What Parts of Usable Security Are Most Important to Users?

Joakim Kävrestad, Steven Furnell, Marcus Nohlberg

What parts of Usable Security are most important to users?

Joakim Kävrestad[1][0000−0003−2084−9119], Steven Furnell[2][0000−0003−0984−7542], and Marcus Nohlberg[3][0000−0001−5962−9995]

[1] University of Skövde, Sweden joakim.kavrestad@his.se
[2] University of Nottingham, United Kingdom steven.furnell@nottingham.ac.uk
[3] University of Skövde, Sweden marcus.nohlberg@his.se

Abstract. The importance of the human aspects of cybersecurity cannot be overstated in light of the many cybersecurity incidents stemming from insecure user behavior. Users are supposed to engage in secure behavior by use of security features or procedures but those struggle to get widespread use and one hindering factor is usability. While several previous papers studied various usability factors in the cybersecurity domain, a common understanding of usable security is missing. Further, usability covers a large range of aspects and understanding what aspects users prioritize is integral for development of truly usable security features. This paper builds on previous work and investigates what usability factors users prioritize and what demographic factors that affects the perception of usability factors. This is done through a survey answered by 1452 respondents from Sweden, Italy and UK. The results show that users prefer security functions to minimize resource consumption in terms of cost, device performance and time. The study further demonstrate that users want security functions to require as little effort as possible and just work. Further, the study determines that nation of residence and IT-competence greatly impacts the perception of usability for security functions while gender and age does so to a much lesser extent.

Keywords: usability · usable security · cyber security · human · user · perception.

1 Introduction

Cybersecurity is a property that is undeniably integral to modern individuals, organisations, and even nations [1, 2]. Much like [3], we consider cybersecurity to be a socio-technical property and a high level of security can only be achieved if social as well as technical factors are considered [4]. The importance of the social, or human, side of security is widely acknowledged by researchers as well as practitioners [5, 6]. Several recent industry reports even suggest that the human element is a part of most cybersecurity incidents, further emphasizing its importance [7, 8]. On this note, a preferable scenario is that users increase their security level through use of security functions such as e-mail encryption or multi-factor

authentication, and security practices such as good password creation and management strategies [9–12]. However, while such practices has been on the market for several decades, they are not in widespread use. As demonstrated in several previous papers, the (perhaps perceived) lack of usability seems to be a big part of the answer to why[13–15].

While the primary task of a security function is to provide security, functions designed to be used by end-users cannot do so unless they are adopted by users, and correctly used. Incorrect use can lead to a false sense of security or even be harmful [9]. For instance, password managers are considered a good way to use unique passwords for various accounts while only having to remember one master password. However, if that password is compromised, all accounts related to it are also compromised [16]. The consequence of security functions or practices not being adopted is obvious, the security they intend to provide is not provided. This is what often happens to so called secure password guidelines which prompt users to use long and complex passwords. Many users are unwilling to follow this guideline and select insecure passwords instead[17]. There are several theories that can be used to explain how users choose to adopt security functions and procedures. Three theories commonly used in cybersecurity can be briefly described as follows:

- Protection Motivation Theory (PMT) where [18] describe that peoples decision to protect themselves against a supposed threat are influenced by how severe and likely the person perceives the threat, how effective a preventative measure is, and the persons perceived ability to engage in that measure.
- Theory of Planned Behaviour (TPB) which highlights that actual behaviour is influenced by a persons perception of how easy or difficult a certain behaviour is [19].
- Technology Acceptance Model (TAM) which in its original form describe that a users decision to adopt a technology is based on how useful she perceives the technology to be, and how easy she perceives it to be to use the technology [20, 21].

Applied to the cybersecurity domain, PMT, TPB, and TAM demonstrate that usability is precursor to user adoption of security functions and practices. User adoption, in turn, is an obvious precursor to whatever security a function or practice is intended to add. As such, usability is a crucial aspect to research in relation to end-user security. While there has been a fair bit of research conducted on usability of security functions, a fundamental issue seems to be that there is no common understanding of what usability means to the cybersecurity community. This is demonstrated how various previous papers consider usability of security functions in vastly different ways. To exemplify, [22] evaluates a subset of usability criteria in the context of phishing, and [23] discusses usability in the context of IoT access control without further describing what usability in that context entails. Further, the System Usability Scale (SUS), presented by [24] as been adopted in the cybersecurity domain by, for instance, [25]. While SUS measures important aspects of usability it does not factor in all aspects that are

considered important in the cybersecurity domain, for instance risk associated with incorrect use [9].

