Understanding the Impact of Dyslexia on Online Privacy and Security

Fahad Alanazi
School of Computing, Dublin City University
Dublin, Ireland
alanazi.fah@gmail.com

Karen Renaud
Computer and Information Sciences
University of Strathclyde
Glasgow, UK
karen.renaud@strath.ac.uk

Irina Tal
Lero, School of Computing, Dublin City University
Dublin, Ireland
irina.tal@dcu.ie

***Abstract*—Dyslexia is a cognitive disability that affects a significant number of the population globally. Incipient research has shown that people with dyslexia experience challenges interacting with systems and security mechanisms that require reading, memory and writing (e.g. passwords). This paper presents an analysis of the challenges that people with dyslexia face when interacting with online systems and the inherent impact on their online security and privacy. People with dyslexia from Ireland and Saudi Arabia were interviewed in this purpose. The findings indicated that dyslexics are at a high risk of having their online security and privacy compromised and that they are struggling with various security and privacy mechanisms due to their condition. The paper concludes that there is a need to further the research in this area of accessible cybersecurity.**

Keywords—accessible cybersecurity, dyslexia, phishing, privacy

I. INTRODUCTION

Digital transformation together with COVID-19 pandemic led to a significant increase in the use of online platforms for education, business, entertainment, and work. For instance, global internet usage surged by 10.2% in 2020, making it the largest surge in the last decade[1] and it is predicted to increase further between 2024-2028 [2]. Following a similar trend, cybercrime has also increased to unprecedented levels, the spike of cyber crimes went as high as 75% during the height of the pandemic, with a particular increase in phishing attacks [3]. Moreover, the pandemic increased the conversation and awareness of the people in general about their online privacy due to the various measures that were taken by various Governments across the Globe [2,3]. Whereas these attacks can affect all people, there is a particular group of people that may be at increased risk: people with dyslexia.

Dyslexia is a cognitive disability that affects the language processing part of the brain, causing difficulties in reading, writing and memorizing. People with dyslexia often struggle with reading out words, learning new words, understanding what they hear, and remembering the sequence of things [1]. Globally, dyslexia affects between 9% and 12% of the world's population[4]. Particularly in Ireland it is estimated to affect 10% of the population[5]. In Saudi Arabia, 40% (160,000) of about 400,000 students with reading challenges have dyslexia.[6]

Due to the text processing issues that people with dyslexia are facing it was recently hypothesized that they may be facing issues with security and privacy mechanisms that require text processing. In a recent paper [4], it was introduced the concept of *accessible cybersecurity* and it was argued that current security and privacy mechanisms may not be accessible and that accessibility should be built in security together with usability. It is also emphasized the need to advance the research in this field and to understand the extent to which people with disabilities, including dyslexics, are struggling with various online security and privacy mechanisms.

While there are guidelines and standards for the design of accessible online systems, these are in general focusing on the user interface, on the look and feel, but are there guidelines for accessible cybersecurity? The answer seems to be no. National and international standards, while promoting inclusivity and accessibility, at a closer look their security and privacy guidelines do not provide accessibility and this is due in part to a lack of understanding in relation to the struggles that people with disabilities in general and dyslexia in particular are facing when dealing with various security and privacy mechansims [5].

In this context, we formulated the following research questions that we aimed to answer in this paper:

- RQ1: What is the impact of dyslexia on online privacy and security?
- RQ2: What are the suggestions that people with dyslexia have for making it easier to maintain their online privacy and security?

[1] ITU, [Online]. Available: https://www.itu.int/itu-d/reports/statistics/2021/11/15/internet-use/#:~:text=In%202020%2C%20the%20first%20year,line%20with%20pre%2Dcrisis%20rates. (Accessed 31st of August, 2023)

[2] https://www.statista.com/forecasts/1146844/internet-users-in-the-world, (Accessed 22nd of May, 2023).

[3] https://cointelegraph.com/news/cybercrime-up-75-during-covid-19-congressional-hearing-details (Accessed 22nd of May, 2023)

[4] https://www.crossrivertherapy.com/research/dyslexia-statistics (accessed on 22nd of May, 2023)

[5] Dyslexia.ie (accessed 22nd of May, 2023)

[6] T. Al-Thaqafi, "Awareness of the learning disorder has improved in Saudi Arabia but experts say more must be done," Arab News, 20 October 2021. [Online]. Available: https://arab.news/p8ngb (Accessed 22nd of May 2023)

- RQ3: To what extent does dyslexia impact the ability to spot phishing attacks?

