Security and Accessibility CAN be friends!

@accessibilityoz

www.accessibilityoz.com

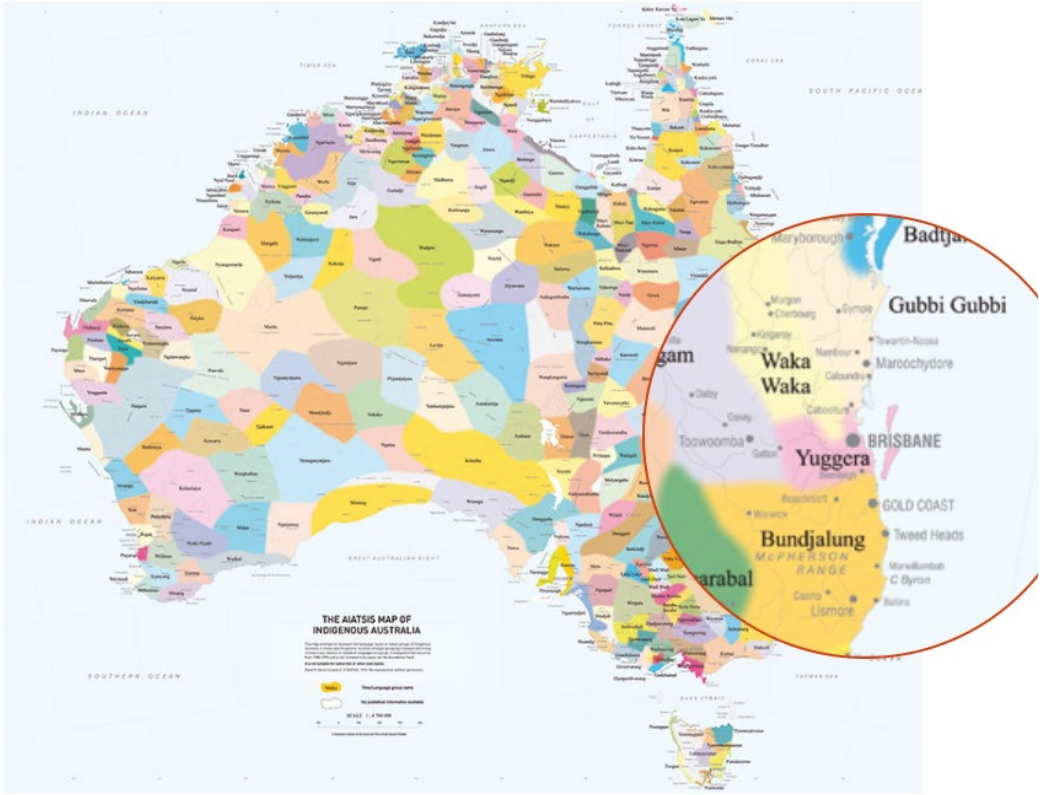
AccessibilityOz

Thank You to Our Sponsors and Hosts!

Without them, this conference couldn't happen.

Land acknowledgement

Acknowledge Yuggera as the traditional owners of this land.



This presentation is on the **AccessibilityOz Conferences page:** www.accessibilityoz.com/about/conferences

@accessibilityoz


Meet our team

- Dyslexia
- Moderate vision impairment
- Severe vision impairment
- Epilepsy
- Migraines
- Physical impairment
- Fibromyalgia
- Multiple Sclerosis
- Crohn's Disease
- PTSD
- Autism
- Long COVID


It’s not just about vision impairments

About Gian

1998

Worked on first accessible website in Australia

Created Australia's first automated accessibility testing tool

Invited Expert to W3C WCAG2 Working Group

Worked on Melbourne 2006 Commonwealth Games

Managed Usability and Accessibility Services at Monash University

@accessibilityoz

AccessibilityOz

Founded AccessibilityOz

AccessibilityOz

Released OzPlayer

OzPlayer

Released OzArt

OzART

Spoke at the United Nations on web accessibility

Inducted into the Australia's Hall of Fame as Accessibility Person of the Year 2019