A recent literature review [26] summarizes how usable security has been discussed in 70 scientific publication from 2015 to 2020. [26] presents 31 aspects of how usability has been studied in the cybersecurity domain, and groups those into 14 themes. Our study seeks to expand on the work conducted by [26] by exploring which of those aspects that are considered the most important by users. The study was performed as a survey reaching more than 1400 respondents and provides insight into what usability features that users perceive as most important. It also investigates how the perception of usability features is impacted by various demographic variables. As such, it provides insight that can support practitioners towards development of usable security functions and procedures. the study further provides the research community with a better understanding of what users considers to be the most important usability aspects, and how demographic aspects impact the perception of usable security.

The rest of this paper is structured as follows; Section 2 describes the methodological approach, section 3 presents and analyses the results which are further discussed in section 4 before the paper is concluded, and directions for future work are presented in section 5.

2 Methodology

With the purpose of collecting quantitative data from a large sample of respondents, a web-based survey was used. The survey panel company Webropol was hired for the distribution of the survey and while this approach restricted the range of possible participants to the members of Webropols panel, it is a practically feasible method to achieve a sample of high quality [27]. It also minimizes demographic bias, and accidental sampling bias common when distributing web based surveys using, for instance, social media [28]. A stratified sampling approach was used to generate a probability sample [29]. The panel members were split into strata based on gender, age, and geographical region. Equal proportions from each strata were then recruited using simple random sampling [30]. The primary target of the survey was Swedish users, and the target sample size for Swedes was set to 800 respondents. With the goal of comparing the results to users from other European nations, samples with a target size of 300 respondents were drawn from UK and Italy. UK and Italy was chosen since they, according to [31], belong to different culture groups than Sweden.

The survey was part of a larger survey and, for the purpose of this paper, contained demographic questions describing the respondents perceived gender, IT-competence and age. The participants were then asked to pick the five most and least important usability aspects from a list of 21 aspects derived from [26]. The original list by [26] included 31 aspects. However, the surveys development and testing phase revealed that several of those were too similar, or could be perceived in different ways by the respondents. They were therefore combined and/or reworded to ensure that that the list of options was easy for the re-

spondents to understand. For instance, [26] describe compatibility with systems and services, and compatibility with other security solutions as two separate usability aspects. In this study, they were combined into one answer option stating *It should work with all sites and services I use so that I only need one tool of each type*. Further, [26] describes several types of interference to the users workflow and those were combined to one statement expressed as *It should not interfere with the way I work*. The complete list of aspects is presented along with the results to save space, and appeared to the participants in randomized order to minimize responder bias. Both questions were followed by a free-text field where the respondents could add additional comments. Before the survey was distributed, it was taken through a pilot procedure in three steps:

1. A small sample was recruited using social media, and those respondents were specifically asked to provide feedback on the structure and readability of the survey.
2. Two respondents were asked to fill out the survey under personal supervision from a researcher, they were also asked to continuously express their thoughts while filling it out.
3. The survey was distributed to a sample of peers who were asked to assess it in relation to the research aim.

For data analysis, the percentage of respondents picking each aspects was first reported and a maximum 95% confidence interval computed as suggested by [32]. Next, the impact of various demographic factors was investigated by testing how the distribution of answers was impacted when the results of the full sample was divided based on nation, gender, IT-proficiency and age, respectively.

The statistical analysis was performed using chi-square because of the non-parametric nature of the collected data [33], and formally measured if the distribution of data points within a demographic group differed from an expected distribution with statistical significance. The conventional significance level of 95% was adopted in this study. Note that, while data is presented as percentages throughout this study, frequencies in absolute numbers was used for the chi-square tests.

3 Results and Analysis

Webropol distributed the survey to a sample of 10 times the target sample size and the survey was open for one week. A total of 1452 respondents completed the survey, and were distributed over the national answer groups as follows:

- Sweden: 834 participants
- Italy: 314 participants
- UK: 304 participants

The respondents were rather evenly divided based on gender and spread through various age groups as shown in Table 1. However, reported level of IT-competence differed between the groups, with Italian respondents reporting to be more IT-competent, on average.

