would prefer fully automated processes. For designers it might be useful to implement both approaches to satisfy the needs of different types of users, e.g. basic and advanced users. For example, by using artificial intelligence algorithms tools can support automation. Conversely, giving users the choice to select their preferred options provides them with the usability characteristic of control.

Interestingly, users generally sought more feedback. Related research posits that showing users many prompts can be frustrating and inconvenient [14]. However, our study highlights a need for more detailed and visible feedback. Furthermore, the need for detailed manuals was evident. In the case of Tor, which is an open source tool this is a challenge for developers.

Another interesting finding is that usability is related to the availability of tools among various platforms. With the widespread use of smart mobile devices, users need to be able to use security and privacy tools on their smartphones.

Design plays an important role in terms of usability. Malwarebytes was the tool that offered the most intuitive interface, with step by step guidance, which may account for users' successful use of the tool. Thus, designers need to create tools that guide the user. Furthermore, aesthetics impact on users' views regarding usability. They want tools to follow modern design trends, while also wishing to see what is happening concerning security and privacy through status indicators and pictures. Though as yet not much researched, another important aspect is the design of security and privacy tools suitable for people with disabilities.

During the interviews users commented on the trade-off between security and usability, citing a slower browsing experience and high security leading to inability to view website content, an issue under heavy discussion in relative literature [5,6,18] and one which needs to be addressed by designers.

Regarding language, the more languages are supported by the tool, the more usable it is. This study shows that, despite being ICT students with advanced English language skills, many users faced problems in understanding some options and completing tasks and some would prefer the tool in their native language. Given the problems experienced, one also expects that less computer-literate users might face more difficulty. Overuse of technical terms should be avoided, with those used being carefully selected and made explicit to users. This study highlights the need for consistency among terms used in security and privacy tools to avoid confusion, e.g. in antimalware tools different terms are employed for similar actions such as "fast scan" and "threat scan".

6 Conclusions

A broad spectrum of usability characteristics of security and privacy tools identified in literature has been analysed from the users' perspective through a scenario-based questionnaire and interviews to shed light on their views and expectations regarding the usability of security and privacy tools.

Findings of this study illustrate that users prefer speedy help, though in some cases look for detailed help. Applying consistency regarding the terms used and taking care with technical terms are issues highlighted by this study. Users clearly prefer all security settings to be gathered together to avoid spending time looking for them and status indicators to show the tool's internal operations in terms of security and privacy. Users prefer intuitive tools that guide them closely to complete tasks successfully.

We identified that while many users prefer automation of some security and privacy processes, others want control over the tool. Furthermore, our findings show concern among users about their personal data and how they are processed by tools. It is also clear that security and privacy tools should support the needs of people with disabilities. Interestingly, when a tool is updated with new features and layout, users accustomed to using it might feel negative towards the changes. Finally, users want security and privacy tools available among various platforms, especially on their smartphones and among different operating systems.

This study was conducted using specific tools and respondents cannot be considered representative users. Furthermore, users' reported intentions may not correspond to their actual behaviour. However, we elicited opinions, expectations and suggestions, resulting in an in-depth analysis of what users consider important regarding the usability of these tools and for what reason. These results provide designers and developers with insights into which usability characteristics users value and how to incorporate them. While there are obvious constraints in terms of complexity, time and cost, security and privacy tools need to be developed in a way that meets users' basic usability expectations.

References

1. Johnston, J., Eloff, J. H., Labuschagne, L.: Security and human computer interfaces, Computer and Security, 22, 675–684 (2003)
2. Furnell, S.: Usability versus complexity-striking the balance in end-user security, Network Security, 13–17 (2010)
3. Wästlund, E., Fischer Hübner, S., Graf, C., Hochleitner, C., Wolkerstorfer, P., Angulo, J.: Towards Usable Privacy Enhancing Technologies: Lessons Learned from the PrimeLife Project, PrimeLife (2011)
4. Enisa report: PETs controls matrix A systematic approach for assessing online and mobile privacy tools (2016)
5. Whitten, A., Tygar, J. D.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, USENIX Security Symposium (348) (1999)
6. Weir, C. S., Douglas, G., Carruthers, M., Jack, M.: User perceptions of security, convenience and usability for ebanking authentication tokens,Computers & Security, 28(1), 47-62 (2009)
7. Lee, Y., Kozar, K. A.:Investigating factors affecting the adoption of anti-spyware systems, Communications of the ACM, 48(8), 72-77 (2005)
8. Nielsen, J.: Usability engineering, Elsevier (1994)
9. Flechais, I., Mascolo, C., Sasse, M. A.:Integrating security and usability into the requirements and design process, Electronic Security and Digital Forensics, 1(1), 12-26 (2007)
10. Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R.:Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service, Information systems journal, 24(1), 61-84 (2014)
11. Krol, K., Philippou, E., De Cristofaro, E., Sasse, A.:"They brought in the horrible key ring thing!"Analysing the Usability of Two-Factor Authentication in UK Online Banking, NDSS Workshop on Usable Security (USEC) (2015)
12. Clark, J.,Van Oorschot, P.C.,Adams, C.:Usability of anonymous web browsing: an examination of tor interfaces and deployability, Symposium on Usable Privacy & Security, 41-51 (2007)
13. Cranor, L. F.,Buchler, N.:Better together: Usability and security go hand in hand, IEEE Security & Privacy, 12(6), 89-93 (2014)
14. Yee, K. P.: Aligning security and usability. IEEE Security & Privacy, 2(5), 48-55 (2004)
15. Nielsen J.:10 Usability Heuristics for User Interface Design, https://www.nngroup.com/articles/ten-usability-heuristics/, last assessed: 20/1/2018
16. Seffah, A., Donyaee, M., Kline, R. B., Padda, H. K.: Usability measurement and metrics: A consolidated model, Software Quality Journal, 14(2), 159-178 (2006)
17. Dhillon, G., Oliveira, T., Susarapu, S., Caldeira, M.: Deciding between information security and usability: Developing value based objectives, Computers in Human Behavior, (2016)
18. ISO9241-11:1998: Ergonomic requirements for office work with visual display terminals, Part 11: Guidance on usability (1998)
19. Howe, A.E., Ray, I., Roberts, M., Urbanska, M.,Byrne, Z.: The psychology of security for the home computer user, IEEE Symposium on Security and Privacy, 209-223 (2012)