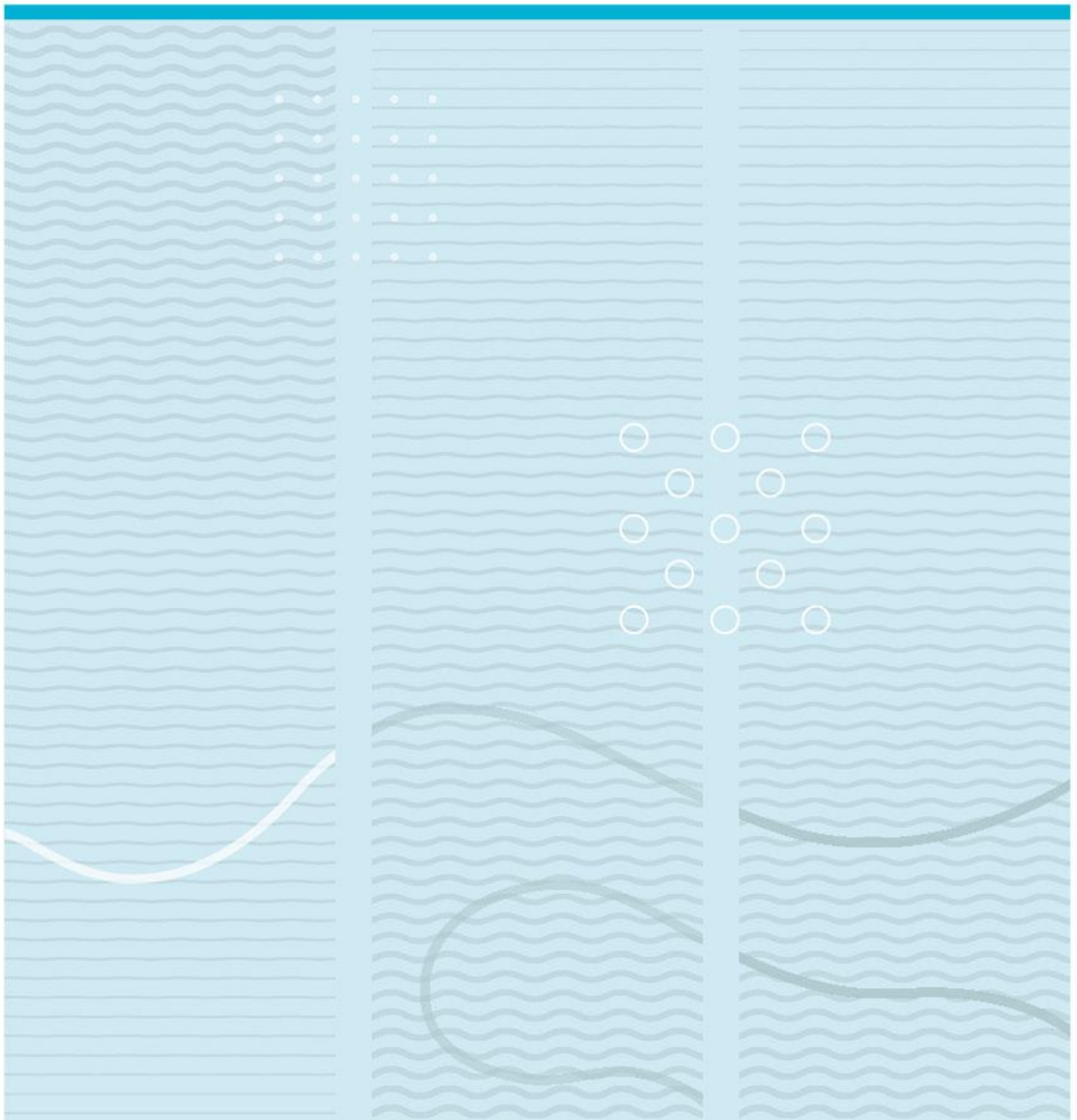


Md. Ohidul Islam

Equitable User Experience in Terms of Privacy and Security Settings

Subtitle



University of South-Eastern Norway
Faculty of ...
Institute of ...
PO Box 235
NO-3603 Kongsberg, Norway

<http://www.usn.no>

© 2023 <Md. Ohidul Islam>

This thesis is worth 60 study points

Acknowledgements

I would like to express my gratitude to the following people and groups who played a vital role in making this research possible:

- My thesis advisor, Joakim Kävrestad, whose guidance, expertise, and support were invaluable throughout this journey. Your patience and encouragement helped shape this work.
- The participants of this study, who generously shared their time, experiences, and insights. Your contributions were essential to the success of this research.
- The University of South Eastern Norway, faculty and staff, for providing the necessary resources, access to the library, and a conducive academic environment.
- My family and friends, for their unwavering support, understanding, and motivation during this challenging academic endeavor.
- All the individuals who, in various ways, contributed to this project but are not named here explicitly.

Your collective assistance has been invaluable in helping me complete this thesis. Thank you for being a part of this academic journey.

Abstract

This thesis addresses the common cybersecurity challenge of promoting user use of security techniques and tools, including encryption software, password guidelines, privacy settings, and phishing detection processes. The difficulty lies in the time and energy consumption connected with these processes, often posing limitations to user compliance. Moreover, users with lowered cognitive ability face additional challenges in using such tools, leading to inclusion issues. To tackle these problems, the research focuses on creating equal availability to web services without harming privacy. The primary goals include developing rules for inclusive website design, proposing user-friendly privacy and security steps, identifying requirements for lower cognitive users, and monitoring the evolution of existing public service websites. The methodology involves a complete literature review, data collection through surveys and interviews, and a detailed analysis of websites' availability and usability. The findings contribute practical recommendations for designing inclusive web services and promoting better cybersecurity practices while considering users' needs with permanently or temporarily lowered cognitive ability.

Contents

1	Introduction	8
1.1	Background	8
1.2	Motivation and Problem Statement	9
1.3	Research Questions	10
1.4	Thesis Goals	10
1.5	Assumptions and Limitations	11
1.6	Thesis Contributions	13
1.7	Thesis Outline	13
2	Related works	15
3	Research Methodology	20
3.1	Research Design	20
3.1.1	Qualitative Methodology	20
3.1.2	Quantitative Methodology	20
3.1.3	Justification of Chosen Methodology	21
3.2	Data Collection	21
3.2.1	Data Sources	22
3.2.2	Data Collection Procedures	26
3.2.3	Privacy and Anonymity	27
3.3	Data Analysis	27
3.3.1	Qualitative Data Analysis	27
3.3.2	Quantitative Data Analysis	28
3.3.3	Integration of Qualitative and Quantitative Findings	28
4	Experiments and Results	30
4.1	Quantitative Analysis - Survey	30
4.2	Key Observations from the Survey Responses	38
4.3	Qualitative Analysis - Interviews	40
4.4	Key Observations from the Interview Responses	45
4.5	Key Observations Based on the Integration of Qualitative and Quantitative Findings	47

5 Discussion	49
6 Conclusion and Future Work	55
6.1 Conclusions	55
6.1.1 Understanding the Challenges	55
6.1.2 Promoting User Adoption	55
6.1.3 Quantitative Insights	55
6.1.4 Toward a More Inclusive and Secure Digital Landscape	56
6.1.5 Recommendations for the Future	56
6.2 Future Works	56
References	58
Appendices	61
A Informed Consent for Interview Participation	61
B Informed Consent for Survey Participation	63

List of Figures

1	Research workflow.	14
2	Shows age distribution of all respondents.	30
3	Overview of Internet uses of the respondents.	31
4	Distribution of preferred devices for accessing the internet and digital services.	31
5	Statistics of common problems using the internet or digital services.	32
6	Figure illustrates the varying degrees of confidence among respondents.	33
7	Respondents experience on any cyberattacks or online scams.	33
8	Respondents awareness of cyberspace’s potential risks and vulnerabilities.	34
9	Response of online safety measurement question.	34
10	Figure shows the frequency of getting information or guidance about online safety and cybersecurity.	35
11	Respondent Satisfaction with Digital Platform Accessibility.	36
12	Participant Responses to the Statement 'I often find it difficult to comprehend security information provided to me by digital services,' Rated on a Scale from 1 (Strongly Disagree) to 5 (Strongly Agree).	36
13	User Agreement with the Statement "I often struggle to understand how to update my device."	37
14	Respondents' Ratings on Password Difficulty.	37
15	User Responses to Government Website Security Measures.	38
16	Accessibility Challenges Faced by Respondents on Government Websites due to Lower Cognitive Abilities.	39

List of Tables

1	Acronyms	7
2	Cybersecurity Challenges.	18
3	Relevant papers summary.	19
4	Data Collection Methods	21
5	Data Analysis Techniques	27
6	Survey and Interview Sample Sizes and Platforms	49

Acronym

Table 1: Acronyms

Short Form	Long Form
WCAG	Web Content Accessibility Guidelines
W3C	World Wide Web Consortium
2FA	Two-factor Authentication
IT	Information Technology
PICS	Privacy, Information, and Cybersecurity
PWAs	Progressive Web Apps
NCSPs	National Cybersecurity Strategic Plans
HCCS	Human-centric Cybersecurity
NDIDs	National Digital Identity Systems
CNIs	Critical National Infrastructures

1 Introduction

1.1 Background

Although the digital landscape has noticed a high jump in availability, mere access to the internet tool does not assure neutral access to digital resources (Hortizuela, 2022a). Many aspects, including complex features and security protocols, can pose significant challenges for humans with lowered cognitive capacity. Complex connections, the absence of various modes (such as symbols related to text or captions replacing audio), encryption software, password rules, and privacy settings can hinder successful use of the digital realm (Hortizuela, 2022a).

The European Union addresses about 100 million people with various forms of lower cognitive ability (digital future, July 2022). The absence of cognitive accessibility runs the risk of removing these users from the many benefits digital services offer, thereby giving rise to an issue of equality. Moreover, this social indicates a significant market part, highlighting the importance for businesses to cater to the needs of this diverse user base (digital future, July 2022).

Cognitive ability refers to a person's mental capacity for thinking, learning, memory, problem-solving, and reasoning, collectively contributing to their intellectual and problem-solving skills. Previous studies highlight the lack of current web principles, especially the W3C and WCAG (Web Content Accessibility Guidelines), in addressing cognitive accessibility (Johansson, 2022). While WCAG contains a central necessity for others with cognitive disabilities, further growth is needed to bridge the gaps. It is worth noting that the benefits of decreasing websites and applications improve beyond users with disabilities. For example, rendering audio of text in low-light forces or offering captions in noisy environments can improve the user knowledge for all (digital future, July 2022). It explains the common reasons why web accessibility requirements are not met and discusses the challenges faced by people with cognitive disorders when using the internet. It also examines the efforts of governments and commercial groups worldwide's efforts to increase web accessibility for people with cognitive disorders (Hortizuela, 2022b).

Additionally, cybersecurity has become a basic worry in today's digital age, with a boosting dependency on web services and online platforms (Gompert & Libicki, 2023). As technology evolves, so do the threats posed by malicious actors seeking to exploit vulnerabilities in security and privacy measures (Ruefle et al., 2014). To counter these threats, various security rules and tools have been developed, including encryption software, password guidelines, privacy settings, and phishing detection processes. However, one common challenge in cybersecurity is impacting users to adopt

and utilize these measures successfully. Studies have shown that many users find these methods too time-consuming and energy-draining, resulting in low usages (Pham, Brennan, & Furnell, 2019). Moreover, users with lowered conceptual ability meet difficulties in understanding and using these tools, leading to a limiting effect (Parsons & Mitchell, 2002).

In light of these considerations, the pursuit of an inclusive approach to rendering digital services accessible for all users has emerged as a compelling focus for this master's thesis. By delineating the requirements of users with diverse cognitive conditions, this research endeavors to contribute meaningfully to the quest for universal digital inclusivity.

1.2 Motivation and Problem Statement

The problem addressed in this thesis is the lack of equal availability of web services for all users, mainly those with permanently or temporarily lowered cognitive ability. The cognitive ability of individuals can vary over time, and some users may have disabilities due to conditions or injuries. This change in cognitive ability creates barriers for specific user groups in adopting and utilizing security and privacy measures (Fischer, David, Crotty, Dierks, & Safran, 2014). For instance, a complex authorization sequence for a public health service may prove unavailable for users with specific cognitive conditions, hindering their ability to access essential services (Vollenwyder et al., 2023). During the COVID-19 pandemic, persons with intellectual disabilities in the United Kingdom accessed the Internet. They mainly utilized it for socializing, using social media, and engaging in online activities. Those who lived with family used social media more, while introvert people engaged in online activities. The best component, according to participants, was social relationships, but some showed concern about technology challenges and internet danger (Caton et al., 2022). Additionally, Accessibility changes in security functions are crucial for creating inclusive and secure digital environments. An example that highlights this need is two-factor authentication (2FA). While 2FA enhances security by requiring users to provide two verification forms, it can pose challenges for individuals with specific disabilities, such as visual issues. Traditional 2FA methods may rely on visual signals like QR codes, which can be unavailable to those using screen readers or with limited vision. By making 2FA accessible through alternative methods like audio prompts or accessible mobile apps, security is not weakened, and a broader range of users can benefit. This approach ensures equal access and strengthens overall security by allowing all users and reducing the risk of solutions or non-compliance due to accessibility barriers. In today's linked world, improving accessibility in security functions is not just a matter of equality; it's a strategic step toward robust, user-friendly, and secure digital systems.