Gender	**Sweden**	**UK**	**Italy**
Female	45.6	53.3	43.9
Male	54.2	46.7	55.7
Other/prefer not to say	0.3	0	0.2
Age	**Sweden**	**UK**	**Italy**
18-25	8.3	1.0	4.1
26-35	20.3	18.1	21.3
36-45	18.8	25.7	31.2
46-55	23.9	18.1	20.7
56-65	15.3	21.4	15.3
66-75	13.3	15.5	7.3
Above 76	0.1	0.3	0
IT-Competence	**Sweden**	**UK**	**Italy**
Professional - working in, Hold a degree in or study IT	9.4	9.9	22.3
Expert user - Interested user that know my way around IT. Usually asked to help people with home routers, printer installations etc	22.3	19.4	27.7
Average user - I use IT with no major problems but need help occasionally	65.1	64.1	38.5
Below Average - I have a hard time using IT and feel like I need help with tasks that others do with ease	3.2	6.6	11.5

Table 1. Demographic overview (in percent)

The respondents were then provided with the following information before they were asked to rate what five usability aspects they perceived as most and least important.

> *This part of the survey concerns what properties a security tool or functions should possess for you to use it. We want you to select the five most and the five least important properties from a list of 21 properties. A security tool or function includes anything designed to improve your level of IT-security and that you can choose to use. Some examples are:*
> - *Password creation guidelines (suggestion for password length, complexity, etc)*
> - *Encryption software, for instance, e-mail encryption tools used to encrypt e-mails or data encryption tools used to encrypt your computer*
> - *Browsing filters that warn you if you are visiting a web site that can be fraudulent*
> - *Malware (eg Viruses and Ransomware) protection software*
>
> *We want to know which of the following properties you consider to be the most important and the least important. The first question will ask you to check the five most important properties and the second will ask you to check the five properties you think is least important.*
> *All questions are followed by a text-box where you can input additional comments.*

The available options and the percentage of respondents choosing each options is displayed in Table 2, sorted in order of preference according to the complete data-set. As seen in the Table 2, a general tendency is that the respondents

Option	**Sweden**	**UK**	**Italy**	**All**
It should not be costly	41.5	50.3	44.0	43.7
It should be easy to understand and navigate the interface	42.6	42.8	32.8	40.5
It should not impact the performance of my device	42.5	46.7	30.3	40.2
It should not take a lot of time to use	41.0	32.6	35.4	38.0
Information about how to use it should be easy to find and understand	36.3	32.2	32.2	34.6
It should work with all sites and services I use so that I only need one tool of each type	37.4	31.0	20.4	32.3
It should not interfere with the way I work	31.5	30.9	24.2	29.9
It should require as little interaction from me as possible	33.3	27.6	21.0	29.5
I should not need to learn how to configure or manage it, and default configuration should be safe to use	30.7	24.3	22.3	27.6
It should not take a lot of time to install	25.2	28.6	27.4	26.4
When I need to make a decision, the tool should provide information about the different options	20.0	20.7	27.7	21.8
It should not put me under time pressure	20.4	19.1	20.4	21.1
It should be developed by, or recommended by someone I trust	20.0	19.4	19.1	19.7
Benefits and effects of using different security options should be clearly presented	14.0	15.8	29.9	17.8
The tool should provide feedback such as progress updates, system status etc	15.4	16.5	16.2	15.8
It should allow me to customize the configuration to my liking and adapt it to my skill level	13.2	14.1	21.7	15.2
I should be able to adjust the interface to my preference	11.3	14.5	25.16	14.9
It should be predictable; similar tasks should work in the same way and it should be easy to recognize requirements and conditions during setup	14.2	13.5	16.9	14.6
It should be possible to handle accounts for different users	8.2	14.5	20.7	12.2
It should be perceived as cool by others	2.6	4.9	12.4	5.2
Maximum 95% CI	3.3	5.6	5.4	2.6

Table 2. Percentage of participants picking the respective options as the *most* important.

favour aspects that minimize cost and resource consumption as well as ease of use. The preferred ease of use properties can be summarized as properties where interaction and time consumed using the security function is minimized. On the other hand, properties speaking to customizability are less favoured. National differences can be observed for several properties, and those will be further explored below.

The results for the second question, asking the respondents to pick the five properties they perceived as least important, are presented in Table 3. It is sorted in order of preference according to the complete data set.