Chair of Mobile Accessibility Testing Guidelines

2025

@accessibilityoz

AccessibilityOz

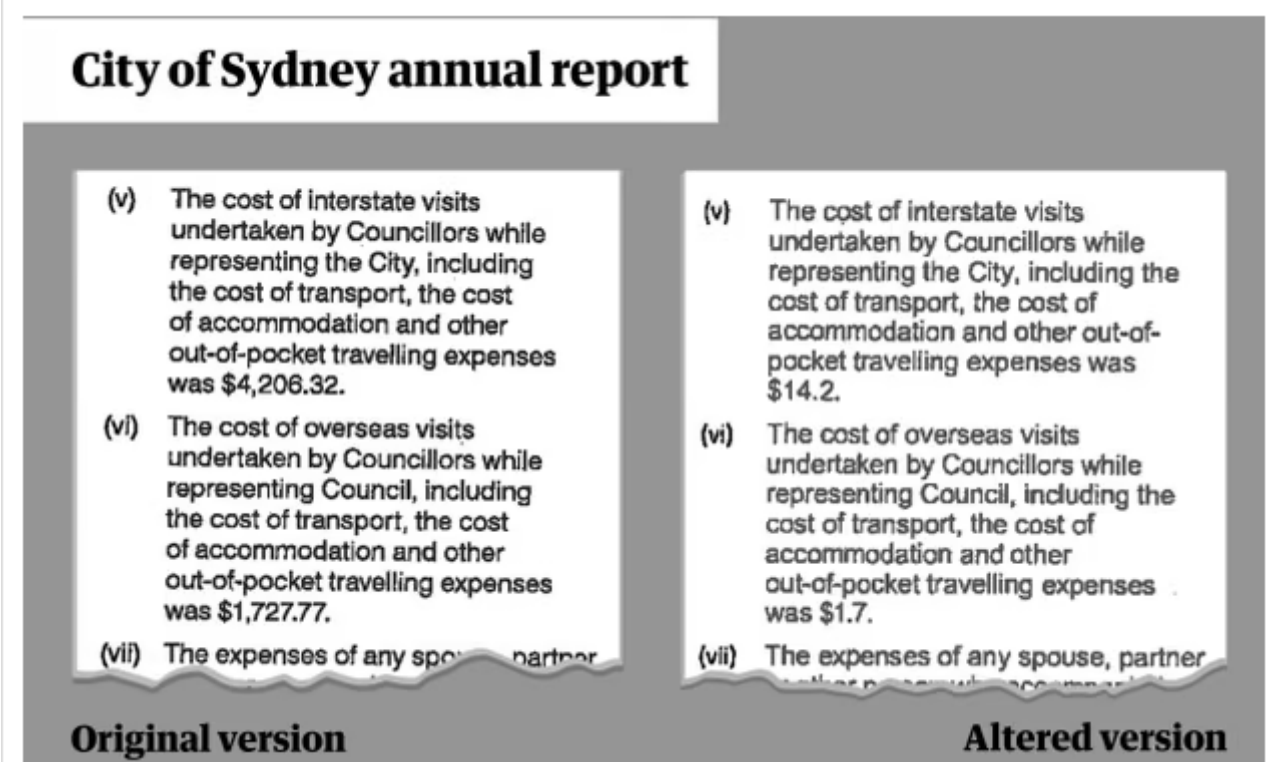
Let’s start with an anecdote…

The excuses for PDFs

Security

AccessibilityOz

PDFs and security



From The Guardian

DDA Web Advisory Notes

Some file formats provide **mechanisms for enhancing the security of documents** by preventing unauthorised editing, copying, or printing. **Some of these mechanisms are not compatible with accessibility for people with a disability**, and document authors should **ensure that security features do not prevent access to the document by assistive technology**.

DDA Web Advisory Notes

If there are concerns about ensuring the authenticity of material published on the web in multiple formats, then a **statement should be included that specifies which format is to be regarded as definitive or authorised**, and noting that additional formats are being provided to maximise access.

What's more secure than PDFs?

What about CAPTCHA?

1.1.1: Non-text Content

All non-text content that is presented to the user has a text alternative that serves the equivalent purpose, except for the situations listed below.

- **CAPTCHA**

  If the purpose of non-text content is to confirm that content is being accessed by a person rather than a computer, then text alternatives that identify and describe the purpose of the non-text content are provided…

1.1.1: Non-text Content

- … and alternative forms of CAPTCHA using output modes for different types of sensory perception are provided to accommodate different disabilities.

Every CAPTCHA is inaccessible

Yes, even Google’s one

Yes, even Google’s one

@accessibilityoz

Especially Google’s one

@accessibilityoz

And the W3C agrees

CAPTCHAs are a controversial topic in the accessibility community. As is described in the paper Inaccessibility of CAPTCHA, CAPTCHAs intrinsically push the edges of human abilities in an attempt to defeat automated processes. Every type of CAPTCHA will be unsolvable by users with certain disabilities. However, they are widely used, and the Web Content Accessibility Guidelines Working Group believes ***that if CAPTCHAs were forbidden outright, Web sites would choose not to conform to WCAG rather than abandon CAPTCHA***.

And the W3C agrees

This would create barriers for a great many more users with disabilities. For this reason the Working Group has chosen to structure the requirement about CAPTCHA in a way that meets the needs of most people with disabilities, yet is also considered adoptable by sites. Requiring two different forms of CAPTCHA on a given site ensures that most people with disabilities will find a form they can use.

