BCS HCI 2023, 36th Int. Conference BCS Human-Computer Interaction Conference

Accessibility barriers with authentication methods for blind and partially sighted people in the Spanish-speaking world

Lourdes Moreno

Universidad Carlos III de Madrid, Spain
lmoreno@inf.uc3m.es

Helen Petrie

University of York, York, UK
helen.petrie@york.ac.uk

Suzanna Schmeelk

University of York (UK), St. John's University (NYC)
ss3134@york.ac.uk

Different authentication mechanisms:

- Passwords
- CAPTCHAs
- Two-factor authentication
- QR codes
- Fingerprint
- Facial recognition

Digital authentication systems are **not accessible** and do **not guarantee privacy and security** for blind and partially sighted people.

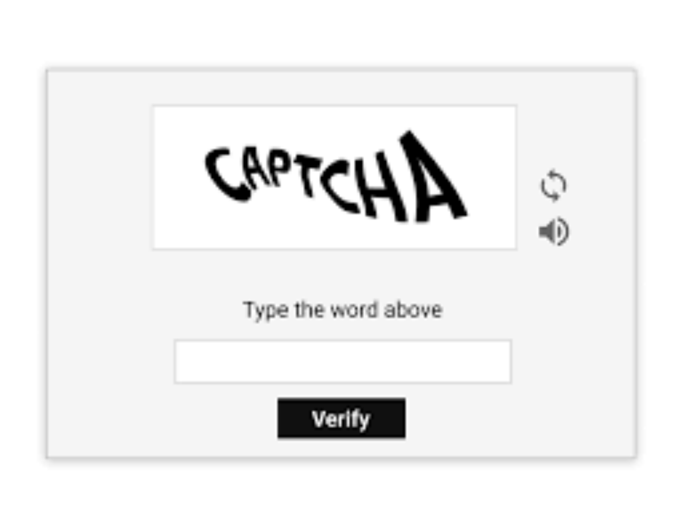
Is assistive technology for blind and partially sighted people considered in the digital authentication systems design?

Accessibility problems in password creation and management:

- with the inability to locate/identify elements.
- with knowing whether authentication had been successful.
- with accessing error messages.
- with mechanisms to prevent auditory shoulder surfing.
- creating strong passwords (strength indicators).
- with password recovery processes.

Access by screen reader is not taken into account.

(Dosono et al., 2015; Hayes et al., 2017; Briotto et al., 2018)

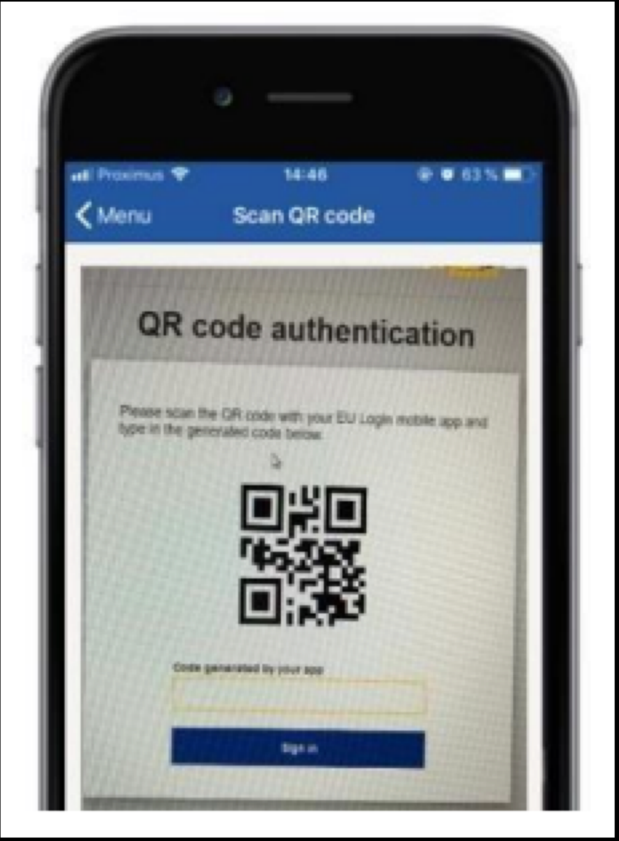


- Audio alternatives for blind users.
- Different solutions of Audio alternatives for blind users.

