Accessible Cyber Security: The Next Frontier?

Karen Renaud*
University of Strathclyde, Glasgow, Scotland

Abstract: Researchers became aware of the need to pay attention to the usability of cyber security towards the end of the 20^{th} century. This need is widely embraced now, by both academia and industry, as it has become clear that users are a very important link in the security perimeter of organisations. Two decades later, I will make the case for the inclusion and importance of a third dimension of human-centred security, that of *accessibility*. I will argue that technical measures, usability and accessibility should be equally important considerations during the design of security systems. Unless we do this, we risk ignoring the needs of vast swathes of the population with a range of disabilities. For many of these, security measures are often exasperatingly inaccessible. This talk is a call to action to the community of human-centred security researchers, all of whom have already made huge strides in improving the usability of security mechanisms.

1 INTRODUCTION

In 1999, Adams and Sasse (Adams and Sasse, 1999) highlighted the tension between security and usability. It can be argued that their paper helped to launch the field of "usable security", with researchers now spanning the globe and a number of conferences dedicated to human-centred security research (Renaud and Flowerday, 2017). In a recent paper, Renaud, Johnson and Ophoff argued that accessibility ought to be considered an essential third dimension of the cyber security domain (Renaud et al., 2020a). Their paper focused on the accessibility of authentication, with particular attention being paid to challenges faced by dyslexics. However, their arguments raise a number of larger issues with respect to accessibility issues that pertain to the wider cyber security domain, which I will explore here.

I will first introduce the concept of accessibility in Section 2, and then talk about the *status quo* of cyber security practice in Section 3, pointing out areas of potential inaccessibility. Section 4 then suggests a way forward for the Cyber Security field before Section 5 concludes. In essence, I am hoping to convince you of the need to pay equal attention to the three dimensions depicted in Figure 1.

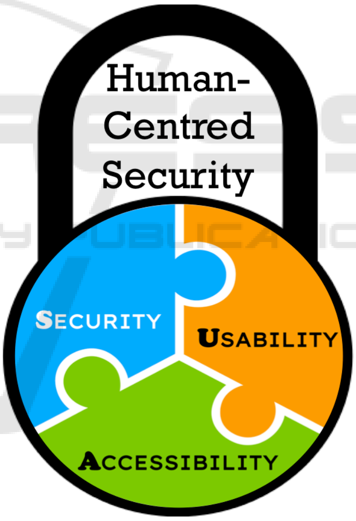

Figure 1: Security, Usability and Accessibility Dimensions of Human-Centred Security.

This paper is essentially conceptual, hoping to highlight the need for accessibility to be given its place in the cyber security domain. Carter and Markel (Carter and Markel, 2001) argue that the most promising route to full accessibility lies in collaboration between vendors, advocacy groups, and the government. Hence, I have written the paper in the hope of triggering exactly such a discourse involving Cyber Security professionals, Human-Centred Security academics and other stakeholders about the emerging and inescapable need to consider accessibility equally important, in addition to security and usability considerations, in the Cyber Security field.

*https://www.karenrenaud.com

Renaud, K.
Accessible Cyber Security: The Next Frontier?.
DOI: 10.5220/0010419500090018
In *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021)*, pages 9-18
ISBN: 978-989-758-491-6

2 ACCESSIBILITY

Petrie *et al.* (Petrie et al., 2015) analysed 50 definitions of accessibility to reveal the following six dimensions: (a) all users regardless of ability, (b) can access/interact with/use websites, (c) with usability characteristics, (d) using mainstream or assistive technologies, (e) design and development processes, and (f) in specific contexts of use. They conclude with a definition of web accessibility that brings all these dimensions together:

> *"all people, particularly disabled and older people, can use websites in a range of contexts of use, including mainstream and assistive technologies; to achieve this, websites need to be designed and developed to support usability across these contexts".*

The W3C argues that an improvement in accessibility benefits all users, including those without disabilities (W3C, 2018a).

2.1 Legislation

Accessibility is a legal mandate (Kuzma, 2010a). The United Nations Convention on the Rights of Persons with Disabilities[1], adopted in December 2006, is the first international legally binding instrument that sets minimum standards for the rights of people with disabilities.

2020 was declared the year of Digital Accessibility in the European Union (EU) with Anderson (Anderson, 2020) reporting that the EU enacted a directive that makes accessibility compulsory for websites published by all public sector bodies and institutions that are governed by public authority. Examples are public universities, local governments and any publicly-funded institution. There is much work still to be done to satisfy this directive (Kuzma, 2010b). However, as the number of court cases increase, it is likely that public institutions will be forced to take accessibility more seriously.

The W3C's Web Accessibility Initiative (WAI) has published a standard for web accessibility called the Web Content Accessibility Guidelines (WCAG) (W3C, 2018b). I have mapped their advice to Petrie *et al.*'s (Petrie et al., 2015) dimensions (Table 1).

WCAG 2.1 (published in June 2018) did not really address cyber security accessibility. Only one instance can be found which refers to the need to provide users with enough time to read and use content, and the ability to pick up an activity they were previously engaged in after re-authenticating an expired session (success criterion 2.2.5).