In order to investigate these research questions, the research methodology centred around semi-structured interviews with people with dyslexia from 2 countries: Ireland and Saudi Arabia, involving 2 different languages and alphabets. The participants were recruited with the helps of the relevant associations in both countries: Dyslexia Association Ireland [7] and Saudi Arabia, respectively. To the best of our knowledge this is the first work in the literature focusing on accessible cybersecurity that considers 2 different languages and alphabets.

The paper is structured as follows: Section II presents the related work, Section III introduces the methodology followed in the study presented in the paper. Section IV presents the findings of the study, while Section V discusses and summarizes these findings. Section VI concludes the paper.

II. Related Work

A. People with dyslexia and online technology

Universal Design advocates for the development of inclusive systems that allow access to everyone without the need for specialised designs or adaptation [6]. However, there are no formal regulations to ensure that all systems adhere to these design principles [6][7]. Consequently, the web is not entirely accessible and friendly to all people, such as the people with dyslexia. For instance, challenges such as unclear navigation, too small graphics and text, difficult language, and complex page layout make online systems challenging for users in general and dyslexic users in particular [8]. While solutions like screen readers, screen magnification, voice synthesisers, spell checkers, and recorders may help people with dyslexia interact with online systems better [9], they are not always available in every system. Despite these challenges, it is almost impossible for people with dyslexia to live without interacting with online systems. Currently, digital literacy and the ability to use online systems are basic requirements in workplaces, entertainment, accessing government services and education [9]. Due to that, making online systems accessible for people with dyslexia while ensuring their online security and privacy is of paramount importance.

The Web Content Accessibility Guidelines (WCAG) is a universal standard that also includes recommendations related to people with dyslexia. WCAG's primary principles include navigation, fonts and graphics, timing, errors and language [6]. While these recommendations address the needs of people with dyslexia, conformance with them is still low, with most websites claiming to adhere to them being inaccessible to people with dyslexia [6] Additionally, they do not provide security recommendations to promote the safety of people with dyslexia.

A thorough analysis done on the accessibility provisined for in the national cybersecurity framework in UK demonstrated that there is a lack of understanding of accessible cybersecurity and vulnerable people including people with dyslexia are not really considered [5]. Other frameworks such as NIST[8], while promoting the inclusivity and accessibility they are failing to actually consider the people with dyslexia in their guidelines. An example in this regard can be the their authentication/password guidelines provided. While NIST guidelines for password considers usability, it fails to include accessibility Authentication mechanisms as discussed next, are one of the mechanisms demonstrated to impose considerable struggle in the case of people with dyslexia. This is also one of the findings of our study.

B. People with dyslexia and Cybersecurity

Accessible cybersecurity it was recently coined in [4]; hence it is a very recent area of research within cybersecurity. There is only some incipient research showing that people with dyslexia are sturggling with cybersecurity mechanisms. The existent studies focused so far on the authentication mechanisms, especially passwords and considered only English speaking participants. According to [10-12] people with dyslexia experience significant difficulties creating and remembering strong passwords. Some of these studies also attempted to explore some acceptable alternatives to text-based passwords such as graphical passwords or musical passwords. Other studies beyond authentication mechanism were not yet conducted, despite the fact that works such [4] and [5] are signalling that there are various other security and privacy mechanisms that may impose challenges to the people with dyslexia.

III. Research methodology

This section discusses the methodology followed in the study. The methodology is inspired from one of the very few studies that involved people with dyslexia in cybersecurity research [11]. The methodology invovled the following main steps:

- Study Design
- Ethics Approval
- Data Collection
- Data Analysis

A. Study Design

In order to understand the dyslexics experience with various online security and privacy measures, their susceptibility to phishing attacks and to answer the outlined research questions, we decided to conduct interviews. Using qualitative analysis methods was preferred as opposed to traditional survey methods, as dyslexics are not comfortable with conventional survey methods [11]. For instance, written questionnaires are unsuitable for people with dyslexia as they have challenges in reading and writing. The qualitative analysis enables the researchers to better understand people with dyslexia due to having a closer interaction with them [13].

