Disclaimer: This is a paper written for learning purposes in class and not peer-reviewed!
Please do not distribute.

"I'm a bit lazy :("
A Study on the Impact of Technical Background on Emotional Response regarding Security & Privacy

Authors:
Camila Fonseca,
Nicole Geymeier

March 22, 2024

Empirische Softwaretechnik

Paderborn University

Abstract

Security & privacy inherently adds overhead into people's affairs. As such, this research focused on the interaction between the field itself and the response of those who make use of it in their day-to-day life, viewing security through a human lens. When dealing with security & privacy, people might become overwhelmed and even stressed, both due to complexity and possible negative consequences, the extent of which may depend on their current knowledge and previous background in tech. We needed to further our understanding about how people feel about their security & privacy measures in order to improve our communication and approach towards end users, so the adoption of security & privacy measures can be improved and be more accessible. We conducted an online survey, with 62 complete responses, to gain insight into their security & privacy measures, behavior and feelings, as well as their background, in order to try to find and highlight a possible connection. We found out that those with a stronger technical background tended to have more positive emotions than their counterparts. The first group's biggest hurdle to adopting more security measures was them taking too much effort for too little perceived returns, whereas people with less technical background pointed at a lack of awareness about extra measures blocking them from adopting them.

1 Introduction

Security & privacy is no topic in and of itself, but usually in-between people and what they want to achieve. Additionally, the consequences of fruits of our effort in adopting measures to protect ourselves are (usually) not apparent in the short-term and only visible when something negative has happened. Nevertheless, security & privacy is a very important issue for individual people and businesses, as there is a lot of potential of damage: personal data can be stolen, credit card information can be misused or companies can face ransomware-attacks. In December 2023, millions of clients of the genomics and biotechnology company "23andme" got hacked. The hackers got access to 6.9 billion users accounts, where some of them included personal data like family trees, birth years and geographic locations [20]. Cyberattacks on medical infrastructure have increased in the last years, with more than 136000 cases in 2022 [8], and as a recent example, a cyberattack on three german hospitals on Christmas Eve 2023 [10].

Even though there are a lot of technical and non-technical options and measures to increase someone's security & privacy, it can be seen that not everybody adopts them. The Hasso Plattner Institute publishes the most-used passwords in Germany each year, where the most-used password (out of data from data leaks) is "123456789" [1] indicating that simple passwords are still widely used. The Cybersecurity & Infrastructure Security Agency of the United States (CISA) is developing a catalog of Bad Practices still used in organizations in an effort to eliminate the worst practices: using unsupported or end-of-life software, using known, fixed or default passwords or credentials and using single-factor authentication [2, 19].

Our aim is to analyse how people feel regarding their chosen security & privacy measures to gain deeper insights into peoples reactions. If there are emotions like feeling overwhelmed prominent, this knowledge could improve communication regarding security & privacy measures, and improve the advice given in order to increase their adoption.

There has already been broad research done in order to measure privacy and security measure adoption [25, 11, 18]. While security & privacy is important for many people according to studies, a deviation from the actual behavior adopted has been found, and named as the privacy paradox [15, 12]. Even though there is already research on the topic, there was not much studied about the feelings and emotional response of people yet. We think this is an important factor as we (as humans) and our decision-making are influenced by emotions and our perceptions of things [16].

To gain a better understanding of people's attitudes and feelings regarding security & privacy, and how these may be affected by a previous background in tech, we conducted an online survey to get information on people's feelings and perceptions. We focused on the following topics:

- Measures: What measures are used, experiences with security incidents
- Emotional impact: Feelings about taken measures and ability to take further measures
- Background: Whether there is a technical background (education, employment, personal interest)

The survey was online in January of 2024 and available in three different languages (english, german and portuguese). We received 62 complete submissions.

In this paper, we answer the following research questions:

- RQ1: Based on a list of the most commonly adopted security & privacy measures, what are the adoption levels for people with a previous tech-related background, and those without?
- RQ2: How does the adoption of these measures differ between backgrounds?
- RQ3: How do people feel about their taken measures? (E.g. Do they feel like they should be doing more / are doing too much? Do they stress that it is not enough?)
- RQ4: How does this subjective emotional response differ between backgrounds?

We find that the adoption rate does not have major differences across background groups, but overall those with a better technical background have higher adoption. Some categories see bigger differences across groups than others. Participants with a better technical background reported more positive feelings and self-descriptions than participants with less technical background. Additionally, people with less technical background felt higher need but worse ability to adapt new measures.

2 Background

This section aims to provide an overview on the topics that serve as base knowledge for our research.

Security Computer security, for the context of this paper, is mainly focused on controlling access to users' devices/accounts, keeping them protected from unauthorised actors. For example, securing authentication mechanisms, such as passwords or encryption keys through the means of external tools and good practices. Protection from external threats also includes protection from malware in its various forms of malicious software such as trojans (Seemingly benign software taking undesirable actions in a hidden manner.), ransomware (Software that locks down the user's device until a ransom is paid to the attacker.) or worms (Software that propagates by infecting other devices, and receives instructions from a remote attacker.) which compromise the three core pillars of Computer Security - Confidentiality, Integrity and Availability.

Privacy Computer privacy is all about controlling the flow of the users' information. It has to do with the users' ability to control who is allowed to access their data, under what conditions - as in, are they allowed to create copies of it, modify it, or share it with others - and to control how it is used. Protecting the data from eavesdropping is a facet of privacy as well, and an area where both privacy and security overlap. An user's privacy may also be breached due to their own actions, even if by accident, in a scenario where their security fails them and they're exposed to a threat such as a phishing attack.

Both privacy and security have technical aspects to it - encryption algorithms, code exploits - but both are also heavily dependent on the individual user behaviour in order to properly protect themselves. A list of the most common security measures have been compiled in the Security Behaviour Intention Scale [9] (SeBIS), which will be used thoroughly throughout this work.

Security being so dependent on an individual's actions, we must take into consideration the emotions that affect their behaviour. However, this is not easily observable nor straightforward to explain, as we can see by the **Privacy Paradox**, which is further explored in the next section, *Related Work*.

Security & Privacy Fatigue As presented by Tian et al. [23], privacy fatigue is defined as a form of fatigue - which is a result of people being overwhelmed with a certain matter, exceeding their ability to deal with it - that is specifically concerning privacy behaviours. In loose terms, this occurs when users become tired of, as an example (also given by Tian et al. in the cited paper), Network Security and loosen their defense against possible risks. Other research knows the term security fatigue as well, where the focus of the matter in which fatigue arises is security behavior. The terms security fatigue and privacy fatigue intertwine and overlap.

3 Related Work

Security & privacy are not trivial to quantify, in order to know how well protected someone is, but what we can do is analyze which measures they employ. In order to make this an attainable goal, we can consult a list of the most common security measures taken by users [25, 4], or examine the users' mental model of privacy [14]. And finally, we have the Security Behaviour Intentions Scale (SeBIS) [9] as a standard to measure end-user security behaviours.

However we must not only take into account people's knowledge of possible measures, but also their perception of risk and privacy level, as people's behaviours, and especially their information disclosure behaviour, are dependent on their perceived security & privacy risk [24], which in turn has an emotional impact that feeds back into altering security & privacy behaviours [13].

As Marlis et al. reported in their work [22], descriptive knowledge does not translate into more pronounced privacy behaviours, despite increasing users privacy concern. However, security & privacy fatigue has a stronger impact on users behaviour than privacy concern [6] which points to emotions having a strong impact on privacy behaviour, and are crucial to take into users' approaches to privacy risks [5].

This discrepancy between knowledge and behaviour has also been described as the privacy paradox [12], and this phenomenon weakens a possible link between technical background (and other factors such as financial resources) and online security & privacy behaviours even further [3].

There are different possible explanations for the privacy paradox presented by Gerber et al. in [12], of which we highlight the following:

- Privacy calculus: attempt to maximize benefits
- Bounded rationality & decision bias: imperfect decisions due to not-exhaustive information or lack of ability to process all information, therefore suffering from different biases
- Lack of personal experience and protection knowledge: privacy attitudes based on heuristics or secondhand experiences not stable enough to influence behavior, no or limited knowledge of technical solutions
- Social influence: expressed attitude reflects unbiased opinion, whereas actual behavior is affected by social factors like social pressure or stigma

However, this previous research does not look into possible connections between technical background and the emotional response of users, only their actual behaviour.

Previous studies [11] showcase the motivations (or lack thereof) that drive people to adopt new

security behaviours, highlighting the convenience / security trade-off that is pervasive in this matter, as well as the opposite outcome - what leads to people dropping previously adopted behaviours, either due to practical needs no longer existing [18] or sheer security & privacy fatigue [17, 23, 21, 7], leading to exhaustion and / or cynicism.

4 Methodology

4.1 Study Procedure

To assess the security & privacy behavior and associated emotions and feelings, we conducted an online survey in January 2024 using LimeSurvey. Additionally to the three main sections Measures, Emotions and Background, we had a short Introduction and a Demographics section, with a total of 32 questions. As we had limited resources in our class project to get survey answers, we provided the survey in three different languages spoken by the authors (english, german and portuguese) to reach more people in our communities. The collected data was imported into a spreadsheet software, where it was then cleaned and analyzed.