WCAG 2.2 introduces a new success criterion called 'Accessible Authentication' (3.3.7). This specifies that "*for each step in an authentication process that relies on a cognitive function test, at least one other method is available that does not rely on a cognitive function test*" (W3C, 2020).

"Cognitive function test" refers to remembering a username and password (or any other secret used by a knowledge-based authentication mechanism). The alternative authentication method must not rely on human cognition. It might be a password manager automatically filling in credentials or a biometric, for example. Sometimes, authentication requires multiple steps. In this case, all steps should comply with this success criterion.

2.2 Disabilities

"Disability" includes people with visual & auditory impairments, motoric & cognitive disabilities (Anderson, 2020). Anderson (Anderson, 2020) reports that it is estimated that, in Europe, there are over 100 million people with disabilities of various kinds. I will now briefly consider the different kinds of disabilities.

2.2.1 Vision & Auditory Disabilities

Some users are completely blind, others have limited vision, and the WebAIM Website (Web Accessibility in Mind) website[2] also lists colour blindness as a disability. Some people are born with poor or no vision, but many people develop vision and auditory issues as they age (Tielsch et al., 1990). The world's population is ageing, as shown by Figure 2, which suggests that the number of people without perfect vision and impaired hearing is steadily increasing.

The heavy dependence of modern day graphical interfaces on visual cues is problematic for the visually disabled (Chiang et al., 2005) and blind users face a large number of barriers to usage (Stanford, 2019). Chiang *et al.* (Chiang et al., 2005) cite Scott *et al.* (Scott et al., 2002), who carried out a study with people suffering from age-related macular degeneration. This ailment leads to visual impairment and severe vision loss. It impacts the centre of the retina, which is crucial in giving us the ability to read and parse text. Scott *et al.* report that the reduced visual acuity, contrast insensitivity, and decreased color vision impacted task accuracy and task completion speed.

[1] https://ec.europa.eu/social/main.jsp?catId=1138\&langId=en

[2] https://webaim.org/articles/motor/motordisabilities

Table 1: Mapping WCAG guidelines (W3C, 2018b) to Petrie *et al.*'s dimensions (Petrie et al., 2015).

WCAG	Petrie *et al.*'s dimensions
1. users must be able to perceive information and user interface (UI) components using their senses	(a) all users regardless of ability
2. UI components and navigation must be operable using interactions users can perform	(b) can access/interact with/use websites
3. information and the operation of the UI must be understandable	(c) with usability characteristics
4. content must be robust enough to be accessible by a wide variety of (assistive) technologies	(d) using mainstream or assistive technologies