(Infiai, 2021; Tariq & Khan, 2018; Yamaguchi et al., 2014; Shirali-Shahreza et al., 2013; Lazar et al., 2012; Sauer et al., 2010; Bigham & Cavender, 2009; von Ahn et al., 2003; Holman et al., 2007)

However, access problems with CAPTCHAs are among the most frequent in digital authentication, even when there are auditory alternatives.

(Schmeelk and Petrie, 2022; Ahmed et al., 2015)



QR code authentication

Please scan the QR code with your EU Login mobile app and type in the generated code below

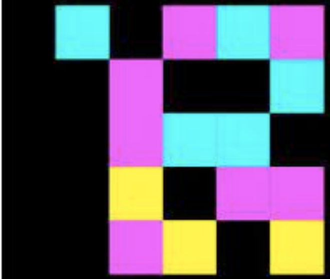
Code generated by your app

Accessibility problems in authentication through **QR codes**:

- when finding exactly where the code is located to interact with it and
- when **placing one's device at the correct distance and angle relating to the code to access it.**

(Schmeelk &Petrie, 2022)

New accessibility solutions



(NaviLens, 2023; Vision Australia, 2021).

Studies on accessibility issues of **authentication systems for blind and partially sighted users** have been found, but almost entirely in the **English-speaking world.**

In order to complement this research, this work presents **a survey in the Spanish-speaking world.**

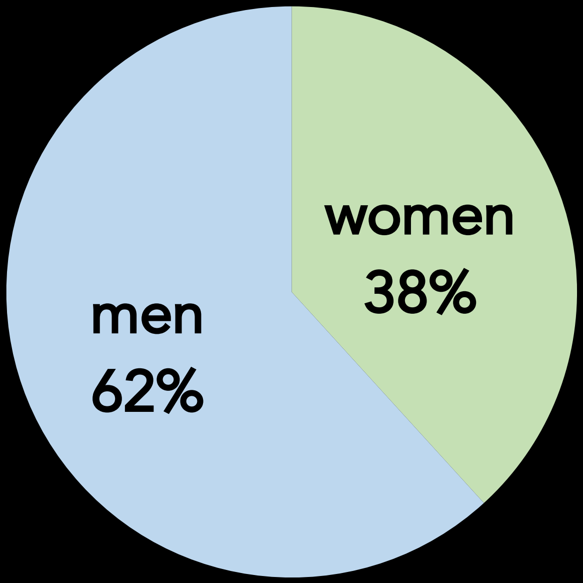
METHOD-Survey

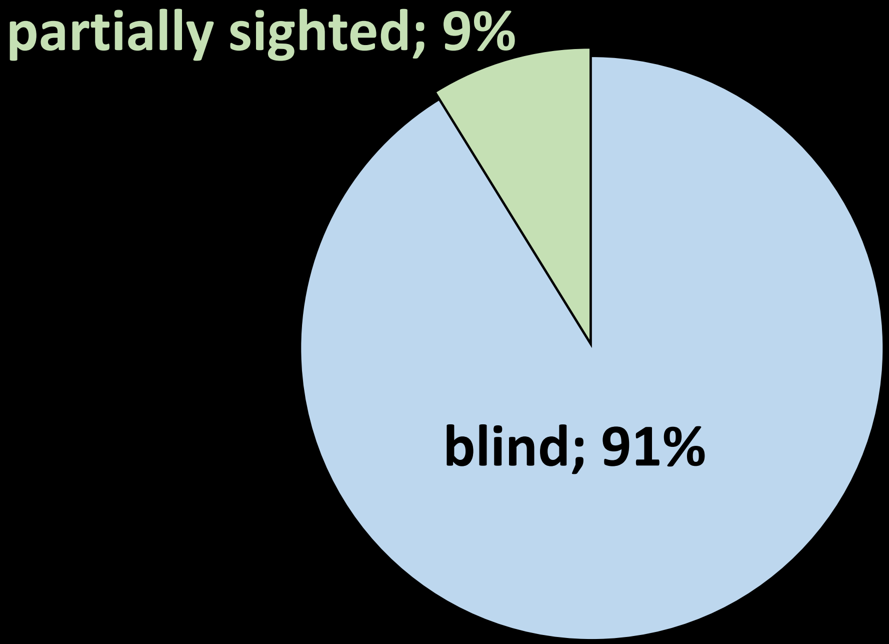
- Spanish online questionnaire.
- Qualtrics survey software.

