Assessing the Cybersecurity Needs and Experiences of Disabled Users

Arwa Binsedeeq[1[0009-0003-5381-047X]], Steven Furnell[1[0000-0003-0984-7542]], Kirsi Helkala[2[0000-0003-3698-4585]], Naomi Woods[3[0000-0002-5692-5163]], Darren Chadwick[4[0000-0002-4963-0973]], Chris Fullwood[5[0000-0002-7714-6783]], Xavier Carpent[1[0000-0003-1697-6940]] and Nicolas Gervassis[1[0000-0003-2739-6263]]

[1] University of Nottingham, Nottingham, UK
[2] Norwegian Defence University College / Norwegian Defence Cyber Academy, Norway
[3] University of Jyväskylä, Jyväskylä, Finland
[4] Liverpool John Moores University, Liverpool, UK
[5] Birmingham City University, Birmingham, UK

alyab4@exmail.nottingham.ac.uk; steven.furnell@nottingham.ac.uk

Abstract. Digital technology is incredibly crucial in today's world. The use of technology is considered a right for both able and disabled users. Accessibility and security are two important concepts in the technology context. Accessibility refers to the level to which a product or service is designed to be utilized by people with disabilities. While security focuses on protecting a product or service from threats and harm. Accessible security refers to the practice of ensuring that digital products and services are not only secure but also accessible to everyone, including people with disabilities. Numerous studies have been conducted on the usage of technologies among people with disabilities. However, little research has been undertaken on accessible cybersecurity. Understanding encounters of disabled individuals with cybersecurity challenges can help develop more accessible and secure technologies and improve user experience. The first step to improving the accessibility of cybersecurity safeguards for users with disabilities is assessing their attitudes and needs. The aim of the study is to explore the cybersecurity attitude, behavior and awareness of people with various types of disability. The survey used to determine the most significant gap for people with disabilities in the accessible cybersecurity context to help them better handle and understand cyber threats in their everyday lives. The survey findings point out that having cybersecurity awareness does not always result in preventing security breaches. There is a gap between theoretical knowledge and practical application. There is a notable concern regarding insufficient technological safeguards. Recommendations are included for software developers to create a more accessible and secure digital environment.

Keywords: Accessibility, Cybersecurity, Accessible security, Disabled Users, Accessibility Challenges, Inclusive Design, User Experience.

1 Introduction

Digital technology has transformed our lives, work, and methods of communication, and continues to play an increasingly vital role in every aspect of our daily lives. The use of technology is considered a right for both able and disabled users [1]. In 2006, the United Nations General Assembly [2] adopted the Convention on the Rights of Persons with Disabilities (CRPD). This convention asserts that access to information technologies, mobility aids, devices and other assistive technologies is a fundamental human right. More people are affected by disabilities than we may realize. In 2021, the World Health Organization [3] estimated that, worldwide, about one billion people have significant disabilities. Thus, it is important to ensure that technologies provide effective tools, functions and features to facilitate accessibility, usability and security for people with disabilities.

Usability relates to the ease with which a product or service can be used by its intended audience [4] while accessibility relates to the level of a product or service is designed and positioned to be used by individuals with disabilities [5]. Security is one of the significant requirements that every user expects when using digital technology [6]. Hence, issues of accessibility and usability are important when considering security, e.g., technology facilitates people with disabilities to engage in secure practices. Accessible security considers factors like user experience, interface design, and the overall flow of the product or service. Accessible security products or services are easy to understand, navigate, and use efficiently, which can improve user satisfaction, productivity and safety. Issues of accessible security are therefore important when considering user protection. Based on universal design principles, all users should have access to secure, usable, privacy-preserving, effective and accessible technology [1]. However, people with disabilities may encounter challenges while using this technology. They need to be provided with the same level of accessibility as people without disabilities without compromising their security. Despite efforts to improve user experience in cybersecurity, research on the accessibility and usability of security is lacking [7-10], especially research focused on users with disabilities [11].