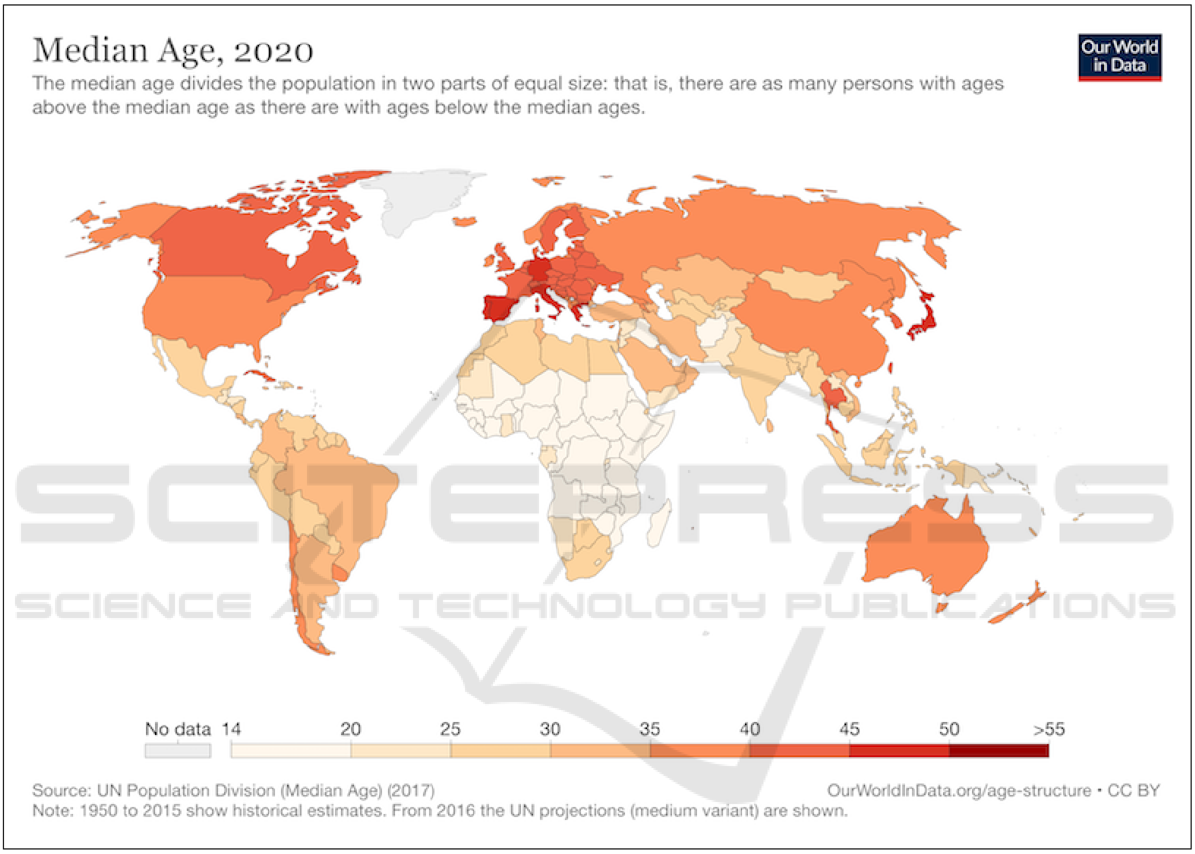

Figure 2: Median age of World population in 2020.

While Braille keyboards may help those who have been blind from a young age, Braille is not taught to those who lose their vision due to age-related decline, so this is not necessarily an option for them. Moreover, with more people accessing the Internet from their Smartphones every year (see Figure 3), and thus interacting with security mechanisms via soft keyboards, poor vision can present insuperable barriers to usage, unless the mechanism designed with accessibility in mind.

2.2.2 Motoric Disabilities

As people age, their dexterity decreases, especially after 65 (Carmeli et al., 2003). Together with age-related vision loss, this is likely to impact their ability to engage with computer keyboards, both traditional and soft (on Smartphones). The WebAIM website lists a range of other motor disabilities, including multiple sclerosis and cerebral palsy. People with these disabilities are likely also to experience difficulties with keyboards, computer mice and trackpads.

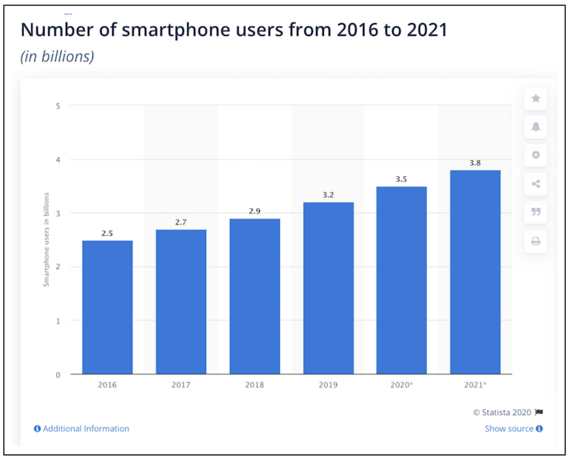

Figure 3: Worldwide Smartphone Diffusion (Statista).

2.2.3 Cognitive Disabilities

A variety of cognitive disabilities are listed on the WebAIM website including: memory, problem-solving attention, reading, linguistic, and verbal & visual comprehension.

All are likely to impact computer usage to different extents. Here, I discuss two as examples of such difficulties: (1) developmental cognitive disabilities, and (2) a reading-related disability (dyslexia), as examples.

Developmental Cognitive Disabilities. Nussbaum (Nussbaum, 2009) addresses the rights of those with limited ability to read, and those who easily become confused or fearful in a new setting. Nussbaum argues that these people could be: "*disqualified from the most essential functions of citizenship*" (p.347). Given that governments and councils are increasingly offering services to their citizens or constituents online (Iqbal et al., 2019), it is likely that this disability group is also going to be forced to use computers and to go online.

Dyslexia. Dyslexia has been defined as (International Dyslexia Organization, 2019): "*a specific learning disability that is neurobiological in origin. It is characterized by difficulties with accurate and/or fluent word recognition and by poor spelling and decoding abilities. Secondary consequences may include problems in reading comprehension and reduced reading experience that can impede growth of vocabulary and background knowledge.*"

Some estimates suggest that up to 20% of English speakers suffer from a form of dyslexia (Michail, 2010). Only a few studies have focused specifically on accessibility difficulties faced by dyslexic users (de Santana et al., 2012; McCarthy and Swierenga, 2010). The UK Home Office (UK Home Office, 2016) and Dyslexia Scotland (Dyslexia Scotland, 2015) provide design guidelines to help address the difficulties experienced by dyslexic users. They do not mention any cyber security related issues.

2.3 Summary

Accessibility is a legal mandate in the EU and the USA, and the need for accessibility is gaining prominence across the globe (Perlow, 2010; Nelson et al., 2019). In 2018, in the USA alone, there were 2285 web accessibility related lawsuits[3].

While comprehensive guidelines exist to inform the design of websites to accommodate a range of physical disabilities, such as poor vision or hearing loss, cognitive disabilities have not yet received as much attention. The next section will consider how the Cyber Security field fares when viewed using the accessibility lens.