4.2 Study Structure and Data Collection

The survey consisted of an Introduction, three main categories and a Demographics section. The Introduction contained two questions to have an initial self-assessment, asking the participants about their familiarity with security & privacy concepts and assessment of the appropriateness of their taken measures. The main categories are Measures, Emotions and Background, and each contained 8 to 12 questions. The Measures section included questions regarding what security & privacy measures were currently in use by the participants, which (if any) security & privacy related incidents they could remember, and how they think their measures were able (or unable) to protect them. In the Emotions section we had questions about the feelings of the participants regarding their taken measures, how they assess their ability, and need, to take further measures, and what the reasons are not to use available security & privacy measures. Regarding the tech background we wanted to know whether the participants had (or are currently doing so) studied or worked in a CS / IT-related field, how they perceive their ability to complete tasks and solve problems on a computer, whether they have (professional) programming and / or experience in the field of security & privacy. The questions about demographics were limited to the age and the gender of the participants.

Some follow-up questions only appeared on positive answers to previous questions, in order to elaborate on specific topics, and therefore the number of questions that are actually displayed varies among the participants. Some other questions contained multiple sub-questions in a list, which were to be answered according to the same metric. To increase the reliability of the given answers, there was a possibility for each question to not be answered, e.g. select the option "No answer". Overall, most of the questions were closed-ended (yes or no) or provided 5-point

Likert-Scales (for familiarity, appropriateness, frequency and agreement). This is especially relevant for SeBIS, as its score is calculated as an average of the 5-point responses for each measure. It is important to note that some of the SeBIS measures are inverted, and as such, it is necessary to invert the scoring of these as well before calculating the final scores. For some questions, we provided multiple answers, for the participant to select all they found applied to themselves. For some topics, there were additional open-ended questions to enable further elaboration, if the participants were willing to provide more information. Those, among others, were marked by us as optional, which extend the duration of the survey to a maximum of 30 minutes, whereas the slim survey was estimated to take up 15 minutes. Besides the confirmation that the participant had read, and accepted, the informed consent sheet, no question was configured to be mandatory and therefore the participants could decline to answer any question.

Prior to sending out the actual survey, we conducted a pilot study to test the survey. This helped to uncover some technical inconsistencies and unclear formulations and we were able to make several improvements in wording and structure of the survey.

4.2.1 Recruitment

As we wanted to measure the impact of a tech-background, we were interested in people with different (both technical and non-technical) backgrounds. Besides being older than 18, there were no further restrictions on the eligibility of the participants. We approached people in our social environment with and without a tech-background, and some of them offered to further distribute the survey in their social environments, which presumably increased the heterogeneity of the participant pool.

4.3 Data Analysis

The raw data from the survey results was imported into Microsoft Excel, where it was cleaned, and analyzed. The quantitative data was aggregated and the qualitative data was translated into english and coded.

Regarding the background section of the data, it's relevant to know that despite the original intention to split the participants into two buckets - people with or without a background in computer or security & privacy related areas - we ended up splitting them into three buckets instead. Since we asked a multitude of questions in order to better understand the participants' background, some of them did not fall neatly into the binary options, leading to the introduction of the third option - "Some technical background". For this split, we took into account education and/or professional experience in the area, general computer-related proficiency, (Measured by the ability to complete tasks or goals, and to solve or work around unexpected problems.) programming experience (Both professional or otherwise.) and the existence of personal projects related to the area.

4.4 Ethical Considerations

Prior to answering in our survey, participants had to read and confirm the informed consent form. We used systems provided directly or indirectly by the University of Paderborn (Limesurvey, Sciebo, Overleaf) to safely collect and store the data. We are aware that a survey regarding security & privacy might unsettle participants about their taken measures. Therefore we provided some resources in the end message of the survey, to serve as a entry point to the topic: recommendations of the US Cyber Defense Agency (CISA) regarding security[1], a password manager (Bitwarden)[2] and a website to check whether email addresses have been in a data breach[3].

This study was reviewed by our professor[4] (and her team) as the principle investigator, and received their approval before starting the actual data collection. For the review, the Standard questionnaire for applications for ethical review by the Paderborn University Ethics Committee was used, which assessed that for this study only a standard procedure / review was necessary, and not an in-depth one. As this is a class project, the supervision laid on our instructors and not the institutional review board (IRB) of the University of Paderborn.

4.5 Limitations

Due to the restricted participant pool, limited to people in social circles of the researchers, and of limited heterogeneity, this study is not representative of the wider population. As the survey relies only on people's answers, it is eschewed by the participants' recall ability and self-reporting bias.

Furthermore we did not perform statistical inference as our statements are not based on statistically confirmed differences. Therefore our results form hypotheses, which could be tested with a representative study setup.

[1] `https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-cyber-safe`
[2] `https://bitwarden.com/`
[3] `https://haveibeenpwned.com/`
[4] Prof. Dr. Yasemin Acar, Paderborn University, Department of Computer Science

5 Results

5.1 Demographics

The survey was online in January of 2024 for 16 days, having received 80 submissions, 62 of which were complete. Of the survey participants with complete responses, 65% were male, 27% were female, 5% were non-binary and 3% chose not to answer as seen in Table 5.1. Among all of the respondents, four selected both 'male' and 'prefer to self-describe' and filled out the free-text area with nonsense, in an attempt to be humorous. For the effects of this study, those were registered solely as 'male'. 44% of the participants had a solid technical background, 27% had some, and 29% had no technical background.

Table 5.1: **Aggregated demographics** for the 62 participants with complete responses

Gender			**Age**			**Background**		
Female	17	(27,4%)	18-25	21	(33,9%)	No	18	(29%)
Male	40	(64,5%)	26-35	17	(27,4%)	Some	17	(27,4%)
Non-binary	3	(4,8%)	36-45	7	(11,3%)	Good	27	(43,5%)
Prefer to self-describe	(4)*	-	46-55	12	(19,4%)			
Prefer not to answer	2	(3,2%)	56-65	4	(6,5%)			
			> 65	0	-			
			No answer	1	(1,6%)			

* These 4 participants also checked 'male' and provided nonsense responses.

5.2 What are the adoption levels of security & privacy behaviours and how do they differ between background groups?

Overall, the SeBIS category with the highest adoption level is **Device Securement**, having an average score of 4.36, with a large gap from the second highest, **Updating**, which is closely followed by **Proactive Awareness**, and finally, we have **Password Generation** as the category with the lowest average adoption level.

Table 5.2: **Most and least adopted measures** of SeBIS, among all groups

Most adopted measures:	**Score**
- I use a PIN or passcode to unlock my mobile phone	4.81
- I use a password/passcode to unlock my laptop of tablet	4.79
- I set my computer screen to automatically lock if I don't use it for a prolonged period of time	4.23
Least adopted measures:	
- I change my passwords, even if it is not needed.	2.02
- I verify that my anti-virus software has been regularly updating itself.	2.84
- When browsing websites, I mouseover links to see where they go, before clicking them.	2.97

Among the background groups, for the **Device Securement** category the results were almost uniform, having a 0.21 amplitude in the average, whereas **Proactive Awareness** and **Password Generation** had a larger gap (0.39 and 0.35, respectively) and lastly **Updating** which had the largest difference of the individual categories, at 0.79. (Further detail can be consulted in section 7.1)

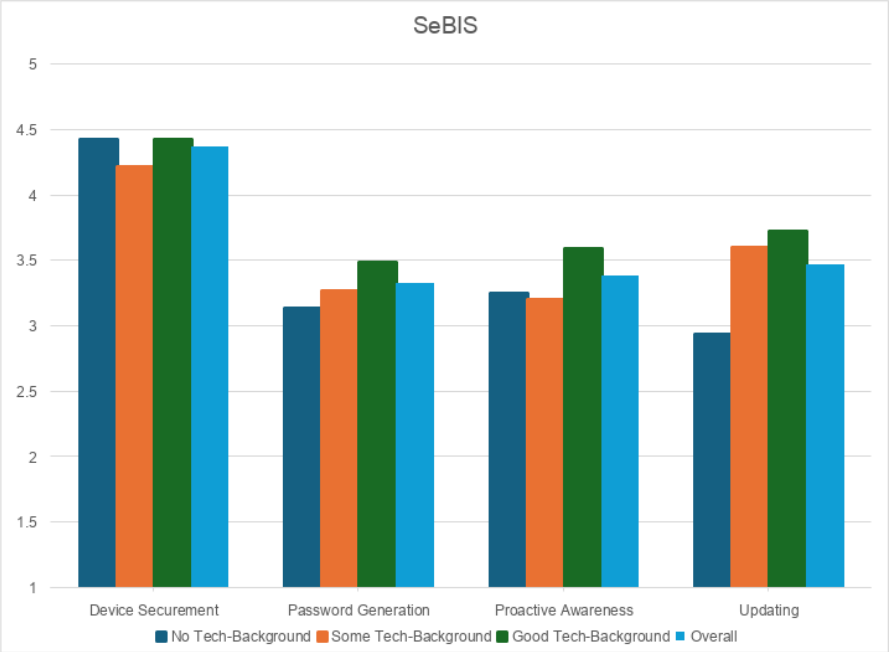
The **Updating** category had a large discrepancy between the "No Tech-Background" group and both "Some" and "Good" tech-background groups, as the gap from the first to the second was of 0.66 points, and from second to the third, 0.13 points.

