The Inclusive Awareness Framework: Security Training That Actually Works

Effective security awareness requires a fundamental redesign focused on inclusion, respect, and effectiveness:

1. Respect-Based Foundation

Treat employees as capable professionals with valuable expertise:

- Eliminate childish language and infantilising imagery
- Address employees as security partners rather than security problems
- Acknowledge the expertise and intelligence of your workforce
- Position security as a shared professional responsibility
- Create clear, straightforward guidance without condescension

Organisations using respect-based security communications may achieve higher engagement and behaviour change compared to patronising approaches.

2. Universal Design Implementation

Create security awareness that works for everyone:

- Develop multi-format content (text, video, audio, interactive)
- Ensure all materials work with assistive technologies
- Create equivalent learning experiences for different abilities
- Design for different cognitive processing styles
- Implement clear language and consistent navigation
- Test with diverse users including those with disabilities

Security awareness designed using universal design principles may achieve better knowledge retention across all employees.

3. Personalised Learning Pathways

Create multiple routes to the same security objectives:

- Provide options accommodating different learning styles (visual, auditory, kinaesthetic, reading/writing)

- Design for different cognitive processing (sequential, global, analytical, intuitive)
- Offer varying engagement levels (brief essentials, comprehensive deep dives)
- Create contextual learning opportunities embedded in workflows
- Allow self-paced options alongside structured courses
- Design for different attention spans and focus capabilities

Organisations implementing personalised security learning pathways may achieve higher behaviour change compared to standardised approaches.

4. Psychologically Safe Learning Environment

Create conditions where security learning flourishes:

- Eliminate all shame-based approaches
- Focus on improvement rather than perfection
- Treat mistakes as learning opportunities
- Implement anonymous reporting for concerns
- Create clear, consistent responses to security incidents
- Acknowledge that security is complex and errors inevitable

Organisations with psychologically safe security cultures may identify and address incidents faster than those using punitive approaches.

5. Outcome-Based Measurement

Measure what matters, not what's easy:

- Track security behaviour change rather than completion rates
- Measure reporting rates as indicators of psychological safety
- Evaluate knowledge retention across diverse user groups
- Assess participation equity across different demographics
- Monitor security incident trends as effectiveness indicators
- Calculate actual ROI based on security improvements

Organisations measuring security behaviour change rather than training completion may achieve better security outcomes.