Additionally, users' opposition to using security measures due to their time and energy-consuming nature creates a pressing need for rules and tools that can be naturally integrated into their online experiences (Herath, Khanna, & Ahmed, 2022). Therefore, there is a demand for creative solutions that pick a balance between robust security and privacy practices and an open user experience for all. The objective of this research is to explore how web services can be made equally accessible to all users, independent of cognitive ability, without compromising on security and privacy aspects. By providing guidelines for open website design, proposing user-friendly privacy and security procedures, and identifying specific requirements for cognitively disabled users, this study aims to address the inclusion problem and motivate greater cybersecurity awareness and execution among diverse user groups.

1.3 Research Questions

The research questions are as follows:

- What are the primary challenges users with lowered cognitive ability face in adopting current cyber-security methods and tools, such as encryption software, password guidelines, privacy settings, and phishing detection processes?
- How can web services be equally accessible to users with lowered cognitive ability, considering their unique needs and limitations?
- What guidelines can be formulated to design websites that are inclusive and accessible to all users, including those with cognitive disabilities?

1.4 Thesis Goals

The goal of this thesis is to promote equal availability of web services for all users, with a specific focus on individuals with lowered cognitive ability. The thesis aims to address the common problem in cybersecurity where users struggle to adopt and follow security rules and tools, including encryption software, password methods, privacy settings, and phishing detection processes. This challenge often arises due to the perceived time and energy consumption associated with these measures, leading to low user execution rates. By recognizing the cognitive diversity among users and the impact it has on their ability to utilize existing security and privacy tools effectively, this research aims to bridge the accessibility gap. The primary objectives of this study are as follows:

- The thesis will conduct a complete literature review and analyze best practices in web availability and inclusive design. Based on these findings, it will discuss possible guidelines for web service providers and developers to create websites that cater to users' needs with lowered cognitive ability while maintaining security and privacy standards.
- To overcome the opposition of users towards time-consuming and energy-draining security measures, the thesis will explore alternative privacy and security procedures that strike a balance between usability and robust cyber-security. These proposed measures will enhance user acceptance and compliance without compromising data protection.
- Through qualitative and quantitative research methods such as surveys and interviews, the thesis will investigate the cognitive challenges faced by users with permanent or temporary cognitive disabilities. For quantitative analysis, ten individuals were interviewed and asked 10 questions each of them. For quantitative analysis, a survey was conducted among around 50 individuals and both of those are discussed in the Experiments and Results section. The study will identify specific requirements and design considerations necessary to ensure that web services are accessible and usable for this user group.

By achieving these objectives, the thesis seeks to advance web accessibility and cybersecurity practices. The ultimate goal is to create a more open online environment that accepts users' needs with diverse cognitive abilities while ensuring their privacy and security. By providing practical recommendations and insights for website designers, developers, and policy-makers, this research fosters greater awareness and implementation of inclusive design principles in the digital realm. Through this multidimensional approach, the thesis aspires to facilitate the development of a more accessible and secure cyberspace for all users, thereby contributing to a safer and more inclusive digital future.

1.5 Assumptions and Limitations

Assumptions are underlying beliefs or conditions that researchers make to simplify their study and draw meaningful conclusions. For this research, we have made the following assumptions:

- **User Cooperation:** The research assumes that users are willing to participate in surveys and interviews and provide accurate and honest responses about their experiences with web services and cyber-security measures.
- **Representativeness:** Almost 98% of the representativeness were aged 18-39 years and all of them are from Bangladesh.

- **Ethical Considerations:** The study assumes that ethical considerations related to data collection and participant anonymity will be upheld throughout the research process.
- **Stability of Technology:** It is assumed that the technology and web service platforms being evaluated will remain stable during the study period and not undergo significant changes that could impact the research results.
- **Relevance of Literature:** The research assumes that the literature reviewed on web availability, cybersecurity, and cognitive disabilities is relevant and provides valuable insights for addressing the research objectives.

Limitations refer to the restrictions or factors that can potentially hinder the scope or quality of the research. The possible limitations for this research can be:

- **Sample Size:** The study's sample size, particularly for qualitative and quantitative research, may be limited, affecting the representation and generalization of the findings.
- **Subjective Perspectives:** Users' perceptions and experiences with web services and cybersecurity may be subjective, potentially leading to variations in the responses collected.
- **Time Constraints:** Conducting a comprehensive study within a limited time frame may restrict the depth and scope of the research.
- **Accessibility of Websites:** The evaluation of existing public service websites may be limited to publicly available information, as accessing certain features or functionalities may require permissions that are not readily obtainable.
- **Changing Landscape:** The rapidly evolving nature of technology and cyber-security may result in certain recommendations becoming outdated over time.
- **Expertise:** While efforts will be made to include insights from various disciplines, the study's interdisciplinary nature may pose challenges in bounding all aspects comprehensively.
- **Resource Constraints:** Limited resources, such as funding and technology, may impact the extent of data collection and analysis.

It is crucial to acknowledge these assumptions and limitations to provide a clear understanding of the research's context and potential implications for the findings and conclusions.

1.6 Thesis Contributions

The thesis contributions are as follows:

- The thesis discusses comprehensive guidelines for web service providers and developers to design websites that are accessible to all users, including those with permanently or temporarily lowered cognitive ability. These guidelines aim to ensure a more inclusive online experience while following to essential security and privacy measures.
- Through qualitative and quantitative research, the study identifies specific cognitive user requirements, shedding light on the challenges faced by users with lowered cognitive ability. This understanding provides valuable insights for designing more user-centric web services.
- By exploring user opinions and attitudes towards cyber-security measures, the research contributes to a better understanding of the factors influencing user adoption. This understanding can inform strategies to improve execution rates and strengthen overall cyber-security practices.
- The thesis offers practical recommendations based on research findings to policymakers, web service providers, and developers. These actionable insights can facilitate the implementation of user-friendly security measures and foster a more inclusive digital environment.

Overall, the thesis's contributions aim to promote a safer and more accessible online environment for all users, particularly those with lowered cognitive ability, and support for the integration of user-centric design practices in cyber-security and web development.

1.7 Thesis Outline

In this section, the thesis provides a complete outline of its critical elements. It begins with a research of related research works in Section 2. Following this, Section 3 elaborates on the thesis methodology, which opens a detailed description of the research design (Section 3.1), insights into the data collection process (Section 3.2), and an in-depth analysis of the data processing procedures (Section 3.3). The subsequent segment, Section 4, delves into examining experimental results. This involves discussing the quantitative analysis through a survey approach (Section 4.1), followed by an evaluation of key observations derived from the survey data (Section 4.2). Additionally, it encompasses the qualitative analysis conducted via interviews (Section 4.3), along with an analysis of the critical

insights extracted from these interview responses (Section 4.4). In Section 5, the thesis presents a comprehensive discussion of the overall research findings and proposes viable solutions to address the identified research problem. It also provides valuable guidelines aimed at mitigating the discussed challenges. Finally, in Section 6, the thesis offers a concluding analysis while identifying potential avenues for future research in the field. Here, Figure 1 illustrates the research workflow.

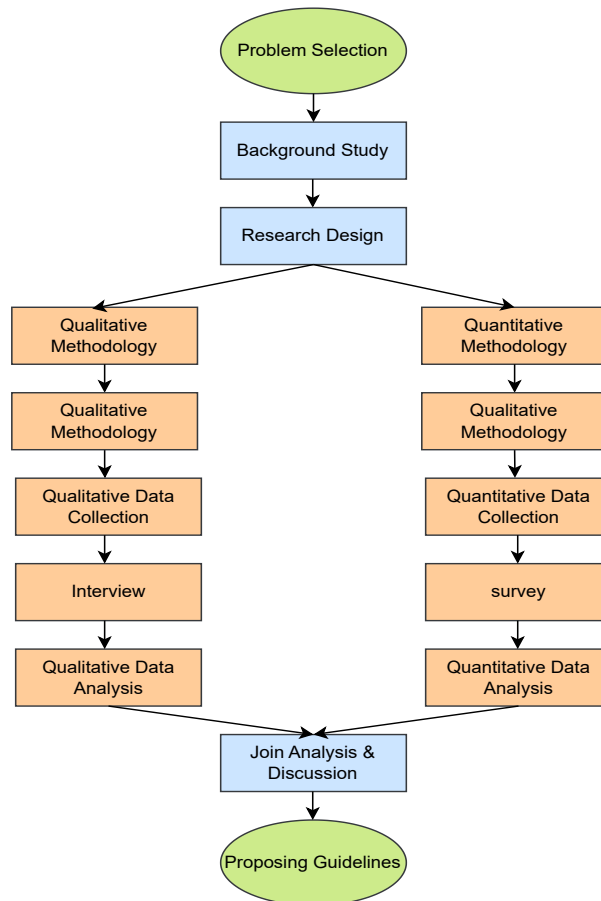


Figure 1: Research workflow.

2 Related works

The rapid growth of technology and the common use of web services have transformed various aspects of modern life, making digital relationships an integral part of daily routines. However, this increased dependency on digital platforms has also brought about new challenges in terms of cybersecurity and web accessibility. Cybersecurity is a critical concern as cyber threats continue to evolve, targeting sensitive information and posing risks to persons and organizations worldwide. The literature review in this chapter presents an overview of relevant research related to web availability, cybersecurity challenges, and the impact of cognitive disabilities on user interactions with web services. The review highlights the existing body of knowledge and identifies gaps that this thesis aims to address.

(Inal, Guribye, Rajanen, Rajanen, & Rost, 2020) explored the current status of digital accessibility practices among user experience (UX) professionals in the Nordic region. It analyses the extent to which digital accessibility is familiar to professionals and highlights the challenges they face in integrating user experience and accessibility practices. The findings shed light on the importance of user-centric design in improving accessibility for all potential users, including those with cognitive disabilities.

(MACAKOĞLU & Peker, 2022) examined web accessibility research from 2002 to 2021, specifically focusing on automated testing methods. It discovers and categorizes 72 relevant articles based on publication kind, year, publisher, testing tool, website type, and accessibility guide. The data show that automated testing methods for web accessibility evaluations has been increasing over the years. This study aims to provide an overview of the topic and act as a road map for future research in web accessibility analysis using automated techniques.

(Kävrestad, Fallatah, & Furnell, 2023) investigated user acceptance of cyber-security training, noting its importance in fostering secure behaviour. It takes a socio-technical approach, considering training, organization, and users. A systematic evaluation of the literature emphasises training methods, with little study on organizational and user-related characteristics. More research on organizational components and variances in user acceptance among different user groups is called for in the paper.

(Hortizuela, 2022a) presented an overview of efforts made by governments, private organizations, and academia to address web accessibility challenges for individuals with cognitive disabilities. By analyzing academic research and government laws, the study defines cognitive accessibility and lists standard parts of web accessibility. The research emphasizes the importance of flexibility, navigation, readability, predictability, and input help in creating web content that allows users with cognitive

disabilities.

(Johansson, Gulliksen, & Lantz, 2015) explored the combination of non-formal adult education methods with scientific tools to improve access to services and products for individuals with mental and cognitive disabilities. The researchers focus on Folkbildning, a concept promoting learning and social relationships, to empower this user group to advocate for their needs and create an accessible society.

(Chalghoumi et al., 2019) investigated the access and use of information technology (IT) by older adults with cognitive disabilities and the role of caregivers in supporting them. It reveals challenges older adults face in utilizing IT and highlights the importance of caregiver involvement in providing support. The research emphasizes the need to consider age and disability-related factors when designing IT services for older adults with cognitive disabilities.

(Kävrestad, Hagberg, Roos, Rambusch, & Nohlberg, 2021) discussed the limitations and guidelines for Privacy, Information, and Cybersecurity (PICS) tools to make them more accessible to users with cognitive disabilities. The study includes interviews with experts and users with cognitive disabilities, exploring themes related to making PICS tools more user-friendly. The research proposes text-to-speech functionality, diverse information presentation, easy-to-digest information, minimal user interaction, and various forms of authentication as key recommendations for designing accessible PICS tools.

(Torrado, Jaccheri, Pelagatti, & Wold, 2022) developed a mobile app, HikePal, to encourage persons with intellectual disabilities to participate in outdoor physical activity. The app's development included expert advice and user testing. Social engagement was discovered to be a crucial motivation, but traditional reward schemes were less effective. The software is designed to provide clear, easy-to-read instructions with visual aids. Field testing was critical, and the team intends to expand testing with a broader range of disabled individuals.

(Pour, Nader, Friday, & Bou-Harb, 2023) examined society's growing vulnerability to cyber-security attacks as well as the need for large-scale empirical data collecting using internet measuring approaches. It presents a taxonomy of cyber-security-related internet measuring studies, compares them to various criteria, and explores future research paths in this crucial topic.

(Kim, 2013) analyzed the cognitive accessibility of websites for people with and without disabilities. They conduct an online poll to assess the accessibility of selected websites and identify areas for improvement. The study highlights the importance of enhancing website accessibility to create a more inclusive online experience for all users, including those with cognitive disabilities.

(Spina, 2019) reviewed the guidelines of WCAG 2.1 and evaluated their importance for cognitive ac-

cessibility. The study identifies key guidelines for cognitive disabilities and suggests improvements to enhance cognitive accessibility in web content.

(Simpson, Adams, Manokara, & Malone, 2022) studied the research and training objectives for support workers in an organization that helps people with intellectual disabilities and autism. According to the findings of the study, employees preferred training for knowledge enhancement, particularly in understanding and managing behaviours. Priorities for research included interventions and carer support, which aligned with global priorities for this group.