Password Generation follows this same pattern (Good > Some > Bad), but with smaller gaps (0.14 and 0.22).

However, **Proactive Awareness** shows a different pattern, having the "Some Tech-Background" group with the lowest score, following by "No Tech-Background" and lastly "Good Tech-Background", with a gap of 0.05 and 0.34, respectively.).

Device Securement has the same pattern, with the respective gaps of 0.21 and 0.005 (Some < Bad < Good).

Figure 5.1: Adoption levels of the measures in SeBIS, for each background



15 participants reported having adopted extra measures asides from the ones already present in SeBIS. Out of the 28 new measures, the most common was two-factor authentication" (Or multi-factor authentication), followed by password managers / safes and adblockers / browser filters, including both website-level filtering and DNS-level domain filtering.

The most and least adopted SeBIS measures can be seen below in Table 5.2. The two most adopted SeBIS measures are equal for all three groups, with the third differing across groups, having "I set my computer screen to automatically lock if I don't use it for a prolonged amount of time" for both "No Tech-Background" and "Good Tech-Background" groups, whereas the "Some Tech-Background" group has the measure "I include special characters in my password even if it's not required.". As for the least adopted measures, both first and third are the same across all groups. The second differs between groups, being "I know which website I'm visiting by looking at the URL bar" for the "Some Tech-Background" group, and " I verify that my anti-virus software has been regularly updating itself" for both "Good Tech-Background" and "No Tech-Background".

The measures with the biggest differences in adoption were:

- "I verify that my anti-virus software has been regularly updating itself" with an amplitude of 1.3, between the "No Tech-Background" and "Some Tech-Background" groups, with the latter being the higher score.
- "I try to make sure that the programs I use are up-to-date." with an amplitude of 1.06 between the "No Tech-Background" and "Good Tech-Background" groups, with the latter being the higher score.
- "When browsing websites, I mouseover links to see where they go, before clicking the URL." with an amplitude of 0.9 between the "No Tech-Background" and "Good Tech-Background" groups, with the latter being the higher score.
- "I know which website I'm visiting by looking at the URL bar, rather than based on its look and feel." with an amplitude of 0.87 between the "Some Tech-Background" and "Good Tech-Background" groups, with the latter being the higher score.

21 of the participants reported having had a security incident in recent memory, of which 8 reported being driven to adopt new measures due to it. 29 of the participants knew of a moment when their adopted measures protected them, and 11 reported being aware of a moment when their adopted measures *failed* to protect them.

When asked about recent security incidents experienced by the participants, the vast majority of the reported incidents were phishing/scam attempts, such as fraudulent emails and copy-cat websites. Some of the responses highlight the fact these low-effort phishing attacks are regular occurrences. Two participants reported having seen ransomware as well, although we did not obtain detail on if the attack was successful or if the malware was merely detected. Other incidents reported include data breaches and service outages due to collateral damage from cyberattacks.

Relatively to noticed security incidents and its impact, the rate at which the participants were driven to adopt new measures remained relatively constant between demographics, but there's more significant differences in the amount of people that noticed their measures protected them. There were 25% more participants with "Good Tech-Background" who had a possible explanation for how their measures protected them, when compared to the other two groups, which had similar results.

As a follow-up to the above incidents, the measures adopted varied depending on each specific case. Both technical measures, such as data backup strategies and deployment of a firewall, and non-technical measures were employed. Renewed attention towards links themselves, and in general while browsing websites, as well as employing throwaway/different e-mail addresses were some examples of the latter type of measures.

Knowing exactly the when, how, or why of a security incident happens is not usually trivial, but it's important feedback to know if our current security measures are actually working, or merely seem to be. Out of 14 participants who shared their insights, 5 received warnings of attempted

(fraudulent) logins, as either an email from the service provider or in the form of Multi-Factor Authentication codes for login attempts they did not do themselves. Two participants noted antivirus warnings as well. Among the other reports, there was also a password manager *not* auto-filling login data in a copy-cat website due to the similar but different URL and a leak of personal data identified by the unique email address used to sign up for that account.

5.3 How do people feel about the measures they're taking and how does it differ between backgrounds groups?

To find out how people feel about their measures, we asked them what descriptions were most accurate, how appropriate they found their measures and what descriptions of feelings fit best for them. The results show that participants with better tech-background chose more positive descriptions and positive feelings, and judge their measures as more appropriate than participants with less tech-background.

Additionally, we wanted to know whether the participants feel they're able to take more measures, if they feel the need to do so, and what the reasons for not taking further measures are. While more participants with a better tech-background felt they have the ability to take further measures and know where they would start, the participants with "No Tech-Background" felt a higher need to take further measures. Accordingly, the main reason for participants with "No Tech-Background" not to take further measures is that they don't know about them.

5.3.1 Assessment of feelings regarding measures currently taken

We provided 4 positive and 6 negative self-descriptions as well as two neutral ones to choose from, and the participants were able to add a description of their own, if they wanted to. On average, each participant selected 2.18 descriptions, ca. one positive (0.92) and one negative (1.06), where only a quarter (16/62) of all participants selected both positive and negative descriptions, and just a few (3/62) participants selected neither a positive nor a negative answer, choosing only neutral ones. The distribution across the groups is shown in Figure 5.2. It is visible that participants with more Tech-Background chose more positive descriptions than those with less Tech-Background.

The specific answers per group are shown in Figure 5.3. The most checked descriptions are a positive and a negative description, followed by a pair of positive and negative description again. With these top 4 answers as examples, the differences across the group are apparent as shown in Table 5.3. Two participants added an own description, which are "Never trust Microsoft" and "Sometime I have the feeling that I have NO power/control".

We asked the participants to assess how appropriate they measures are on a 5-point Likert scale before and after we showed them typical measures. The average answer per person was 3.71 (before) and 3.87 (after), therefore the assessment changed slightly in a positive direction. As

Figure 5.2: Average answers of best fitting descriptions

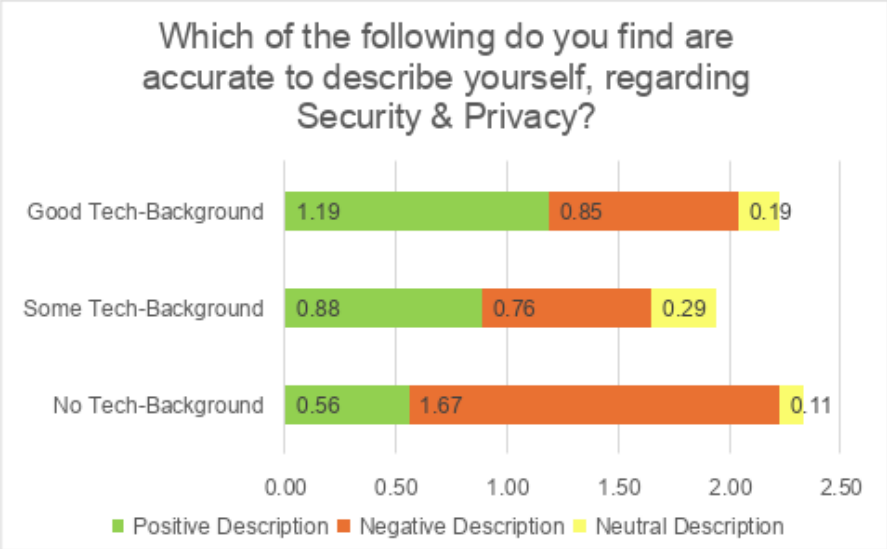
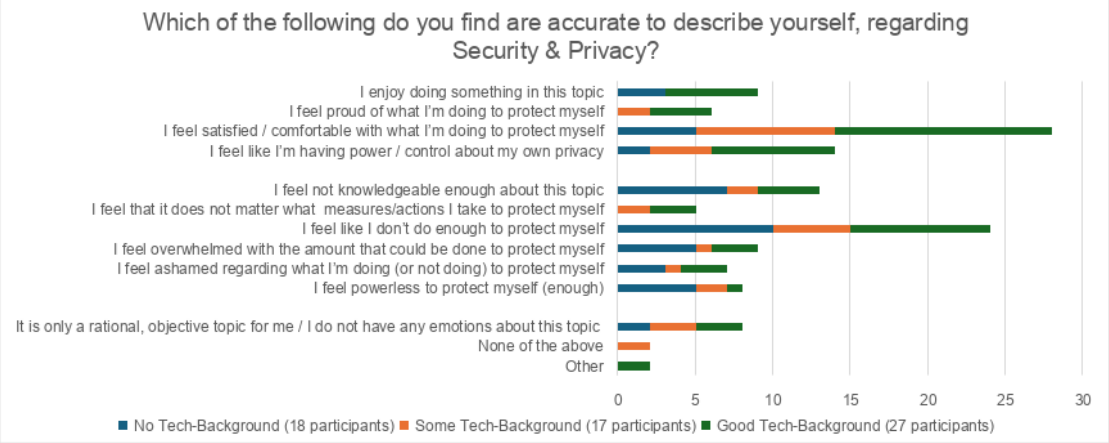


Figure 5.3: Specific descriptions selected by each group



some persons decrease their answer and some increase, those changes cancel out in the overall average as each participant made a positive or negative change of 0.71. The changes are not equally distributed over the groups as shown in Table 5.4

The showing of / asking about measures improved the assessment of the "No Tech-Background" group, whereas the difference for the "Some" and "Good" tech-background groups is relatively small. The average change is with the "No Tech-Background" group the highest (more than one point on the scale) as well as for the other groups. This allows the conclusion that increased background, therefore presumably increased knowledge before seeing the measures-list leads to less change of assessments and therefore lower volatility with more tech-background.