This study is an expansion of an initial assessment presented by Furnell, Helkala, and Woods [12], who provide a literature review and some real-world examples that identify current authentication methods with people with different types of disabilities. We used empirical methods to assess the accessible security for people with different disabilities. In this paper, we explore the cybersecurity attitude, behavior and awareness of people with various types of disability. We investigate what is the most significant gap for people with disabilities in the accessibility cybersecurity context to help them better handle and understand cyber threats in their everyday lives. We map needs and issues seeking to understand how persons with disabilities may be vulnerable to various cyber threats. The aim of the study is to address the following questions:

- To what extent do users with disabilities encounter accessible security issues when utilizing the current safeguards?
- To what extent does current technology implementation represent accessibility barriers to cybersecurity for people with disabilities?

The remainder of the paper is structured as follows: Firstly, we provide an overview of disability and technology in Section 2. Next, we outline the survey methodology, including sample considerations, in Section 3. Descriptive statistical results are presented in Section 4. The discussion takes place in section 5. The final section provides the conclusion with acknowledgment.

2 Disability and Technology Overview

Disability is growing significantly in the population. Globally, over one billion individuals are estimated to live with some form of disability [3]. This corresponds to approximately 15% of the global population. Disabled World [13] defines disability as "a condition or function judged to be significantly impaired relative to the usual standard of an individual or group. The term is used to refer to individual functioning, including physical impairment, sensory impairment, cognitive impairment, intellectual impairment mental illness, and various types of chronic disease". In an assessment of the International Classification of Functioning, Disability and Health (ICF) checklist of the World Health Organization (2003), Furnell et al. [12, 14] suggest that it might be preferable to distinguish between types of disability according to their interaction with information and communication technologies. They propose ten categories of disability, aligning with the ICF checklist: Intellectual, Attention, Memory, Visual, Hearing, Competence, Life functions, Speech, Dexterity and Walking.

Technology design should grant users ease of access and use with a reasonable amount of effort regardless of their abilities based on universal design. Numerous studies have been conducted on the usage of technologies among people with disabilities and special needs individuals, including their acceptance of technologies and their advantages challenging the utilization of technologies [15, 16]. In the meantime, security innovations and technologies are developed. However, little research has been undertaken in the area of accessible cybersecurity [10]. Accessible cybersecurity is not just about technical considerations. It is about creating a secure digital environment accessible for everyone including disabled people.

Previous research has focused on users with visual impairments more than on users with other types of impairment [11, 17] and has examined forms of authentication for people with vision impairments to investigate users' challenges. Findings have shown that people with vision impairments face various difficulties related to the user interface. Moreover, when usability was evaluated, there were limitations related to sample size. Some previous research had been conducted on accessibility authentication for vision, hearing, and motor-impaired users. Andrew et al. [11], in a theoretical study on security authentication for people with various disabilities (namely, visual, hearing, cognitive and motor impairments) suggests that more effort should be focused on accessibility and usability for people who have a disability. They point out a gap in the research on accessible cybersecurity for users with disabilities. The first step to improve the accessibility of cybersecurity safeguards for users with disabilities is to assess their attitudes and needs. Our work will investigate accessible cybersecurity issues in

general, other than accessible authentication. It is mapping the accessibility of cybersecurity issues for different types of disability. We surveyed 122 participants with deferent types of disabilities. Understanding their encounters with cybersecurity challenges can help develop more accessible and secure technologies and improve user experience generally.

3 Research Methodology

The research population includes people who have disabilities and are regular users of information technology (IT) and seeks information from those with self-declared disabilities of different types. Participants were recruited via the mailing list for Naidex, an event for disabled people, their families and professionals in the United Kingdom focusing on disability, independent living, and healthcare (see www.naidex.co.uk).

The survey was designed to understand the preferences of people with disabilities and the challenges they face in relation to accessing and using security features. The authors can provide the full survey instrument upon request, which includes 15 questions categorized into 5 themes.