And the W3C agrees

Because some users with disabilities will still not be able to access sites that meet the minimum requirements, the Working Group provides recommendations for additional steps. Organizations motivated to conform to WCAG should be aware of the importance of this topic and should go as far beyond the minimum requirements of the guidelines as possible.

What about audio CAPTCHAs?

Also inherently inaccessible:

- Most bots can interpret speech – so the audio is often distorted (and therefore inaccessible)
- Audio CAPTCHAs are one and done – it is transient whereas a visual CAPTCHA is not persistent (and therefore inaccessible)
- The method to turn on the audio CAPTCHA may not be accessible

Everyone convinced?

What is the alternative?

If you **must** have CAPTCHA:

- Provide more than two modalities of CAPTCHA for a given action (and make sure they work!);
- Provide access to a human customer service representative who can bypass CAPTCHA; and
- Do not require CAPTCHAs for authorized users.

It’s best to remove CAPTCHA altogether

What is the alternative to CAPTCHA?

Better alternatives:

- Multi-factor authentication
- Human test questions (e.g. Is fire hot or cold? Is grass green or purple?)
- Honeypot traps (fields that must be left blank, or the form is not submitted)
- Server-side spam filters and server-side validation

What is the alternative to CAPTCHA?

- Confirmation page (a screen after form submission that reads “Here is your information. Are you happy to submit this?”)
- Timestamp your forms (if the form is submitted faster than humanly possible, odds are it’s a spambot)
- Proof of work JavaScript code
- Heuristics of the user
- Limited-use accounts

Need to convince someone else?

https://tinyurl.com/a11y-captcha

@accessibilityoz

Let’s talk forms

@accessibilityoz

WCAG: paradoxical to security?

- 2.2.1: Timing adjustable
- 3.3.1: Error Identification
- 3.3.3: Error Suggestion
- 3.3.4: Error Prevention (Legal, Financial, Data)
- 3.3.7: Redundant Entry
- 3.3.8: Accessible Authentication (Minimum)

2.2.1: Timing adjustable

For each time limit that is set by the content, at least one of the following is true:

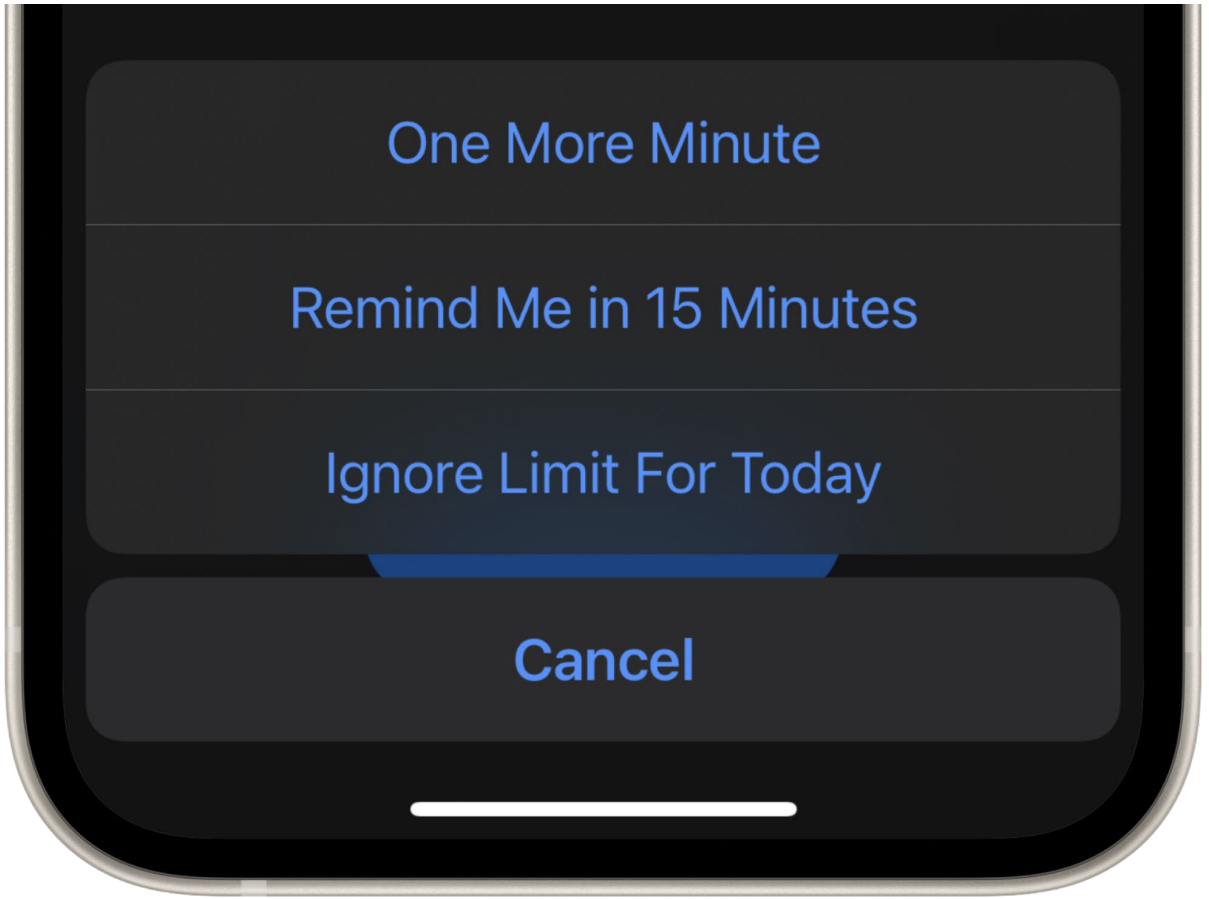
- **Turn off:** The user is allowed to turn off the time limit before encountering it; or
- **Adjust:** The user is allowed to adjust the time limit before encountering it over a wide range that is at least ten times the length of the default setting; or