Table 5.3: **Top 4 selected descriptions**

	Description	No Tech-Background		Some Tech-Background		Good Tech-Background
+	I feel satisfied / comfortable with what I'm doing to protect myself	28% (5/18)	$<$	53% (9/17)	$\sim$	52% (14/27)
+	I feel like I'm having power / control about my own privacy	11% (2/18)	$<$	24% (4/17)	$<$	30% (8/27)
-	I feel like I don't do enough to protect myself	56% (10/18)	$>$	29% (5/17)	$\sim$	33% (9/27)
-	I feel not knowledgeable enough about this topic	39% (7/18)	$>$	12% (2/17)	$\sim$	15% (4/27)

Table 5.4: **Appropriateness of measures**

	Avg. answer before measures	Avg. answer after measures	Difference	Avg. change
No Tech-Background	3.17	3.61	+ 0.44	1.11
Some Tech-Background	4	3.89	- 0.12	0.70
Good Tech-Background	3.89	4.04	+ 0.15	0.44

Providing 2 positive, 4 negative, 2 neutral feelings and the opportunity to write an own feeling, we asked the participants, how they feel regarding the existing measures they've taken. Each person responded with 2.08 feelings in average, where 0.81 were positive and negative each and 0.47 neutral ones. Nearly a third (19/62) of the participants selected both negative and positive feelings and a few (8/62) participants selected neither a positive or a negative feeling, only neutral ones. Participants with "No Tech-Background" selected way fewer feelings (1.5) than the participants of the other groups (2.29 - "Some Tech-Background" and 2.33 - "Good Tech-Background"). While the positive feelings outweigh the negative ones for the groups with "Good Tech-Background" and "Some Tech-Background", it is the other way round for the "No Tech-Background". The distribution across the groups is shown in Figure 5.4.

The specific answers per group are shown in Figure 5.5. The most checked feelings are "I feel they are not enough" and "I'm happy with them". The first was chosen relatively (regarding the group-size) the most by participants with "No Tech-Background", whereas the second one is checked more often by participants with "Some Tech-Background" and "Good Tech-Background" and not that often by participants with "No Tech-Background".

Figure 5.4: Average answers of feelings

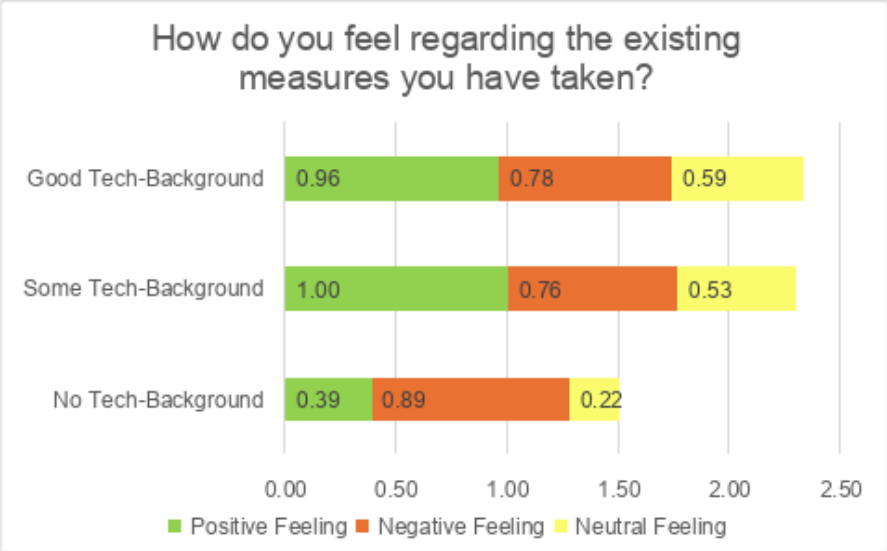
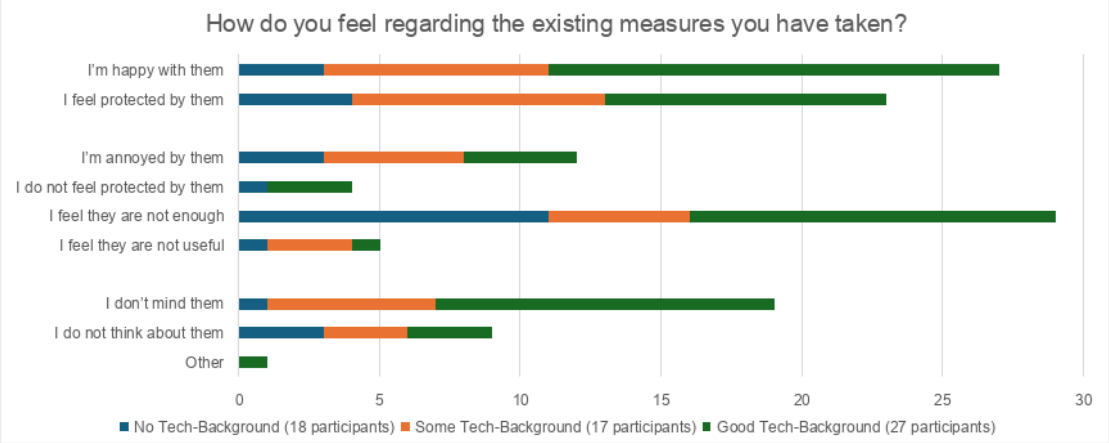


Figure 5.5: Specific feelings selected by each group



5.3.2 Assessment of feelings regarding new measures

Asking the participants, whether they feel like they would be able to take further measures, most participants answered with "Yes, I would be able to do it (technically) or would be able to find out how to do it". Nearly a third (19/62) of the participants answered "No", almost equally split in "I don't know more measures I could take" and "I don't know how to do them or it is too complicated (but I know more measures)". The self-sufficiency increases with more tech-background and accordingly the "No"-responses decrease with more tech-background as shown in Table 5.5.

Table 5.5: **Ability to take more measures**

		Yes		No (total)		Other		No, but*		No**	
No Tech-Backgr.	(18 P.)	10	(56%)	8	(44%)	0	-	6	(33%)	2	(11%)
Some Tech-Backgr.	(17 P.)	11	(65%)	5	(29%)	1	(6%)	1	(6%)	4	(24%)
Good Tech-Backgr.	(27 P.)	19	(70%)	6	(22%)	2	(7%)	2	(7%)	4	(15%)

* "No, I don't know how to do them or it is too complicated (but I know more measures)"
** "No, I don't know more measures I could take"

When asked what measures they would be able to do, many participants named measures related to passwords, specifically "Change passwords (more often)", "Use stronger passwords" and "Adopt a password manager". Measures regarding authentication are mentioned, which are "2-Factor authentification" and "Adopt security tokens". Further named measures are related to "Proactive Awareness", "Data encryption" and "Backups". There were other single instances of measures, which could not be clustered together. The codes including the number of mentions can be found in the appendix in Table 7.3.

39% (24/62) of the participants answered, they feel the need to do take further measures and almost a third of them (7/24) knows, which measures they would take first. There are again differences across the background groups apparent as shown in Table 5.6.

Table 5.6: **Need to take more measures**

		Feel need to take more measures		Know, which measures would take first*	
No Tech-Background	(18 P.)	9	(50%)	1	(11%)
Some Tech-Background	(17 P.)	5	(29%)	1	(20%)
Good Tech-Background	(27 P.)	10	(37%)	5	(50%)

* From those, who feel the need to take more measures

Therefore more people from the "No Tech-Background" group felt, they should take more measures, but most of them didn't know, where to start. Those who know where to start, named measures related to authentication, including "Password storage / generation" and more secure "Authentication methods", as well as more "Proactive awareness" and "Backups". The codes including the number of mentions can be found in the appendix in Table 7.4.

