Plan Overview

A Data Management Plan created using DMPonline

Title: An Empirical Study to Develop an Accessible Authentication Framework for People with Disabilities

Creator: David George Cropley

Principal Investigator: David G. K. Cropley

Data Manager: David G. K. Cropley

Project Administrator: David G. K. Cropley

Affiliation: Other

Template: DCC Template

ORCID iD: 0009-0000-1026-9239

Project abstract:

This research aims to develop a Framework to guide computer application developers in creating Accessible Authentication systems. In other words, the research investigates the under-researched area of making login systems easier for people with disabilities. Through two sets of interviews, with additional questionnaires to refine the data, the research empirically constructs a dataset to determine the extent of authentication issues among people with disabilities. It methodically analyses the data to produce a Framework that identifies patterns in problems and offers suggestions for improvement. As an additional measure, this research will be supported by a prototype application that demonstrates both the effectiveness of the Framework and its implementation. The first round of interviews (n=15) has already been conducted with participants with disabilities, with the intention of gathering first-hand information that will support the fundamental hypothesis that difficulties with logging in to systems, a process known as authentication, are compounded in some way due to their disability, making logging in much harder or impossible in some cases. The nature and extent of these problems have been analysed to provide empirical evidence that they are real, and a subsequent basic Framework has been developed to highlight the issues and suggest solutions. Background knowledge is built through a systematic review that highlights a distinct ‘usability problem’ in the field of Human-Computer Interaction (HCI), with direct ramifications for how we perceive and classify the usability of related HCI systems. This research tackles the problem head-on by demystifying it through empirical analysis, followed swiftly by suggestions for remediation via the Framework. A practical demonstration of the Framework's effectiveness is expected later in the work with the development of a prototype authentication application known as Authentibility.

ID: 209185

Start date: 22-01-2024

End date: 22-01-2031

Last modified: 06-08-2026

Copyright information:

The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customise it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan's text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal

An Empirical Study to Develop an Accessible Authentication Framework for People with Disabilities

Data Collection

What data will you collect or create?

1 set of interviews with people with disabilites (n=15) - includes participant agreement forms, audio recordings and transcripts - 2 GB of data (mp3 - so as comptible with NVivo, MS docx)
1 set of interviews with cybersecurity experts (n=15) - includes participant agreement forms, audio recordings and transcripts - esitimated 2 GB of data (mp3 - so as comptible with NVivo, MS docx)
1 set of surveys with people with disabilities (n=50) - includes survey answer sheets - esitmated 500MB of data (text|)
1 set of surveys with cybersecurity experts (n-50)- includes survey answer sheets- esitmated 500MB of data (text|)
NVivo analysis files for the data. Estimated 10GB+ by end of project in backups.
IBM SPSS files.
Saved in student BU OneDrive.
Existing peer-to-peer literature can be included. Estimated 2GB of PDF files.

How will the data be collected or created?

Interviews.
Online Surveys.
Literature Reviews.

Documentation and Metadata

What documentation and metadata will accompany the data?

Documentation will be via journals, conference and workshop papers, thesis synthesis and data repositories.

Ethics and Legal Compliance

How will you manage any ethical issues?

Ethical issues were presented to the ethics board at Bournemouth University and approval was granted before commencing.
All participants will be given anonymity.
Sensitive data is stored securely in the University OneDrive, and physical copies are kept in a locked safe.

How will you manage copyright and Intellectual Property Rights (IPR) issues?

Data will be anonomous and released open source in public repositories.

Storage and Backup

How will the data be stored and backed up during the research?

Electronic data is exclusively held in the University OneDrive.
Physical data is stored in a locked safe.

How will you manage access and security?

Question not answered.

Selection and Preservation

Which data are of long-term value and should be retained, shared, and/or preserved?

Data is kept until the completion and acceptance of the thesis; after that, all copies of the data will be destroyed, except those published under the anonymous guidelines.
Research impact can include improving accessibility for people with disabilities.

What is the long-term preservation plan for the dataset?

Question not answered.

Data Sharing

How will you share the data?

Raw identifiable data will never be shared.
Only anonymised data will ever be shared.
Anonymous data will be shared via the Bournemouth University BORDaR repository or academic publications, which will usually include DOIs.
Some data is already available and more will follow over the course of the research.

Are any restrictions on data sharing required?

Exclusive use of the raw data is expected to continue for no more than the duration of the research.
Interview participants agree to the use of the data as long as it remains anonymous.

Responsibilities and Resources

Who will be responsible for data management?

I, the researcher, David Cropley, remain solely responsible for implementing the DMP.

What resources will you require to deliver your plan?

No extra training or expertise is needed. I have attended the Data Management Researcher Development Programme at Bournemouth University and understand the implications.
BORDaR do not charge for their repository of data.
NVivo training and software, OneDrive access and funding for journal submissions are all provided by Bournemouth University as part of the PhD program.

Planned Research Outputs

Publication - "Challenges with Electronic Identity Authentication: A Qualitative Study with Participants with Disabilities"

The background to this research paper examines why people with disabilities often have additional problems with authentication (i.e., logging in to online services). While the primary focus is on accessible authentication, we also explore its relevance to electronic identification and consider the post-authentication stage of authorization (allowing continued use of a particular service once logged in). While people without disabilities regularly log into websites and applications without too much thought for the process, with an end-goal or task in mind to be achieved with the service that they are accessing, extra barriers exist for people with disabilities. We discover how there is a societal gap in terms of ease-of-use, as previous studies show that people with disabilities can find this step difficult, frustrating, or virtually impossible. For people who have a disability, complications will arise in this process, and we examine the nature of these problems identified by this group. A series of interviews (n = 15) is analyzed using Constructivist Grounded Theory methods to identify patterns in participants' responses and develop a theory explaining why Accessible Authentication is a problem. While aiming to follow a constructivist methodology, this paper categorizes common traits revealed by participants in interviews. The key findings reveal that most users with disabilities say that the ability to authenticate effectively is reduced by accessibility barriers; in other words, participants felt hindered when logging in because of their disability. This leads us to conclude, with some degree of confidence, that the data implies a lack of accessibility for users of traditional authentication systems. A further area of concern for the participants is that maintaining security alongside ease-of-use was important to them (albeit with no clear winner between usability and security preferences), so future work on improving accessibility should ensure that users with disabilities' information is not left vulnerable, while maintaining a sufficient level of accessibility for people with disabilities. Further to this, suggestions for achieving an accessible solution are presented in a preliminary Theoretical Framework.

Planned research output details

Title	DOI	Type	Release date	Access level	Repository(ies)	File size	License	Metadata standard(s)	May contain sensitive data?	May contain PII?
Challenges with Electronic Identity Authentication ...	10.3390/electronics15071476 ...	Publication	2026-04-01	Open	None specified		Creative Commons Attribution 4.0 International	None specified	No	No