Once we decided upon the method, we have developed the interview questions. As the study was designed to be conducted in Ireland and Saudi Arabia, the questions in English were translated into Arabic. The Arabic version was then translated back in English by an independent third party and the result was analysed to make sure that the meaning of the questions was not altered. We decided then on the participants recruitment

[7] https://dyslexia.ie/

[8] https://www.nist.gov/cyberframework

methods, the way to conduct interview, data collection, retention and disposal and described all this in the ethics application and the relevant documents that are described below.

B. Ethics approval

Prior to conducting the study, ethics approval was sought and obtained from the School of Computing Ethics Committee at Dublin City University. The participants were informed through the Plain Language Statement about the purpose of the study, the researchers involved, the type of data to be collected, etc. They were also presented with an informed consent form. These documents were presented to them and a recording/live reading was provided as well as per their choice. Only after these steps were completed and their consent was given they were subjected to the interview. The plain language statement and informed consent form were also translated in Arabic.

C. Data collection

The participants were recruited through the relevant dyslexia associations in both countries and were interviewed in candid conversations to allow them to explain their experiences. These interviews were conducted physically or online through video conferencing software. The interviewers had a list of questions that were read out to the participants and then recorded the responses through handwritten scripts later used in data analysis. We allowed for free feedback from the interviewees as well, so the interviews were semi-structured in that regard.

a) Participants

The participants in the interview were people with dyslexia above 18. They were recruited with the help of Dyslexia Association Ireland and Dyslexia Association in Saudi Arabia. The interviews were conducted in English and Arabic. They cut across all the age groups, 18-24: 1, 25-44: 10, 45-65: 2. A majority of them had been diagnosed with dyslexia at different ages, and were in different career fields. Table 1 shows a summary of the participants' demographics.

TABLE I. Participants demographics

ID	Age Bracket	Gender	Diagnosed
1.	25-44	Male	Yes
2.	18-24	Female	Yes
3.	25-44	Female	No
4.	25-44	Female	Yes
5.	25-44	Male	Yes
6	25-44	Female	Yes
7.	25-44	Male	Yes
8.	45-65	Male	Yes
9.	25-44	Male	Yes
10.	45-65	Female	Yes
11.	45-65	Male	Yes
12.	25-44	Female	Yes
13.	25-44	Female	Yes
14.	25-44	Male	Yes

D. Data analysis

The data recorded from the interviews were analysed using manual thematic analysis, a well-known technique used in qualitative research [11]. This analysis involved analysing the handwritten notes. Thematic analysis enabled identifying the issues and themes highlighted by the participants around the research questions in the study. The responses given by the respondents were analysed and categorised to identify patterns and traits that would help answer the research questions. This information was then used to create a graphical representation of some of the report's findings.

Next section details the main findings following our data analysis.

IV. Findings

Participants described their experiences interacting with online platforms and how dyslexia affects their online security and privacy. Their responses were used to answer our research questions as shown below.

A. Impact of dyslexia on online privacy and security

Most participants reported having a risky behaviour, which significantly affected their online security. These behaviours include using the same password for multiple accounts, disclosing passwords to friends and family to ask for assistance, and writing down passwords in software applications or books to avoid forgetting them. Figure 1 shows the riskiest behaviour that participants reported.

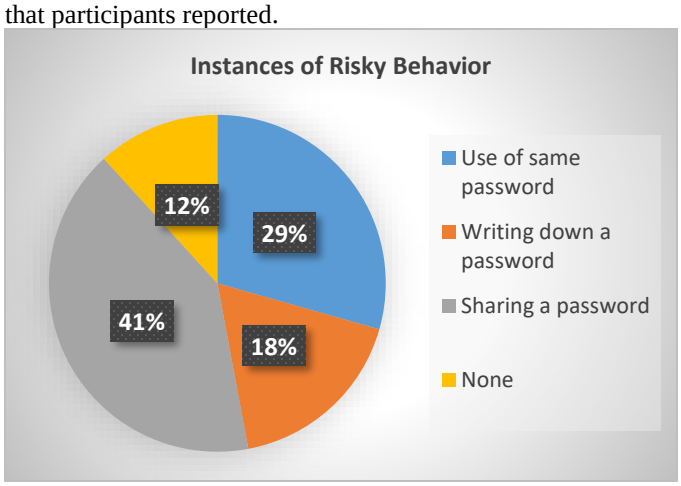

Figure 1: Risky behaviors shown by the participants

The inability to remember passwords was the main reason behind reusing passwords for different platforms. Here's Participant 1's response about that:

> "… I probably should not be telling you this, but I use the same password for everything because I find it very difficult to remember (a) password. I use the same variety of passwords. I found this technology has excelled, so recently, I'd use apple's password ability. They use a very strong password, so I started to use those strong passwords, but I even find that stressful

asking myself: Am I going to forget that, it does create an anxiety factor."

