



Inclusive Authentication & Account Recovery

A Practical Guide for Healthcare, Charity, and Security Professionals

Snow White

BSc (Hons) Ethical Hacking

2026

Note that Information contained in this document is for educational purposes.

1 WHO THIS GUIDE IS FOR

This guide is intended for:

- Healthcare professionals working with people living with Multiple Sclerosis (MS)
- Disability and digital inclusion charities
- Cybersecurity practitioners and system designers
- UX and service designers involved in authentication systems

No specialist cybersecurity background is required to use this guide.

2 WHY INCLUSIVE SECURITY MATTERS

People living with Multiple Sclerosis may experience:

- Cognitive fatigue or slowed processing
- Memory difficulties
- Motor or sensory impairments
- Fluctuating symptoms that vary day-to-day

Many authentication and account recovery systems unintentionally assume consistent attention, memory, and speed. These assumptions can create **both accessibility barriers and security risks**, such as:

- Increased susceptibility to phishing
- Repeated account lockouts
- Unsafe coping behaviours (e.g. password reuse, account sharing)

Inclusive security aims to reduce these risks **without weakening protection**.

3 COMMON RISKS TO WATCH FOR

When reviewing or designing authentication systems, be cautious of:

- **Time-limited codes** that expire too quickly
- **CAPTCHAs** that rely on visual, audio, or rapid interaction
- **Complex recovery flows** that require recalling information
- **Error messages** that are confusing, punitive, or inconsistent
- **Account existence indicators** that reveal whether a user is registered

These issues disproportionately affect users with cognitive or neurological conditions.

4 PRACTICAL DO'S AND DON'TS

Do

- Provide multiple authentication and recovery options
- Use clear, plain language at every step
- Allow retries without immediate lockout
- Explain what is happening during login or recovery
- Offer device-based or approval-based authentication where possible

Don't

- Rely solely on memory or transcription tasks
- Use CAPTCHAs as the only bot mitigation method
- Enforce strict time pressure without alternatives
- Penalize repeated mistakes without guidance
- Reveal whether an account exists through system responses

5 PRIVACY AND TRANSPARENCY

Inclusive systems should:

- Use uniform responses to avoid account detectability
- Minimize the personal data shown in alerts or emails
- Clearly explain how recovery and authentication processes work
- Avoid unnecessary data collection during recovery

These practices support user trust and align with privacy-by-design principles.

6 RELATIONSHIP TO STANDARDS AND RESEARCH

These recommendations align with:

- WCAG 2.2 Accessible Authentication success criteria
- Industry best practices in usable security
- Threat modelling methods (STRIDE and LINDDUN) adapted for accessibility

A full academic version of these guidelines, including threat mappings and methodology, is available alongside this guide.

7 FINAL NOTE

Although developed with a focus on Multiple Sclerosis, many of these recommendations are applicable to users with other cognitive, neurological, or fatigue-related conditions.

Inclusive security benefits **all users** by improving clarity, resilience, and trust.