1. **Consent**: participants were required to provide explicit consent before proceeding.
2. **General Information**: Q2 to Q7 encompassed inquiries regarding gender, age, occupational status, types of disability, types of support received, and types of online service devices utilized.
3. **Personal Experiences of Cybersecurity Incidents**: Q8 and Q9, aimed to gather insights into participants' encounters with cybersecurity incidents.
4. **Opinion Ratings of Security Knowledge**: From Q10 to Q13, respondents were presented with statements pertaining to various aspects of cybersecurity knowledge (including the use of devices and services, dealings with cybersecurity, protecting against threats, and the accessibility and usability of security technologies).
5. **Open-ended Questions**: including Q14-Q15, accompanying free-text response boxes allowed participants to elaborate any responses would help to improve cybersecurity for people with disabilities, plus any further general comments.

The method received ethics approval and was promoted via the Naidex mailing list during summer 2022. A total of 148 individuals initially visited the survey page. Of these, 137 participants completed the survey, while 11 participants selected "do not wish to participate". Additionally, 5 participants chose to complete the questionnaire but did not provide any answers. A further 8 participants were excluded because they chose 'No disability/impairment' when asked to specify their types of disability. Excluding these, along with two rows of dummy data from the survey pilot, resulted in a total of 122 valid responses. It is important to ensure that the questions being asked are reliable indicators of the underlying construct being studied. One way to evaluate the internal consistency of the questions is to use a measure called Cronbach's alpha. In our survey-based research, a value of 0.67 indicates high internal consistency, meaning that the set of questions analyzed is generally reliable and consistent in measuring the intended construct. The data were analyzed descriptively and thematically to explore

potential relationships between variables and determine further insights into the participants' experience.

4 Findings

This section presents the main findings from the survey, beginning with general information about the respondent group, and then leading into the examination of their use of digital technologies and their related experiences with cybersecurity.

4.1 Demo graphical information

In total, 71 were male, 49 were female and 3 were non-binary. The age distribution among the participants is illustrated in Fig. 1. Notably, 70% of the sample were aged 50 years or older. Unexpectedly, it is noteworthy to observe that the smallest participant group is aged 18-24, a demographic typically anticipated to have greater exposure to technology. This prompts the consideration of additional research to explore further and contextualize the outcomes of this study.

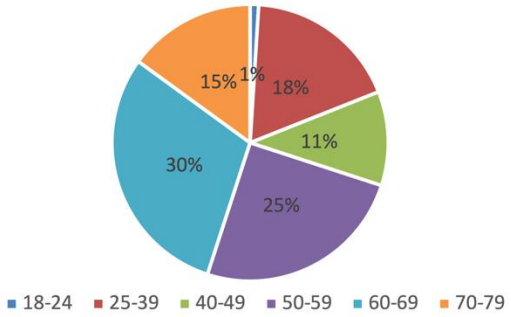

Fig. 1. Participant age groups.

Nearly half of the participants (49%) reported being unemployed. This finding aligns with the age-related aspect discussed earlier, as a significant portion of the participants belong to the older adult demographic. Conversely, only 3% of the participants indicated a student status. The remaining participants are either engaged in paid employment (25%) or voluntary employment (22%). Despite the imbalance in occupational status within the participant group, which could potentially introduce bias to the study results, the distribution provides valuable insights into the diverse occupational backgrounds of the participants.

The distribution of responses across various disability categories is illustrated in Fig. 2. Primarily, mobility or physical disabilities emerge as prevalent among the participants, notably those affecting the lower body (33%). Although representing a minority within the sample, participants with less prevalent types of disability indicated their accessible chance to technology. This underscores the need for tailored approaches to address the unique challenges associated with these specific disabilities.

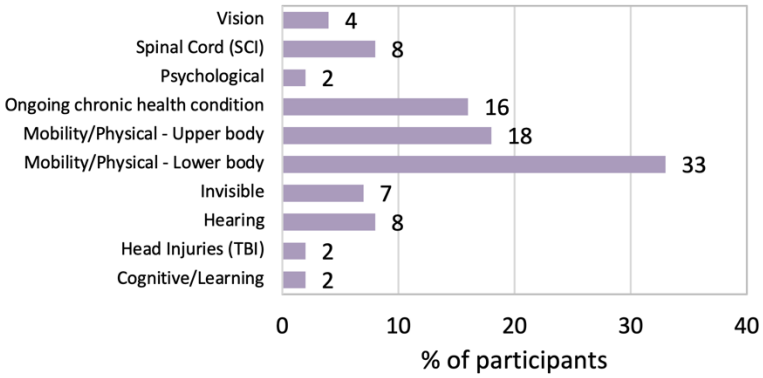

Fig. 2. Disability types reported by the participants.