3 THE CYBER SECURITY DOMAIN

Cyber criminals continue to ply their trade, and the number of successful attacks continue to increase. It is very important for all individual citizens to secure their devices and computers, but knowing how to do this is undeniably challenging (Xavier and Pati, 2012; Nthala and Flechais, 2017; Nicholson et al., 2019). Governments are well aware of this but they no longer consider themselves to be shepherds protecting their flocks, as they used to some decades ago. They now take the view that citizens should be given advice and then be left to take care of themselves i.e. they are *responsibilized* (Renaud et al., 2020b). As such, governments focus primarily on providing advice and building capabilities (Tsinovoi and Adler-Nissen, 2018). This government cyber responsibilization of citizens is built on the following five assumptions:

1. **Citizens will Obtain Accurate Advice.** Advice is provided online, and there is an assumption that people will find it. Yet most people will search for advice using Google (Renaud and Weir, 2016). Given that are thousands of experts providing cyber security-related advice online, it is likely that people will become overwhelmed with the amount of conflicting advice (Redmiles et al., 2020). Hence, this is a flawed assumption, because it assumes "one truth" when it comes to

[3]https://blog.usablenet.com/2018-ada-web-accessibility-lawsuit-recap-report

advice to be followed, whereas Redmiles *et al.* (Redmiles et al., 2020) demonstrated that this is not the case: even experts disagree about which pieces of advice are in the top-5 to be followed.

2. **Citizens will Act on Their Knowledge.** There is evidence that knowledge, on its own, does not change behaviour (McCluskey and Lovarini, 2005; Worsley, 2002; Finger, 1994), particularly in the cyber security context (Sawaya et al., 2017).
3. **Risk Perceptions will be Accurate:** this, too, is a flawed assumption because humans are poor at understanding risk (Siegrist and Árvai, 2020; Gigerenzer, 2015)
4. **Risk Perceptions Predict Actions:** this is a somewhat over-simplified assumption because the link between perceptions and behaviour is far more complex. Risk perceptions do feed into behaviours, but so do the other factors such as control perception (Van Schaik et al., 2017), domain (Weber et al., 2002) and age (Machin and Sankey, 2008), to mention but three influences.
5. **Citizens will Report Attacks:** this relies on people knowing that their devices have indeed been compromised and second, reporting the attack. In the first place, even large companies with the resources to ensure high levels of cyber security sometimes do not know that they have been attacked (Thielman, 2016). Indeed, IBM's latest report suggests that the average time to detect a data breach is 280 days (IBM, 2020). If large wealthy companies do not detect attacks, how can we expect the average citizen to do so? In the second place, as O'Donnell (O'Donnell, 2019) points out, victims of cyber attacks often do not report them because they might be ashamed of falling victim and worry about being blamed, or they do not believe there is any point in doing so. Moreover Varonis (Varonis, 2020) reports that 64% of citizens of the USA do not know how to report a cyber attack.

These assumptions are clearly flawed for all citizens, but even more so for those with cognitive and other disabilities. The upshot is that citizens are left to ensure their own cyber security, by themselves, without much external support. That being so, the usability and accessibility of cyber security measures that the average user has to interact with becomes critical.

Let us now briefly consider how this might be particularly challenging for disabled computer users.

3.1 Accessibility Issues

If we consider the four aspects of accessibility mentioned in Table 2, we see that the first three apply equally to cyber security activities. Yet the fourth is problematic in this domain. Assistive tools are designed to ease the usual web-related activities, not cyber security actions. For example, spellcheckers (Rello et al., 2015) and other assistive tools used by dyslexics (Pařilová, 2019; Athènes et al., 2009) cannot alleviate password-related issues, nor do electronic readers offer assistance (Rello et al., 2013) because password entry is obfuscated and these tools, if they could access these passwords, would then compromise password secrecy.

Moreover, usability of cyber security mechanisms is not the same as usability of a web page. Using an example from authentication again: one of the primary usability recommendations is to allow users to undo actions, and to provide assistance. Neither of these is possible with authentication. Web sites will consider a wrong password a possible indication of an impersonation attempt. No hints can be provided, because that would compromise the strength of the mechanism and might help an impersonator to guess the password.

Many cyber security warnings are displayed in red, but this is likely to be a problem for colour blind users with red-green deficiency. The prevalence of this deficiency in European Caucasians is about 8% in men and about 0.4% in women and between 4% and 6.5% in Chinese and Japanese males (Birch, 2012). Whereas red stands out for people who are not colour blind, it does not draw attention for colour blind computer users. Hence a full reliance on colour is a clear accessibility failure.

Some examples of cyber-related accessibility issues will now be provided. This list is not intended to be exhaustive, but serves to give a flavour of the issues disabled users face every day.

3.1.1 Authentication

One thing no web user can avoid is authentication, and the dominant authentication mechanism is the password. Renaud *et al.* (Renaud et al., 2021) interviewed dyslexics and identified issues with creating, retaining and entering passwords. Those with vision loss are also likely to struggle due to possible not being able to read the password creation requirements. Consider that someone who has become blind during retirement might not have memorised the QWERTY keyboard and thus will not easily be able to interact with any password authentication mechanism. Finally, users with motor issues, such as those with arthritis, are also likely to struggle with password entry, perhaps making mistakes and getting locked out of their accounts.

Now, consider the increasing popularity of two-factor authentication. Many of these mechanisms send a four digit code to the person's mobile phone for entry into the website. Dyslexics might easily swap digits around, those with poor vision will struggle to see the code, and those with impaired mobility might struggle to type in the number. Alternatives that allow people either to approve or decline the authentication attempt on their phones are somewhat better, but the buttons might be too small for those with vision impairments to identify and distinguish the approve and disapprove buttons from each other.