- Three sections
  - Passwords: creating, entering, and changing.
  - Other authentication systems: password management systems, CAPTCHAs, two-factor authentication, fingerprint and facial recognition, and QR codes.
  - Demographic information, assistive technologies, knowledge of online security.

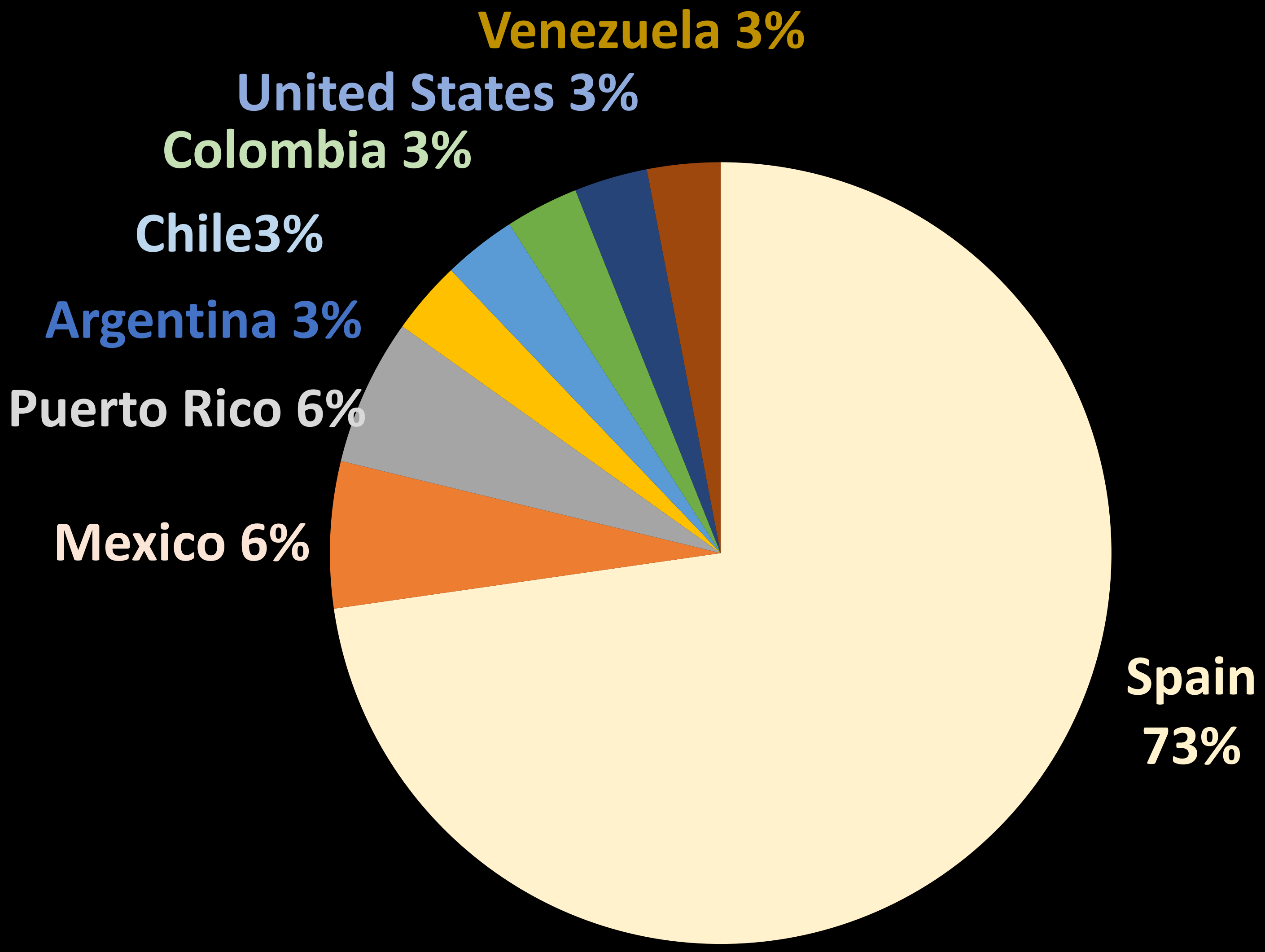
METHOD-Participants

- Advertising and recruiting on social networks (LinkedIn, Facebook, and Twitter) and contacting associations of blind people in Spain.
- 34 users
- Average age: 35.3 years (from 16 to 67).