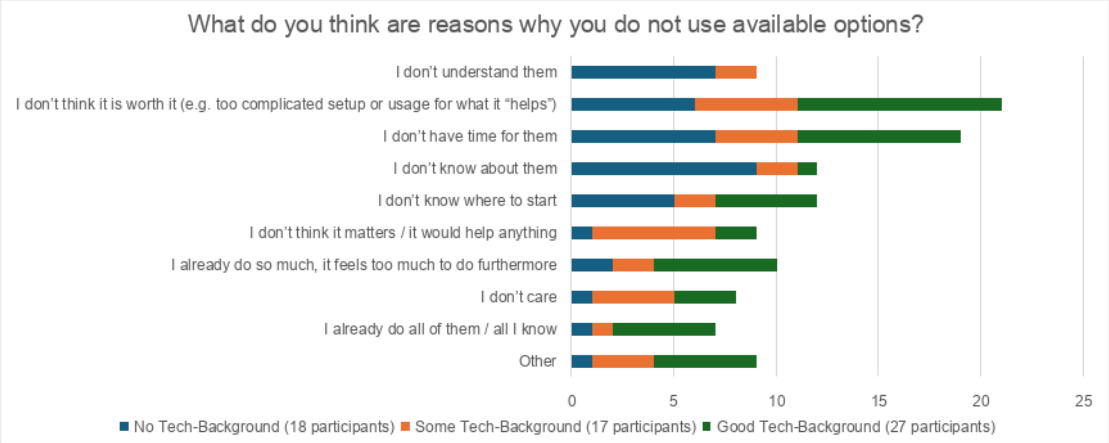
Furthermore we asked the participants what they think the reasons are, why they do not use available options. We provided 9 different reasons and they were able to add an own reason. Each participant answered with 1.87 reasons in average, where the participants from the "No Tech-Background" group gave more reasons (2.22) than the groups with "Some Tech-Background" (1.82) or "Good Tech-Background" (1.67). The reasons and the answers are shown in Figure 5.6, the most responded reasons are:

- I don’t think it is worth it (e.g. too complicated setup or usage for what it “helps”) (21/62 - 34%)
- I don’t have time for them (19/62 - 31%)
- I don’t know about them (12/62 - 19%)
- I don’t know where to start (12/62 - 19%)

The top reason for each group is:

- No Tech-Background: I don’t know about them (9/18 - 50%)
- Some Tech-Background: I don’t think it matters / it would help anything (6/17 - 35%)
- Good Tech-Background: I don’t think it is worth it (e.g. too complicated setup or usage for what it “helps”) (10/27 - 37%)

Figure 5.6: Specific reasons selected by each group



9 participants stated own reasons, which are mostly related to "Cost-benefit / Too much work". Other instances state that their "Measures are good enough" or at least "that not every amateur can steal my data", further reasons are "Forgetfulness" and "Financial burden". The codes including the number of mentions can be found in the appendix in Table 7.5.

6 Discussion

We found out that from the categories used in SeBIS, Updating is the category most affected by technical background, even though the differences are not major.

What is more important is that people in the "No Tech-Background" group tended to feel worse about their security & privacy related measures than the other groups. However, they also saw the greatest change in the assessment of the appropriateness of their measures, after seeing the SeBIS measures, where they had a great improvement.

Participants in the "No Tech-Background" group felt the highest need to take more measures, however, they referred not knowing how to start. Overall the biggest reason to not use more measures is cost/benefit-related, as people don't think it is worth the effort or they don't have time for them. If security measures were easier and / or faster in their setup and usage, this could improve the adoption of these measures among all users.

Our results show that having more knowledge about the subject matter does make people feel better about it, so educational content could go a long way into reducing anxiety / negative emotions caused in people. If this content managed to reach the "No Tech-Background" participants as well, it would raise awareness of the possible measures themselves, mitigating the previously mentioned not-knowing-where-to-start issue.

As most of the measures that the participants mentioned they wanted to improve are password-related, this can broadly and at a relatively low cost in both effort and monetary cost, be accomplished via adoption of a password manager. This would tackle different password-related issues at once (overview over passwords/accounts, easier use of different passwords, stronger passwords or less of a strain on peoples' memory, among others).

6.1 Limitations

In conducting our survey, we discovered some of its shortcomings. The measures that are a part of SeBIS do achieve their goal in being some of the most common/adopted security & privacy measures and a great baseline, but they also are on the lower-end of complexity, some of them being "bare-minimum" of security-related measures (Such as having a PIN on a mobile device.). Therefore they may lead people into being overconfident in their current security behaviours, leading to unaddressed gaps in their security that they have no idea exist. Even if more complex measures would not be realistic for a large part of the population, it is still good to be aware of them and practice caution in general, not falling into dangerous thinking that all risk is gone.

Our choice to place the emotion-related segment of the survey after the measure-related section may also have distorted the answers to it. By asking measure-related questions beforehand we might have influenced people into thinking about these measures, and consequently affected their emotions. However, we found it important to introduce these measures as a concept, specially for survey-takers without any security & privacy-related technical knowledge, so that there could be no misinterpretation of our questions, and people didn't feel lost in answering.

Furthermore our results are only hypotheses as we did not perform statistical inference.

A large limitation in our research is demographically-related: Our participant pool is rather small, somewhat imbalanced regarding the technical background, focused only on participants from Germany and Portugal and we were nowhere close to reaching thematic saturation.

We recommend to extend the research to other populations and with more participants to gain further insights and with the limitations above mentioned in mind, to improve the research regarding the setup and analysis.

7 Conclusion

As the decision-making of users is impacted by emotions, we analyzed the emotions of our participants regarding their security & privacy measures.

Just as our results show, higher knowledge of the topic leads to an improvement in how people feel about security & privacy, and it's a great starting point to increase wider adoption of starting-point security measures that can go a long way. Not knowing about the existence of tools and measures was cited as the biggest reason towards non-adoption of further measures by people with no previous technical knowledge, despite them being the group with the highest need to adopt more measures. It is therefore a bottleneck created by lack of knowledge, but not unwillingness towards adopting new behaviours, or negative emotions towards security & privacy.

On the other hand, for people with more technical background knowledge it is the cost/benefit ratio which is the most named reason to not take further measures. As such, security measures / tools should be made easier and faster in their setup and usage to drive up their adoption. The cause for this reluctance is, then, a mirror of what happens for the "No Tech-Background" group, which is presented above.

In conclusion, people with different technical backgrounds and levels of knowledge have very different needs, and emotions, driving their behaviours, and attempts to drive adoption for behaviours or measures must be made taking into account their target audience.

Bibliography

[1] *"123456789" statt sicherem Passwort*. https://www.tagesschau.de/inland/gesellschaft/passwoerter-deutschland-unsicher-100.html. Accessed: 2024-01-16. 2023.

[2] *Bad Practices*. https://www.cisa.gov/news-events/news/bad-practices-0. Accessed: 2024-01-16. 2021.

[3] Susanne Barth et al. "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources". In: *Telematics and Informatics* 41 (2019), pp. 55–69. ISSN: 0736-5853. DOI: https://doi.org/10.1016/j.tele.2019.03.003. URL: https://www.sciencedirect.com/science/article/pii/S0736585317307724.

[4] Ashley A. Cain, Morgan E. Edwards, and Jeremiah D. Still. "An exploratory study of cyber hygiene behaviors and knowledge". In: *Journal of Information Security and Applications 42 (2018)*. 2018.

[5] Hichang Cho, Pengxiang Li, and Zhang Hao Goh. "Privacy Risks, Emotions, and Social Media: A Coping Model of Online Privacy". In: *ACM Trans. Comput.-Hum. Interact.* 27.6 (Nov. 2020). ISSN: 1073-0516. DOI: 10.1145/3412367. URL: https://doi.org/10.1145/3412367.

[6] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung. "The role of privacy fatigue in online privacy behavior". In: *Computers in Human Behavior* 81 (2018), pp. 42–51. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2017.12.001. URL: https://www.sciencedirect.com/science/article/pii/S0747563217306817.

[7] W Alec Cram, Jeffrey G Proudfoot, and John D'Arcy. "When enough is enough: Investigating the antecedents and consequences of information security fatigue". en. In: *Inf. Syst. J.* 31.4 (July 2021), pp. 521–549.

[8] Christina Czeschik. "Cyberangriffe im Gesundheitswesen: Gefahren und Gegenmaßnahmen". In: *Dtsch Arztebl International* 22.12 (2023), [561]–. eprint: https://www.aerzteblatt.de/pdf.asp?id=235650. URL: https://www.aerzteblatt.de/int/article.asp?id=235650.

[9] Serge Egelman and Eyal Peer. "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)". In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. CHI '15. Seoul, Republic of Korea: Association for Computing Machinery, 2015, pp. 2873–2882. ISBN: 9781450331456. DOI: 10.

1145/2702123.2702249. URL: https://doi.org/10.1145/2702123.2702249.

[10] Ernestas Naprys. *Three hacked German hospitals shut down systems, LockBit suspected*. https://cybernews.com/news/lockbit-hacked-three-german-hospitals/. Accessed: 2024-01-16. 2023.

[11] Michael Fagan and Mohammad Maifi Hasan Khan. "Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice". In: *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, June 2016, pp. 59–75. ISBN: 978-1-931971-31-7. URL: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan.

[12] Nina Gerber, Paul Gerber, and Melanie Volkamer. "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior". In: *Computers & Security* 77 (2018), pp. 226–261. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2018.04.002. URL: https://www.sciencedirect.com/science/article/pii/S0167404818303031.

[13] Hsiao-Ying Huang and Masooda Bashir. ""Seeking Privacy Makes Me Feel Bad?": An Exploratory Study Examining Emotional Impact on Use of Privacy-Enhancing Features". In: *Advances in Information and Communication*. Ed. by Kohei Arai, Supriya Kapoor, and Rahul Bhatia. Cham: Springer International Publishing, 2020, pp. 600–617. ISBN: 978-3-030-39445-5.

[14] Ruogu Kang et al. ""My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security". In: *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. Ottawa: USENIX Association, July 2015, pp. 39–52. ISBN: 978-1-931971-249. URL: https://www.usenix.org/conference/soups2015/proceedings/presentation/kang.

[15] Spyros Kokolakis. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon". In: *Computers & Security* 64 (2017), pp. 122–134. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2015.07.002. URL: https://www.sciencedirect.com/science/article/pii/S0167404815001017.