2.2.1: Timing adjustable

- **Extend:** The user is warned before time expires and given at least 20 seconds to extend the time limit with a simple action (for example, "press the space bar"), and the user is allowed to extend the time limit at least ten times; or
- **Real-time Exception:** The time limit is a required part of a real-time event (for example, an auction), and no alternative to the time limit is possible; or

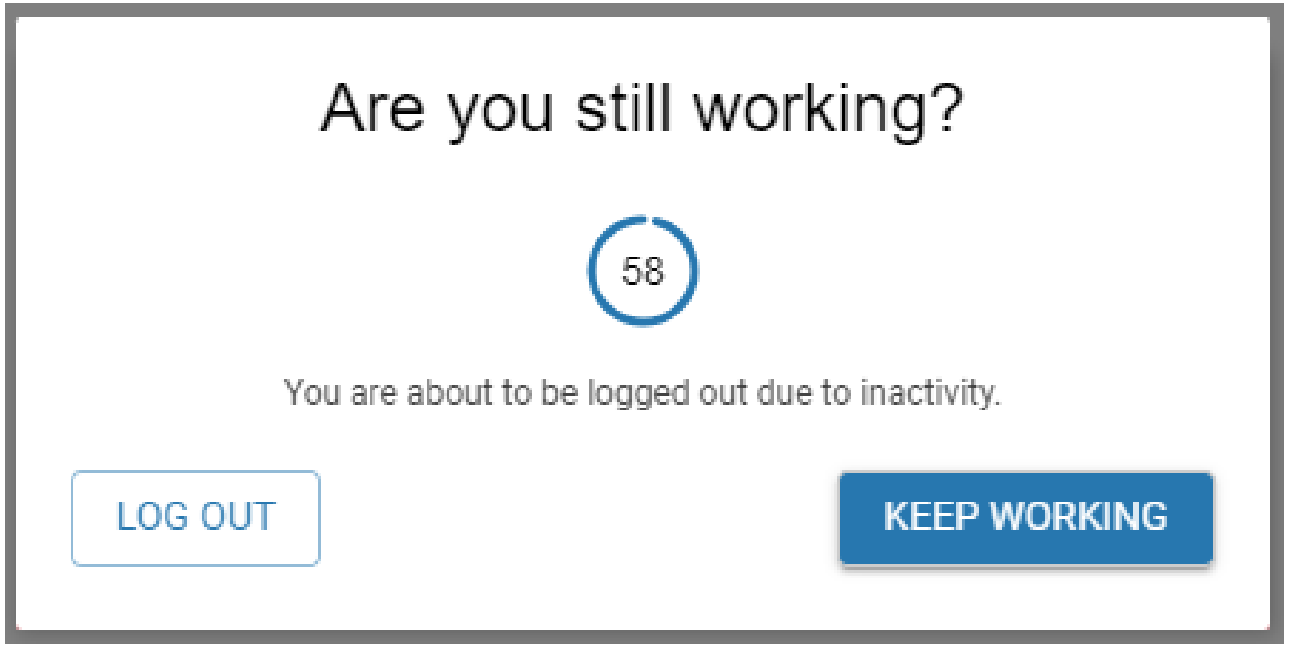
2.2.1: Timing adjustable

Provides both options to turn off or extend

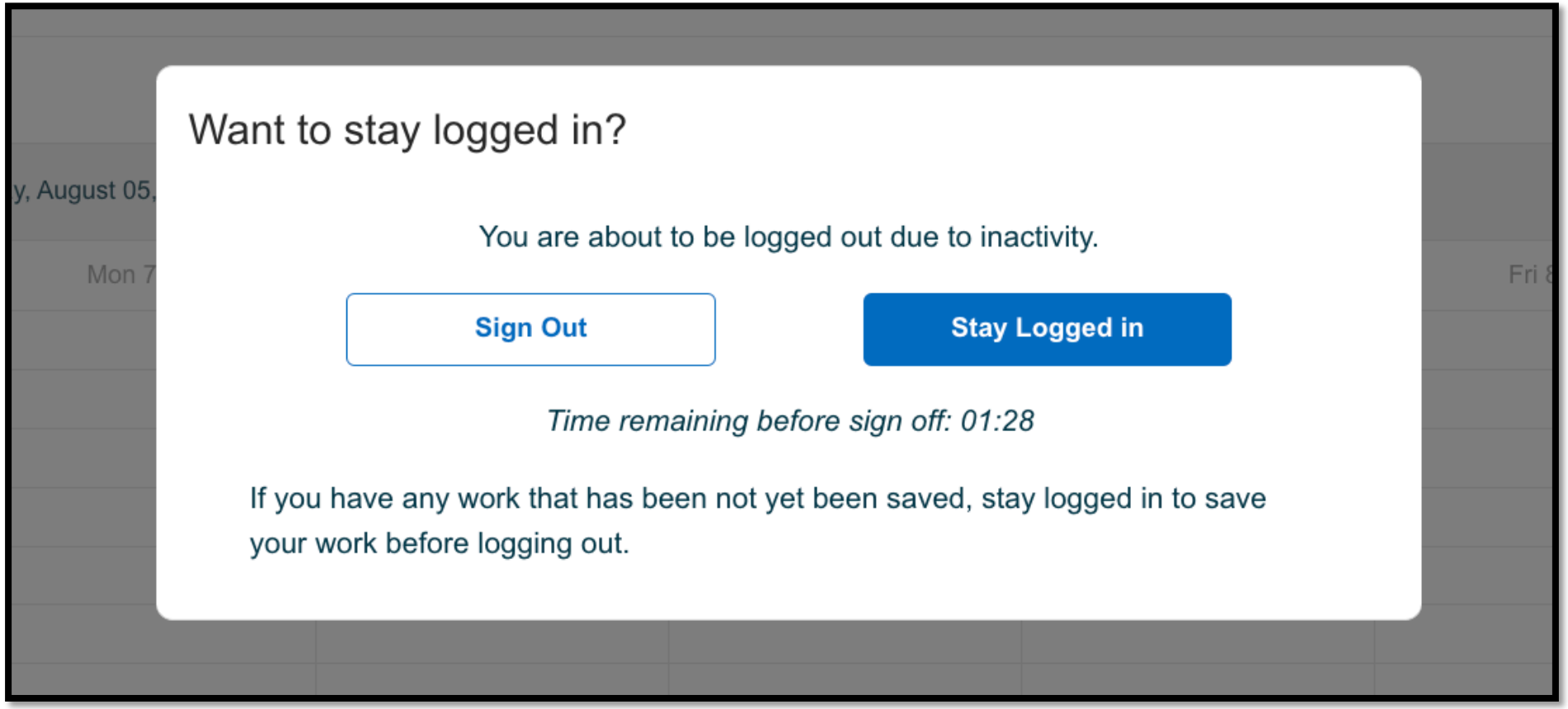


2.2.1: Timing adjustable

Provides option to extend



Provides option to extend



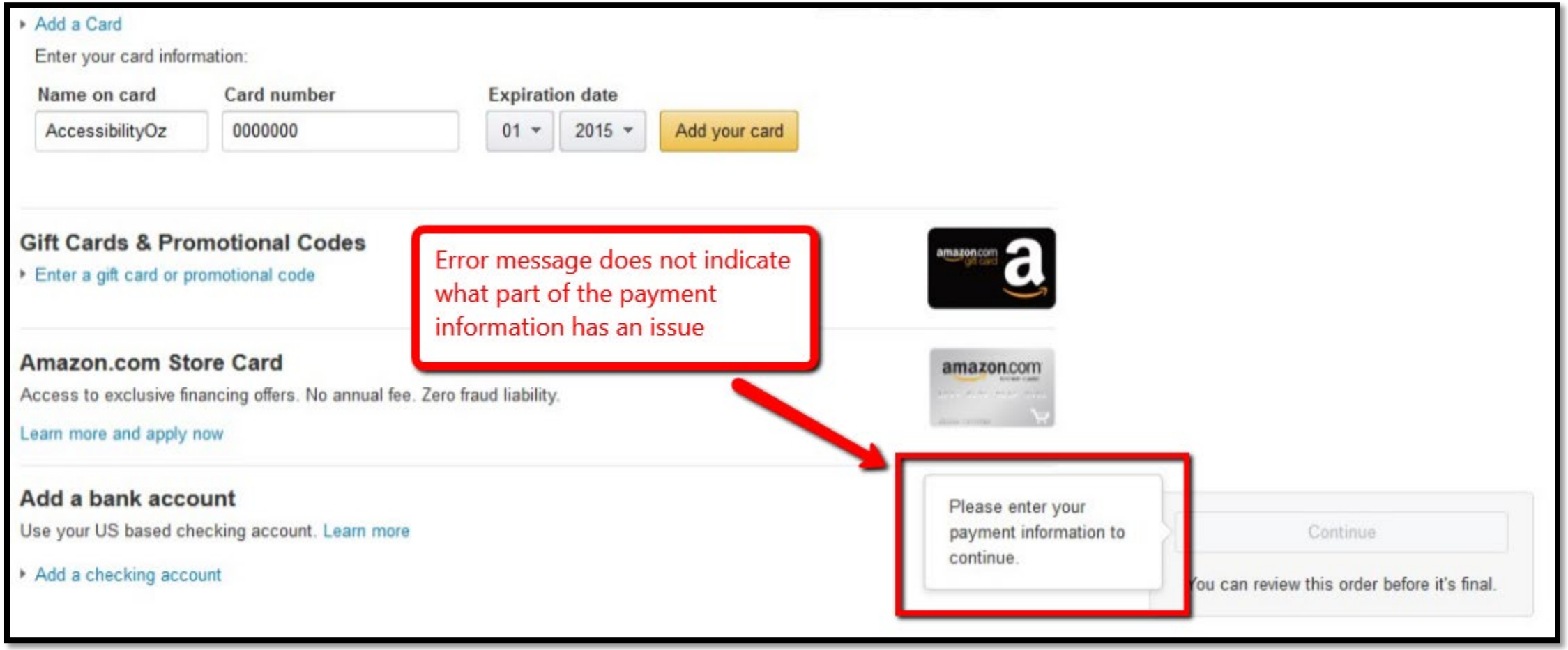
2.2.1: Timing adjustable