Option	**Sweden**	**UK**	**Italy**	**All**
It should be perceived as cool by others	79.6	66.8	39.8	68.3
It should be possible to handle accounts for different users	48.8	38.8	25.5	41.7
I should be able to adjust the interface to my preference	36.1	29.9	28.0	33.6
It should allow me to customize the configuration to my liking and adapt it to my skill level	36.9	30.6	22.6	32.5
It should be developed by, or recommended by someone I trust	31.4	29.0	32.8	31.2
The tool should provide feedback such as progress updates, system status etc	33.6	28.0	26.1	30.8
It should not take a lot of time to install	31.1	22.0	27.4	28.4
It should not put me under time pressure	24.2	29.3	31.5	26.9
When I need to make a decision, the tool should provide information about the different options	19.8	30.3	27.7	23.7
Benefits and effects of using different security options should be clearly presented	23.7	19.1	22.3	22.5
It should be predictable; similar tasks should work in the same way and it should be easy to recognize requirements and conditions during setup	21.1	24.0	23.9	22.3
It should require as little interaction from me as possible	16.2	22.0	28.7	20.1
It should not be costly	17.2	18.8	28.0	19.8
I should not need to learn how to configure or manage it, and default configuration should be safe to use	17.4	22.7	20.4	19.2
It should work with all sites and services I use so that I only need one tool of each type	13.9	20.1	16.6	15.8
It should not interfere with the way I work	13.1	15.1	20.7	15.2
It should not take a lot of time to use	10.0	17.1	21.0	13.8
It should not impact the performance of my device	10.8	14.8	19.1	13.4
Information about how to use it should be easy to find and understand	8.2	11.8	19.4	11.4
It should be easy to understand and navigate the interface	7.1	9.9	18.5	10.1
Maximum 95% CI	2.7	5.3	5.4	2.4

Table 3. Percentage of participants picking the respective options as the *least* important.

As seen in Table 3, the least preferred options follow the same line as the most preferred option. Customizability options are in this case selected over options speaking to ease of use and limited need for interaction. Further, Tables 2 and 3 suggest that the participants do not care about how cool the functions are perceived by others and are not interested in spending time and money on security features and functions.

The next part of the analysis investigated how the results are impacted by the examined demographics aspects; nation, perceived gender, perceived IT-competence and age. Chi-square was used to measure if the distribution of data points within a demographic group differed from an expected distribution, given the complete data set. The analysis first measured the effect of each individual demographic on each data point. The analysis then measured the effect of gender, age and IT-competence within each national answer group. As such, 168 tests were performed and, given the permitted space, not presented in detail. To exemplify, the first test measured the impact of *nation* on the option *It should not be costly* for the question *most*. Key statistics are presented in Table 4

Answer	**Sweden**	**UK**	**Italy**	**chi-square**	**Sig.**
Yes - Observed	344	153	138	7.475	0.024
Yes - Expected	364.7	132.9	137.3		
No - Observed	490	151	176		
No - Expected	469.3	171.1	176.7		

Table 4. Example of statistical analysis using chi-square and the option *It should not be costly* for the question *most*

The hypothesis tested in this example is that *Nation impacts the number of respondents who perceive "It should not be costly" as one of the most important usability aspects for security features.* The hypothesis is supported given that the p-value is below 0.05, which is true in this case. Table 5 provides an overview of the demographic aspects that were shown to have a significant impact on what usability aspects respondents rank as most important. Significant tests are marked with an asterisk (*).

As shown by Table 5, demographics do impact what usability aspects respondents perceive as most important and nation of residence and perceived IT-competence are the most prominent demographic aspects while age and gender impacts far fewer of the usability aspects. It could, however, be noted that nation and IT-competence impact the same aspects in nine cases and the sample from Italy is distributed differently than the other sampling groups on the demographic of IT-competence (as seen in Table 1). Thus, it is hard to say if the perception of those aspects is impacted by IT-competence, nation, or both. Table 6 provides an overview of the demographic aspects that were shown to have a significant impact on what usability aspects respondents rank as least important, significant tests are marked with an asterisk (*). While there is some variation between Tables 5 and 6, nation and IT-competence are the demographic factors influencing the perception of most usability aspects. Gender and age, on the other hand, influence below 25% of the aspects.