(Lara & Bokoch, 2021) examined the relationship between social media use and cognitive functioning, particularly attention span and working memory. The research evaluates differences in cognitive functioning based on time spent interacting with social media platforms. The findings provide insights into the potential impact of social media on cognitive abilities and have implications for long-term memory.

(Shpigelman & Gill, 2014) explored Facebook use among individuals with disabilities, highlighting their interaction with the platform and the support they receive from caregivers. It addresses concerns related to privacy, security, and accessibility for persons with cognitive disabilities on social media. The research underscores the importance of making social networking sites more accessible for all user groups, including individuals with cognitive disabilities.

(Roumeliotis & Tselikas, 2022) investigated the growth of Progressive Web Apps (PWAs), which employ web technologies to imitate the capabilities of native apps. It also speaks to the growing significance of web accessibility for people with disabilities. The study gives a systematic review with the goal of determining how well PWAs enable accessibility.

(AlDaajeh et al., 2022) emphasized the critical need for cyber-security education in protecting a country's digital infrastructure and sovereignty. It examines National Cybersecurity Strategic Plans (NCSPs) and recommends the GQO+Strategies paradigm for curriculum reform in order to connect educational programs with national cyber-security goals. The suggested strategy intends to close the skills gap and assist in the creation of a strong cyber-security workforce, thereby improving national security.

The literature review presents a diverse range of studies focusing on web accessibility, cybersecurity challenges, and user interactions for individuals with cognitive disabilities. These studies highlight the importance of user-centric design, accessibility guidelines, and user involvement in creating an inclusive digital environment. They provide valuable insights into the current practices, challenges, and potential improvements to enhance web accessibility for users with lowered cognitive ability. The gaps identified in existing literature set the stage for further exploration and development of

practical guidelines to address these challenges and improve digital inclusivity. Table 2 demonstrates some significant Cybersecurity Challenges.

Table 2: Cybersecurity Challenges.

Cybersecurity Challenge	Description
Encryption Software	Encryption steps involve intricate steps and concepts, which can be difficult for individuals with cognitive impairments to grasp, hindering their ability to secure their online interactions and data.
Password Guidelines	Complex password requirements, such as length, character variety, and frequent changes, can pose significant barriers for users with lowered cognitive abilities, potentially leading to password-related security dangers.
Privacy Settings	Navigating the maze of privacy settings and understanding their implications can overwhelm users with cognitive challenges, resulting in unintended privacy compromises and difficulties in controlling their online presence.
Phishing Detection Processes	Recognizing phishing attempts demands cognitive vigilance, which can be challenging for individuals with cognitive disabilities. Failing to identify phishing emails increases susceptibility to cyber threats and scams.

Furthermore, Table 3 analyzes some of the most relevant papers related to this study.

Table 3: Relevant papers summary.

Reference	Year	Contribution	Limitations
(Macakoğlu, Peker, & Medeni, 2023)	2023	It addresses issues of accessibility, usability, and security, putting light on differences between colleges in different areas. The study provides practical ideas for improving the quality of these web pages so that they can successfully serve prospective students and provide equitable access to information. This research is useful for institutions looking to increase their web presence and better serve prospective students.	The fundamental disadvantage of this article is that it primarily relies on automated testing techniques for review, which may not capture the whole user experience and associated accessibility, usability, and security issues. It lacks subjective feedback from actual users. For a more full study, future studies should include user experience testing and deeper security checks.
(Renaud & Coles-Kemp, 2022)	2022	It highlights the critical need to include accessibility issues alongside security and usability in the design of security and privacy systems. It emphasizes the difficulties that people with disabilities and those with limited resources and resilience confront when accessing internet services and protecting their digital assets. The document encourages stakeholders to work together to overcome accessibility challenges in cyber security. Its contribution is to raise awareness about the significance of inclusivity in security design and encourage further research and practical initiatives to make security measures more accessible to all.	It emphasizes the need to incorporate accessibility issues into cyber security, elevating usability to the same level. It advocates for more knowledge and study in this area to and encryption for all users, particularly those with vulnerabilities. However, the study lacks precise practical answers and technological details, instead functioning as a conceptual call to action for future human-centred security research.
(Hilowle, Yeoh, Grobler, Pye, & Jiang, 2023)	2023	It investigates how human-centric cybersecurity (HCCS) elements influence the adoption of National Digital Identity Systems (NDIDs). Security, privacy, perceived risk, usability, adaptability, cultural and social interference, and cybersecurity knowledge are all addressed. The study, which included 203 Australian citizens, discovered that these HCCS characteristics substantially impact NDID adoption. It emphasizes the need for human-centric features in NDID deployment, especially in risk-averse cultures, and emphasizes the necessity for cybersecurity education and awareness to increase adoption.	The study discovered that security, privacy, perceived risk, usability, flexibility, and cultural and societal interference had a major impact on the desire to use NDIDs. Adoption was hampered by a lack of cybersecurity understanding and trust, emphasizing the importance of cybersecurity education and awareness. The paper adds to the NDID and HCCS literature by providing policymakers and stakeholders with insights to improve NDID implementation and security. The study is constrained, however, by its focus on Australian citizens and reliance on self-reported data.
(Maglaras, Ferrag, Janicke, Buchanan, & Tassioulas, n.d.)	2023	The concept of "securability" is introduced in this study to balance security and reliability in Critical National Infrastructures (CNIs). It emphasizes the significance of protecting CNIs from cyber attacks and provides solutions for improving cybersecurity. The article recommends additional research to solve the cybersecurity and reliability gaps in CNIs.	The paper analyses the severe impact of energy sector failures on important services and provides a method for addressing threats to severe National Infrastructures (CNIs) that combines cybersecurity and dependability. It suggests that more research in this area is required.

3 Research Methodology

3.1 Research Design

This section outlines the research design adopted for this study, covering both qualitative and quantitative research methods. The mixture of these methodologies offers a complete approach to exploring the complex interplay between web accessibility, cybersecurity challenges, and cognitive disabilities, providing a well-rounded understanding of the research objectives.

3.1.1 Qualitative Methodology

Qualitative research will be conducted to gain in-depth insights into the experiences, perceptions, and challenges faced by users with lowered cognitive ability when interacting with web services and cybersecurity measures. This approach involves semi-structured interviews with a diverse sample of participants from the target user group. Through open-ended questions, participants will be encouraged to share their thoughts, preferences, and difficulties related to web accessibility and security rules.

The qualitative methodology is well-suited for exploring the subjective experiences of users and uncovering nuanced factors that may affect their relations with digital platforms (Burck, 2005). It enables more profound research of cognitive user needs and provides valuable context to inform the development of user-centric guidelines for inclusive design and user-friendly security measures.

3.1.2 Quantitative Methodology

Quantitative research will be employed to assess the extent of web availability and usability of existing public service websites for users with cognitive disabilities. User surveys will be conducted to gather quantitative data on user preferences, attitudes toward security measures, and adoption rates.

The quantitative methodology allows for the systematic measurement of website accessibility and the collection of data from a larger sample size. It provides statistical insights into the current state of web accessibility and cybersecurity adoption, allowing the recognition of trends and patterns among users with cognitive disabilities.

3.1.3 Justification of Chosen Methodology

Combining qualitative and quantitative methodologies is ideal for addressing the research objectives. Qualitative research allows for deep research of cognitive user requirements and identifying specific challenges they face in accessing web services and complying with security measures. By engaging directly with users through interviews, this approach captures rich and specific data that can inform the growth of guidelines specific to their needs.

Quantitative research complements qualitative findings by providing quantitative website accessibility measures and user attitudes. It offers a broader viewpoint on the incidence of web accessibility issues and the efficiency of current security measures. The quantitative approach provides numerical accuracy and generality to the study's findings.

The chosen methodology aligns with the interrelated nature of the research, bridging insights from user experience, cybersecurity, and cognitive disability fields. It enables a complete understanding of the complex dynamics between accessibility, security, and cognitive user requirements, ultimately guiding the creation of practical proposals and rules for creating more and user-friendly web services. By employing a mixed-methods approach, this research aims to achieve a complete and well-rounded research of the research objectives, improving the robustness and validity of the study's findings.

3.2 Data Collection

This section outlines the various data sources that will be utilized to gather complete knowledge for addressing the research objectives. The research design includes a mix of qualitative and quantitative data collection methods to ensure a complete understanding of web accessibility, cybersecurity challenges, and cognitive disabilities. The data collection method is summarized in the following table:

Table 4: Data Collection Methods

Data Collection Method	Description
Surveys	Questionnaires distributed to a broad user sample for quantitative data.
In-Depth Interviews	Semi-structured interviews conducted with users with cognitive disabilities.
Observations	Systematic observations of users by Surveys and In-terviews are thoroughly analyzed.

3.2.1 Data Sources

Qualitative Data Sources: In-depth interviews were conducted with users who have permanently or temporarily lowered cognitive ability. Participants were selected through intentional sampling to represent different cognitive disabilities. For the interview, 10 lowered cognitive ability participants were selected voluntarily, and their information will not be disclosed publicly. Additionally, the interview was taken in Bengali, as all the participants were from Bangladesh. Semi-structured interviews allowed participants to share their experiences, preferences, and challenges related to web interactions, security procedures, and overall digital experiences.

The following questions were asked during the interviews:

1. Can you tell me about the websites you use, like online stores or social media? What do you do on these websites?
2. Are there things that are hard to do on websites? What things do you find difficult or not so easy?
3. Do you know about things like making your information private or keeping your account safe on websites? Do you use these things, and do they seem hard to use?
4. Have you ever had a problem with privacy or safety online? Did something make you confused or unsure? Can you tell me about it?
5. Are there websites that you like because they are easy to use? What things on these websites make you happy?
6. Why do you think it's important for websites to work well for people who may have some difficulty understanding things? What things do you think could make websites better for everyone?
7. Did you ever get messages or things online that you thought were not true? How do you feel about knowing if something is real or not? What helps you stay safe online?
8. Can you think of times when you felt that websites or online places were made for you? What things on these websites helped you a lot?
9. Do you use any special tools on the computer or phone to help you when you go online? What do these tools do and how do they help you?

10. If you could tell people who make websites how to make them better, what would you say?
What things do you think would help you and others?

Quantitative Data Sources: 53 users with permanently and temporarily lowered cognitive abilities participated in the survey. Users shared their email and phone numbers, which won't be disclosed publicly. All the participants were from Bangladesh and participated in the survey voluntarily. The survey gathered quantitative data on user attitudes toward security measures, thinking, challenges, and preferences in web interactions. The survey also assessed the adoption rates of security procedures among users of lower cognitive ability. This quantitative assessment provided measurable data on the compliance of websites with accessibility standards.

The following questions were asked in the survey:

1. What is your age?

- Below 18 years
- 18-39 years
- 40-59 years
- 60 years or older

2. How often do you use the internet or digital services?

- Daily
- Weekly
- Monthly
- Rarely

3. Which devices do you use to access the internet or digital services? (Select all that apply)

- Smartphone
- Tablet
- Laptop
- Desktop computer
- Other

4. Have you ever encountered any difficulties while using the internet or digital services?

- Yes
- No

5. If yes, please specify the difficulties you have faced. (Open-ended)

6. How confident are you in protecting your personal information while using digital services?

- Very confident
- Somewhat confident
- Not very confident
- Not at all confident

7. Have you ever experienced any cyberattacks or online scams?

- Yes
- No

8. If yes, please briefly describe your experience. (Open-ended)

9. Are you aware of the potential risks and vulnerabilities present in cyberspace?

- Yes
- No

10. What measures do you take to ensure your online safety? (Select all that apply)

- Using strong and unique passwords
- Keeping software and devices up to date
- Avoiding suspicious emails or messages
- Not sharing personal information online
- Other:

11. If other please write

12. How often do you receive information or guidance about online safety and cybersecurity?

- Regularly

- Occasionally
- Rarely
- Never

13. Are you satisfied with the accessibility of websites and digital services you use?

- Yes
- No

14. If no, please describe the difficulties you face in accessing websites or digital services. (Open-ended)

15. Rate how well you agree to the following statement: I often find it difficult to comprehend security information provided to me by digital services.

- Strongly agree
- Agree
- Neutral
- disagree
- Strongly disagree

16. Rate how well you agree to the following statement: I often find myself struggle to understand how to use update my device.

- Strongly agree
- Agree
- Neutral
- disagree
- Strongly disagree

17. Rate how well you agree to the following statement: I often find it difficult to remember passwords.

- Strongly agree

- Agree
- Neutral
- disagree
- Strongly disagree

18. How important do you think it is for websites and digital services to be accessible to people with cognitive disabilities?

- Very important
- Somewhat important
- Not very important
- Not at all important

19. Would you be interested in participating in user testing or providing feedback to improve the accessibility of websites and digital services?

- Yes
- No

3.2.2 Data Collection Procedures

Qualitative Data Collection: Semi-structured interviews will be conducted in a one-on-one format with participants. Interviews will be audio-recorded with participant consent and later transcribed for analysis. Interviews will be guided by open-ended questions that explore participants' experiences with web accessibility, privacy concerns, and the challenges they encounter when using security procedures. A thematic analysis approach will be employed to identify patterns and themes in the qualitative data.

Quantitative Data Collection: User surveys will be distributed online, and participants will be invited to complete the survey at their convenience. The survey will include structured questions that capture quantitative data on user attitudes, preferences, and adoption rates of security measures. Data from surveys will be analyzed using statistical methods to identify trends and correlations.