- **Essential Exception:** The time limit is essential and extending it would invalidate the activity; or
- **20 Hour Exception:** The time limit is longer than 20 hours.

3.3.1: Error Identification

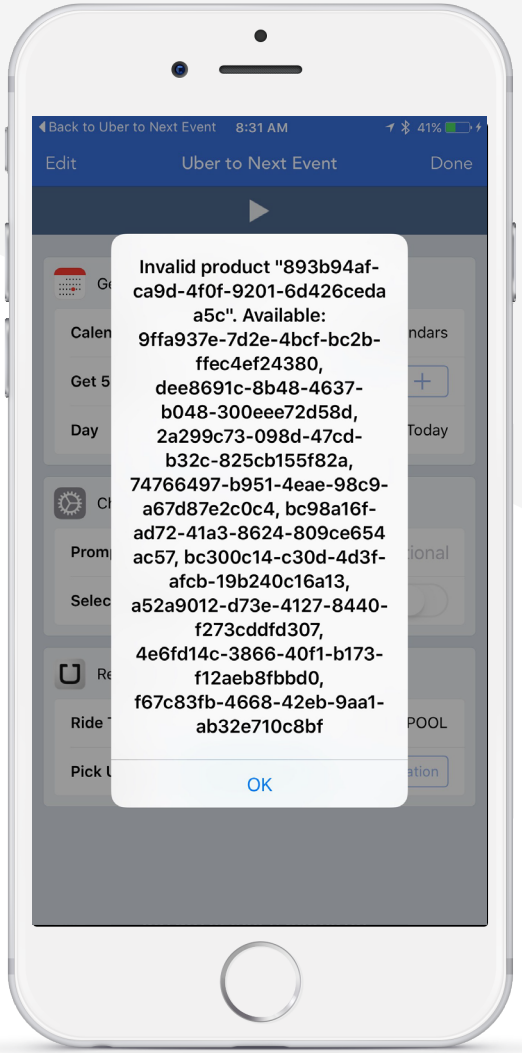
If an input error is automatically detected, the item that is in error is identified and the error is described to the user in text.