[16] Jennifer S. Lerner et al. "Emotion and Decision Making". In: *Annual Review of Psychology* 66.1 (2015). PMID: 25251484, pp. 799–823. DOI: 10.1146/annurev-psych-010213-115043. eprint: https://doi.org/10.1146/annurev-psych-010213-11504. URL: https://doi.org/10.1146/annurev-psych-010213-115043.

[17] Robert Luzsa and Susanne Mayr. "Links Between Online Privacy Fatigue, Technology Attitudes and Sociodemographic Factors in a German Population Sample". In: *Mensch und Computer 2022*. MuC '22. ACM, Sept. 2022. DOI: 10.1145/3543758.3547540. URL: http://dx.doi.org/10.1145/3543758.3547540.

[18] Moses Namara et al. “Emotional and Practical Considerations Towards the Adoption and Abandonment of VPNs as a Privacy-Enhancing Technology”. In: *Proceedings on Privacy Enhancing Technologies* 2020.1 (Jan. 2020), pp. 83–102. ISSN: 2299-0984. DOI: 10.2478/popets-2020-0006. URL: http://dx.doi.org/10.2478/popets-2020-0006.

[19] Richard Tracy. *A Cybersecurity Stop Sign: CISA Introduces Bad Practices*. https://www.forbes.com/sites/forbestechcouncil/2021/08/12/a-cybersecurity-stop-sign-cisa-introduces-bad-practices/. Accessed: 2024-01-16. 2021.

[20] Shiona McCallum and Joe Tidy. *23andMe: Profiles of 6.9 million people hacked*. https://www.bbc.com/news/technology-67624182. Accessed: 2024-01-16. 2023.

[21] Brian Stanton et al. “Security Fatigue”. In: *IT Professional* 18.5 (2016), pp. 26–32. DOI: 10.1109/MITP.2016.84.

[22] Marlis Stubenvoll and Alice Binder. “Is knowledge power? Testing whether knowledge affects chilling effects and privacy-protective behaviors using browser histories”. In: *Computers in Human Behavior* 150 (2024), p. 107949. ISSN: 0747-5632. DOI: https://doi.org/10.1016/j.chb.2023.107949. URL: https://www.sciencedirect.com/science/article/pii/S074756322300300X.

[23] Xinluan Tian, Lina Chen, and Xiaojuan Zhang. “The Role of Privacy Fatigue in Privacy Paradox: A PSM and Heterogeneity Analysis”. In: *Applied Sciences* 12.19 (2022). ISSN: 2076-3417. DOI: 10.3390/app12199702. URL: https://www.mdpi.com/2076-3417/12/19/9702.

[24] Lu Yu et al. “A meta-analysis to explore privacy cognition and information disclosure of internet users”. In: *International Journal of Information Management* 51 (2020), p. 102015. ISSN: 0268-4012. DOI: https://doi.org/10.1016/j.ijinfomgt.2019.09.011. URL: https://www.sciencedirect.com/science/article/pii/S026840121831137X.

[25] Yixin Zou et al. “Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices”. In: *2020 CHI Conference on Human Factors in Computing Systems*. 2020.