3.2.3 Privacy and Anonymity

The privacy and anonymity of participants will be prioritized throughout the data collection process. Participants' identities will be kept confidential, and all collected data will be securely stored and accessible only to authorized researchers. Participants' consent will be obtained before conducting interviews or surveys, and they will have the option to withdraw from the study at any time without consequences. Audio recordings of interviews will be anonymized during transcription, replacing participants' names with pseudonyms to ensure confidentiality.

For website evaluations and surveys, no personally recognized information will be collected. All collected data will be aggregated and reported in a way that ensures anonymity and prevents the identification of individual participants. Data will be used solely for research purposes and will be treated with the utmost care to protect participants' privacy.

By following demanding privacy and privacy measures, this research aims to create a safe and respectful environment for participants while gathering valuable data to inform the study's findings and recommendations.

3.3 Data Analysis

Data analysis is a crucial phase in the research process, serving as the bridge that connects the collected information to meaningful insights. In this study, we employ a multi-approach to analyze qualitative and quantitative data. The following table summarizes the data analysis techniques of this study.

Table 5: Data Analysis Techniques

Data Analysis Type	Description
Qualitative Analysis	Interpretive analysis of interview audios, focusing on themes and patterns.
Quantitative Analysis	Statistical analysis of survey data of 53 individuals.
Mixed-Methods Integration	Integration of both qualitative and quantitative findings for a comprehensive understanding.

3.3.1 Qualitative Data Analysis

The qualitative data collected through semi-structured interviews will undergo rigorous analysis to identify patterns, themes, and insights related to web accessibility, cybersecurity challenges, and

cognitive disabilities. The analysis will follow a thematic approach, involving several stages:

- **Data Transcription:** Audio recordings of interviews will be transcribed verbatim, ensuring accurate representation of participants' responses.
- **Data Familiarization:** Researchers will immerse themselves in the data, reading and re-reading transcripts to gain a comprehensive understanding of participants' narratives.
- **Coding:** Codes will be assigned to segments of data that represent meaningful concepts, themes, or patterns. Coding will be both deductive, guided by pre-defined research objectives, and inductive, allowing for emergent themes to surface from the data itself.
- **Theme Development:** Codes will be organized into broader themes that encapsulate key findings and insights. Themes will be refined and defined, capturing the essence of participants' experiences and perspectives.
- **Data Interpretation:** Researchers will interpret the themes in the context of research objectives, drawing connections between participants' narratives and the broader implications for web accessibility and security measures.

By engaging in a thorough qualitative analysis, this research aims to uncover the complex dynamics and challenges faced by users with lowered cognitive ability, contributing to the formulation of inclusive design guidelines and user-friendly security procedures.

3.3.2 Quantitative Data Analysis

The quantitative data collected from user surveys will be analyzed using statistical methods. Descriptive statistics will be used to summarize user attitudes, preferences, and adoption rates of security measures. Inferential statistics, such as correlation analysis, may be employed to identify relationships between variables and draw meaningful conclusions from the survey data. By quantitatively analyzing website accessibility and user survey data, this research aims to provide objective measurements and statistical insights into the prevalence of accessibility challenges and user behaviors, enhancing the understanding of the research area.

3.3.3 Integration of Qualitative and Quantitative Findings

The qualitative and quantitative findings will be integrated to provide a complete understanding of the research topic. The insights gained from qualitative analysis will enrich the quantitative findings

by providing context, depth, and meaning to statistical results. Qualitative findings will be used to validate and explain quantitative trends and patterns, enhancing the overall robustness and validity of the study's conclusions.

Through the combined analysis of qualitative interview data, quantitative survey data, and website evaluation results, this research endeavors to offer a holistic and nuanced exploration of the intersection between web accessibility, cybersecurity challenges, and cognitive disabilities.

4 Experiments and Results

This section will analyze the qualitative and quantitative data that were gathered about the topic. Then it will be commenced by examining the quantitative data obtained from the survey conducted for this thesis. Then, the qualitative data will be analyzed.

4.1 Quantitative Analysis - Survey

To complete the survey, a database of lower-cognitive people living in Bangladesh was collected from the "Advanced Machine Intelligence Research Lab-AMIRL" and sent the survey through Google Forms. Here, the survey will be analyzed by each question's response and statistical explanations.

Question 1: What is your age?

In the survey, 53 respondents were categorized by age. A striking 98.1% fell in the 18-39 years range, indicating a mainly young participant group. Only one respondent, or approximately 1.9%, was aged between 40-59. None of the respondents were below 18 or above 60 years old, highlighting the narrow age range of the survey sample. Figure 2 gives the age distribution of all respondents using Pie-Chart.

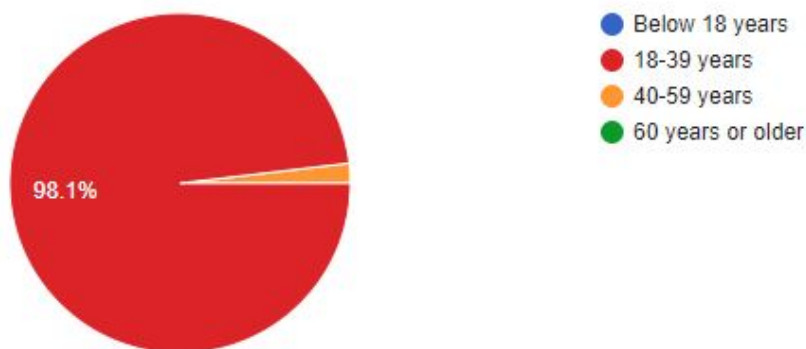


Figure 2: Shows age distribution of all respondents.

Question 2: How often do you use the internet or digital services?

The survey then focuses on the frequency of internet and digital service usage among the respondents. Most respondents, comprising a significant 86.6%, reported using the Internet and digital services daily. This high percentage underscores the pervasive role of digital technology in daily life. In contrast, only a minimal 1.9% of participants indicated weekly usage, suggesting that the majority rely on digital services for more frequent tasks. Monthly usage was reported by 7.5% of respondents,

signifying a less consistent pattern of engagement with digital services. A small fraction, 3.8%, mentioned rare usage, emphasizing that a minority infrequently relies on the internet and digital services for their needs. Figure 3 gives an overall statistics of how often the respondents use the internet.

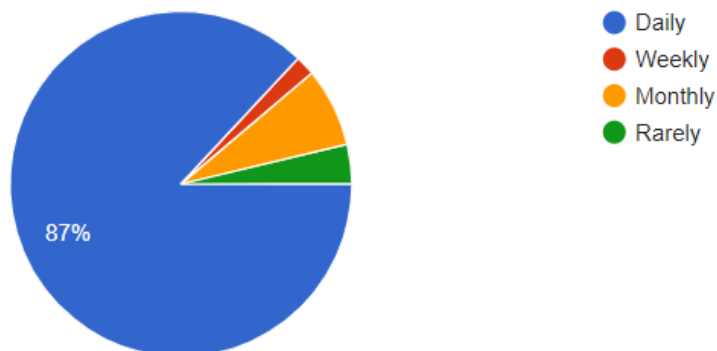


Figure 3: Overview of Internet uses of the respondents.

Question 3: Which devices do you use to access the internet or digital services?

In terms of preferred devices for using the internet and digital services, the results revealed a clear preference for smartphones, with a significant majority of 94.3% (50 respondents) favoring this portable option. Laptops also emerged as a popular choice, with 52.8% (28 respondents) indicating its usage. Desktop computers, typically associated with stationary work, garnered 24.5% (13 respondents) of the responses. Meanwhile, tablets were chosen by 15.1% (8 respondents) of participants, showcasing their appeal for specific tasks. A smaller portion of respondents, 5.7% (3 respondents), opted for 'Other' devices, indicating diverse preferences beyond the listed options. These findings reflect the evolving landscape of digital device usage among respondents. Figure 4 shows the distribution of preferred devices for accessing the internet and digital services.

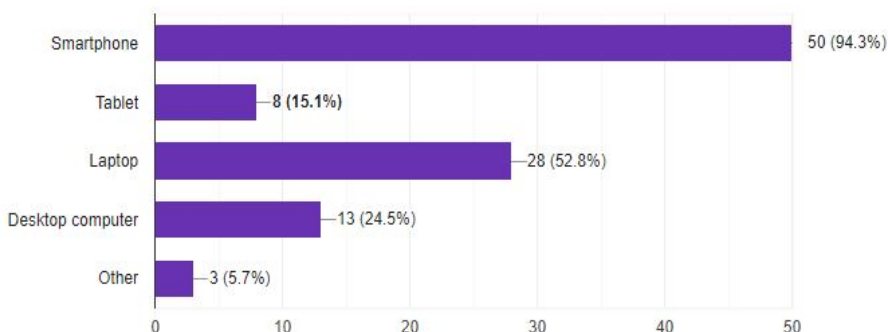


Figure 4: Distribution of preferred devices for accessing the internet and digital services.

Question 4: Have you ever faced any of the following problems while using the internet or digital

services?

After that, various internet and digital service-related concerns were assessed through multiple-choice questions. Results revealed that a significant portion of respondents faced these issues. Worries about their private information being compromised were prevalent, with 31 individuals, accounting for 58.5%, expressing such concerns. Approximately 41.5% of respondents, or 22 individuals, reported receiving strange emails or messages that caused them to worry. Furthermore, 22.6% of participants (12 individuals) indicated that they struggled to understand how to maintain online privacy. Worries about potential scams or deceptive tactics online were reported by 45.3% of respondents, totaling 24 individuals. Making solid passwords proved to be challenging for 28.3% of the participants, with 15 individuals highlighting this issue. These findings underscore individuals' diverse range of concerns while navigating the digital landscape, emphasizing the need for improved digital literacy and cybersecurity awareness. Some of the most common problems while using the internet or digital services are given in Figure 5.

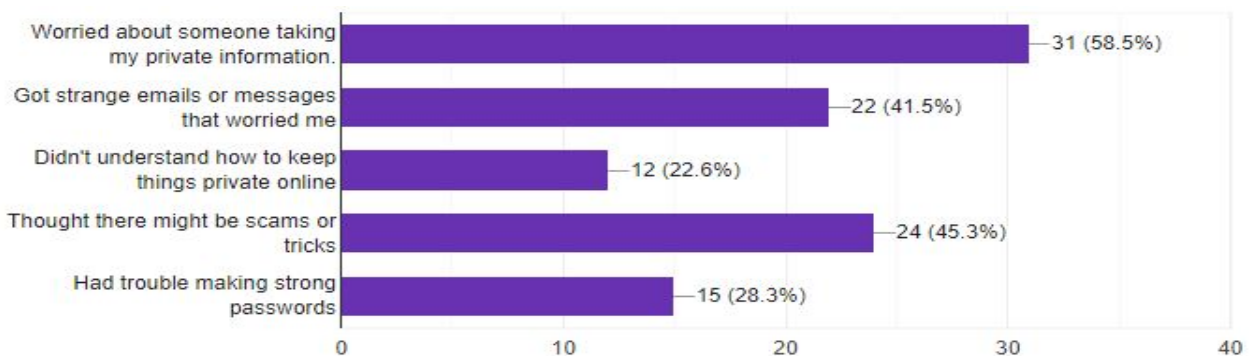


Figure 5: Statistics of common problems using the internet or digital services.

Question 5: How confident are you in protecting your personal information while using digital services?

The data from the survey indicates varying levels of confidence among respondents regarding protecting their personal information while using digital services. A substantial portion, 39.6%, expressed being "Very confident" in their ability to safeguard their data. Meanwhile, 24.5% stated they were "Somewhat confident," reflecting a moderate level of assurance. On the other hand, 26.5% admitted to feeling "Not very confident," suggesting a degree of apprehension, while 9.4% indicated they were "Not at all confident," signifying a notable lack of trust in their personal information's security. This distribution of responses is visually represented in the pie chart of Figure 6, illustrating the varying degrees of confidence among the 53 survey participants.

Question 6: Have you ever experienced any cyberattacks or online scams?

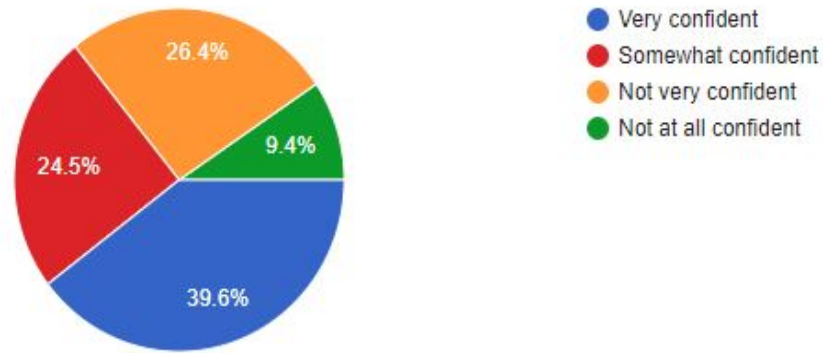


Figure 6: Figure illustrates the varying degrees of confidence among respondents.

The pie chart represents responses to a survey question about personal experiences with cyberattacks or online scams. Out of 53 total respondents, 33.7% (20 individuals) answered "Yes," indicating that they have encountered such incidents. In contrast, 62.3% (33 individuals) responded with "No," signifying they haven't experienced cyberattacks or online scams. The chart in Figure 7 clearly illustrates that a substantial majority of respondents have been fortunate enough to avoid such incidents, while a notable minority has faced these digital threats. It highlights the prevalence of online security challenges in the modern digital landscape and the need for continued vigilance in cybersecurity.