An investigation into the challenges faced by dyslexics in authenticating (Renaud et al., 2020a) highlights the fact that this user group need also to be considered when it comes to web accessibility. They are likely to face difficulties creating, retaining and entering passwords, and will also struggle to peruse terms and conditions documents commonly displayed by websites. This means that the consent they grant to such websites is not truly informed.

Users with cognitive issues relating to memory (e.g., age-related decline), reading (e.g., dyslexia), numbers (e.g., dyscalculia), or perception-processing will thus be unable to authenticate without difficulty (W3C, 2020).

Bear in mind that many users will have multiple disabilities, such as poor vision *and* hearing difficulties. In this case, a CAPTCHA which attempts to identify bots might constitute an insurmountable obstacle to usage, even if both audible and visual alternatives are provided.

3.1.2 Phish Detection in Emails

The usual advice is to examine the embedded link very carefully before clicking on it. Consider the steps that a user has to take to do this: (1) hover over the link to reveal the *actual* destination, (2) parse the URL carefully to validate it. Now, consider someone with vision loss, who might have difficulties focusing on a URL, especially if it is long and complex. This is likely to be impossible for someone with even moderate macular degeneration to achieve, for example.

Dyslexics, who struggle with sequences of characters, are likely also to struggle with this process. If a Phishing email embeds multimedia without text alternatives, it would be impossible for a hearing-impaired individual to detect any possible deception (Pascual et al., 2015). The use of complex language might also flummox these users.

3.1.3 Fake Websites and Dangerous App Detection

Mirchandani (Mirchandani, 2003) carried out a study with people with developmental cognitive disabilities. They struggled to identify web links some ended up randomly clicking on the text on the page. Their keyboard skills were described by the researchers as "hunt and peck". In particular, they were put off when clicking on a link launched a new page. They also struggled to switch between browser tabs and typing in URLs often required assistance. With all these difficulties, it is likely that they do not have the ability to judge between a 'good' and 'bad' link, and between legitimate and harmful apps.

Whereas a sighted user might well use a search engine to confirm the "goodness" of a particular website, disabled users may struggle. Jay *et al.* (Jay et al., 2007) found that sighted people used a number of visual cues in order to search for links on a webpage. Such cues are not available to users with impaired vision. Hearing impaired users might also struggle with the everyday search engines. If disabled users are not able to verify an app or website as would an able user, this makes their devices more vulnerable. Fajardo *et al.* (Fajardo et al., 2009) presents a search engine that supports the use of sign language to carry out a search, a welcome movement in the right direction in terms of easing searching for one specific group of disabled users.

3.1.4 Mobile Devices

The need to secure a device by encrypting it can be achieved by ensuring that this is the default when setting up the phone, so that end users do not have to engage with this measure - an accessibility triumph. Using a PIN to control access to the device will present challenges to those with poor vision, who might not be able to see the soft keyboard well enough. The same will apply to those with dexterity challenges, having to use a keyboard that does not align with use by large and aging fingers.

Going through the list of applications to control permissions does indeed require not only adequate vision to be able to read the application names and permissions, but also requires the cognitive ability to make sense of what the permissions mean. Those with hearing loss might also be affected if their knowledge fund has been affected by lifelong hearing loss (Kushalnagar, 2019).

3.1.5 Summary

This section provides a few examples, but the full range of cyber security related inaccessibility is likely to be far more diverse and affect a wide range of disabled users.

4 A WAY FORWARD

Governments are offering most services online, so that citizens, both abled and disabled, will have no choice but to go online as well. This means that they will also interact with cyber security mechanisms and measures during their everyday lives (Alzahrani et al., 2018). Hence, everyone working in cyber security has to consider the accessibility of cyber security measures in designing and deploying security measures. Those designing these measures have to ensure that they do indeed provide the required level of security but also that they maximise both usability and accessibility.

I do not pretend to have solutions — I am merely pointing to the need to find better solutions to enhance accessibility. The solutions will require concerted efforts from determined and talented researchers. It is fortunate that the usable security domain has many of these.

In this section, I will suggest some directions for future research, with no claims to exhaustiveness. I am hoping that other researchers will take up the accessibility challenge and carry out research to improve accessibility for all users. Some suggested directions are:

1. **Outline the Basics:** One of the standard accessibility guidelines is to ensure that alt-text is provided for all visuals. In the cyber security domain, for example, if a visual nudge is provide, such as a password strength meter, those with poor vision will not be able to see what this is trying to communicate. An alternative to a visual communication measure should always be provided to ensure accessibility.
2. **Provide Alternatives:** The WCAG guideline already mandates an alternative to authentication. This principle ought to be applied to other measures too. So, for example, the visual display of a password strength meter should offer an audible or haptic feedback measure for users with poor vision. CAPTCHAs often provide an audible alternative but for ageing users with both vision and hearing impairments this is probably not going to be sufficient, especially since both of these add 'noise' to prevent automated solving. Such noise makes it very difficult for those with imperfect vision or hearing to decipher the actual signal. Finding an alternative would be a good avenue for future research. The use of biometrics, in particular, should be investigated for more widespread use. Some consumers already actively use face and other biometrics to authenticate to their phones. With increasingly powerful built-in cameras on a range of devices, it seems as if biometrics' time has come, in terms of providing a usable and accessible alternative. Some initial moves in this direction are encouraging (Hassanat et al., 2015; Tanaka and Knapp, 2002; Kokila et al., 2017).
3. **Design Accessibility Into the Cyber Security Measure:** what we have learnt is that accessibility, similar to security and usability, cannot be bolted on at the end of the design and testing process. It has to be a consideration all the way through the requirements gathering, design, development and testing parts of the life cycle. Hence cyber-security related software design guidelines are needed. Testing should be carried out with disabled as well as able users. Kerkmann and Lewandowski (Kerkmann and Lewandowski, 2012) provide practical guidelines for researchers who want to conduct an accessibility study. Theirs is specifically aimed at web accessibility but would provide a good starting point for developing similar guidelines for testing the accessibility of cyber security mechanisms.
4. **Develop Cyber Security User Interface Accessibility Guidelines:** we can start with the WCAG accessibility guidelines, and then extend them to encapsulate the cyber security domain. For example, there is now a requirement for captioning on all multimedia, and a number of successful court cases have ensured that companies realise this (Disability Rights Education & Defense Fund, 2012). If an organisation chooses to raise Cyber Security awareness using an online course, which includes videos, these *must* be captioned.
5. **Develop Accessibility Heuristics to support Expert Review:** The usability field has developed a range of heuristic guidelines to support expert review of interfaces (Nielsen, 1992). The idea would be to develop a similar range of heuristics for accessibility assessment of cyber security measures. This will help businesses to redesign their cyber security measures that users have to interact with (Anderson,).
6. **Establish Venues for Dissemination:** the establishment of conferences such as SOUPS and

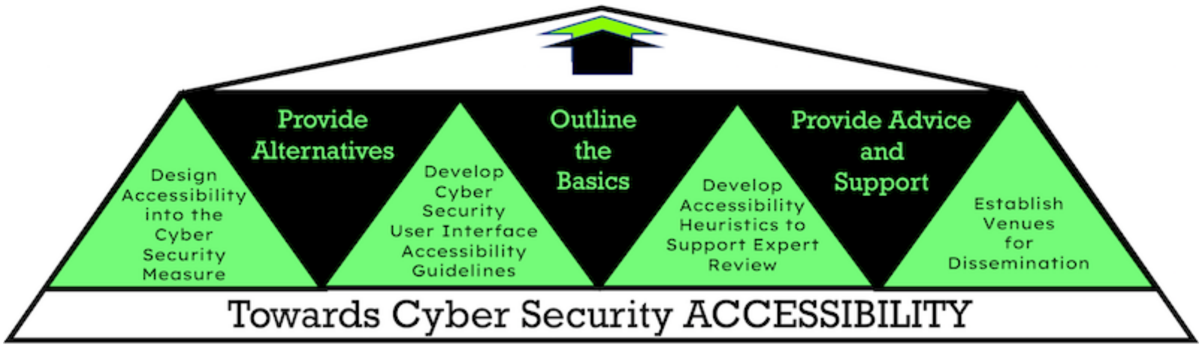

Figure 4: Constructing Accessibility.

USEC have played a role in encouraging research in the usable security domain. We need similar conferences for accessible security too, or at least dedicated streams in other human-related conferences such as CHI and perhaps SOUPS as well.

7. **De-Responsibilize: Provide Advice AND Support:** one of the stakeholders in this domain is government, especially those who cyber responsibilize their citizens. Given that disabled users may struggle even more than others to act on any advice that is issued by governments, there is a clear need for them to provide more support to end users. The way this ought to be provided is yet another rich avenue for future research.

5 CONCLUSION

I am writing this paper on the 3rd December, which happens to be International Day of People with Disabilities. Cyber security is a relatively new field, and efforts to improve its usability are barely two decades old. As the field of human-centred security matures, it seems appropriate for us also to consider accommodating the needs of *all* computer users. Our efforts to improve accessibility are bound also to make cyber security more manageable for the rest of the population, in addition to enhancing access for those with disabilities. It might be time for an offshoot discipline of “Accessible Security” to be established. With this paper, I hope to raise awareness of the need for more research in this area. I trust that human-centred security researchers will bear accessibility in mind in their future research endeavours.

REFERENCES

Adams, A. and Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12):40–46.

Alzahrani, L., Al-Karaghouli, W., and Weerakkody, V. (2018). Investigating the impact of citizens’ trust toward the successful adoption of e-government: A multigroup analysis of gender, age, and internet experience. *Information Systems Management*, 35(2):124–146.

Anderson, B. Lessons every organization can learn from surging accessibility lawsuits. https://codemantra.com/surging-accessibility-lawsuits/ Accessed 3 December 2020.

Anderson, B. (2020). 2020 – The Year of Digital Accessibility in the European Union (EU). https://codemantra.com/directive-eu-20162102-accessibility-law/ Accessed 5 December 2020.

