

STRIDE Threat Analysis Table

Using the Level 1 DFD, I applied STRIDE to each core process. A key finding is that denial-of-service and spoofing risks disproportionately affect users with MS due to fatigue, cognitive fog, and motor challenges. As a result, the threat model prioritizes adaptive lockout thresholds, phishing-resistant authentication, and accessible recovery flows that reduce cognitive load without weakening security.

Based on level 1 DFD: P1 - P4

P1 - Registration

Stride Category	Threat Description	MS-Specific Impact	Mitigation Strategy
S - Spoofing	Attacker impersonates user during registration (e.g. phishing site collects credentials)	Cognitive fog or fatigue may reduce ability to detect fake registration pages	Use domain-bound passkeys, clear domain indicators, no password reuse, and simple anti-phishing cues
T - Tampering	Registration data altered in transit	User may not notice subtle changes due to fatigue or attention issues.	Ensure TLS, input validation, server-side integrity checks
R - Repudiation	User denies having registered an account	Memory difficulties may make confirmation unclear	Clear confirmation messages, optional confirmation email with accessible wording
I – Information Disclosure	Personal data exposed during registration	Increased risk if user relies on assistance from others	Minimise data collected, mask inputs, WCAG-compliant forms
D – Denial Of Service	Excessive failed attempts lock out registration	Fatigue may cause repeated errors, triggering lockout	Gentle rate-limiting, adaptive lockout thresholds, accessible error guidance
E – Elevate of Privilege	Attacker gains higher access during registration	User unlikely to detect abnormal behaviour	Server-side role enforcement, no client-side trust

P2 - Login / Authentication

Stride Category	Threat Description	MS-Specific Impact	Mitigation Strategy
S - Spoofing	Phishing steals login credentials or MFA approvals	Cognitive fatigue increases phishing susceptibility	Passkeys, phishing-resistant MFA, consistent login flows
T - Tampering	Login requests or responses modified	Errors may be misinterpreted by user	TLS, message authentication, secure cookies
R - Repudiation	User disputes having logged in	Memory issues may affect recall	Audit logs (D3), session history visible to user
I – Information Disclosure	Error messages leak account existence	May enable targeted scams	Generic error messages, no account enumeration
D – Denial Of Service	Lockouts from repeated failures	Motor or cognitive impairments increase error likelihood	Progressive lockout, alternative auth paths, recovery prompts
E – Elevate of Privilege	Compromised session tokens reused	User may not detect session hijacking	Secure session management, device binding, re-auth on risk

P3 - Account Recovery

Stride Category	Threat Description	MS-Specific Impact	Mitigation Strategy
S - Spoofing	Attacker initiates recovery pretending to be user	Recovery is cognitively demanding	Rate-limit recovery, CAPTCHA-free but behaviour-based checks
T - Tampering	Recovery token modified or replayed	User may struggle with time-sensitive codes	One-time tokens, expiry, server-side validation (D2)
R - Repudiation	User denies requesting recovery	Memory issues may cause confusion	Clear recovery confirmations and summaries
I – Information Disclosure	Recovery reveals account existence	Enables targeted attacks	Uniform recovery responses regardless of account status
D – Denial Of Service	Repeated recovery attempts lock user out.	Fatigue increases failed attempts	Allow multiple accessible recovery methods
E – Elevate of Privilege	Attacker completes recovery and takes over account	User may not detect takeover quickly	Post-recovery alerts, step-up authentication

P4 - Security & Session Management

Stride Category	Threat Description	MS-Specific Impact	Mitigation Strategy
S - Spoofing	Attacker triggers false security alerts	Can confuse or overwhelm users with MS	Clear , concise alerts with consistent wording
T - Tampering	Audit logs altered	Undermines trust and investigation	Write-once logs, integrity protection
R - Repudiation	User disputes lockouts or alerts	Cognitive fog may impair recall	Transparent logs, user-accessible activity history
I – Information Disclosure	Security alerts expose sensitive info	May increase reliance on others for help	Minimal disclosure in alerts
D – Denial Of Service	Over-aggressive security controls lock user outs	Disproportionately affects users with MS	Adaptive risk scoring, human-centred thresholds
E – Elevate of Privilege	Misconfigured sessions grant excessive access	Hard for user to notice	Least-privilege sessions, continuous validation