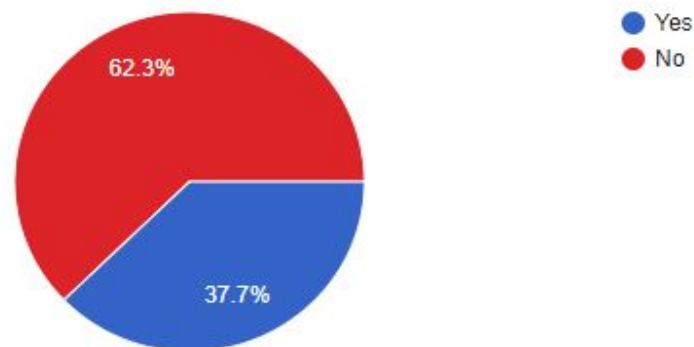


Figure 7: Respondents experience on any cyberattacks or online scams.

Question 7: Are you aware of cyberspace's potential risks and vulnerabilities?

When asked about their awareness of potential risks and vulnerabilities in cyberspace among the [articipant, the majority, comprising 71.7% of the respondents, answered "No," indicating that they were not aware of these risks. Conversely, 28.3% of the respondents answered "Yes," signifying their awareness of the potential dangers in the online realm. This distribution is visually represented in a pie chart in Figure 8, with the larger portion of the chart dominated by the "No" responses,

highlighting the prevailing lack of awareness among the surveyed individuals regarding cybersecurity risks and vulnerabilities in cyberspace.

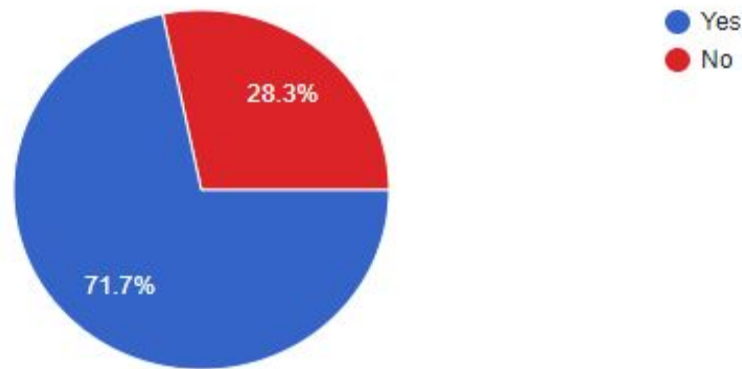


Figure 8: Respondents awareness of cyberspace's potential risks and vulnerabilities.

Question 8: What measures do you take to ensure your online safety?

The survey asked respondents about the measures they take to ensure their online safety through a multiple-choice question. Among the 53 replies received, it was observed that a significant majority prioritize using strong and unique passwords (44 respondents or 83%). Additionally, a substantial portion of respondents emphasize keeping their software and devices up to date (20 respondents or 37.7%). Moreover, many participants reported avoiding suspicious emails or messages (29 respondents or 54.7%) and not sharing personal information online (27 respondents or 50.9%) as essential safety measures. A smaller fraction of respondents indicated using other methods (5 respondents or 9.4%) beyond the provided options, reflecting the diversity of approaches individuals employ to safeguard their online security. Figure 9 shows the distribution of the measurements to ensure online safety according to respondents.

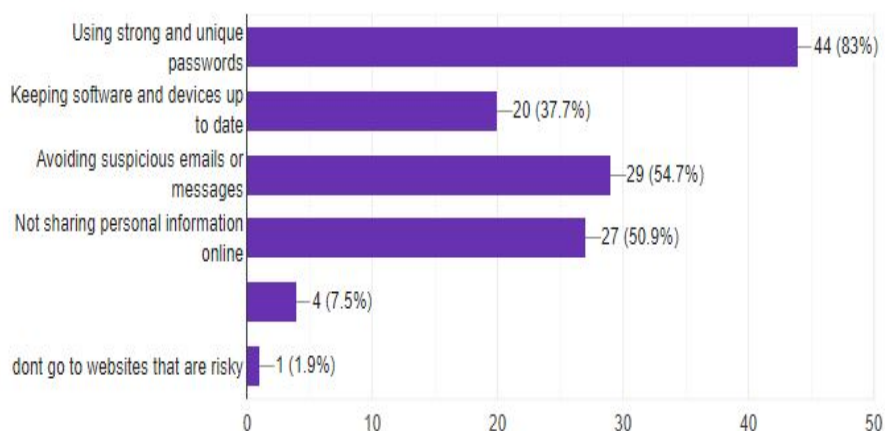


Figure 9: Response of online safety measurement question.

Question 9: How often do you receive information or guidance about online safety and cybersecurity?

Then participants were asked how often they receive information or guidance about online safety and cybersecurity. The responses were divided into four categories: Regularly, Occasionally, Rarely, and Never.

The pie chart in Figure 10 representing these responses revealed that the distribution was relatively balanced. A total of 15 respondents, or 28.3%, indicated that they receive information regularly. An equal number, of 15 respondents, also reported receiving information occasionally, constituting another 28.3% of the sample. Meanwhile, 16 respondents, or 30.2%, stated that they received information about online safety and cybersecurity rarely. The smallest proportion, 7 respondents, or 13.2%, revealed that they never received such guidance. This distribution suggests a varied level of exposure to online safety and cybersecurity information among the surveyed participants.

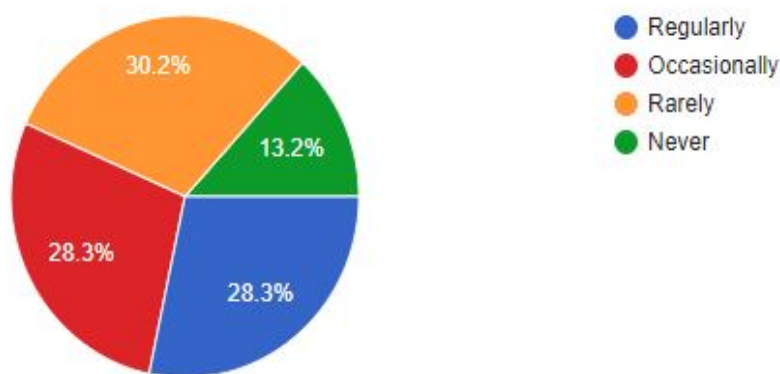


Figure 10: Figure shows the frequency of getting information or guidance about online safety and cybersecurity.

Question 10: Are you satisfied with the accessibility of websites and digital services you use?

Moreover, the participants were asked about their satisfaction with the accessibility of websites and digital services. Among the responses, 36 people (67.9%) answered affirmatively with "Yes," indicating satisfaction, while 17 individuals (32.1%) responded negatively with "No," signifying dissatisfaction. This information was visually depicted in a pie chart in Figure 11, highlighting the significant majority who expressed contentment with the accessibility of the digital platforms they utilize.

Question 11: Rate how well you agree to the following statement: I often find it difficult to comprehend security information provided to me by digital services.

Additionally data were collected on the survey participants agreement with the statement, "I often find it difficult to comprehend security information provided to me by digital services." Respondents rated their agreement on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree). The

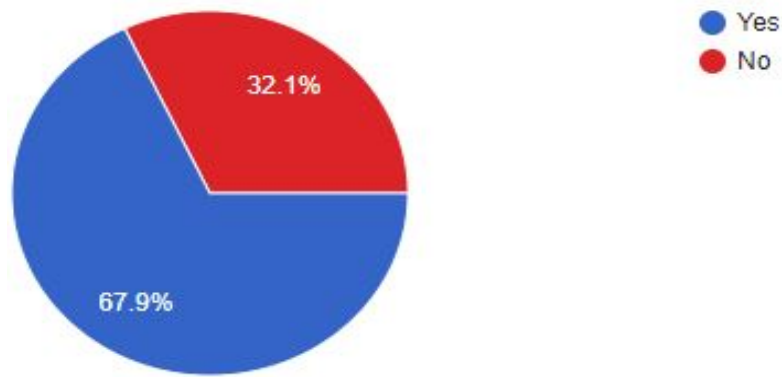


Figure 11: Respondent Satisfaction with Digital Platform Accessibility.

results indicated varying degrees of agreement: 18.9% strongly disagreed (rated 1), 11.3% somewhat disagreed (rated 2), 32.1% had a neutral stance (rated 3), 15.1% somewhat agreed (rated 4), and 22.6% strongly agreed (rated 5). These responses were visualized in a bar chart in Figure 12 to provide a clear overview of the distribution.

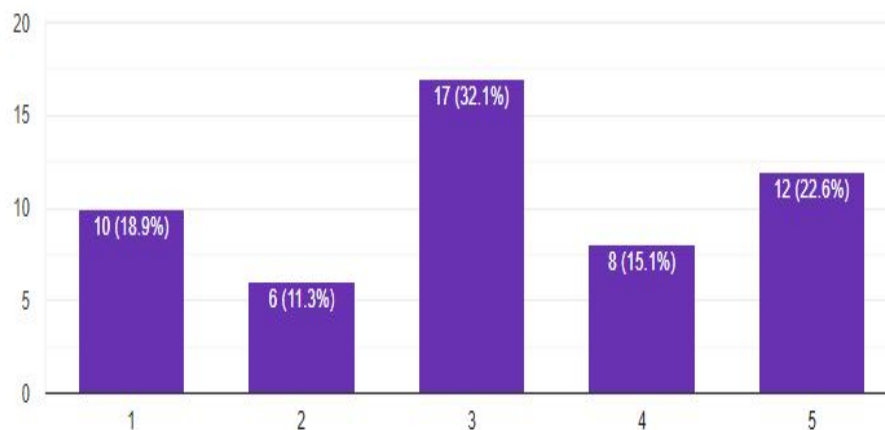


Figure 12: Participant Responses to the Statement 'I often find it difficult to comprehend security information provided to me by digital services,' Rated on a Scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

Question 12: Rate how well you agree to the following statement: I often find myself struggle to understand how to use update my device.

The survey question also aimed to gauge users' experiences with updating their devices, asking them to rate their agreement on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree). Out of the 53 respondents, a significant 28.3% (15 individuals) strongly disagreed with the statement, indicating a substantial portion of respondents encountered difficulties with device updates. Meanwhile, 13.2% (7 individuals) chose a rating of 2, signifying that they somewhat disagreed with the statement. A larger percentage, 24.5% (13 individuals), rated their agreement as 3, suggesting some uncertainty or

mild struggle. Additionally, 17% (9 individuals) each selected ratings of 4 and 5, indicating moderate and strong agreement with the statement, respectively. These responses are visually represented in a bar chart in Figure 13.

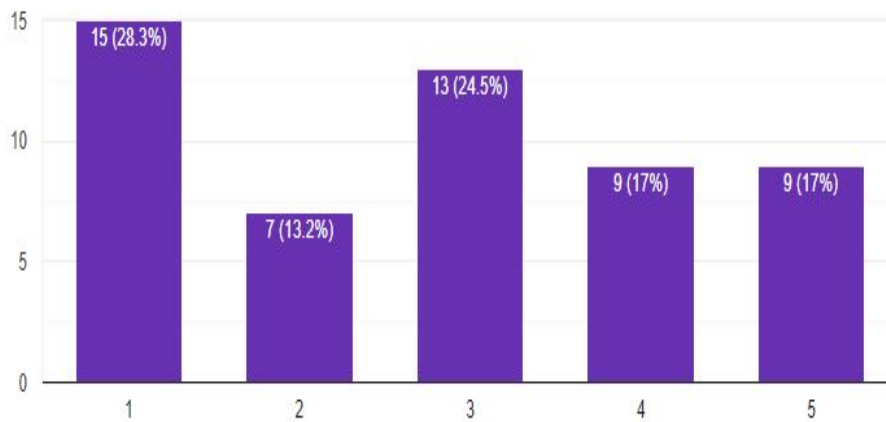


Figure 13: User Agreement with the Statement "I often struggle to understand how to update my device."

Question 13: Rate how well you agree to the following statement: I often find it difficult to remember passwords.

Furthermore, among the 53 respondents, their agreement with the statement "I often find it difficult to remember passwords" was rated on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree). Strongly Disagree (1) received 12 responses (22.6%). Disagree (2) had 4 responses (7.5%). Neutral (3) was chosen by 8 respondents (15.1%). Agree (4) received 10 responses (18.9%), and Strongly Agree (5) had the highest number of responses with 19 (35.8%). This data was visually represented in a bar chart in Figure 14 to provide a clear view of respondents' perceptions regarding password difficulty.

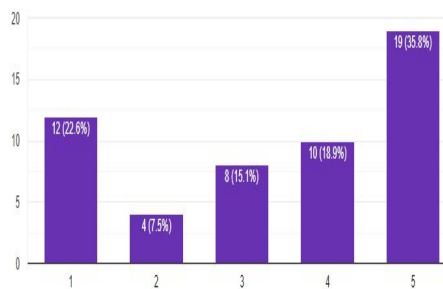


Figure 14: Respondents' Ratings on Password Difficulty.

Question 14: Have you ever had difficulty using a government website because of tough security measures like creating a strong password, using two-factor authentication, or verifying your email or phone?

Participants were also asked whether they encountered difficulties while using government websites due to stringent security measures such as creating strong passwords, using two-factor authentication, or verifying their email or phone. The results showed that 62.3% (33 individuals) answered "Yes," indicating they had faced challenges, while 37.7% (20 individuals) responded with "No." This data was visually represented in a pie chart in Figure 15, highlighting the prevalence of security-related usability challenges experienced by many respondents when accessing government websites.