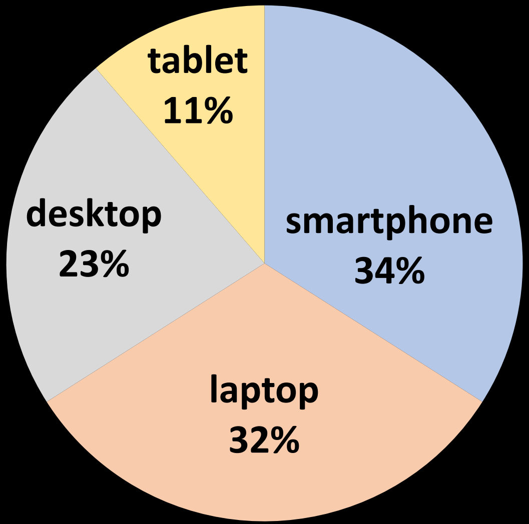




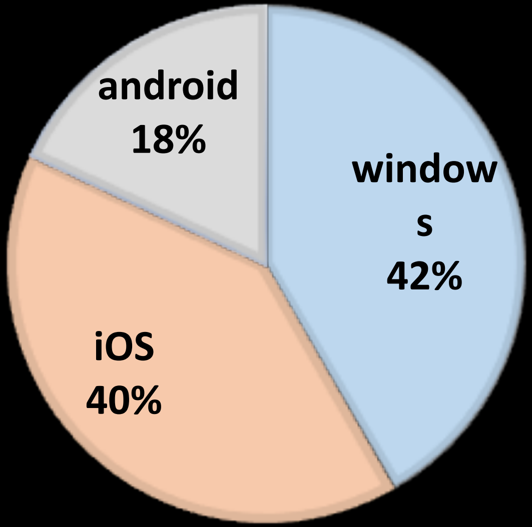
METHOD-Participants



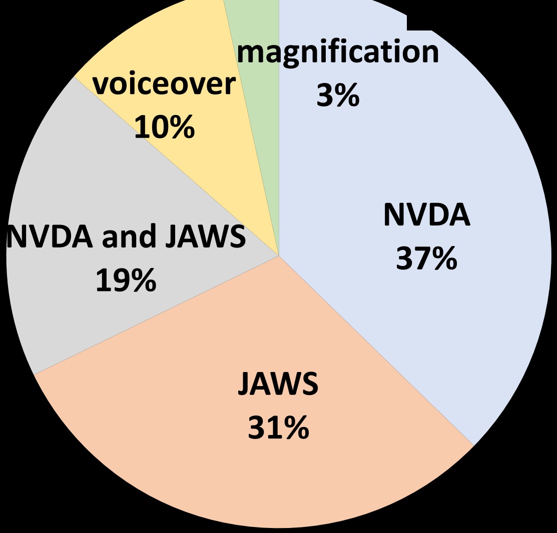
METHOD-Participants