Information about the devices used by the participants is provided in Fig. 3. This comprehensive overview sheds light on the diverse technological preferences among participants, showcasing a predominant reliance on portable and personal computing devices over smart devices.

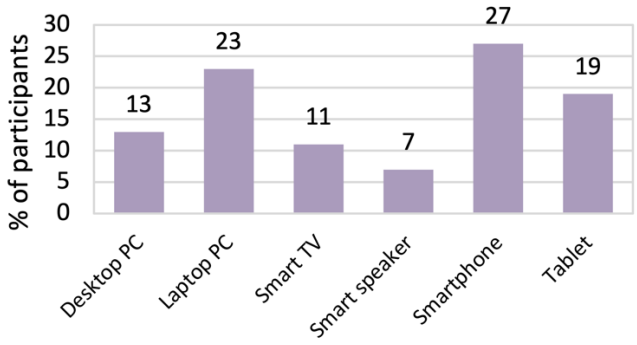

Fig. 3. Types of online services devices.

4.2 Personal Experience of Cybersecurity Incidents

Half of the respondents (52%) reported having had personal experiences with cybersecurity incidents, while 42% claimed not to have encountered such incidents and 6%, responded with ‘Don't know’. This emphasizes the prevalence of such incidents in their digital experience. Further investigation into the nature of these encounters can provide insights into the difficulties that users will encounter as a result, and related information is presented in Fig. 4.

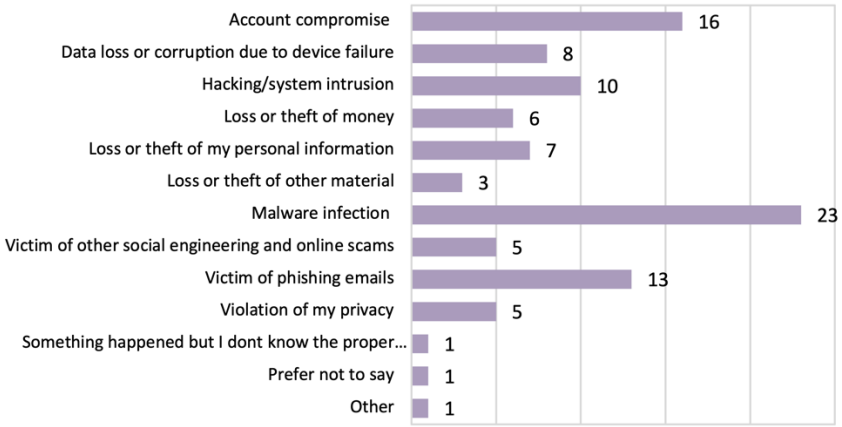

Fig. 4. Types of cybersecurity incidents encountered.

These results highlight the diverse range of cybersecurity challenges faced by participants. They reflect that cybersecurity incidents have varying implications for individuals with different disabilities. The most cybersecurity incidents included malware infection followed by account compromise, phishing emails and hacking/system intrusion. These results highlight the diverse range of cybersecurity challenges faced by participants. Furthermore, the relatively lower percentages in certain categories, such as "Prefer not to say", "Something happened but I don't know the proper name for it" and "Other", they haven't declared, suggest that there may be incidents not adequately captured by existing survey options, emphasizing the evolving nature of cybersecurity concerns. It should be noted that while the survey captured *encounters* with incidents, it did not seek to further explore the *consequences* of their occurrence, as this was considered to increase the risk of participants sharing sensitive personal information. The questionnaire included details of helplines and related websites in case being reminded of incidents prompted respondents to feel they needed further help.

4.3 Using Devices and Services

Responses to questions related to the experience of using devices and services are presented in Table 1, showcasing the participants' opinions on their ability to use digital devices and online services effectively, as well as their utilization of accessibility features or additional technologies for assistance. Note that here, and in other tables, the highlighted cell represents the highest percentage of respondents.