Writing down passwords was another common trend participants disclosed. Some participants reported storing their passwords in electronic form by storing them in excel sheets and password management software, while others preferred writing them down in books. Here are two responses from the participants:

> "I have to write my password in an excel sheet paired to the name of the service; that is my practical way to get them sorted." Participant 9

> "I have my password book; everything goes in here; this is like my bible, and in my phone log, I have something called the last pass. It's an app you can get, and so the app has all your passwords in it…."

Disclosing passwords to friends and family was another challenge that increased the security risk. Some participants reported having to share their passwords with others, even though they knew it was a security risk, to avoid being locked out of their own accounts. Here is the response from participant 14:

> "… sometimes I ask my college and family member to help me, I have to share my password, and to others, I always feel exposed."

Participants also reported the inability to use one-time passwords and confirmation codes sent to their devices when needed to verify their accounts or transactions in online systems. One-time passwords often have a time limit and are sent to users as text messages. Participants reported being unable to memorize the code sent to their devices and spell them correctly on the online platforms, with some either having to ask for help or avoiding online shopping altogether. Below are a few related responses from the participants:

> "…I would find myself missing the time limit, or I'd need a second message or even get my password locked. It all happened, and it depends on what the website is using…." Participant 1

> "Time limit is difficult to handle. Online payments and banking are very difficult: long card number, CVC, all the details to introduce is very challenging.": participant 2

All the participants reported difficulties using text-based CAPTCHA, an online test used to verify a user is human. Most participants reported being unable to go past this security test without help, and some had to abandon using an online system when encountering this test. Here are some responses about text-based CAPTCHA:

> "I can't read it, and I don't like it; I don't like dealing with it because it makes me feel uncomfortable." Participant 8

> "… it's the worst thing I can see on the internet. It gives me headache and pain" -participant 5

Participant 9 noted that CAPTCHA compromises their security; once they encounter it, they have to seek help, which may expose their information to other parties. Below is the response:

> "… whenever I came across CAPTCHA, I know that I have to get help, and that impacted my privacy, having to ask for help."

Some participants also reported their inability to create strong passwords for their accounts. A strong password should contain a combination of uppercase and lowercase letters, numbers, and special characters and must have a length of at least seven characters [19]. Some participants noted that they prefer shorter passwords that are often weak and insecure but easy to remember. Here is the response from Participant 1:

> "…long passwords with a different character at lengths put together if I were typing it in I'd find difficult especially around the I and L weather they're capital or whether they are lower case I find those very difficult if there is a different text font used it can be challenging to read do there are other areas…."

Moreover, they also highlighted their struggle with the privacy policies. Respondents noted that they often could not read the policies embedded in websites to promote their safety in the online space, mainly due to lengthy information written in law jargon and unfriendly font. Consequently, most of them are unaware of how the information they put online is used. As noted by some respondents, this also reduces their confidence in using online systems, making them only visit the sites they know.

> "It is absolutely disappointing to know that most of the policies are very complicated and require a lawyer to understand it, and it violates the user's right and its right to own his/her data.": Participant 5

> "Honestly, I don't trust it; currently, it's hard to read. If they provide the choice of enlarging the text, I might be able to read it….": Participant 6

> "I find it complex, very long, and hard to understand.": Participant 9

The participants also expressed their distrust of most websites, especially since they have severely fallen victim to phishing attacks. Due to the fear of falling prey again, some participants reported quitting using social media, online shopping, and other online services.

> "… I'd only go to a website I know and am comfortable with; even using eBay, I'd be suspicious of that. In regards to reading them, I'd more or less ignore them because the website I'd use I'd know, so if it were a new website I had never heard of, I'd be very suspicious. Still, generally, I'd not read them (privacy policies); it's too much information.": Participant 1

> "After I faced a lot of issues (related to) online services, I stopped using it completely… It impacted me big time, and I'm not using any of these (online

systems) because I don't want to get scammed." Participant 8.