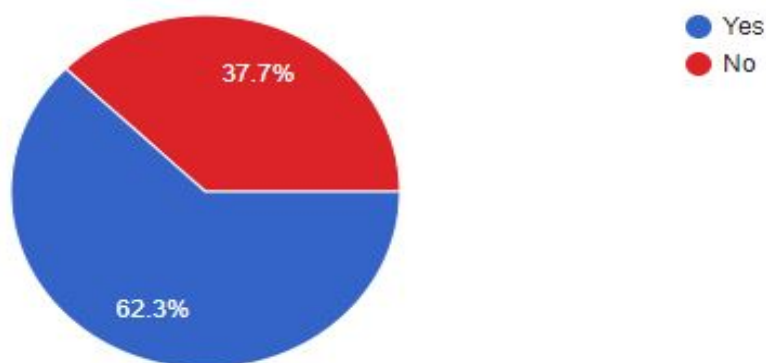


Figure 15: User Responses to Government Website Security Measures.

Question 15: Did you have difficulty using government websites to access services because of lower cognitive abilities?

Finally, the participants were asked whether they encountered difficulties while using government websites to access services due to lower cognitive abilities. The responses were as follows: 54.7% (29 individuals) responded with "Yes," indicating that they faced challenges, while 45.3% (24 individuals) selected "No," signifying that they did not experience such difficulties. These results were visually represented in a pie chart in Figure 16, highlighting the prevalence of issues related to lower cognitive abilities when accessing government services online. This data underscores the importance of designing user-friendly and inclusive government websites to cater to the diverse needs of all citizens.

4.2 Key Observations from the Survey Responses

The following observations highlight the importance of addressing privacy and security concerns, tailoring safety measures to varying confidence levels, and the need for more consistent safety information dissemination.

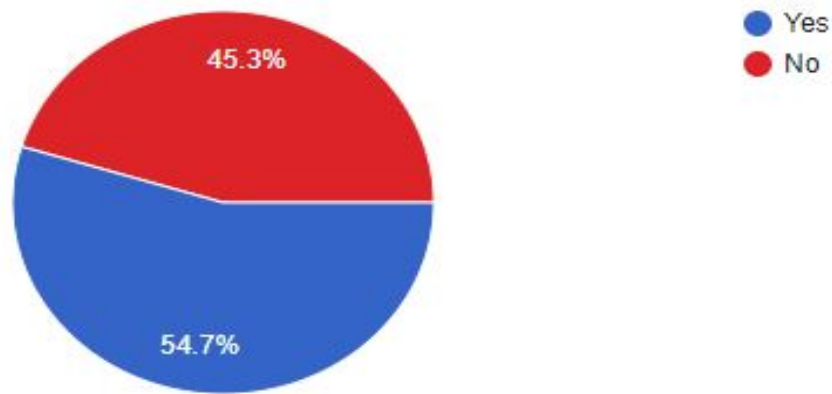


Figure 16: Accessibility Challenges Faced by Respondents on Government Websites due to Lower Cognitive Abilities.

- **Age and Internet Usage Frequency:** Most respondents (18-39 years old) reported daily internet and digital service usage. This suggests a high level of online engagement among younger adults.
- **Device Usage:** Smartphone usage is prevalent across all respondents, followed by laptops and desktop computers. A few respondents also use tablets. This highlights the importance of ensuring website and service accessibility on various devices.
- **Privacy and Safety Concerns:** Many respondents expressed concerns about their private information being taken and receiving strange or worrying emails/messages. These privacy and safety concerns are widespread among the participants.
- **Confidence in Online Safety:** Respondents' confidence in protecting personal information online varied; some felt very confident, while others were not confident. This discrepancy in confidence levels could be significant for tailoring online security measures.
- **Experience with Cyberattacks:** Many respondents reported experiencing cyberattacks or online scams. This indicates that online security threats are not uncommon.
- **Awareness of Risks:** Most participants were aware of cyberspace's potential risks and vulnerabilities, which is a positive sign. However, this awareness doesn't always translate into confidence in online safety.
- **Safety Measures Taken:** Most respondents reported using strong and unique passwords, keeping software and devices up to date, and avoiding suspicious emails/messages. These are good cybersecurity practices.

- Frequency of Safety Information: Respondents receive information or guidance about online safety and cybersecurity at varying frequencies, from regularly to never.
- Accessibility Satisfaction: Participants' satisfaction with the accessibility of websites and digital services they use is generally positive, with most reporting they are satisfied.

4.3 Qualitative Analysis - Interviews

To complete the interview, 10 interested individuals from the database were selected. During the interview, each participant was first informed of the previous participants' answers and was asked to provide a new and unique answer. The answers were then summarized in one line, and they were presented to the participants to have their confirmation if the single line represents their whole answer. These individuals' responses are summarized into a single line for better readability. Also, some responses were avoided and tried to get responses that were not similar. As in the surveys, there were many repeated responses for each question; hence, the focus was given to unique responses for every individual. Here, the interview questions will be analyzed and each individual's answers.

Question 1: Can you tell me about the websites you use, like online stores or social media? What do you do on these websites?

- "I go on Facebook to talk to my family."
- "I use Amazon to order books."
- "YouTube is where I watch funny videos."
- "I visit Google for looking up things."
- "Twitter is where I read interesting news."
- "I like playing games on Miniclip."
- "I visit Instagram to see photos."
- "I use Zoom to join virtual meetings."
- "Netflix is where I watch movies."
- "I shop on eBay for collectibles."

Question 2: Are there things that are hard to do on websites? What things do you find difficult or not so easy?

- "Lots of buttons on a page confuse me."
- "Creating a profile can be tricky."
- "I get lost in websites with too much text."
- "Online forms with many fields are confusing."
- "Small fonts make reading hard for me."
- "Complex navigation menus are challenging."
- "Some websites have unclear instructions."
- "Finding the 'back' button can be tough."
- "Sometimes links aren't easy to click."
- "Pop-up ads make me lose focus."

Question 3: Do you know about things like making your information private or keeping your account safe on websites? Do you use these things, and do they seem hard to use?

- "I've heard about privacy settings but don't use them."
- "I use passwords, but remembering them is tough."
- "Account settings can be hard to find."
- "I'm not sure about changing passwords."
- "Privacy policies are long and complex."
- "Sometimes I share too much info."
- "Security questions can be tricky."
- "I'm unsure about two-factor authentication."

Question 4: Have you ever had a problem with privacy or safety online? Did something make you confused or unsure? Can you tell me about it?

- "I got a strange email once, and it worried me."
- "I've had my account locked, and I was unsure why."
- "Accidentally sharing my phone number made me uneasy."
- "I wasn't sure if a message was real."
- "Sometimes, I clicked on fake links."
- "I got phishing emails, and it was confusing."
- "I accepted friend requests from strangers."
- "I couldn't tell if a website was secure."
- "I received scam calls that worried me."
- "My account was hacked, and I didn't know what to do."

Question 5: Are there websites that you like because they are easy to use? What things on these websites make you happy?

- "Google's simplicity makes it easy."
- "Amazon suggests things I might want."
- "YouTube's video suggestions are helpful."
- "Twitter is straightforward to use."
- "Miniclip games are easy to start."
- "Facebook's layout is clear."
- "Instagram's photos are fun to see."
- "Zoom's 'Join' button is noticeable."
- "Netflix's large icons are great."
- "eBay's search bar is user-friendly."

Question 6: Why do you think it's important for websites to work well for people who may have some difficulty understanding things? What things do you think could make websites better for everyone?

- "Simple websites help everyone, not just some people."
- "Using clear pictures and less text is better for everyone."
- "Websites should talk to us, not just show words."
- "Big buttons make it easy for everyone."
- "Not everyone can understand complex stuff, so websites should keep it simple."
- "More videos with easy explanations can help everyone."
- "Using clear colours makes it easier for everyone to read."
- "Helpful search bars are good for everyone."
- "No one likes confusing websites." "Using common words is good for everyone."

Question 7: Did you ever get messages or things online that you thought were not true? How do you feel about knowing if something is real or not? What helps you stay safe online?

- "I got an email about winning a million dollars, but I knew it was a lie."
- "Sometimes I can't tell if a message is true, and that worries me."
- "I check with my family if something seems strange online."
- "My friend told me to be cautious, so I ask questions."
- "Sometimes fake news confuses me."
- "I use Google to check if things are true."
- "I'm learning how to spot scams."
- "I got messages about free stuff, but I knew it was too good to be true."
- "I use websites I trust."
- "I don't click on strange links."

Question 8: Can you think of times when you felt that websites or online places were made for you? What things on these websites helped you a lot?

- "I like when websites have a voice that talks to me."
- "Simple games with easy rules are the best."
- "Some websites use my language, and that's great."
- "Websites that show big pictures are welcoming."
- "Facebook is nice; it helps me stay connected."
- "YouTube suggests videos I can understand."
- "Some sites have easy quizzes."
- "I can listen to books online, and that's good."
- "Websites with big icons are friendly."
- "I like sites with less clutter."

Question 9: Do you use any special tools on the computer or phone to help you when you go online?

What do these tools do, and how do they help you?

- "I use a screen reader to read text aloud."
- "There's a keyboard with big buttons that I like."
- "I have a tool that remembers my passwords."
- "My computer talks to me, and it's cool."
- "I use voice commands to navigate."
- "Sometimes I need help from a person."
- "A special mouse helps me click things."
- "I use headphones to hear better."
- "Some websites have text-to-speech, and I use it."
- "I have a magnifier to see small text."

Question 10: If you could tell people who make websites how to make them better, what would you say? What things do you think would help you and others?

- "Websites should have less stuff on the pages."
- "Use big buttons; small ones are hard to click."
- "Put videos and less text; words are tough."
- "Make the text clear to read."
- "Use bright colors to get our attention."
- "Don't use complex words; keep it simple."
- "Voice commands would be great."
- "Website instructions should be easy."
- "Put 'back' buttons in an easy spot."
- "Websites should talk to us, not just show words."

4.4 Key Observations from the Interview Responses

In the qualitative data analysis, the responses from individuals with lowered cognitive abilities offer valuable insights into their experiences, perceptions, and challenges when interacting with web services and cybersecurity measures. This analysis aims to capture the essence of their perspectives through thematic coding and categorization. Here's an overview of the analysis based on the 10 responses for each of the 10 questions:

Question 1: Website Usage

- The responses indicate that individuals with lowered cognitive abilities primarily use popular social media platforms (e.g., Facebook) and e-commerce sites (e.g., Amazon) for social interaction, content consumption, and online shopping. These services are well-known and widely utilized by the general public, aligning with their familiarity.

Question 2: Challenges on Websites

- The participants find websites with excessive complexity, confusing navigation, and text-heavy content challenging. Additionally, profile setup on social media platforms is cited as a potential difficulty, highlighting the importance of clear and straightforward user interfaces.

Question 3: Privacy and Safety Awareness

- There's an awareness of privacy settings and the use of passwords, but there's a need for clearer guidance, as some respondents expressed uncertainty in making necessary adjustments.

Question 4: Privacy and Safety Incidents

- Instances of encountering potential privacy and safety issues online are reported, such as receiving questionable messages and concerns over the authenticity of communications. Participants seem to rely on their intuition and external support (e.g., family or friends) to address these issues.

Question 5: User-Friendly Websites

- Respondents value simplicity in websites, which includes the use of clear visuals, easily understandable content, and prominent features. They appreciate platforms like Google, eBay, and YouTube for their user-friendliness.

Question 6: Importance of Web Accessibility

- Participants emphasize the importance of accessible websites that cater to everyone, regardless of cognitive abilities. Their suggestions include the use of images and videos, straightforward language, and minimizing complexity.

Question 7: Dealing with Misinformation

- Participants express concerns about identifying false information online. They rely on trusted sources and individuals for verification, emphasizing the importance of reliable content.

Question 8: Websites Tailored to Users

- Websites that incorporate voice-based interactions and simple games are mentioned as favorable experiences. Personalization, in the form of language options or content recommendations, enhances user engagement.

Question 9: Assistive Tools

- Special tools such as screen readers, keyboards with large buttons, and password management software are recognized as beneficial for enhancing online experiences. Participants also seek user-friendly features like voice commands.

Question 10: Recommendations for Website Improvement

- The respondents provide valuable insights for website developers. They recommend keeping websites uncluttered with user-friendly features, including big buttons, multimedia content, clear text, and simplified language. Additionally, they highlight the importance of voice commands and transparent website instructions.

Overall, the qualitative analysis of these responses indicates a desire for web services and cybersecurity measures that prioritize simplicity, clarity, and inclusivity. Participants' awareness of potential risks and their strategies for mitigating them reflect a need for improved online safety measures. Their input will inform the development of web services that better cater to users with lowered cognitive abilities, enhancing their digital experiences.

4.5 Key Observations Based on the Integration of Qualitative and Quantitative Findings

Our research aimed to gain a deeper understanding of the experiences and perspectives of individuals with lowered cognitive abilities when interacting with web services and cybersecurity measures. Through a combination of qualitative interviews and quantitative surveys, we uncovered valuable insights that shed light on various aspects of web accessibility and online safety as perceived by our target user group.

- **Different Online Activities:** The respondents shared insights into their online activities. It was apparent that the internet serves as a versatile platform where individuals communicate with friends on social media platforms such as Facebook, engage in online shopping experiences on platforms like Amazon, and expand their knowledge through platforms like YouTube. Furthermore, they expressed a preference for websites that were straightforward, intuitive, and easy to navigate.
- **Challenges Faced on Websites:** Many participants revealed the challenges they face while using websites. The abundance of buttons and options on some websites can be confusing, and setting up profiles on social media platforms can be perceived as a complex task. The overwhelming presence of text and numerous links on certain websites often leads to individuals getting lost or overwhelmed.