Try to give more information than this…



3.3.1: Error Identification

But definitely provide better information than this

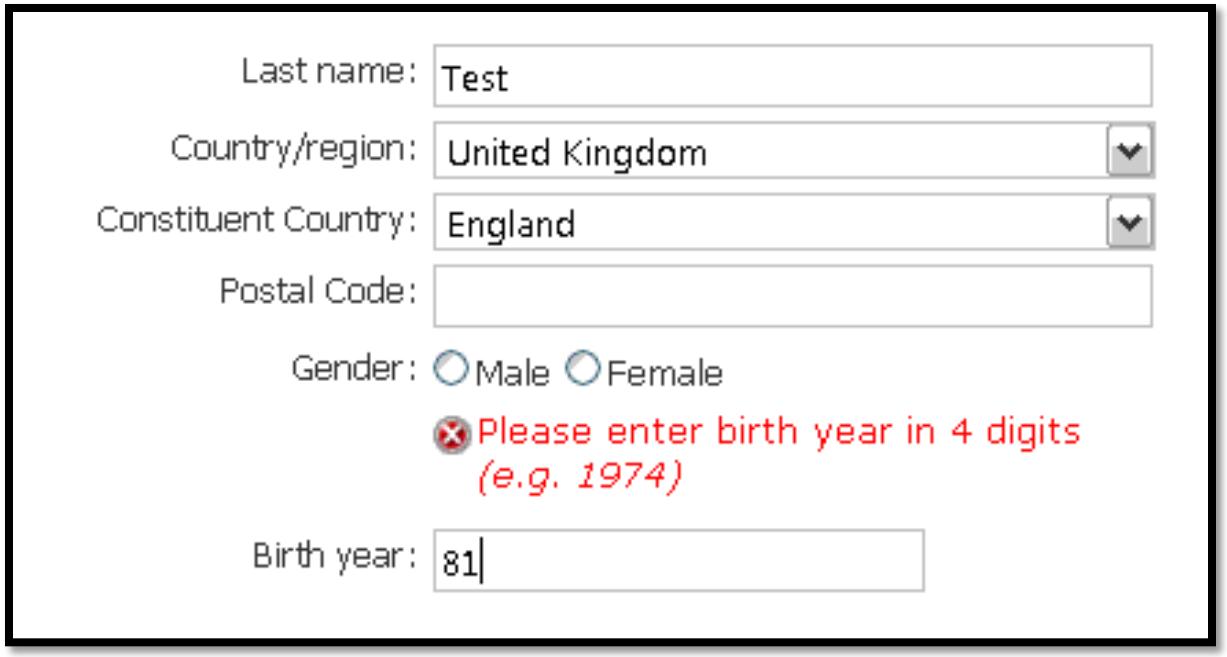


3.3.3: Error Suggestion

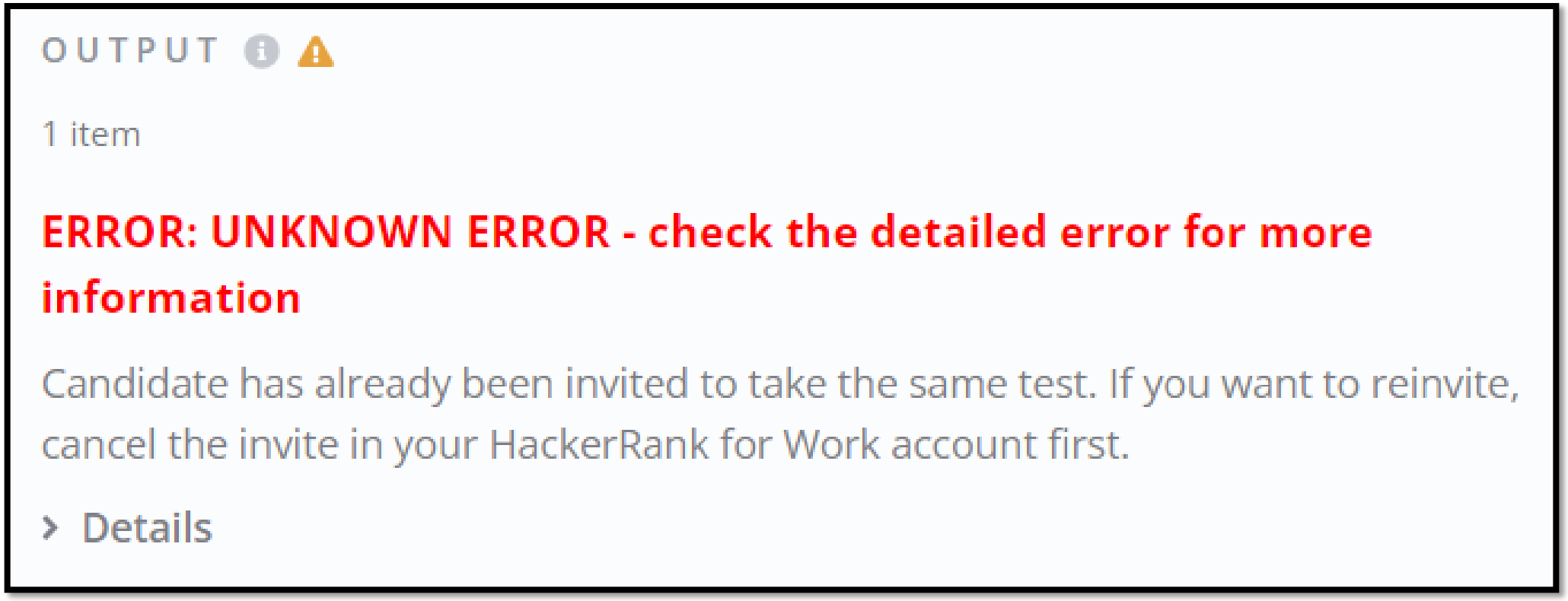
If an input error is automatically detected and suggestions for correction are known, then the suggestions are provided to the user, unless it would jeopardize the security or purpose of the content.