B. *What suggestions do people with dyslexia have for making it easier to maintain their online privacy and security?*

Most participants said that they preferred image or audio-based authentication and systems as they found them easier to use. For instance, one participant noted that CAPTCHA systems that use images and audio are easier to use compared to text-based verification.

> It's very annoying and very challenging for me to get right; if it has a voice, then it can handle it: Participant 13
>
> "…I prefer the picture where I have to identify something in it; that one is much easier; it will probably take me a second to get it.": Participant 4

Similarly, they found it easier to use online systems with password autofill and autosuggestion capabilities. Here is a response from participant 5:

> "I use a special app to create new random passwords, and the app will save and encrypt the password for me, and I will access it using a multi-factor authentication via my mobile phone."

The participants also preferred websites with accessibility settings, for example, allowing text magnification or using huge fonts as they are easier to read. Below are some responses on this topic:

> "After the update of the application and accessibility, it's easier for me to use social media now.": Participant 14
>
> "…I use mac accessibility mood to enlarge texts and use it, but few of them can be hard and do not support these features.": Participant 12

Participants also showed the ineffectiveness of some methods used in training against phishing attacks. Some noted that most phishing awareness training was based on text and was unsuitable for people with dyslexia. They described text-based training as highly ineffective since dyslexia impairs a person's reading capabilities. They proposed audio and video-based training, noting that it suits them better.

> "The training was not developed for people with dyslexia, and I didn't get trained as it meant to be, create a training specialised for people with dyslexia." Participant 8
>
> "The presentation material was full of small text. It would have been useful to create a dyslexic version with bigger text or rely on more video and audio…": Participant 9

C. *To what extent does dyslexia impact the ability to spot phishing attacks?*

Most participants reported having fallen victim to phishing attacks due to having dyslexia. Of all the fourteen participants, 11 reported having been victims of phishing attacks, resulting in loss of access to their account and having their money stolen. Below are narrations from some participants:

> "They impersonated DHL, a logistics company, and the address and contact were like it was from DHL. It was impossible for me to verify even the shipment number was legitimate and had my data, but when I received the package, I discovered I was deceived… when I opened my shipment package there was only one paper writing on it 'you have been deceived'…": Participant 5
>
> "They stole my account, and that's why I don't have any email (account).": Participant 11
>
> "…they took all my maximum limit of purchase" Participant 14

Although some participants who had received training on phishing attacks were able to remain safe from attacks, most of the participants, trained or untrained, reported having been victims of phishing attacks. As shown in figure 2, most participants who had already received some training still fell victim to cyber-attacks.

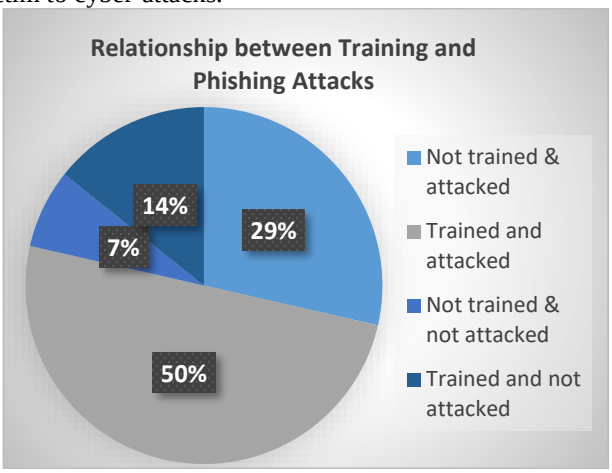

Figure 2:Relationship between phishing attack awareness and attacks

Most participants cited their inability to scrutinize the contents of the phishing emails sent to them as the main challenge that exposed them to phishing attacks.

> "I read words backward, especially if I was busy or there was something on my mind.": Participant 13
>
> "…there are some difficulties like reading and verifying the originality of the email, but sometimes I am able to enlarge the content and read it, or sometimes I copy it and paste it somewhere to read.": Participant 12.

> "I had difficulties reading and replying to emails on time, but with the right tools now I'm a little bit better…In my old days, I usually clicked the link, and I always had malware on my laptop or any devices I opened my email on. However, after I got educated about my condition, I became more careful and tried not to click any link unless I knew the sender's email.": Participant 14.
>
> My email was affected because most an email contains text, so I can't read it. Sometimes I play it with a reader, but it's still not always clear.": Participant 7

V. Discussion

Our findings confirmed that dyslexia has a particular impact on the dyslexics online security and privacy. Most of the coping mechanisms used by dyselxics people when interacting with online systems are risky and often expose them to security and privacy issues. Interestingly, some respondents reported knowing the security risks posed by their behaviour, while also noting that they do not seem to have an alternative.