- **Awareness of Online Safety:** While participants had heard of the importance of keeping personal information private online, they expressed difficulties in putting this into practice. The utilization and recall of passwords emerged as a common challenge among the respondents. They often found it challenging to manage their accounts securely.
- **Encountering Online Safety Issues:** Some respondents shared their experiences with online safety issues. They highlighted instances where they received suspicious or misleading messages online, making it challenging to differentiate between authentic and deceptive content. Account lockdowns were also a source of confusion and concern.
- **Preference for User-Friendly Websites:** Users generally favor websites that are user-friendly, emphasizing features such as large buttons, clear images, and simple language. The respondents believe that websites should incorporate more visual content and straightforward vocabulary to enhance accessibility for everyone.
- **Utilization of Assistive Tools:** Several interviewees revealed their reliance on assistive tools to enhance their online experiences. These tools, such as screen readers and special keyboards, have proven invaluable in aiding reading and typing, thereby facilitating smoother interactions with digital platforms.
- **User-Provided Suggestions:** In response to the query on improving websites, participants emphasized the need for platforms to incorporate more images, videos, and simplified language. They believe that user-friendliness should be a priority, benefiting all individuals, not just those with specific needs.

These observations are fundamental in providing insights into the diverse experiences of individuals with lowered cognitive abilities in the realm of web accessibility and online safety. The amalgamation of both qualitative and quantitative data sources has afforded a comprehensive perspective, shedding light on challenges, preferences, and areas where online platforms can be more inclusive and user-friendly.

5 Discussion

In this study, we employed a mixed-methods research approach to comprehensively investigate the web accessibility and cybersecurity experiences of individuals with lowered cognitive abilities. The integration of quantitative and qualitative data collection methods allowed us to gain a deeper understanding of their unique challenges, preferences, and perceptions regarding online interactions.

Table 6: Survey and Interview Sample Sizes and Platforms

Sample	Size	Platforms
Survey	N = 53	Online survey conducted among individuals aged 18-59 years. Participants accessed the survey on a variety of devices (Smartphone, Tablet, Laptop, Desktop computer, Other) and reported their experiences with web services and cybersecurity.
Interview	N = 10	Semi-structured interviews conducted with individuals who have lowered cognitive abilities, aged 18-59 years. Participants were selected through purposive sampling and shared insights into their online experiences, challenges, and preferences related to web accessibility and security measures.

As indicated in Table 6, the author employed two primary data collection methods: surveys and interviews. The survey component reached a total of 53 respondents, targeting individuals aged 18-59 years. These participants engaged with the survey through various platforms, including smartphones, tablets, laptops, desktop computers, and other devices. The survey was designed to capture quantitative data related to participants' online experiences, their use of different devices, and their perspectives on web accessibility and cybersecurity.

In addition, the author conducted in-depth semi-structured interviews with 10 participants within the same age range, who have lowered cognitive abilities. To ensure a diverse representation, purposive sampling was applied to select our interviewees. These participants, as detailed in Table 6, revealed insights into their online experiences, disclosing the specific challenges they face when accessing web services and navigating cybersecurity measures. The interviews provided a qualitative dimension to the research, shedding light on their experiences, preferences, and difficulties in a more profound and personal manner.

The survey data collected from 53 lower cognitive ability respondents sheds light on several critical digital engagement and cyber-security awareness aspects. Notably, a substantial majority of respondents expressed a high level of confidence in protecting their personal information while using digital services, with a significant portion also reporting satisfaction with the accessibility of websites and digital platforms. However, the survey revealed many participants faced concerns about online pri-

vacancy and security, including difficulties comprehending security information and creating strong passwords. Additionally, a notable proportion of respondents faced challenges related to the usability of government websites due to stringent security measures. At the same time, a majority experienced difficulties accessing such sites due to lower cognitive abilities. These findings highlight the importance of enhancing digital literacy, improving cyber-security awareness, and designing user-friendly online interfaces, particularly for government services, to ensure inclusivity and user satisfaction in the digital realm.

To create a better online user experience for the elderly and people with lower cognitive abilities, government websites should follow the following guidelines:

- **Simplified User Interfaces:** Maintaining simplified user interfaces is essential for creating websites that are easy to access and understand, particularly for individuals with lower cognitive abilities. These interfaces feature clear and intuitive design elements to reduce cognitive load. For example, a website with simplified user interfaces might have a clean layout, large, easy-to-read buttons, and easy navigation menus. This design approach helps users quickly find what they need and minimizes confusion, making the online experience more user-friendly for elderly and lower-cognitive individuals.
- **Larger and Readable Fonts:** Including larger and readable fonts is crucial for improving website text legibility, especially for individuals with visual problems and lower cognitive abilities. This involves using fonts that are clear and easy to read. For example, a website could use a sans-serif font like Arial or Calibri in a sufficiently large size to ensure clarity. Furthermore, it's essential to ensure a high contrast between the text and the background, such as using dark text on a light background, which aids users with visual impairments in discerning the content more easily. These practices make the web content more accessible and user-friendly for a broader audience, including elderly and lower cognitive individuals.
- **Multimodal Content:** Implementing multimodal website content enhances accessibility and accommodates wide learning styles and cognitive abilities. This approach involves presenting information in multiple formats, including text, images, and audio. For instance, an educational website could offer written articles, followed by relevant images and audio stories. This caters to users who may prefer reading, visual learning, or auditory learning, providing a more inclusive experience. By offering information through various sensory channels, websites become more user-friendly for elderly individuals and those with lower cognitive abilities, ensuring that

a broader audience can comprehend and engage with the content effectively. This approach aligns with the goal of creating a more inclusive online environment.

- **Consistent Layouts:** A clear layout and structure across web pages are crucial for user-friendly online experiences. This means maintaining the exact placement and design of critical elements throughout the website, such as navigation menus, headers, and content sections. For example, if the logo and primary menu are at the top of the homepage, they should stay there on all other pages. Consistency creates a sense of familiarity, allowing consumers to anticipate where they will find information. This is especially useful for people with lesser cognitive ability who may struggle with changes in layout. A consistent structure makes the website more accessible and user-friendly to a wide range of visitors.
- **Clear Instructions:** Clear guidelines are essential for guiding users through various interactions on a website. These instructions should be straightforward and concise, making it easy for users to understand and perform the desired actions. For instance, when filling out a contact form, an explicit instruction could be: "Please enter your name and email address."
- **Image Descriptions:** Include describing alt text for images to make web content accessible to users who rely on screen readers. Alt text provides a textual description of the image, enabling those with visual impairments to understand the content and context. For example, if a government website has an image showing a vaccination center location on its COVID-19 information page, the alt text for the image might read: "Image: A map showing the location of the Main Street Vaccination Center, open from 9 AM to 5 PM on weekdays." By including alt text, government websites can ensure that all users, including those with visual disabilities, can access and comprehend the information conveyed through images. This is a crucial accessibility feature, especially when disseminating important public health or emergency information.
- **Text-to-Speech Functionality:** Integrate a text-to-speech feature that enables users to read website content aloud, assisting individuals with reading or cognitive challenges. For instance, on a government website, a user with a cognitive impairment can click a button to have official documents or important announcements read aloud, ensuring they receive critical information even if they struggle with reading or comprehension. This feature enhances accessibility and inclusivity, making government websites more user-friendly and accommodating to a broader audience, including those with cognitive difficulties or reading disabilities.
- **Simple Navigation:** Maintain clear and organized navigation menus to access various website

sections quickly. For example, on a government website, the main menu should prominently list essential services such as taxation information, public health updates, and social support programs. This uncomplicated navigation design ensures that users, including the elderly and those with lower cognitive abilities, can quickly locate the information or services they need without confusion. Simplifying the navigation enhances the user experience, especially for individuals needing help with complex menu structures or extensive sub.

- **Progress Indicators:** Employ progress bars or indicators during multi-step processes, like filling out forms or making online transactions. For instance, on a government website's online application for social benefits, a progress bar can display stages such as personal information, income details, and confirmation. This feature helps users, including the elderly and those with lower cognitive abilities, track their progress and understand their steps in the application process. Progress indicators reduce anxiety and improve user comprehension, ensuring individuals with varying cognitive abilities can complete complex tasks efficiently and confidently.
- **Avoid Pop-Ups:** Websites should minimize pop-up windows or modal dialogs. These elements can be confusing and disruptive for some users, especially those with lower cognitive abilities. For instance, a news website can avoid using pop-up ads that might interrupt the reading experience. By reducing pop-ups, websites create a smoother and less distracting user journey, which is particularly beneficial for users who may find abrupt interruptions challenging to navigate. This contributes to a more user-friendly and accessible web experience.
- **Link Clarity:** Ensure links have descriptive text that conveys their destination. For instance, instead of "Click Here," use "Read the full article about online security." This practice benefits elderly and lower cognitive users who rely on explicit cues to understand where a link will take them. By providing descriptive link text, websites improve user comprehension and make navigation more intuitive for a broader audience, enhancing the online experience for everyone.
- **Error Handling:** Create user-friendly error messages that are easily understood and offer guidance on resolving issues. For instance, if a form submission doesn't work, please send a message like, "There was an issue with your submission. Please check that all required fields are filled correctly." This approach helps elderly and lower cognitive users identify and address errors without frustration, contributing to a smoother online experience. Clarity in error messages is essential to prevent confusion and encourage users to confidently complete their tasks.
- **Keyboard Accessibility:** Websites should be designed to be navigable using keyboard inputs

alone. This is essential for users who rely on keyboard navigation due to physical disabilities or those using screen readers. For example, users should be able to move through the website, access links, and interact with elements using keyboard shortcuts. This accessibility feature ensures everyone, including those with cognitive limitations, can navigate the site without barriers, promoting inclusivity and a better user experience.

- **Compatibility with Assistive Technologies:** Websites should be thoroughly tested and optimized to work seamlessly with standard assistive technologies like screen readers and voice command software. For example, when users with visual problems use screen readers to browse a website, the site should provide alternative text for images and have a logical reading order. This ensures that all users, regardless of their abilities, can access and interact with the website effectively, promoting a more inclusive online experience.
- **User Testing:** Regular user testing should be conducted with individuals from diverse backgrounds, including those with lower cognitive abilities and the elderly. For instance, a government website could involve users with various cognitive levels to navigate the site and provide feedback. This feedback is invaluable for identifying usability issues and making necessary improvements to enhance accessibility.
- **Plain and Consistent Forms:** Forms on the website should be designed to be simple and user-friendly. This includes clear labels for form fields and placeholders that guide users on what information to input. Complex or multi-field forms should be avoided, as they can be overwhelming for users, especially those with lower cognitive abilities. For instance, a government website's contact form should have clear labels for name, email, and message fields, making it easy for all users to understand and complete the form.
- **Clear Privacy Policies:** Websites should have easily accessible and transparent privacy policies that explain how user data is handled. This is particularly important to address users' concerns about sharing personal information. For example, a government website that collects user data for official purposes should provide a clear and concise privacy policy that outlines what data is collected, how it will be used, and how it will be protected. This transparency builds trust with users, including those with lower cognitive abilities, and ensures they understand how their information is managed.
- **Help and Support:** Websites should provide accessible help and support options to assist users, including those with lower cognitive abilities. For instance, a government website could offer

a live chat feature with trained support agents, a well-organized FAQ section with easy-to-understand answers, and clear contact information for users to seek assistance when needed. These options ensure that users can easily access help and support, enhancing their overall experience and usability of the website.

Integrating two data collection methods gave us a holistic understanding of the digital interactions of individuals with cognitive limitations. This comprehensive approach better positioned us to identify potential solutions to this problem.

6 Conclusion and Future Work

6.1 Conclusions

In an era where automation is reshaping every aspect of our lives, the issue of availability and security has never been more critical. This thesis explores the challenges and opportunities related with promoting user adoption of security rules and tools, including encryption software, password guidelines, privacy settings, and phishing detection processes, specifically focusing on individuals with lowered cognitive abilities.

The survey and qualitative analysis presented in this thesis have shed light on the current state of digital accessibility and security from the perspective of users with diverse cognitive abilities. The findings reveal several key knowledge and implications.

6.1.1 Understanding the Challenges

The qualitative data analysis conducted through in-depth interviews with individuals who have permanent or temporary cognitive impairments explained the numerous challenges they encounter while managing the digital landscape. Complex security interfaces, insufficient alternatives such as symbols or captions, and the absence of cognitive accessibility requirements in existing web guidelines were identified as primary obstacles.

6.1.2 Promoting User Adoption

The qualitative data highlighted the significance of user-friendly design and the need for clear, easy-to-understand security protocols. Implementing user-focused design strategies, simplified security measures, and fostering an environment that caters to the diverse needs of all users are essential for promoting digital security practices.

6.1.3 Quantitative Insights

The survey responses from a wide range of users revealed many individuals concerned about online privacy, safety, and security. Age, confidence levels, and prior experiences with cyber threats significantly influence these concerns. Therefore, a one-size-fits-all approach to cyber-security may not be practical.

6.1.4 Toward a More Inclusive and Secure Digital Landscape

It is evident from this research that promoting accessibility and security is not only a matter of meeting the needs of individuals with cognitive disabilities but is an endeavour with far-reaching benefits. A more accessible and secure digital environment not only ensures the protection of personal information and privacy but also extends these benefits to users without cognitive problems.