Device

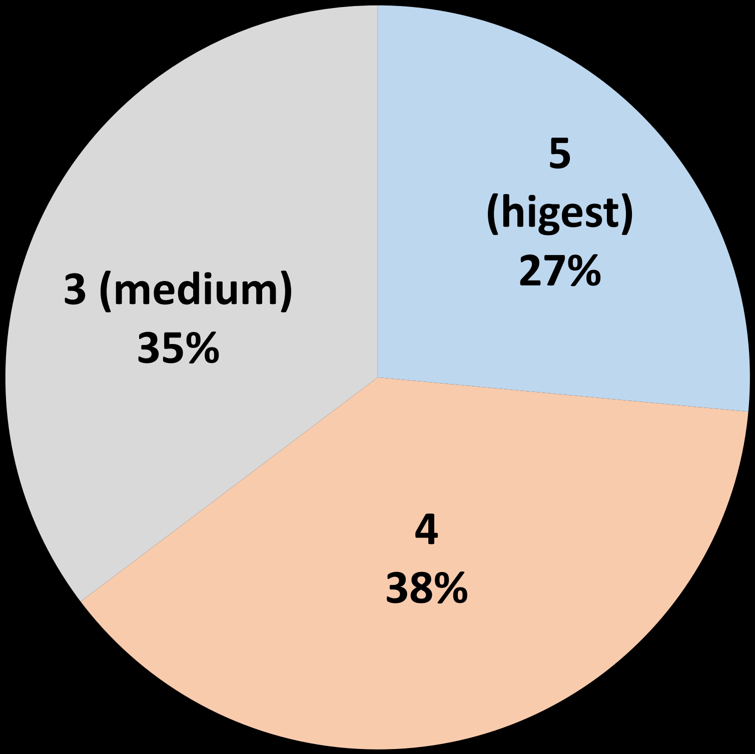


Operating System

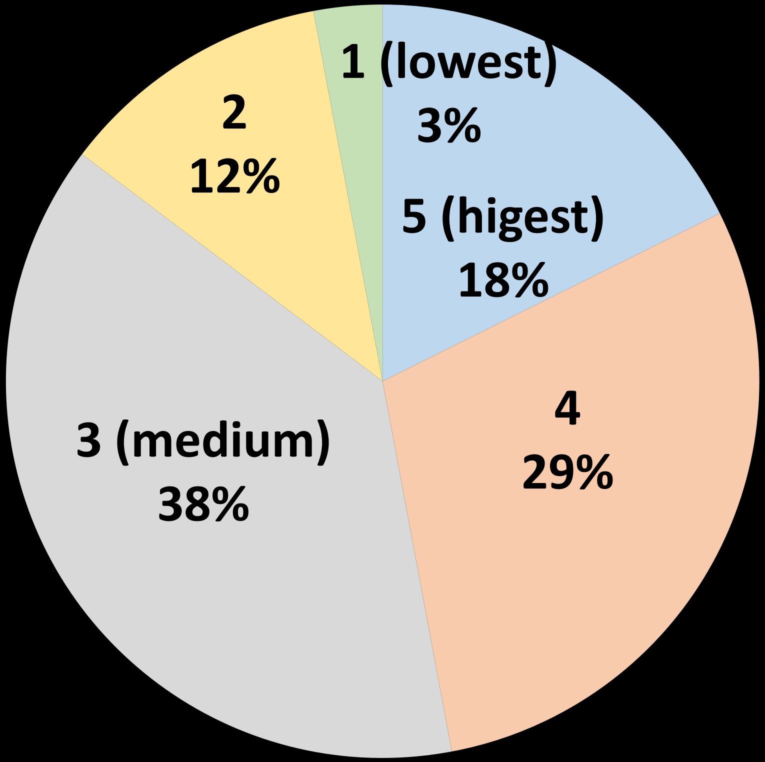


Assistive Technology (screen reader, magnification)