Appendix

7.1 Detailed results to SeBIS

Figure 7.1: SeBIS - Device Securement

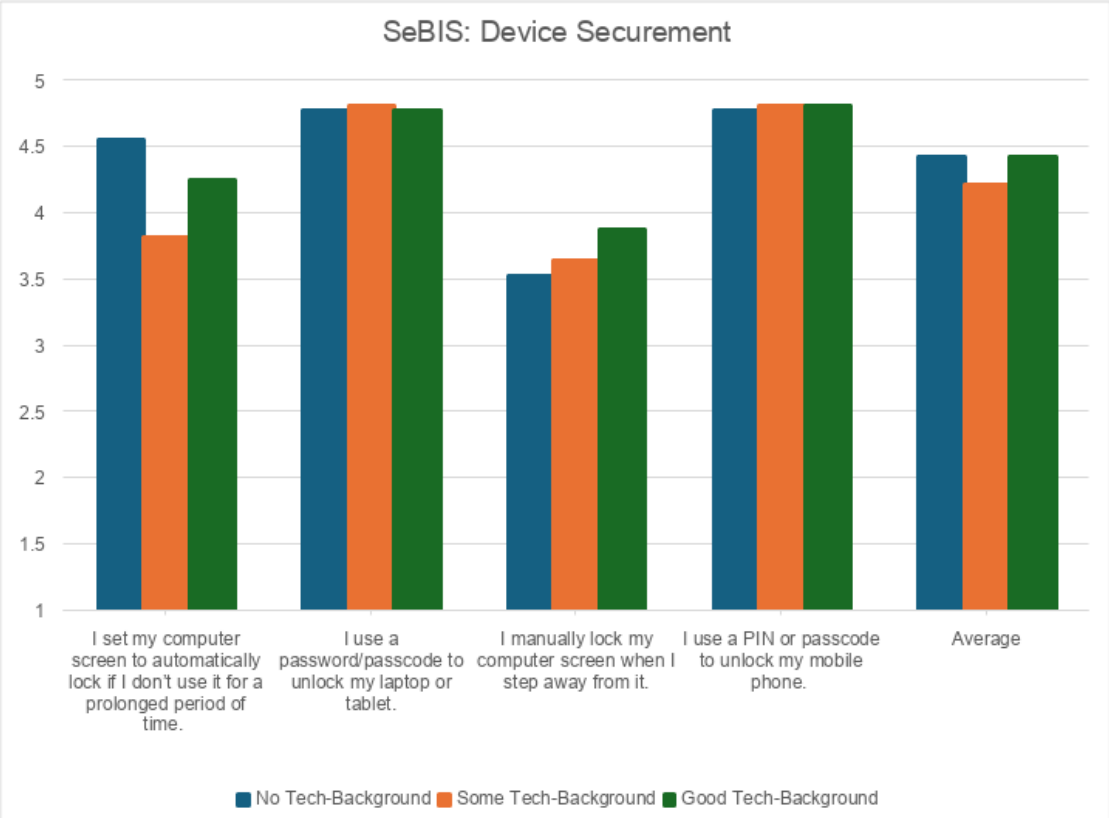


Figure 7.2: SeBIS - Password Generation

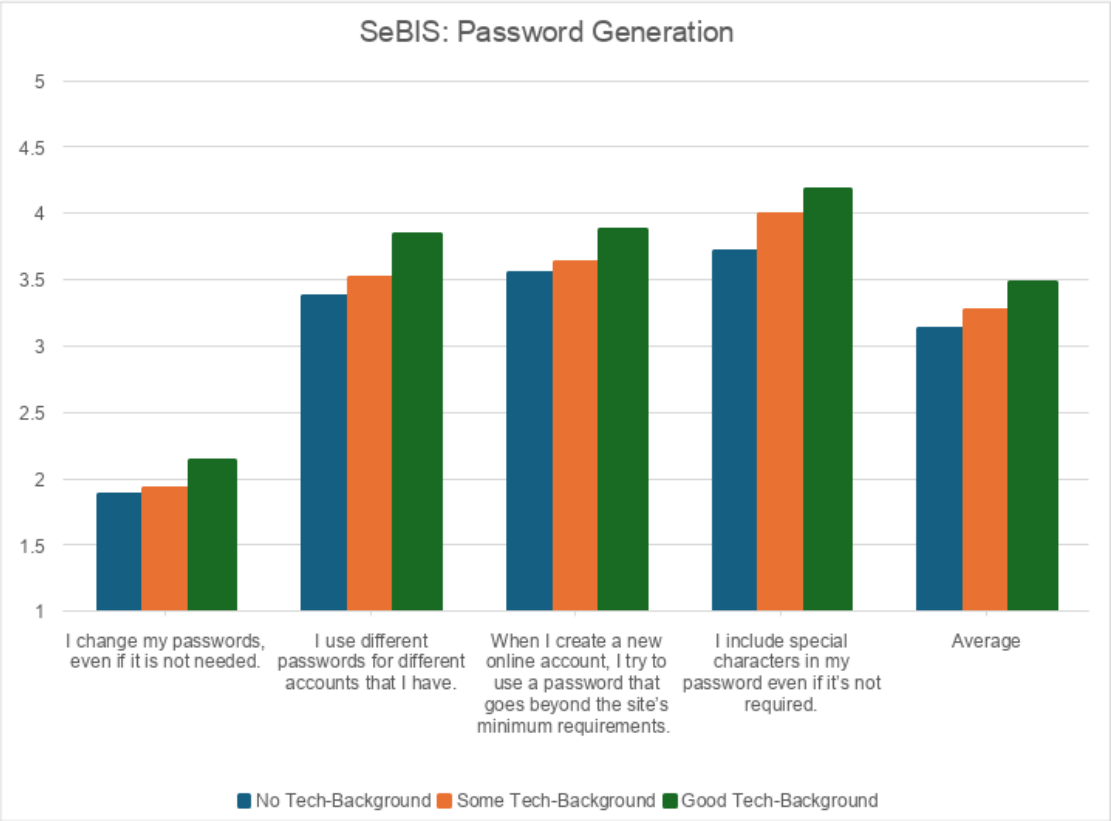


Figure 7.3: SeBIS - Proactive Awareness

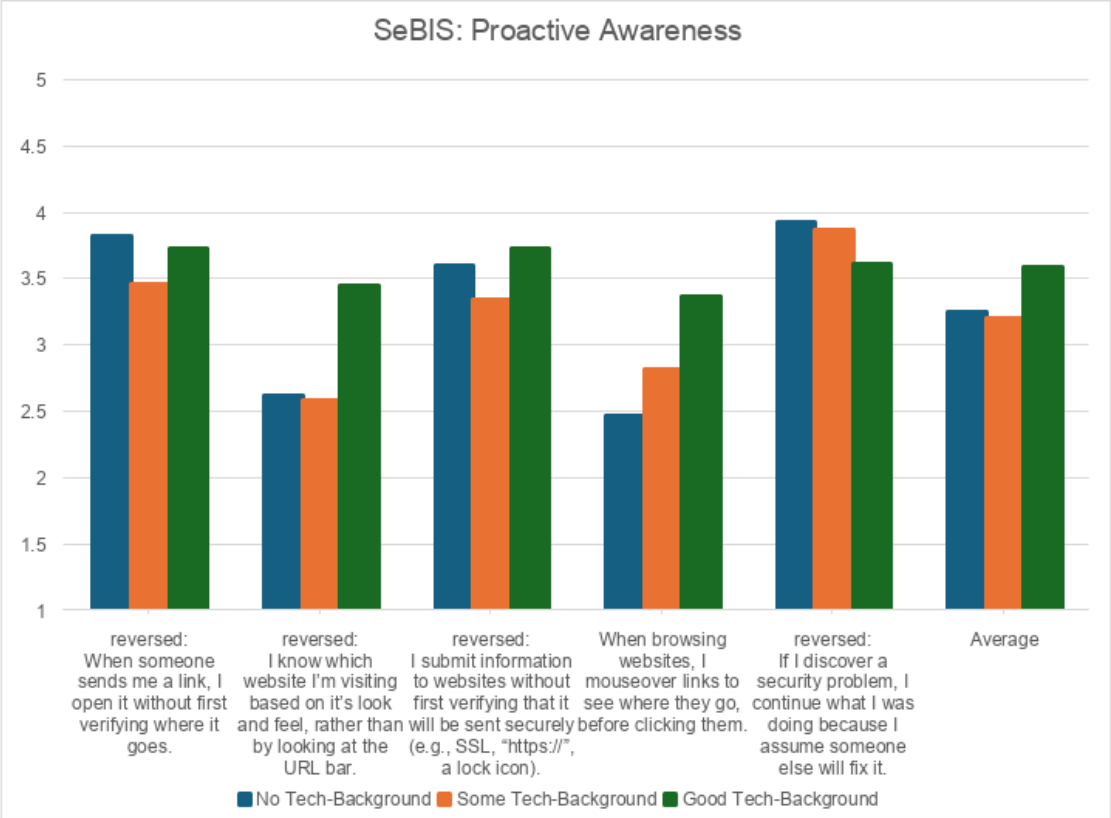
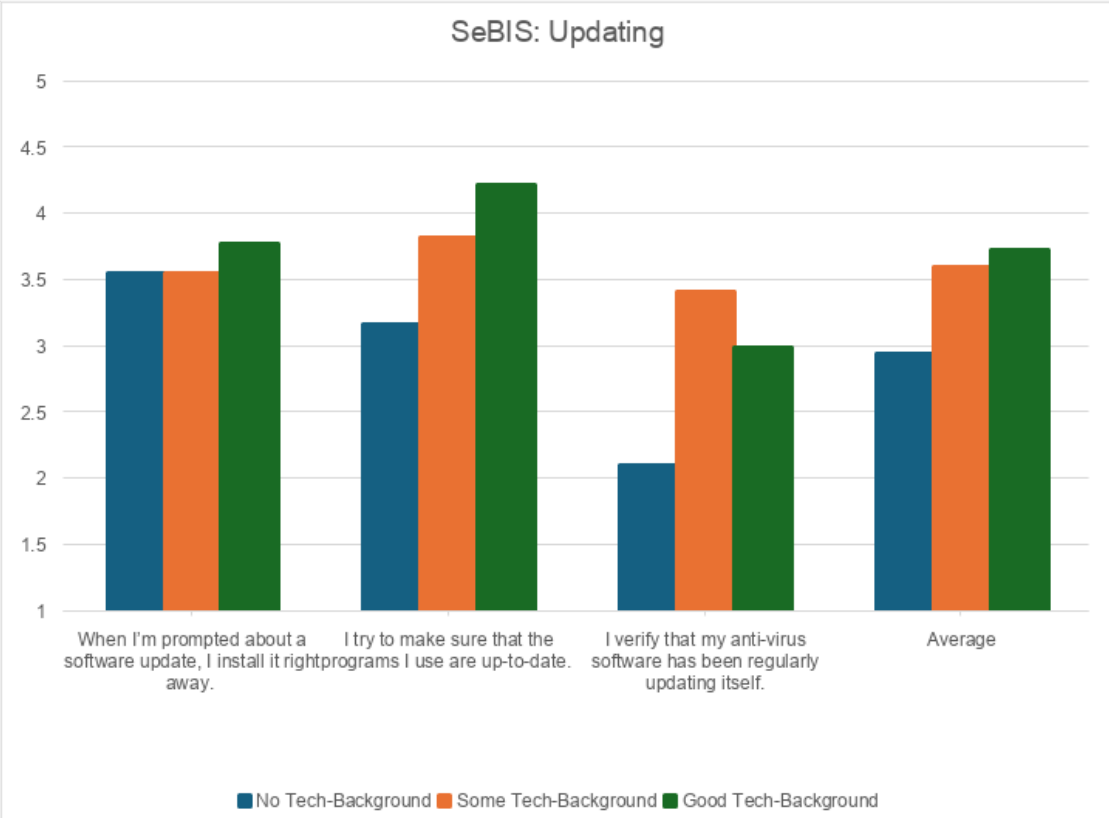


Figure 7.4: SeBIS - Updating



7.2 Codes

Table 7.1: **Codes** for "Do you use other security or privacy related measures, we did not list?"

Two-factor authentication	5
Password managers / safes	4
Adblockers / Browser filters	4
Signing / Encryption	3
Biometric authentication	2
Throwaway emails	2
Physical security tokens	2
Other	6
Adding context to previous answers; not a new measure	2

Table 7.2: **Codes** for "Have you had any security/privacy-related incident in recent memory?" and follow-up question "What happened?"

Phishing / Scam / Spam	14
Data breaches	2
Ransomware	2
Other	3

Table 7.3: **Codes** for "Do you feel like you would be able to take further measures?" and follow-up question "What measures do you have in mind?"

Passwords	Change passwords (more often)	8
	Use stronger passwords	8
	Adopt a password manager	6
Authentication	2-Factor authentication	5
	Adopt security tokens	2
Other	Proactive awareness	5
	Data encryption	3
	Backups	2
	Other	7

Table 7.4: **Codes** for "Do you know which measures (you do not already take) you would take first?" and follow-up question "What are they?"

Authentication	Password storage / generation	3
	Authentication methods	2
Other	Proactive awareness	3
	Backups	1

Table 7.5: **Codes** for "What do you think are reasons why you do not use available options?", where participants specified own reasons as "Other: "

Cost-benefit / Too much work	5
Measures are good enough	2
Forgetfulness	1
Financial burden	1

7.3 Main - Survey

For each question there was the opportunity to select "No answer".

Title: Human Factors in Security and Privacy

Description: Research project looking into how computer Security and Privacy interacts with people's daily lives.

Welcome message: Thank you for taking time to participate in our survey! The survey will take ca. 15 minutes. No question is truly mandatory, so you may decline to answer, for any reason. There are a few questions marked with ◇ (optional). Those will extend the duration of the survey to a max. of 30 minutes, and will provide us with extra insight beyond the bare minimum required for our research. We don't want to test your knowledge and won't judge your answers - we are truly interested in any and all responses. :)

7.3.1 Introduction

Q21 - Are you familiar with the concepts of digital security and privacy? [Not At All Familiar / Slightly Familiar / Somewhat Familiar / Moderately Familiar / Extremely Familiar]

Text block after any answer in Q21: Digital Security relates to securing yourself online - passwords, accounts, and devices, for example. Digital privacy has to do with protecting your data, especially online, from being misused or accessed by others.

Q1 - Do you think your measures to protect your (online) privacy and security are appropriate (for your needs)? [Inappropriate / Slightly Inappropriate / Neutral / Slightly Appropriate / Appropriate]

7.3.2 Measures

Q5 - Each statement below describes a specific security behavior. Please indicate how often you follow the respective behaviors. There are no wrong answers. [Never / Rarely / Sometimes / Often / Always]

- I set my computer screen to automatically lock if I don't use it for a prolonged period of time.
- I use a password/passcode to unlock my laptop or tablet.
- I manually lock my computer screen when I step away from it.
- I use a PIN or passcode to unlock my mobile phone.
- I change my passwords, even if it is not needed.
- I use different passwords for different accounts that I have.
- When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.
- I include special characters in my password even if it's not required.
- When someone sends me a link, I open it without first verifying where it goes. *
- I know which website I'm visiting based on it's look and feel, rather than by looking at the URL bar. *
- I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon). *
- When browsing websites, I mouseover links to see where they go, before clicking them.
- If I discover a security problem, I continue what I was doing because I assume someone else will fix it. *
- When I'm prompted about a software update, I install it right away.
- I try to make sure that the programs I use are up-to-date.
- I verify that my anti-virus software has been regularly updating itself.