For the first statement, the majority of participants (89%) have different levels of positive agreement towards their proficiency in using digital devices and online services. Regarding the second question, it is interesting to note that more than half of the participants expressed positivity towards their use of accessibility features or additional technologies to assist their use of digital devices and online services. However, the other half of the participants either disagreed or had a neutral sense. They may still encounter issues related to the usage of accessibility features or additional technology.

These findings indicate a generally positive sentiment toward participants' perceived effectiveness in using digital devices. It implies that individuals with disabilities are familiar with utilizing digital devices and services as broad as users without disabilities. However, the utilization of accessibility features or additional technologies for assistance faces some unclear impediments. It might suggest that participants are adept at using digital devices but may lack the application of tools that cater to diverse user needs for devices and services.

Table 1. Use of devices and services.

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1- I am able to use digital devices and online services effectively	55%	34%	7%	3%	1%
2- I make use of accessibility features or additional technologies to assist my use of digital devices and online services	24%	31%	30%	10%	5%

4.4 Dealings with Cybersecurity

Participants' perceptions of handling cybersecurity are shown in

. The majority of respondents (75%) strongly agree that they understand the need for cybersecurity. A substantial majority of 93% of respondents exhibit a positive attitude towards cybersecurity awareness by combining the "Strongly Agree" and "Agree" percentages. In addition, positive comfort levels for a large 79% of respondents express agreement in their understanding of cybersecurity. By nearly similar response, a generally positive sentiment regarding respondents' confidence levels in using cybersecurity technologies was found, with a majority (75%) expressing an agreement stance while a small percentage (11%) stated different levels of disagreement. A notable portion (14%) provided a neutral response that might highlight inquiries to participants have not related clear view with the technology in cybersecurity trust purposes. According to provided statistics, 67% of respondents have agreement feel confident about knowing where and how to get support to manage online threats. A substantial majority of respondents (90%) were willing to use cybersecurity solutions for protecting themselves. These percentages provide a positive overview of the respondents' attitudes towards their knowledge and ability to seek support in managing online threats. It also suggests that a large portion of the participants recognize the importance of using cybersecurity technologies to safeguard themselves, their data, and their devices.

The data from the final two statements, about the appropriateness of cybersecurity features for users with disabilities and one's own disability, show some similarities. Most participants express neutral sentiments regarding the appropriateness of cybersecurity features for general disabilities and for their own disability by 37% and 33%, respectively. These similarities could reflect the reliability and robustness of the data

on the one hand, and it might imply some issues that the needs of people with disability are seldom taken into account when designing cybersecurity technology and solutions. Nevertheless, a substantial portion of respondents express positive sentiments regarding the appropriateness of cybersecurity features for general disabilities (48%) and for their own disability (61%).

Table 2. Dealings with cyber security.

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1- I understand the need for cyber security	75%	18%	6%	2%	0%
2- I feel comfortable with my understanding of cyber security	36%	43%	14%	7%	0%
3- I am confident I can use cyber security technologies	30%	45%	14%	9%	2%
4- I know where and how to get support to manage online threats	28%	39%	19 %	13%	1%
5- I am willing to make use of cyber security technologies to protect myself, my data and/or my devices.	49%	41%	6%	3%	2%
6- I feel that the design and implementation of cyber security features are generally appropriate for users with disabilities	18%	30%	37%	11%	5%
7- I feel that the design and implementation of cyber security features are generally appropriate for my own disability	30%	31%	33%	3%	4%

4.5 Protecting Against Threats

The responses to statements about protecting against threats reveal diverse perspectives among participants are illustrated in Table 3. More than half participants (54%) acknowledge agree and strongly agree feeling at risk from cyber threats which suggests a significant awareness of potential dangers in the digital landscape. However, a neutral stance falls under the next level of participants perception with 26%. It might indicate a need for more information regarding specific cyber threats.