This section discusses the research questions by evaluating how each was captured in the aforementioned interviews.

1) What is the impact of dyslexia on online privacy and security?

We established that people with dyslexia face challenges in creating and remembering strong passwords, compromising their online security. All participants in this study described at least one risky behaviour in relation to passwords likely to compromise their online safety. For instance, sharing, reusing, or writing down passwords are all behaviours flagged as risky due to their risk of causing security breaches [14]. Writing down a password exposes it to co-workers, friends, family, and others who may use it illegally to access a person's online account. Similarly, storing it in soft form poses an escalated risk as cyber attackers may access it if they gain remote access to a person's computer. Reusing a password is equally dangerous, as once a password is compromised, the attacker may use it to access multiple accounts belonging to one victim. Sharing passwords with friends and family poses an equal threat as they may use them to carry out unauthorised transactions without the owners' consent. These findings correspond with the authors of [9], who concluded that the inability to create and remember passwords was a significant challenge that people with dyslexia are facing.

2) What suggestions do people with dyslexia have for making it easier to maintain their online privacy and security?

Since text-based authentication systems are unfriendly, the participants recommended using audio and video-based authentication systems. For instance, although all participants reported having challenges with text-based CAPTCHA, most noted that it would only take a few seconds to go past that security check if it used audio or pictures. These findings are consistent with those described by the authors of [15], who recommended developing CAPTCHA tests that are easy for all people, including those with a disability, and challenging for bots to pass.

Our study also identified that people with dyslexia require more time to verify their accounts using one-time passwords. Systems requiring verification by sending a one-time password to mobile devices often have a time limit beyond which the code fails to work. Due to the inability to beat such time limits, the participants proposed the use of shorter codes, more extended time limits, and the option of having an audio-based verification.

Another improvement that the respondents proposed was increasing accessibility to websites by allowing text magnification. Websites and web applications that do not support text magnification are not user friendly to people with dyslexia, especially if they contain a lot of text. Therefore, simplifying the text and enabling magnification can help in improving accessibility for people with dyslexia.

Since people with dyslexia are unable to create and remember strong passwords, autosuggestion and autofill can help mitigate their challenges. Some respondents noted that systems that support password autosuggestion, then save the passwords for autocomplete in subsequent login attempts are more friendly as they protect them from the agony of having to remember the passwords.

3) To what extent does dyslexia impact the ability to spot phishing attacks?

This study showed that people with dyslexia are at a heightened risk of falling prey to phishing attacks. We discovered that people with dyslexia have more difficulty identifying phishing emails due to their challenges with text processing. Moreover, the training received by people with dyslexia aimed at helping them to identify phishing attacks is not efficient since it is not designed to meet their needs. Most of the participants in our study that attended such training reported not having benefited from them at all. The majority of the participants in the study reported that they perceived an increased vulnerability to such attacks due to their condition.

4) Summary

Our study builds on very recent research works that advocate for the need for accessible security. Works like [10-12], highlighted a struggle of people with dyslexia with authentication mechanisms. The current work furthers the state of the art and reinforces the struggle related to the authentication methods such as passwords, while also revealing struggles with mechanisms such as CAPTCHA, privacy policies, standard cybersecurity training that it is ineffective for them (in the particular case of phishing attacks) and an increased vulnerability to the phishing attacks. Dyslexics are forced into adopting coping mechanisms such as keeping plaintext passwords on their computers and books, sharing sensitive data with other people and reusing passwords. While adopting such coping mechanisms some of them are well aware about the security risks, but they also feel they have no choice. Moreover, they also feel their privacy invaded when sharing sensitive data. The trust in the various systems is affected and they perceive an increased risk to their online privacy and security due to their condition.

The study had participants from two different countries, using two very different alphabets, however, the findings are homogeneous across the participants in the two countries, and the language seems not to have an impact. To the best of our knowledge, this is the first study that considers another language than English.