3.3.3: Error Suggestion

Use “for example” and / or provide details on input required



If it’s a common mistake…



3.3.4: Error Prevention (Legal, Financial, Data)

For web pages that cause legal commitments or financial transactions for the user to occur, that modify or delete user-controllable data in data storage systems, or that submit user test responses, at least one of the following is true:

- **Reversible**: Submissions are reversible.

3.3.4: Error Prevention (Legal, Financial, Data)

- **Checked**: Data entered by the user is checked for input errors and the user is provided an opportunity to correct them.
- **Confirmed**: A mechanism is available for reviewing, confirming, and correcting information before finalizing the submission.

3.3.7: Redundant Entry

Information previously entered by or provided to the user that is required to be entered again in the same process is either:

- auto-populated, or
- available for the user to select.

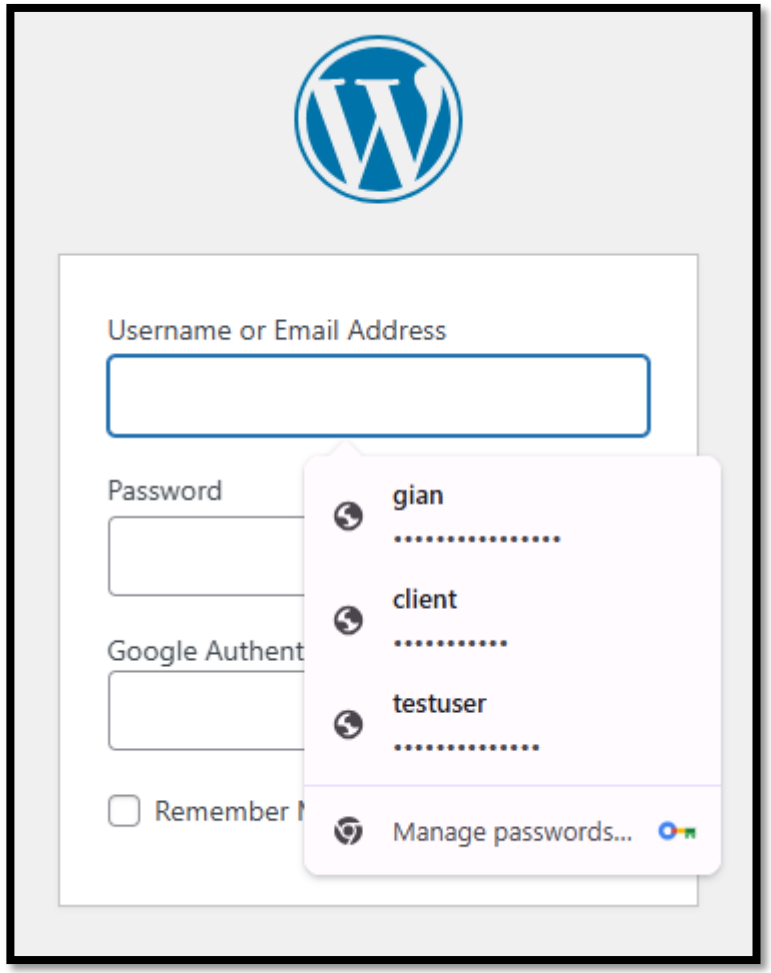
3.3.7: Redundant Entry

Except when:

- re-entering the information is essential,
- **the information is required to ensure the security of the content**, or
- previously entered information is no longer valid.

3.3.7: Redundant Entry

Use the <autocomplete> attribute



3.3.7: Redundant Entry

A cognitive function test (such as remembering a password or solving a puzzle) is not required for any step in an authentication process unless that step provides at least one of the following:

- **Alternative**: Another authentication method that does not rely on a cognitive function test.
- **Mechanism**: A mechanism is available to assist the user in completing the cognitive function test.

3.3.7: Redundant Entry

- **Object Recognition**: The cognitive function test is to recognize objects.
- **Personal Content**: The cognitive function test is to identify non-text content the user provided to the website.

Thank you for coming today

@accessibilityoz

AccessibilityOz

Access this presentation and all links at **www.accessibilityoz.com/about/conferences/**

@accessibilityoz

accessibilityoz.com

AccessibilityOz

enquiries
@accessibilityoz.com