Option	Nation	Age	IT-comp.	Gender
It should not be costly	*	*	*	
It should be easy to understand and navigate the interface	*		*	*
It should not impact the performance of my device	*		*	
It should not take a lot of time to use	*			
Information about how to use it should be easy to find and understand		*		*
It should work with all sites and services I use so that I only need one tool of each type	*		*	
It should not interfere with the way I work	*	*		
It should require as little interaction from me as possible	*			
I should not need to learn how to configure or manage it, and default configuration should be safe to use	*			
It should not take a lot of time to install		*	*	
When I need to make a decision, the tool should provide information about the different options	*			
It should not put me under time pressure			*	
It should be developed by, or recommended by someone I trust				
Benefits and effects of using different security options should be clearly presented	*		*	
The tool should provide feedback such as progress updates, system status etc			*	
It should allow me to customize the configuration to my liking and adapt it to my skill level	*		*	*
I should be able to adjust the interface to my preference	*		*	*
It should be predictable; similar tasks should work in the same way and it should be easy to recognize requirements and conditions during setup				
It should be possible to handle accounts for different users	*		*	
It should be perceived as cool by others	*	*	*	

Table 5. Overview of what demographics that had a significant impact on what usability aspects that were perceived as *most* important, in the complete data set (n=1452). It is ordered with most frequently picked option in the complete sample on top.

4 Discussion

The aim of this study was twofold; the first aim was to analyze what usability aspects that users consider most important for security functions, and the second was to identify demographic aspects which affect how those usability aspects are perceived. The study continued on the work by [26] and derived 21 usability aspects from the list of 31 usability aspects presented there. The study was

Option	Nation	Age	IT-comp.	Gender
It should be perceived as cool by others	*	*	*	
It should be possible to handle accounts for different users	*	*	*	
I should be able to adjust the interface to my preference	*		*	
It should allow me to customize the configuration to my liking and adapt it to my skill level	*		*	
It should be developed by, or recommended by someone I trust				
The tool should provide feedback such as progress updates, system status etc	*		*	*
It should not take a lot of time to install	*	*	*	*
It should not put me under time pressure	*			*
When I need to make a decision, the tool should provide information about the different options	*			
Benefits and effects of using different security options should be clearly presented				
It should be predictable; similar tasks should work in the same way and it should be easy to recognize requirements and conditions during setup				
It should require as little interaction from me as possible	*			
It should not be costly	*			
I should not need to learn how to configure or manage it, and default configuration should be safe to use				
It should work with all sites and services I use so that I only need one tool of each type	*			
It should not interfere with the way I work	*	*	*	
It should not take a lot of time to use	*		*	
It should not impact the performance of my device	*	*	*	
Information about how to use it should be easy to find and understand	*		*	*
It should be easy to understand and navigate the interface	*		*	

Table 6. Overview of what demographics that had a significant impact on what usability aspects that were perceived as *least* important, in the complete data set (n=1452). It is ordered with most frequently picked option in the complete sample on top.

conducted using a web based survey in order to generate a large sample of respondents, and resulted in a data set with survey data from 1452 individual respondents from Sweden, Italy and UK. The survey was carefully developed by the research team and evaluated in a three-step pilot procedure to ensure that is was appropriate for the study aim and easy to understand for respondents.

The first aim was meet by two questions where the respondents were asked to rate the five usability aspects they perceived as most and least important. The intent was to let the two question combined serve as a form of triangulation around the question of what aspects the respondents considered to be most important [34]. The results show that the usability aspects perceived as most important are those reflecting resource minimization and ease of use. The aspects perceived as least important reflect customizability interfaces and behaviour. One respondents commented as follows; *"Needs to be free. Runs in the background with no input from me. Should run without impacting on my use of technology"*. That quote is a good summary of the study's results in regards to the first aim. This notion aligns well with previous research suggesting that users just want cybersecurity to work.

The second aim was meet by dividing the dataset based on nation, gender, age and reported IT-competence and analyzing if any of those factors significantly impacted the respondents perception of the usability aspects. Repeated chi-square tests revealed that nation and IT-competence both affected the perception of up to 75% of the included usability factors while age and gender both only impacted about 25%. It should be noted that that the distribution of answers to the demographic question about IT-competence is uneven between the national sample groups, and that can impact the results in this case. Still, the results do suggest that nation of residence does impact how users perceive the importance of usability aspects. This notion aligns well with previous research suggesting that both culture and IT-competence are important factors in human aspects of cybersecurity [35]. However, the study also suggest that age and gender does not affect how users prioritize usability aspects of security functions to any large extent, and this is surprising due to previous research suggesting age and gender to be important factors in cybersecurity in general [36–39].