VI. Conclusion

This paper conducted a study based on interviews in two different countries with two different languages and alphabets that aimed to understand the impact of dyslexia on the online privacy and security. Our findings have shown that people with dyslexia are struggling with various security and privacy mechanisms: authentication mechanisms (passwords, OTPs), privacy policies, CAPTCHA, and they are at a very high risk to fall for phishing attacks. Standard trainings on phishing attacks are not efficient due in part to the fact that these trainings are not designed to meet their learning needs.

The existent national and international frameworks lack clear specifications for accessible cybersecurity, especially in the particular case of the people with dyslexia. To some extent, this is understandable as the call for accessible cybersecurity it is quite a recent one. There is a need to further the research in this area and first understand the dimension of the problem by conducting studies similar to the one presented in this paper, followed by the proposal of specific solutions and guidelines to be then adopted in the frameworks and standards.

VII. Acknowledgement

This work was supported by the Science Foundation Ireland grant 13/RC/2094_P2 and co-funded under the European Regional Development Fund through the Southern & Eastern Regional Operational Programme to Lero - the Science Foundation Ireland Research Centre for Software (www.lero.ie). For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

References

[1] W. Tunmer and G. K, “Defining dyslexia,” Journal of Learning Disabilities, vol. 43, no. 3, pp. 229-243, 2010

[2] R. Trestian, G. Xie, P. Lohar, E. Celeste, M. Bendechache, R. Brennan, and I. Tal, “Privacy in a time of covid-19: How concerned are you?”, IEEE Security & Privacy, 19(5), 26-35, 2021.

[3] P. Lohar, X. Guodong Xie, M. Bendechache, R. Brennan, E. Celeste, R. Trestian, and I. Tal, "Irish attitudes toward COVID tracker app & privacy: sentiment analysis on Twitter and survey data”, ACM Proceedings of the 16th International Conference on Availability, Reliability and Security, pp. 1-8, 2021

[4] K. Renaud, “Accessible cyber security: the next frontier?,” in ICISSP, 2021.

[5] K. Renaud and L. Coles-Kemp, “Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge,” SN Computer Science, vol. 3, no. 5, pp. 1-14, 2021.

[6] G. Berget, J. Herstad and E. F. Sandnes, “Search, Read and Write: An Inquiry into Web Accessibility for People with Dyslexia,” Universal Design 2016: Learning from the Past, Designing for the Future: Proceedings of the 3rd International Conference on Universal Design, vol. 229, p. 450, 2016.

[7] H. Petrie, S. A and C. Power, “Towards a unified definition of web accessibility,” in *Proceedings of the 12th International Web for al conferences*, 2015.

[8] J. E. McCarthy and S. J. Swierenga, “What we know about dyslexia and web accessibility: a research review,” *Universal Access in the Information Society*, vol. 9, no. 2, pp. 147-152, 2010.

[9] F. V. de Santana, R. de Oliveira and M. C. Almeida Leonelo Baranauskas, “Web Accessibility and People with Dyslexia: a Survey on Techniques and Guidelines”.

[10] Evtimova, Polina, and James Nicholson. "Exploring the Acceptability of Graphical Passwords for People with Dyslexia." In Human-Computer Interaction–INTERACT 2021: 18th IFIP TC 13 International Conference, Bari, Italy, August 30–September 3, 2021, Proceedings, Part I 18, pp. 213-222. Springer International Publishing, 2021.

[11] K. Renaud, G. Johnson and J. Ophoff, “Accessible authentication: dyslexia and password strategies,” *Information and Computer Security*, vol. 29, no. 4, pp. 604-624, 2021.

[12] K. Renaud, G. Johnson and J. Ophoff, “Dyslexia and password usage: accessibility in authentication design,” in *International Symposium on Human Aspects of Information security and assurance*, 2020.

[13] D. Zambo, “Using Qualitative methods tto Understand the Educational Experiences of Students with Dyslexia,” *The Qualitative Report*, vol. 9, no. 1, pp. 80-94, 2004.

[14] L. Zhang-Kennedy, S. Chiasson and P. van Oorschot, “Revisiting Password Rules: Facilitating Human Management of Passwords,” in *2016 APWG Symposium on Electronic Crime Research eCrime*, 2016.

[15] R. Gafni and I. Nagar, “CAPTCHA: Impactt on User Experience of Users with Learning Disabilities,” Interdisplinary Journal of e-skills and Lifelong Learning, vol. 12, no. 1, pp. 207-233, 2016.