When participants were asked about the impact of their disability on their ability to protect themselves, and if it makes them more susceptible to online threats, over 40 % expressed disagreement with the statements. This suggests that some people with disabilities may feel that their online protection abilities are not impacted by their disability. However, a subset of the participants claims to be more vulnerable to online threats which requires further investigation. A portion of respondents, over 40%, either strongly agree or agree on feeling there is not enough protection provided for people with disabilities online. While a similar percentage of participants falls under the neutral category. This suggests that they are unsure of the adequacy of online protection for people with disabilities. This proposes that there is a segment of the population that feels online protection for people with disabilities is insufficient.

In terms of statements about depending upon other people to ensure protection, 57% of participants disagree with the statement, suggesting that they do not heavily rely on others for their protection. Meanwhile**,** 29% of respondents indicate that they still depend on other people to help ensure they are protected. Understanding the factors that contribute to individuals feeling the need to depend on others for protection is significant to improve their independence stance. Despite the smallest percentage of participants expressing disagreement that their prior experiences have contributed to their ability to handle cybersecurity threats, nearly half of the participants, 47%, believe it does. The participants have a positive disagreement for being frightened of using technology because of cyber threats. Most participants (72%) disagree with suggesting that they do not feel frightened of using technology due to cyber threats. Further exploration into the factors contributing to this confidence could provide valuable insights for enhancing user resilience and cybersecurity awareness.

Table 3. Threats and protecting against them.

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1- I feel at risk from cyber threats	15%	39%	26%	19%	1%
2- I feel that my disability affects my ability to protect myself online	7%	13%	23%	36%	22%
3- I feel that my disability makes me more of a target for online threats	9%	19%	29%	31%	11%
4- I feel that there isn't enough protection provided for people with disabilities online	18%	26%	42%	10%	3%
5- I depend upon other people to help ensure I am protected	13%	16%	14%	32%	25%
6- I feel better able to handle cyber security threats because of my prior experience of them	17%	30%	42%	8%	3%
7- I am frightened of using technology because of cyber threats	6%	5%	17%	39%	33%

4.6 The Accessibility and Usability of Security Technologies

Participants' perceptions regarding the accessibility and usability of security technologies are presented in Table 4. It highlights participants' opinions on how the design and implementation of cybersecurity features influence their ability to protect personal and device security and render them vulnerable to cybersecurity threats.

The participants expressed concerns about the presentation of cybersecurity technologies, with nearly half of participants feeling limited (46%) about their ability to protect themselves and their devices based on the current presentation of security features. This indicates that a significant number of participants feel that the current presentation of cybersecurity technologies is lacking in supporting their sense of security. Participants' responses indicate a range of sentiments regarding vulnerability to cybersecurity threats

stemming from the design and implementation of features. While 34% of the respondents disagreed with this statement, 30% feel vulnerable and 36% had neutral stances. This implies that there is a considerable group of participants who either perceive a level of vulnerability or are uncertain about the effectiveness of the current design and implementation of cybersecurity features in mitigating threats.

Table 4. Accessibility and usability of security technologies.

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
1- My ability to protect myself, my data and/or my devices is limited by how cyber security technologies or features are presented	12%	34%	36%	11%	7%
2- I feel vulnerable to cyber security threats because of the design and implementation of the cyber security features on my device(s)	7%	23%	36%	25%	9%

4.7 Open Ended Questions

The respondents were also able to offer free-text comments relating to general feedback, as well as suggestions for improving cybersecurity for users with disabilities. A total comment for supporting the survey questions and offering additional thoughts was 27 responses provide insights into respondents' experiences, perspectives, and expertise related to cybersecurity. The most prominent points highlighted in responses were:

- Hacking and phishing scams were the most recurrent personal security experiences.
- Concerns about accessibility of authentication methods for those with disabilities.
- Challenges of securing information through authentication mechanisms and addressing password security.
- Attributing responsibility to banks and website providers rather than individuals.
- The significance of security risks for all users, not exclusively those with disabilities.

In terms of the participants' suggestion for improving cybersecurity for people with disabilities, the participants provided 21 responses. The comments collectively underscore several recurring themes as follows:

- A discernible demand for customized cybersecurity programs, accessible information, simplified explanations, adaptive interfaces and customizing authentication methods for disabilities needs is required.
- Challenges in current cybersecurity measures, especially biometrics.
- The need for research on supporting individuals with cognitive, learning, and mental health disabilities, and into specific vulnerabilities encountered by individuals with disabilities is emphasized.