By extending the work by [26], this study contributes to the academic community with increased understanding about what the concept of usable security entails. It does so by providing an analysis of what usability aspects that users consider to be most important and is, to the best of our knowledge, the first publication of that sort. This paper also demonstrate the complex nature of the human aspects of cybersecurity and emphasizes the need for continued research in pursuit of generalizable results that can help the community move towards better cybersecurity behaviour with cost-effective means.

As a contribution to practitioners, the results of this survey insight depicting what security aspects to focus on when implementing security features. Since the results of this survey shed light on what usability features that are prioritized by the most users, it also shows which of those aspects a feature appealing to as many users as possible should include. Perhaps at least as important, it uncovers which aspects that are perhaps not worthwhile to put efforts into.

5 Conclusions and future work

The first part of this study asked the respondents to rank the five most and five least important usability aspects of security functions. The available aspects are presented in Table 2. As a summary, the results suggest that respondents prioritize resource effective security functions. The functions should not be costly, impact device performance, or require a lot of time to use. This notion is emphasized by several free-text comments stating that *"it should just be there and work"*. The results also show that the respondents want security functions to be easy to use and to understand. As a general rule, usability aspects speaking to more advanced use are found at the bottom of the list of preferred aspects. Those aspects include customizability, ability to handle multiple accounts and existence of feedback from the security features.

The second part of the analysis evaluated if nation, gender, age or IT-competence had an impact on what usability aspects that are most or least preferred. This analysis showed that nation and IT-competence had the most widespread impact with nation impacting the perception of about 75% of the aspects, and IT-competence impacting about 55%. It should here be noted that the answers to the demographic question about IT-competence are unevenly distributed between the national sample groups, and that can impact the results in this case. Finally, age and gender both impacted the perception of less than 25% of the included usability aspects, suggesting that those demographics are not as important when it comes to the perception of usability in relation to security functions.

This paper shows that several demographic aspects can impact the usability aspects that users prioritize for security functions. Given the limitations of space, it was not possible to dwell into the nature of this effect and further analysis of the demographic effect in this, or other, data sets is a natural continuation of this work. Further areas for future work could be to expand on this study by including more demographic aspects such as disabilities or more different nation groups.

References

1. Huskaj, G., Wilson, R.L.: An Anticipatory Ethical Analysis of Offensive Cyberspace Operations. In: Cruz, T., Simoes, P. (eds.) In: Proceedings of the 15th International Conference on Cyber Warfare and Security. Academic Conferences and Publishing International Ltd. (2020)
2. Vroom, C., Von Solms, R.: Towards information security behavioural compliance. Computers & security 23(3), 191–198 (2004)
3. Al Sabbagh, B., Kowalski, S.: St(cs)2 - featuring socio-technical cyber security warning systems. In: Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec). pp. 312–316 (2012)
4. Paja, E., Dalpiaz, F., Giorgini, P.: Managing security requirements conflicts in socio-technical systems. In: Ng, W., Storey, V.C., Trujillo, J.C. (eds.) Conceptual Modeling. pp. 270–283. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)