METHOD-Participants

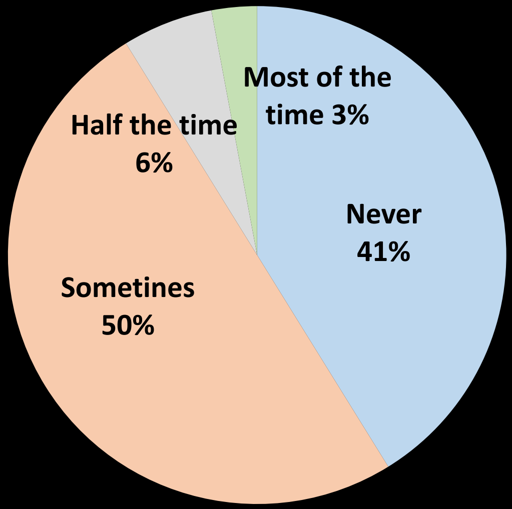


Expertise in the use of computers

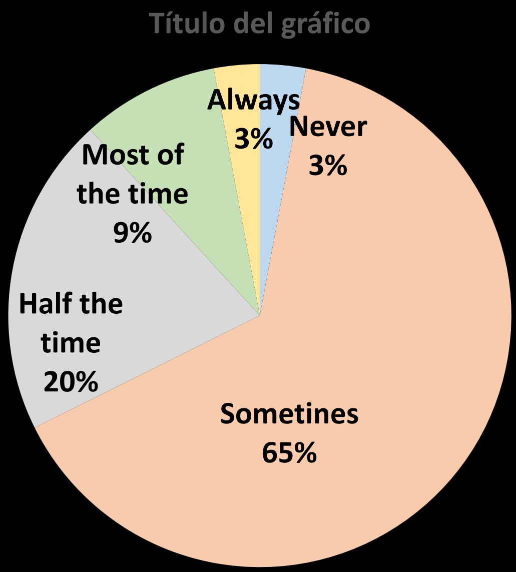


Knowledge of online security systems

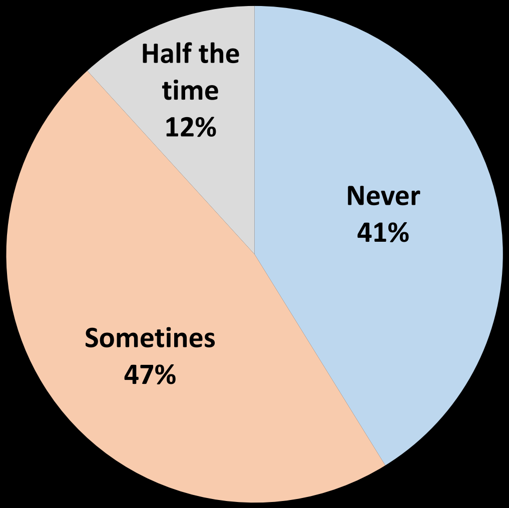
RESULTS- Barriers when creating and using passwords



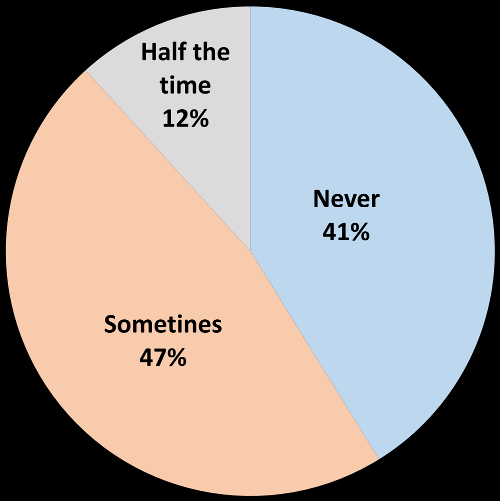
when creating a password



with password strength meters



when using passwords



when changing a password

RESULTS- Barriers when creating and using passwords

When creating a password

- There is a lack of accessibility in the instructions on the composition of the password, e.g. minimum length and special characters required.

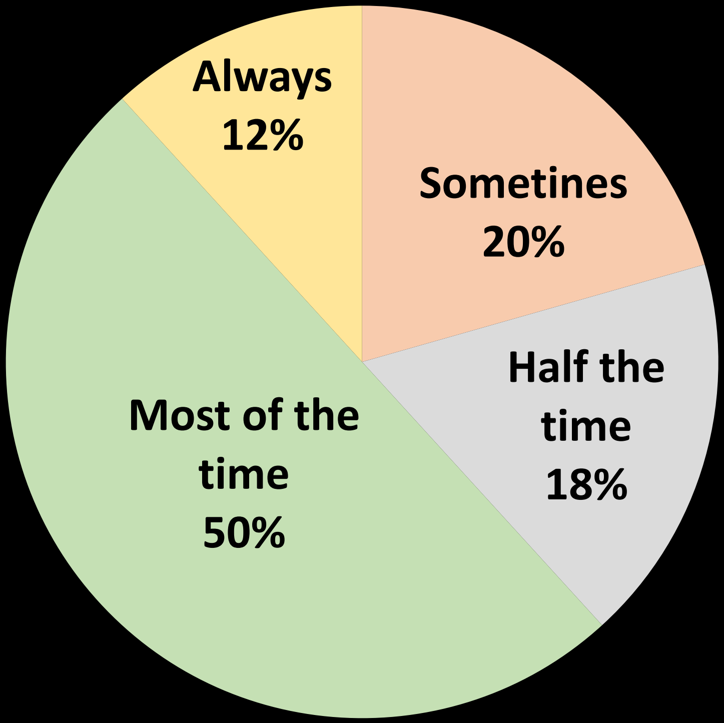
Password strength meters

- The description of the indicators is not accessible (is the password “strong” or “very strong”?).