6.1.5 Recommendations for the Future

This thesis underscores the necessity for future research and initiatives. It recommends the following:

- **Developing Inclusive Guidelines:** The World Wide Web Consortium (W3C) and the Web Content Accessibility Guidelines (WCAG) must expand their requirements to include cognitive accessibility standards, ensuring a more inclusive web.
- **User-Centric Design:** Digital service providers should prioritize user-centric design principles, simplifying complex security rules and providing clear instructions for users of all cognitive abilities.
- **User Education:** Early user education campaigns to raise awareness about online threats and safety measures are crucial.
- **Collaboration and Testing:** Collaboration between service providers and individuals with cognitive disabilities in the testing and development phases can lead to more effective and user-friendly security practices.

In conclusion, this thesis calls for a concerted effort to create a digital environment where all users can participate, communicate, and transact securely and comfortably. By acknowledging the challenges, embracing inclusivity, and implementing user-focused measures, we can foster a safer and more accessible digital landscape, benefitting not only those with cognitive disabilities but society as a whole. The journey toward enhancing digital accessibility and security for all is a collective one, and it is a journey well worth embarking upon.

6.2 Future Works

The exploration of digital accessibility and security, particularly concerning users with cognitive disabilities, is an evolving field. This thesis highlights several areas for potential future research and

development:

- **Refinement of Cognitive Accessibility Guidelines:** Future work could delve into the development and improvement of comprehensive cognitive accessibility guidelines. This entails creating clear standards and recommendations for web developers to design digital interfaces that cater to users with varying cognitive abilities.
- **Usability Testing with Target Users:** Conducting extensive usability testing with individuals who have cognitive impairments would provide invaluable insights into the effectiveness of new design approaches. This data would help in optimizing digital environments for accessibility and security.
- **Education and Awareness Programs:** Implementing and assessing the impact of educational programs focused on increasing awareness of online threats and security measures, specifically designed for users with cognitive disabilities, is a promising avenue for future work.
- **Technological Solutions:** Research into innovative technological solutions, such as assistive technologies or dedicated software tools, could enhance the digital experience for users with cognitive impairments. These solutions could help users interact with digital platforms more securely and effectively.
- **Cross-Industry Collaboration:** Encouraging collaboration among stakeholders, including web developers, researchers, policymakers, and individuals with cognitive disabilities, is pivotal. Future work could explore frameworks for such collaboration, ensuring that the digital ecosystem evolves to meet the diverse needs of all users.
- **Impact Assessment:** Conducting longitudinal studies to assess the long-term impact of inclusive design and security measures on the digital experiences and safety of individuals with cognitive disabilities is essential. These assessments can provide data to support further advancements.
- **Regulatory Developments:** Ongoing monitoring and analysis of regulatory developments related to digital accessibility and cyber-security are crucial. Future work should involve evaluating the usefulness of these regulations and proposing enhancements as needed.

In summary, there is a multitude of opportunities for future research and action in the realm of digital accessibility and security. By addressing these areas, we can work toward a digital landscape that prioritizes inclusivity, promotes user adoption of security practices, and ensures a safer and more accessible online experience for all individuals, regardless of their cognitive abilities.

References

- AlDaajeh, S., Saleous, H., Alrabaei, S., Barka, E., Breiting, F., & Choo, K.-K. R. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, 119, 102754.
- Burck, C. (2005). Comparing qualitative research methodologies for systemic research: The use of grounded theory, discourse analysis and narrative analysis. *Journal of family therapy*, 27(3), 237–262.
- Caton, S., Hatton, C., Gillooly, A., Oloidi, E., Clarke, L., Bradshaw, J., ... others (2022). Online social connections and internet use among people with intellectual disabilities in the united kingdom during the covid-19 pandemic. *new media & society*, 14614448221093762.
- Chalghoumi, H., Gauthier-Beaupré, A., Wang, R. H., Chu, C. H., Auger, C., & Sun, W. (2019). Access and use of information technology by persons with cognitive disabilities: Perspectives of older adults and their caregivers. In *2019 7th international conference on ict & accessibility (icta)* (pp. 1–4).
- digital future, S. E. (July 2022). *Web accessibility*.
- Fischer, S. H., David, D., Crotty, B. H., Dierks, M., & Safran, C. (2014). Acceptance and use of health information technology by community-dwelling elders. *International journal of medical informatics*, 83(9), 624–635.
- Gompert, D. C., & Libicki, M. (2023). Towards a quantum internet: post-pandemic cyber security in a post-digital world. In *Survival february–march 2021: A house divided* (pp. 113–124). Routledge.
- Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: a systematic literature review. *Journal of Cybersecurity and Privacy*, 2(1), 1–18.
- Hilowle, M., Yeoh, W., Grobler, M., Pye, G., & Jiang, F. (2023). Improving national digital identity systems usage: Human-centric cybersecurity survey. *Journal of Computer Information Systems*, 1–15.
- Hortizuela, R. D. (2022a). Towards web equality: Efforts on web accessibility for persons with cognitive disability. *International Journal of Research in Science & Engineering (IJRISE) ISSN: 2394-8299*, 2(03), 1–16.
- Hortizuela, R. D. (2022b). Towards web equality: Efforts on web accessibility for persons with cognitive disability. *International Journal of Research in Science & Engineering (IJRISE) ISSN: 2394-8299*, 2(03), 1–16.
- Inal, Y., Guribye, F., Rajanen, D., Rajanen, M., & Rost, M. (2020). Perspectives and practices of digital

- accessibility: A survey of user experience professionals in nordic countries. In *Proceedings of the 11th nordic conference on human-computer interaction: Shaping experiences, shaping society* (pp. 1–11).
- Johansson, S. (2022). *Hur mycket kognitiv tillgänglighet finns det i wcag 2.1*.
- Johansson, S., Gulliksen, J., & Lantz, A. (2015). User participation when users have mental and cognitive disabilities. In *Proceedings of the 17th international acm sigaccess conference on computers & accessibility* (pp. 69–76).
- Kävrestad, J., Fallatah, W., & Furnell, S. (2023). Cybersecurity training acceptance: A literature review. In *International symposium on human aspects of information security and assurance* (pp. 53–63).
- Kävrestad, J., Hagberg, A., Roos, R., Rambusch, J., & Nohlberg, M. (2021). Usable privacy and security from the perspective of cognitive abilities. In *Ifip international summer school on privacy and identity management* (pp. 105–121). Springer.
- Kim, B. (2013). Responsive web design, discoverability, and mobile challenge. *Library technology reports*, 49(6), 29–39.
- Lara, R. S., & Bokoch, R. (2021). Cognitive functioning and social media: Has technology changed us? *Acta psychologica*, 221, 103429.
- Macakoğlu, Ş. S., Peker, S., & Medeni, İ. T. (2023). Accessibility, usability, and security evaluation of universities' prospective student web pages: a comparative study of europe, north america, and oceania. *Universal Access in the Information Society*, 22(2), 671–683.
- MACAKOĞLU, S., & Peker, S. (2022). Web accessibility performance analysis using web content accessibility guidelines and automated tools: a systematic literature review. In *2022 international congress on human-computer interaction, optimization and robotic applications (hora)* (p. 1-8). doi: 10.1109/HORA55278.2022.9799981
- Maglaras, L., Ferrag, M. A., Janicke, H., Buchanan, W. J., & Tassiulas, L. (n.d.). Bridging the gap between cybersecurity and reliability for critical national infrastructures.
- Parsons, S., & Mitchell, P. (2002). The potential of virtual reality in social skills training for people with autistic spectrum disorders. *Journal of intellectual disability research*, 46(5), 430–443.
- Pham, H. C., Brennan, L., & Furnell, S. (2019). Information security burnout: Identification of sources and mitigating factors from security demands and resources. *Journal of Information Security and Applications*, 46, 96–107.
- Pour, M. S., Nader, C., Friday, K., & Bou-Harb, E. (2023). A comprehensive survey of recent internet measurement techniques for cyber security. *Computers & Security*, 103123.

- Renaud, K., & Coles-Kemp, L. (2022). Accessible and inclusive cyber security: a nuanced and complex challenge. *SN Computer Science*, 3(5), 346.
- Roumeliotis, K. I., & Tselikas, N. D. (2022). Evaluating progressive web app accessibility for people with disabilities. *Network*, 2(2), 350–369.
- Ruefle, R., Dorofee, A., Mundie, D., Householder, A. D., Murray, M., & Perl, S. J. (2014). Computer security incident response team development and evolution. *IEEE Security & Privacy*, 12(5), 16–26.
- Shpigelman, C.-N., & Gill, C. J. (2014). Facebook use by persons with disabilities. *Journal of Computer-Mediated Communication*, 19(3), 610–624.
- Simpson, K., Adams, D., Manokara, V., & Malone, S. (2022). Research and training priorities of staff supporting individuals with intellectual disabilities with or without autism. *Journal of Policy and Practice in Intellectual Disabilities*, 19(3), 277–287.
- Spina, C. (2019). Wcag 2.1 and the current state of web accessibility in libraries. *Weave: Journal of Library User Experience*, 2(2).
- Torrado, J. C., Jaccheri, L., Pelagatti, S., & Wold, I. (2022). Hikepal: A mobile exergame to motivate people with intellectual disabilities to do outdoor physical activities. *Entertainment Computing*, 42, 100477.
- Vollenwyder, B., Petralito, S., Iten, G. H., Brühlmann, F., Opwis, K., & Mekler, E. D. (2023). How compliance with web accessibility standards shapes the experiences of users with and without disabilities. *International Journal of Human-Computer Studies*, 170, 102956.

Appendices

Appendix A Informed Consent for Interview Participation

02 October 2023

Name of the participant

Nedre Ullevål 7 0850 Oslo, Norway

Dear Name,

Subject: Informed Consent for Interview Participation

I am writing to request your participation in an interview study conducted by Md. Ohidul Islam, a department of computer science student at the University Of South-Eastern Norway. The purpose of this study is to gain insights into web accessibility and cybersecurity challenges faced by individuals with cognitive disabilities. Your input as a participant is invaluable to the success of this research.

Please take a moment to review the following information about the study and what your participation will involve. If you agree to participate, we kindly request your signature at the end of this letter to signify your informed consent.

Study Information:

- Title: Equitable User Experience in terms of privacy and security settings.
- Principal Investigator (Thesis Student): Md. Ohidul Islam
- Supervisor: Joakim Kävrestad - Institution: University of South-Eastern Norway
- Purpose: The study aims to explore and better understand the experiences, perceptions, and challenges related to web accessibility and cybersecurity from the perspective of individuals with cognitive disabilities.

Your Participation: - You will be invited to participate in an in-depth interview. The interview will be conducted by Md. Ohidul Islam and will be audio-recorded for accuracy and analysis purposes. The interviews are expected to last approximately 15 minutes and will take place via Zoom/Meet.

- Your input will be used solely for research purposes and will remain confidential. Any personal information that may identify you will be anonymized and kept secure.
- You have the right to withdraw from the interview without any penalty or consequences.

Risks and Benefits: Participation in this study carries minimal risks. The potential benefits include contributing to research that may improve web services and cybersecurity for individuals with cog-

nitive disabilities.

Contact Information: If you have any questions about the study or wish to discuss it further, please do not hesitate to contact Md. Ohidul Islam at ohidulnirob@gmail.com or +47 96699404.

Confidentiality: Your confidentiality and privacy are of utmost importance. The data collected during the interview will be kept secure and confidential.

I have read and understand the information provided above, and I am willing to participate in this study. By signing below, I provide my informed consent to take part in the interview:

Participant's Signature:

My Signature: Md. Ohidul Islam

University Of South-Eastern Norway

Appendix B Informed Consent for Survey Participation

15 September 2023

Name of the participant

34/1A, Pallabi, Mirpur, Dhaka-1216, Bangladesh

Dear Name,

Subject: Informed Consent for Survey Participation

I am writing to request your participation in a survey study conducted by Md. Ohidul Islam, a Department of Computer Science student at the University Of South-Eastern Norway. The purpose of this survey is to gain insights into web accessibility and cybersecurity challenges faced by individuals with cognitive disabilities. Your input as a participant is invaluable to the success of this research.

Please take a moment to review the following information about the study and what your participation will involve. If you agree to participate, we kindly request your signature at the end of this letter to signify your informed consent.

Study Information:

- Title: Equitable User Experience in terms of privacy and security settings.
- Principal Investigator (Thesis Student): Md. Ohidul Islam
- Supervisor: Joakim Kävrestad - Institution: University of South-Eastern Norway
- Purpose: The study aims to explore and better understand the experiences, perceptions, and challenges related to web accessibility and cybersecurity from the perspective of individuals with cognitive disabilities.

Your Participation: - You are invited to participate in a survey. This survey is expected to take approximately 5 minutes and will be conducted online at <https://forms.gle/K6oiMyPxGNuEmMG7A>. - Your responses will be used solely for research purposes and will remain confidential. Any personal information that may identify you will be anonymized and kept secure. - You have the right to withdraw from the survey at any time without any penalty or consequences.

Risks and Benefits: Participation in this study carries minimal risks. The potential benefits include contributing to research that may improve web services and cybersecurity for individuals with cognitive disabilities.

Contact Information: If you have any questions about the study or wish to discuss it further, please do not hesitate to contact Md. Ohidul Islam at ohidulnirob@gmail.com or +47 96699404.

Confidentiality: Your confidentiality and privacy are of utmost importance. The data collected during the surveys will be kept secure and confidential.

I have read and understand the information provided above, and I am willing to participate in this study. By signing below, I provide my informed consent to take part in the survey:

Participant's Signature:

My Signature: Md. Ohidul Islam

University Of South-Eastern Norway