Athènes, S., Raynal, M., Truillet, P., and Vinot, J.-L. (2009). Ysilex: a friendly reading interface for dyslexics. In *ICTA 2009, International Conference on Information & Communication Technologies : from Theory to Applications*, Hammamet, Tunisia.

Birch, J. (2012). Worldwide prevalence of red-green color deficiency. *Journal of the Optical Society of America*, 29(3):313–320.

Carmeli, E., Patish, H., and Coleman, R. (2003). The aging hand. *The Journals of Gerontology Series A: Biological Sciences and Medical Sciences*, 58(2):M146–M152.

Carter, J. and Markel, M. (2001). Web accessibility for people with disabilities: An introduction for web developers. *IEEE Transactions on Professional Communication*, 44(4):225–233.

Chiang, M. F., Cole, R. G., Gupta, S., Kaiser, G. E., and Starren, J. B. (2005). Computer and world wide web accessibility by visually disabled patients: Problems and solutions. *Survey of Ophthalmology*, 50(4):394–405.

de Santana, V. F., de Oliveira, R., Almeida, L. D. A., and Baranauskas, M. C. C. (2012). Web accessibility and people with dyslexia: a survey on techniques and guidelines. In *Proceedings of the International Cross-Disciplinary Conference on Web Accessibility*, pages 1–9.

Disability Rights Education & Defense Fund (2012). Nad v. netflix. https://dredf.org/legal-advocacy/nad-v-netflix/ Accessed 5 December 2020.

Dyslexia Scotland (2015). Dyslexia and ICT. https://www.dyslexiascotland.org.uk/our-leaflets.

Fajardo, I., Vigo, M., and Salmerón, L. (2009). Technology for supporting web information search and learning in sign language. *Interacting with Computers*, 21(4):243–256.

Finger, M. (1994). From knowledge to action? exploring the relationships between environmental experiences, learning, and behavior. *Journal of Social Issues*, 50(3):141–160.

Gigerenzer, G. (2015). *Risk Savvy: How to make good decisions*. Penguin.

Hassanat, A., Al-Awadi, M., Btoush, E., Al-Btoush, A., Alhasanat, E., and Altarawneh, G. (2015). New mobile phone and webcam hand images databases for personal authentication and identification. *Procedia Manufacturing*, 3:4060–4067.

IBM (2020). Cost of a data breach report 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ Accessed 5 December 2020.

International Dyslexia Organization (2019). Definition of dyslexia. https://dyslexiaida.org/definition-of-dyslexia/ Accessed 5 December 2020.

Iqbal, M., Nisha, N., and Rifat, A. (2019). E-government service adoption and the impact of privacy and trust. In *Advanced Methodologies and Technologies in Government and Society*, pages 206–219. IGI Global.

Jay, C., Stevens, R., Glencross, M., Chalmers, A., and Yang, C. (2007). How people use presentation to search for a link: expanding the understanding of accessibility on the web. *Universal Access in the Information Society*, 6(3):307–320.

Kerkmann, F. and Lewandowski, D. (2012). Accessibility of web search engines. *Library Review*.

Kokila, B., Pravinthraja, S., Saranya, K., Savitha, S., and Kavitha, N. (2017). Continuous Authentication System Using Multiple Modalities. *International Journal of Pure and Applied Mathematics*, 117(15):1129–1142.

Kushalnagar, R. (2019). Deafness and Hearing Loss. In *Web Accessibility*, pages 35–47. Springer.

Kuzma, J. M. (2010a). Accessibility design issues with uk e-government sites. *Government Information Quarterly*, 27(2):141–146.

Kuzma, J. M. (2010b). Accessibility design issues with UK e-government sites. *Government Information Quarterly*, 27(2):141–146. http://www.sciencedirect.com/science/article/pii/S0740624X0900135X.

Machin, M. A. and Sankey, K. S. (2008). Relationships between young drivers' personality characteristics, risk perceptions, and driving behaviour. *Accident Analysis & Prevention*, 40(2):541–547.

McCarthy, J. E. and Swierenga, S. J. (2010). What we know about dyslexia and web accessibility: a research review. *Universal Access in the Information Society*, 9(2):147–152.

McCluskey, A. and Lovarini, M. (2005). Providing education on evidence-based practice improved knowledge but did not change behaviour: a before and after study. *BMC Medical Education*, 5(1):40.

Michail, K. (2010). *Dyslexia: The experiences of university students with dyslexia*. PhD thesis, University of Birmingham.

Mirchandani, N. (2003). Web accessbility for people with cognitive disabilities: Universal design principles at work! *Research Exchange*, 8(3).

Nelson, A., Weiss, D. J., van Etten, J., Cattaneo, A., McMenomy, T. S., and Koo, J. (2019). A suite of global accessibility indicators. *Scientific Data*, 6(1):1–9.

Nicholson, J., Coventry, L., and Briggs, P. (2019). "If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–11.

Nielsen, J. (1992). Finding usability problems through heuristic evaluation. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–380.

Nthala, N. and Flechais, I. (2017). "if it's urgent or it is stopping me from doing something, then i might just go straight at it": a study into home data security decisions. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 123–142. Springer.