Using and changing password

- The password entry field is not accessible via keyboard/screen reader.
- The reading order of elements is not logical
- Timeout issues

RESULTS- Barriers with the CAPTCHA



CAPTCHAs do not provide an accessible alternative.
When it provides an audio alternative:

- The audio is not understandable.
- The entry field in which to enter the answer is not accessible.

RESULTS- Barriers to two-factor authentication systems

- 91.2% have used or tried to use them.
- 52.9% use them successfully.

- Timeouts issues.
- It is easy to authenticate successfully if all the authentication operations are on the same device.

RESULTS- Barriers with other with other mechanisms

with facial recognition systems

- 64.7% have used or tried to use them.
- Blind users cannot correctly orient their faces to the camera.
- They need someone to help them.

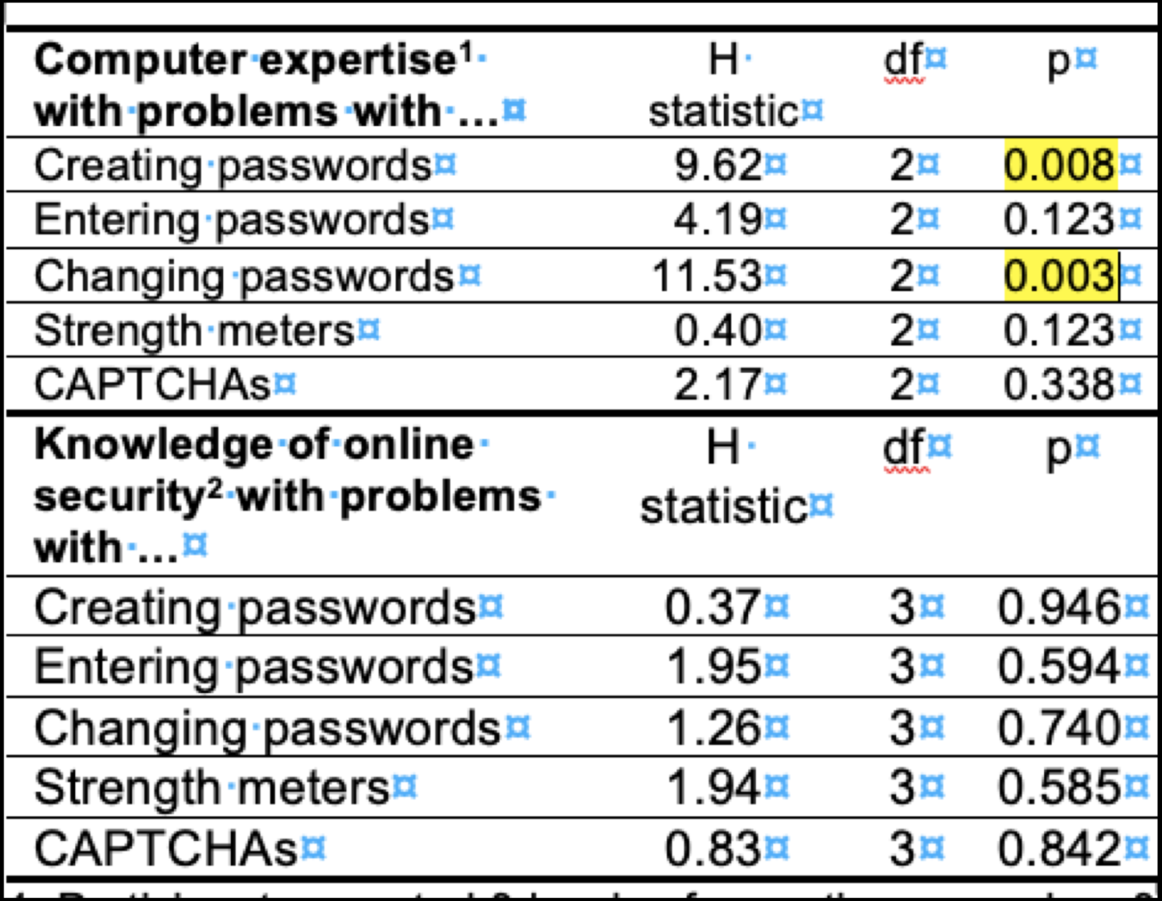
with fingerprint recognition systems

- 79.4% have used or tried to use them.
- Many of the participants reported success (Apple devices)
- It is difficult to identify where one should place one’s finger because the location is indistinguishable by touch.