The survey responses illustrate a diverse range of perspectives on cybersecurity which aligns with the participants' varied responses in other survey questions. The comments underscore the difference of individual experiences with cybersecurity and the varied levels of awareness among survey participants. The respondents' suggestions

also provide valuable insights into the specific challenges and needs of individuals with disabilities in the realm of cybersecurity. At the same time, while the open questions enabled some qualitative data to be collected, a more substantial qualitative study could reveal more extensive insights. More generally, the demographics of the relatively small sample, including age and occupational status and disability types, may have potential implications for the generalizability of the findings. Future research should aim for a more balanced representation across demographics and disability groups.

5 Discussion

Approximately 50% of participants had personal experiences of cybersecurity incidents. However, they acknowledged the necessity for protection and expressed understanding, comfort and confidence in using cybersecurity technologies (Table 2). Despite this there appears to be a gap between knowledge and practical application.

As shown in Table 3, around half of participants (54%) feel at risk from cyber threats which suggests a significant awareness of potential dangers in the digital environment. Their concerns do not prevent them from using technology as shown in Table 1. Moreover, they do not feel frightened of using it due to cyber threats as shown in the last statement in Table 3. However, the percentage of participants feeling at risk from cyber threats contrasts with Murray [18], who surveyed 143 non-disabled users. In that study, when asked about privacy and protection of their personal data, only 30% were very or extremely concerned [8]. As such, users with disabilities may have cybersecurity higher concerns than the general population. However, further investigation is required to ascertain whether this difference is attributable to disability status.

According to Table 4, 46% of people feel that the presentation of cybersecurity technologies or features limits their ability to protect themselves. Moreover, Table 3 shows that 58% of people don't believe that their disability hinders their ability to protect themselves. They also do not believe that their disability affects their ability to protect themselves online or makes them more vulnerable to online threats. This suggests that the presentation of security features is a challenge for these users, regardless of disability. It is crucial to indicate that users with disabilities are not inherently more susceptible to incidents than others. Equally, there is no anticipation of them being less susceptible either. Although users with some forms of disability are likely to need the most support, the core point is that we expect them to experience the same challenges as users at large. Meanwhile, people with disabilities are one of the most heterogeneous groups societally hence their cybersecurity experiences and needs will also vary considerably. Nevertheless, understanding their encounters can help in developing more accessible and secure technologies and improving user experience.

According to Table 3, participants prefer to handle cybersecurity threats themselves, as they do not want to rely on others to ensure their protection. They also acknowledged in their feedback that they expect service and website providers, such as banks, to provide adequately accessible and protective systems for them to use. However, they have indicated a limited ability to protect themselves due to the way cybersecurity technologies or features are presented (Table 4). They also had concerns regarding accessible

authentication methods and time consumption, and suggest some requirements to enhance technology's support for their security as follows:

- P52: For me, there needs to be research done into accessible interfaces … Sometimes I'm not quick enough when entering the code meaning that I may have to re-enter several different codes to get in. This can feel extremely frustrating. The card reader is too small for me to use. For example, it does not have adequate gaps between the buttons, this leads to me sometimes having a spasm and entering the wrong number
- P68: voice control not good with security software
- P101: Far too technical with explanations of how these work usually incomprehensible at times.

In order to address these needs and concerns, further research is necessary to evaluate how cybersecurity features are designed and implemented to accommodate users with different types of disabilities. This will contribute to improving the user experience with cybersecurity technologies.

6 Conclusion

This research result is a foundational mapping tool for understanding the cybersecurity landscape within the disabilities community. While participants exhibit a commendable range of cybersecurity awareness, their experiences reflect previous exposure to cybersecurity incidents, suggesting that awareness does not necessarily serve as a preventive measure against breaches. Users frequently engage in security practices that compromise safety for the sake of accessibility and usability. Additionally, there is a discernible inclination to seek convenient technological solutions for cybersecurity, underscoring a notable concern regarding insufficient technological safeguards.