*: These phrases are reversed, therefore the resulting score must be reversed as well.

Q5.1 - Do you use other security or privacy related measures, we did not list? [Optional, free text]

Q2 - Have you had any security/privacy-related incident in recent memory? (For example, you've received a phishing email, found a copy-cat of a popular website designed to steal unsuspecting clients' money, or were a victim of a ransomware attack.) [Yes / No]

Q2.0.1 - What happened? [Follow-up on "Yes" in Q2, optional, free text]

Q2.1 - Did the incident(s) drive you to adopt any new measures or behaviors? [Follow-up on "Yes in Q2, optional, Yes / No]

Q2.1.1 - What were those? [Follow-up on "Yes" in Q2.1, optional, free text]

Q3 - Have you had moments where you know your adopted security/privacy measures protected you? [Optional, Yes / No]

Q3.1 - Do you know how or why they helped to protect you? [Follow-up on "Yes" in Q3, optional, free text]

Q4 - Have you had moments where you know your adopted security/privacy measures failed to protect you? [Optional, Yes / No]

Q4.1 - Do you know how or why they failed to protect you? [Follow-up on "Yes" in Q4, optional, free text]

7.3.3 Emotional Impact/Effect

Text block: Conclusion of security measures:

- Device Securement (automatically lock, password/code for laptop/tablet and phone, manually locking when stepping away)
- Password Generation (different passwords for different accounts, special characters, change passwords)
- Proactive Awareness (Verifying links before clicking, checking URLs of websites, verifying secured websites, react on security problems)
- Updating (install software updates right away, keep programs up-to-date, verify anti-virus software is updating itself)

Q6 - After seeing common security and privacy measures, do you think your measures to protect your (online) privacy and security are appropriate (for your needs)? [Inappropriate / Slightly Inappropriate / Neutral / Slightly Appropriate / Appropriate]

Q8 - How do you feel regarding the existing measures you have taken? [Checkboxes]

- I'm happy with them
- I'm annoyed by them
- I don't mind them
- I feel protected by them
- I do not feel protected by them

- I feel they are not enough
- I feel they are not useful
- I do not think about them
- Other: [Free text]

Q9 - Do you feel like you would be able to take further measures? [Radiobuttons]

- No, I don't know more measures I could take
- No, I don't know how to do them or it is too complicated (but I know more measures)
- Yes, I would be able to do it (technically) or would be able to find out how to do it
- Other: [Free text]

Q9.1 - What measures do you have in mind? [Follow-up on "No, I don't know how to do them . . . " or "Yes, . . . " in Q9, free text]

Q10 - Do you feel the need to take further measures? [Yes / No]

Q10.1 - Do you know which measures (you do not already take) you would take first? [Follow up on "Yes" in Q10, Yes / No]

Q10.1.1 - What are they? [Follow-up on "Yes" in Q10.1, free text]

Q11 - What do you think are reasons why you do not use available options? [Checkboxes]

- I don't understand them
- I don't think it is worth it (e.g. too complicated setup or usage for what it "helps")
- I don't have time for them
- I don't know about them
- I don't know where to start
- I don't think it matters / it would help anything
- I already do so much, it feels too much to do furthermore
- I don't care
- I already do all of them / all I know
- Other: [Free text]

Q12 - Which of the following do you find are accurate to describe yourself, regarding Security & Privacy? [Checkboxes]

- I feel not knowledgeable enough about this topic

- I enjoy doing something in this topic
- I feel that it does not matter what measures/actions I take to protect myself
- I feel proud of what I'm doing to protect myself
- I feel like I don't do enough to protect myself
- I feel satisfied / comfortable with what I'm doing to protect myself
- I feel overwhelmed with the amount that could be done to protect myself
- I feel like I'm having power / control about my own privacy
- I feel ashamed regarding what I'm doing (or not doing) to protect myself
- I feel powerless to protect myself (enough)
- It is only a rational, objective topic for me / I do not have any emotions about this topic
- None of the above
- Other: [Free text]

7.3.4 Background

Q13 - Did/do you study for a CS/IT-related area? [Yes / No]

Q14 - Did/do you work in an area related to CS/IT? [Yes / No]

Q15 - Please describe your CS/IT-Related education / field of work. [Follow up on "Yes" in Q13 or Q14, optional, free text]

Q16 - To what extent do you agree or disagree with the following statements? [Strongly Disagree, Disagree, Neutral, Agree, Strongly Agree]

- I can complete my tasks/goals while operating a computer.
- I can solve problems that may come up while operating a computer.

Q18 - Describe your perceived proficiency level with a computer. [Optional, free text]

Q19 - Do you have any experience programming? [Yes / No]

Q19.1 - Do you have any professional experience programming? [Follow up on "Yes" in Q19, Yes / No]

Q19.2 - Do you have personal projects related to software/hardware? [Follow up on "Yes" in Q19, Yes / No]

Q20 - Do you think about your privacy or security online? [Not at All / Rarely / Sometimes / Often / Always]

Q22 - Do you have professional experience surrounding Security & Privacy topics? [Yes / No]

7.3.5 Demographics

Text block: These questions are only for assessing the homogeneity of the respondents demographics and will not be used for the research itself. We will use only aggregated demographics in our paper.

Q23 - What is your gender? [Checkboxes]

- Female
- Male
- Non-Binary
- Prefer to self-describe
- Prefer not to answer

Q23.1 - [Follow up on "Prefer to self-describe" in Q23, free text]

Q24 - What is your age? [Radiobuttons]

- 18-25
- 26-35
- 36-45
- 46-55
- 55-65
- > 65

Endmessage: Thank you very much for participating in our survey! Are you interested in the results of our research and want to receive the paper, once it is finished? Then click here to submit your email address. Your email address will be stored separately from your previous answers, so they will not be connected in any way. Your email will not be used for any other purposes such as marketing, nor will it be shared with third parties or stored in a publicly accessible database. It will be disposed of as soon as the results are sent. If you want to have a look at some of the mentioned security/privacy measures, here are some resources that may be helpful!:

- Recommendations from the US cyber defense agency
  `https://www.cisa.gov/news-events/news/4-things-you-can-do-keep-yourself-c`
- A password manager can help to manage passwords, especially if you're using long, complicated passwords
  `https://bitwarden.com/`

- A website, where you can check, whether your email address has been in a data breach `https://haveibeenpwned.com/`

7.4 Mail collection - Survey (optional)

Title: Mail collection for results

Q1 - Insert your email-address, if you want to receive the results of this survey. [Mandatory]

End message: We thank you for your interest! It is estimated that these results will be available around the end of January.

7.5 Consent Form

Project Title	**S&P measures and emotional response in relation to tech-background**
Principle Investigator and Contact Person	Prof. Dr. Yasemin Acar, Paderborn University, Department of Computer Science
Student Researchers	**Camila Fonseca, Nicole Geymeier**
Project Description	In this study we aim to study people's perceptions, behaviors and emotional responses regarding digital Security and Privacy, and how it may be impacted by their background.
Eligibility	**Should be above 18**
Procedure	For this study, you will fill out a survey, on the Limesurvey platform. You will answer questions about your perceptions, behaviors, and reactions about digital security habits. The survey will take you approximately 10 - 15 minutes to fill out. Only aggregated data and pseudonymized citations are published.
Risks & Benefits	There are no risks nor benefits to the participants.
Duration	This survey takes about 10-15 minutes to fill out, excluding optional/extra questions. Including all of the optional/extra questions, it takes about 30 minutes.
Compensation	There is no monetary compensation for participation in this study.
Confidentiality	There is no personal identifiable information collected in the main survey. Demographic data such as age and gender is aggregated. Email addresses are collected in a separate survey, and not linked to the survey answers. It is completely optional to provide it. These are collected only to later send the study results and will be

	deleted as soon as the study concludes.
Subjects' Rights	Your participation is voluntary. You may terminate your participation at any time by leaving the study environment or notifying the investigator. Partial results may be stored de-identified. You may withdraw your consent to the use of your personal data at any time by emailing cffonseca@ua.pt or ntresser@mail.uni-paderborn.de . Or send an email to humanfactors@lists.upb.de. Please note that while we will delete all personal data at your request, once we have de-identified the data and can no longer associate it with your request, it may still be used for our research.
Future use of research data	To maximize the benefits of your participation in this project, by further contributing to science and our community, your de-identified information may be stored for future research. Research data at Paderborn University are typically stored for 10 years in order to be available for questions and concerns with the research.
Contact	For additional questions about this research, you may contact Camila Fonseca or Nicole Geymeier. Email: cffonseca@ua.pt or ntresser@mail.uni-paderborn.de

By signing this consent form, I am affirming that...

- I am age 18 or older.
- I am comfortable using the English language to participate in this study.
- I meet the requirements to participate in this study.
- I have read and understood the above information. All of the questions that I had about this research have been answered.
- I have chosen to participate in and continue this study with the understanding that I may stop participating at any time without penalty or loss of benefits to which I am otherwise entitled.
- I am aware that I may revoke my consent at any time.

I hereby consent (Art. 6 para. 1 lit. a GDPR) that my submitted personal data may be stored and processed. I have read the privacy policy for the form. I am aware of the right of withdrawal.