Nussbaum, M. (2009). The capabilities of people with cognitive disabilities. *Metaphilosophy*, 40(3-4):331–351.

O'Donnell, A. (2019). How do i report internet scams/fraud? https://www.lifewire.com/how-do-i-report-internet-scams-fraud-2487300 Accessed 5 December 2020.

Pařilová, T. (2019). *DysTexia: An Assistive System for People with Dyslexia*. PhD thesis, Masarykova univerzita, Fakulta informatiky.

Pascual, A., Ribera, M., and Granollers, T. (2015). Impact of web accessibility barriers on users with a hearing impairment. *Dyna*, 82(193):233–240.

Perlow, E. (2010). Accessibility: global gateway to health literacy. *Health Promotion Practice*, 11(1):123–131.

Petrie, H., Savva, A., and Power, C. (2015). Towards a unified definition of web accessibility. In *Proceedings of the 12th Web for all Conference*, pages 1–13.

Redmiles, E. M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., Stevens, R., and Mazurek, M. L. (2020). A comprehensive quality evaluation of security and privacy advice on the web. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 89–108.

Rello, L., Baeza-Yates, R., Saggion, H., Bayarri, C., and Barbosa, S. D. (2013). An ios reader for people with dyslexia. In *Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 1–2.

Rello, L., Ballesteros, M., and Bigham, J. P. (2015). A spellchecker for dyslexia. In *Proceedings of the 17th International ACM SIGACCESS Conference on Computers & Accessibility*, pages 39–47.

Renaud, K. and Flowerday, S. (2017). Contemplating Human-Centred Security & Privacy Research: Suggesting future directions. *Journal of Information Security and Applications*, 34:76–81.

Renaud, K., Johnson, G., and Ophoff, J. (2020a). Dyslexia and password usage: accessibility in authentication design. In *International Symposium on Human Aspects of Information Security and Assurance*, pages 259–268. Springer.

Renaud, K., Johnson, G., and Ophoff, J. (2021). Accessible authentication: Dyslexia and password strategies. *Information and Computer Security*. To Appear.

Renaud, K., Orgeron, C., Warkentin, M., and French, P. E. (2020b). Cyber security responsibilization: an evaluation of the intervention approaches adopted by the Five Eyes countries and China. *Public Administration Review*, 80(4):577–589.

Renaud, K. and Weir, G. R. (2016). Cybersecurity and the unbearability of uncertainty. In *Cybersecurity and Cyberforensics Conference (CCC)*, pages 137–143. IEEE.

Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A., and Yamada, A. (2017). Self-confidence trumps knowledge: A cross-cultural study of security behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 2202–2214.

Scott, I. U., Feuer, W. J., and Jacko, J. A. (2002). Impact of graphical user interface screen features on computer task accuracy and speed in a cohort of patients with age-related macular degeneration. *American Journal of Ophthalmology*, 134(6):857–862.

Siegrist, M. and Árvai, J. (2020). Risk perception: Reflections on 40 years of research. *Risk Analysis*.

Stanford, B. (2019). Barriers at the ballot box: the (in) accessibility of uk polling stations. *Coventry Law Journal*, 24(1):87–92.

Tanaka, A. and Knapp, R. B. (2002). Multimodal interaction in music using the electromyogram and relative position sensing. *NIME 2002*.

Thielman, S. (2016). Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*, 15:2016.

Tielsch, J. M., Sommer, A., Witt, K., Katz, J., and Royall, R. M. (1990). Blindness and visual impairment in an American urban population: the Baltimore Eye Survey. *Archives of Ophthalmology*, 108(2):286–290.

Tsinovoi, A. and Adler-Nissen, R. (2018). Inversion of the ‘duty of care’: Diplomacy and the protection of citizens abroad, from pastoral care to neoliberal governmentality. *The Hague Journal of Diplomacy*, 13(2):211–232.

UK Home Office (2016). Dos and don’ts on designing for accessibility - accessibility in government. https://accessibility.blog.gov.uk/2016/09/02/dos-and-donts-on-designing-for-accessibility/ Accessed 26 November 2020.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., and Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75:547–559.

Varonis (2020). 64% of americans don’t know what to do after a data breach — do you? https://www.varonis.com/blog/data-breach-literacy-survey/ Accessed 5 December 2020.

W3C (2018a). Accessibility. https://www.w3.org/standards/webdesign/accessibility Accessed 26 November 2020.

W3C (2018b). Web Content Accessibility Guidelines (WCAG) 2.1. https://www.w3.org/TR/WCAG21/.

W3C (2020). Understanding Success Criterion 3.3.7: Accessible Authentication. https://www.w3.org/WAI/WCAG22/Understanding/accessible-authentication.

Weber, E. U., Blais, A.-R., and Betz, N. E. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making*, 15(4):263–290.

Worsley, A. (2002). Nutrition knowledge and food consumption: can nutrition knowledge change food behaviour? *Asia Pacific Journal of Clinical Nutrition*, 11:S579–S585.

Xavier, U. H. R. and Pati, B. P. (2012). Study of internet security threats among home users. In *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, pages 217–221. IEEE.