5. Furnell, S., Esmael, R., Yang, W., Li, N.: Enhancing security behaviour by supporting the user. Computers Security 75, 1–9 (2018)
6. Cybint: 15 alarming cyber security facts and stats. (2020), https://www.cybintsolutions.com/cyber-security-facts-stats/
7. EC-Council: (2019), https://blog.eccouncil.org/the-top-types-of-cybersecurity-attacks-of-2019-till-date/
8. Soare, B.: Vectors of attack (2020), https://heimdalsecurity.com/blog/vectors-of-attack/
9. Whitten, A., Tygar, J.D.: Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: USENIX Security Symposium. vol. 348, pp. 169–184 (1999)
10. Aljahdali, H.M., Poet, R., Ieee: The affect of familiarity on the Usability of Recognition-based graphical Password Cross cultural Study Between Saudi Arabia and the United Kingdom, pp. 1528–1534. IEEE International Conference on Trust Security and Privacy in Computing and Communications
11. Alsaiari, H., Papadaki, M., Dowland, P., Furnell, S.: Graphical one-time password (gotpass): A usability evaluation. Information Security Journal 25(1-3), 94–108
12. Das, S., Dingman, A., Camp, L.J.: Why johnny doesn't use two factor a two-phase usability study of the fido u2f security key. In: Proceedings of the International Conference on Financial Cryptography and Data Security
13. Florencio, D., Herley, C.: A large-scale study of web password habits. In: Proceedings of the 16th international conference on World Wide Web. pp. 657–666. ACM
14. Benenson, Z., Lenzini, G., Oliveira, D., Parkin, S., Uebelacker, S.: Maybe poor johnny really cannot encrypt: The case for a complexity theory for usable security. In: NSPW 15p. pp. 85–99 (2015)
15. Lerner, A., Zeng, E., Roesner, F.: Confidante: Usable encrypted email: A case study with lawyers and journalists. 2017 IEEE European Symposium on Security and Privacy (EuroSP) pp. 385–400 (2017)
16. Chaudhary, S., Schafeitel-Tähtinen, T., Helenius, M., Berki, E.: Usability, security and trust in password managers: A quest for user-centric properties and features. Computer Science Review 33, 69–90 (2019)
17. Haga, W.J., Zviran, M.: Question-and-answer passwords - an empirical-evaluation. Information Systems 16(3), 335–343
18. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change1. The journal of psychology 91(1), 93–114 (1975)
19. Ajzen, I.: From intentions to actions: A theory of planned behavior. In: Action control, pp. 11–39. Springer (1985)
20. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS quarterly pp. 319–340 (1989)
21. Davis, F.D.: A technology acceptance model for empirically testing new end-user information systems: Theory and results. Ph.D. thesis, Massachusetts Institute of Technology (1985)
22. Marchal, S., Armano, G., Gröndahl, T., Saari, K., Singh, N., Asokan, N.: Off-the-hook: An efficient and usable client-side phishing prevention application. IEEE Transactions on Computers 66(10), 1717–1733 (2017)
23. He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., Ur, B.: Rethinking access control and authentication for the home internet of things (iot). In: 27th USENIX Security Symposium (USENIX Security 18). pp. 255–272
24. Brooke, J.: Sus-a quick and dirty usability scale. Usability evaluation in industry 189(194), 4–7 (1996)

25. Khan, H., Hengartner, U., Vogel, D.: Usability and security perceptions of implicit authentication: Convenient, secure, sometimes annoying. In: Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). pp. 225–239
26. Lennartsson, M., Kävrestad, J., Nohlberg, M.: Exploring the meaning of "usable security". In: International Symposium on Human Aspects of Information Security and Assurance. pp. 247–258. Springer (2020)
27. Rivers, D.: Sampling for web surveys. In: Joint Statistical Meetings. p. 4 (2007)
28. Culotta, A.: Reducing sampling bias in social media data for county health inference. In: Joint Statistical Meetings Proceedings. pp. 1–12. Citeseer (2014)
29. Henry, G.T.: Practical sampling, vol. 21. Sage (1990)
30. Scheaffer, R.L., Mendenhall III, W., Ott, R.L., Gerow, K.G.: Elementary survey sampling. Cengage Learning (2011)
31. Inglehart, R., Welzel, C.: The wvs cultural map of the world. World Values Survey (2010)
32. Wheelan, C.: Naked statistics: Stripping the dread from the data. WW Norton & Company (2013)
33. Fowler Jr, F.J.: Survey research methods. Sage publications (2013)
34. Lincoln, Y.S., Guba, E.G.: Naturalistic inquiry (1985)
35. Joinson, A., van Steen, T.: Human aspects of cyber security: Behaviour or culture change? Cyber Security: A Peer-Reviewed Journal 1(4), 351–360 (2018)
36. Bansal, G., Hodorff, K., Marshall, K.: Moral beliefs and organizational information security policy compliance: The role of gender. Proceedings of the Eleventh Midwest United States Association for Information Systems pp. 1–6 (2016)
37. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L.: Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior 69, 437–443 (2017)
38. McGill, T., Thompson, N.: Gender differences in information security perceptions and behaviour. In: 29th Australasian Conference on Information Systems (2018)
39. Fatokun, F., Hamid, S., Norman, A., Fatokun, J.: The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: An empirical investigation on malaysian universities. In: Journal of Physics: Conference Series. vol. 1339, p. 012098. IOP Publishing (2019)