with QR codes

- 85.3% have used or tried to use them, but many barriers
- Locate correctly the camera on the QR code

RESULTS- Relationship between experience of barriers in authentication and computer and security expertise



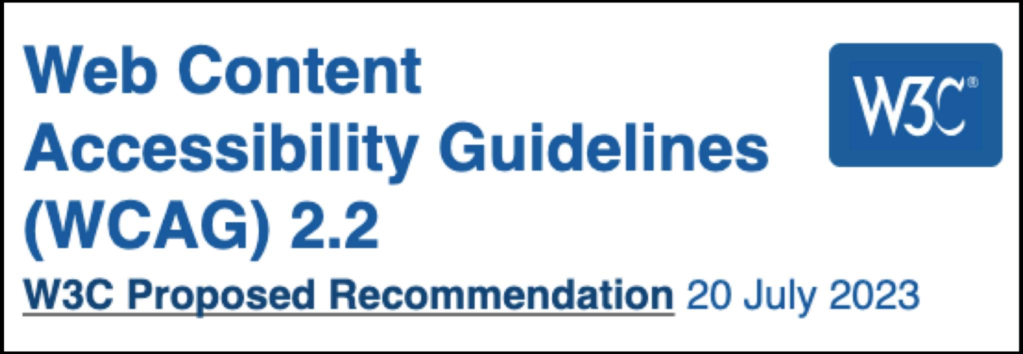
Computer expertise[1] with problems with …	H statistic	df	p
Creating passwords	9.62	2	0.008
Entering passwords	4.19	2	0.123
Changing passwords	11.53	2	0.003
Strength meters	0.40	2	0.123
CAPTCHAs	2.17	2	0.338
Knowledge of online security[2] with problems with …	**H statistic**	**df**	**p**
Creating passwords	0.37	3	0.946
Entering passwords	1.95	3	0.594
Changing passwords	1.26	3	0.740
Strength meters	1.94	3	0.585
CAPTCHAs	0.83	3	0.842

Participants with the **highest computer expertise rating** had a significantly **lower** frequency of problems both **creating and changing their passwords.**

CONCLUSIONS

Digital authentication systems do not comply with the accessibility standards (WCAG):

- There is not a correct **keyboard access.**
- The **logical reading order** is not followed.
- **Time-outs** are not well-defined.
- It is not possible to **access the information** on the password strength meters.



Web Content Accessibility Guidelines (WCAG) 2.2

W3C Proposed Recommendation 20 July 2023

Two new Success Criteria have been included:

- **3.3.8 Accessible Authentication** (Minimum) (Level AA)
- **3.3.9 Accessible Authentication** (Enhanced) (Level AAA)

CONCLUSIONS

- **Auditory CAPTCHAs** are not necessarily usable and accessible. More research and development effort is needed.

- Authentication mechanisms using **facial recognition** and **QR codes** currently pose many accessibility barriers to ensure they are accessible.

- Regarding **two-factor authentication system,** **t**here are products on the market that are accessible, but more research and development effort is needed.

- **Fingerprint recognition syst**ems are one of the more accessible authentication systems, particularly on Apple devices.

CONCLUSIONS

- **Blind and partially sighted people who are more expert can somewhat overcome the barriers**. Further research is needed because authentication systems must be accessible, not just those with high computer expertise.

Future research

- Differences in the Spanish-speaking world research results with the English-speaking world will be analyzed.
- User testing will be conducted on blind and partially sighted people in the USA, UK, and Spain to obtain objective knowledge of how users interact with the different authentication systems.

interaction
A Specialist Group from BCS

BCS HCI 2023, 36th Int. Conference BCS Human-Computer Interaction Conference

Accessibility barriers with authentication methods for blind and partially sighted people in the Spanish-speaking world

Lourdes Moreno

Universidad Carlos III de Madrid, Spain
lmoreno@inf.uc3m.es

Helen Petrie

University of York, York, UK
helen.petrie@york.ac.uk

Suzanna Schmeelk

University of York (UK), St. John's University (NYC)
ss3134@york.ac.uk

uc3m | Universidad Carlos III de Madrid
COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

HULAT
Human Language & Accessibility Technologies

UNIVERSITY of York