The findings indicate a need for further investigations, particularly in accessible authentication and security features issues, to understand how individuals with disabilities interact with and secure their digital environments. The identified areas of concern provide a clear direction for future research endeavors, aiming to enhance the cybersecurity experience for individuals with disabilities. Accessible security concerns for individuals with disabilities were raised, emphasizing the need for inclusive security measures. Continuous improvement of cybersecurity features, considering diverse user perspectives, is essential for creating a robust and inclusive cybersecurity framework.

Acknowledgments. The authors would like to thank ROAR B2B, the Naidex event organizers, for mounting the online and promoting it to the Naidex community. Additionally, we extend thanks to Bradley Maule-ffinch, Group Managing Director, and his colleagues for their valuable support and feedback.

References

1. Wang, Y. Universal authentication: towards accessible authentication for everyone. in Proceedings of the Symposium on Usable Privacy and Security (SOUPS). 2017. Citeseer.
2. United Nations. Convention on the Rights of Persons with Disabilities (CRPD). 2006; Available from: https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html#Fulltext.
3. World Health Organisation. Disability. 2023; Available from: https://www.who.int/news-room/fact-sheets/detail/disability-and-health.
4. Geraci, A., IEEE standard computer dictionary: Compilation of IEEE standard computer glossaries. 1991: IEEE Press.
5. W3C. Introduction to Web Accessibility. 2024; Shawn Lawton Henry:[Available from: https://www.w3.org/WAI/fundamentals/accessibility-intro/#context.
6. W3C. Web content accessibility guidelines (WCAG) overview. 2021; Available from: https://www.w3.org/WAI/standards-guidelines/wcag/(accessed.
7. Mihajlov, M., B. Jerman-Blazič, and S. Josimovski. A conceptual framework for evaluating usable security in authentication mechanisms-usability perspectives. in 2011 5th international conference on network and system security. 2011. IEEE.
8. Bedford, M., R.t. Brink, and R. Scollan. Usability of Biometric Authentication Methods for Citizens with Disabilities. 2019.
9. Correia, W., M. Penha, J. Macedo, W. Santos, J. Quintino, M. Anjos, A. Santos, and F. Silva. Full mobile accessibility is a matter of respect: GuAMA update process for motor and hearing disability users. in Proceedings of the 18th Brazilian Symposium on Human Factors in Computing Systems. 2019.
10. Renaud, K. and L. Coles-Kemp, Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge. SN Computer Science, 2022. 3(5): p. 346.
11. Andrew, S., S. Watson, T. Oh, and G.W. Tigwell. A review of literature on accessibility and authentication techniques. in Proceedings of the 22nd International ACM SIGACCESS Conference on Computers and Accessibility. 2020.
12. Furnell, S., K. Helkala, and N. Woods. Disadvantaged by Disability: Examining the Accessibility of Cyber Security. in HCI. 2021.
13. Disabled World Disabilities: Definition, Types and Models of Disability. 2022; Available from: https://www.disabled-world.com/disability/types/.
14. Furnell, S., K. Helkala, and N. Woods, Accessible authentication: Assessing the applicability for users with disabilities. Computers & Security, 2022. 113: p. 102561.
15. Correia, W., M. Penha, J. Macedo, W. Santos, J. Quintino, M. Anjos, A. Santos, and F. Silva, Full mobile accessibility is a matter of respect: GuAMA update process for motor and hearing disability users, in Proceedings of the 18th Brazilian Symposium on Human Factors in Computing Systems. 2019, Vitória, Espírito Santo, Brazil. p. Article 58.
16. Nasir, N.A.M., H. Hashim, S.M.M. Rashid, and M.M. Yunus, Exploring the Potential Usage of Mobile Technologies Among the Hearing-Impaired Students in Learning English as a Second Language (ESL). International Journal of Interactive Mobile Technologies, 2021. 15(19).
17. Dosono, B., J. Hayes, and Y. Wang. " I'm Stuck!": A Contextual Inquiry of People with Visual Impairments in Authentication. in SOUPS. 2015.
18. Murray, C., Smartphone Security Risks: The Extent of User Security Awareness, in Management of Information Systems. 2014, The University of Dublin p. 115.