CSIRO PUBLISHING

ORIGINAL ARTICLE
https://doi.org/10.1071/IB23065

Brain Impairment ASSBI

Co-developing 'The CyberABIlity Scale' to assess vulnerability to cyberscams for people with acquired brain injury: Delphi and cognitive interviews with clinicians and people with acquired brain injury

Jao-Yue J. Carminati[A,B,*], Jennie L. Ponsford[A,B] and Kate Rachel Gould[A,B]

For full list of author affiliations and declarations see end of paper

***Correspondence to:**
Jao-Yue J. Carminati
Turner Institute for Brain and Mental Health, School of Psychological Sciences, Monash University, Clayton, Vic. 3800, Australia
Email: Jao.Carminati@monash.edu

Handling Editor:
Cynthia Honan

Received: 3 August 2023
Accepted: 15 December 2023
Published: 29 January 2024

Cite this:
Carminati J-YJ *et al.* (2024)
Brain Impairment **25**, IB23065.
doi:10.1071/IB23065

ABSTRACT

Background. Although individuals with acquired brain injury (ABI) may be vulnerable to cyberscams, the lack of existing measures documenting cybersafety behaviours in people with ABI limits our understanding of ABI-specific risk factors, the frequency of this problem, and the ability to evaluate evidence-based interventions. *The CyberABIlity Scale* was developed to assess vulnerability in people with ABI via self-rated statements and practical scam-identification tasks. This study aimed to develop and refine *The CyberABIlity Scale* through feedback from clinicians and people with ABI. **Methods.** Scale feedback was collected via three rounds of clinician surveys ($n = 14$) using Delphi methods and two rounds of cognitive interviews with participants with ABI ($n = 8$). Following each round, feedback was quantitatively and qualitatively summarised, and revisions were made accordingly. **Results.** Key revisions included removing 12 items deemed irrelevant. Instructions and rating scales were revised to improve clarity. Cognitive interviews identified 15 comprehension errors, with further revisions made to support response clarity for participants with ABI. Clinicians and participants with ABI endorsed the content and face validities of *The CyberABIlity Scale*. **Conclusions.** Following further validation, *The CyberABIlity Scale* has the potential to be an effective screening measure for online vulnerability for people with ABI within clinical and research settings.

Keywords: acquired brain injury, cognitive interviewing, cyberscams, cybercrime, delphi method, measure development, validation.

Introduction

People become frequently socially isolated after sustaining an acquired brain injury (ABI; Ponsford *et al.* 2014). Online activities (e.g. social networking, online dating, email) may enhance social connection and information access after ABI (Vaccaro *et al.* 2007; Tsaousides *et al.* 2011; Brunner *et al.* 2015, 2019, 2020). However, the inherent risks and challenges of online engagement may be heightened for people with ABI (Brunner *et al.* 2021). Cognitive and communication impairments may create difficulty in using technology independently (McDonald *et al.* 2013; Charters *et al.* 2015), causing individuals with ABI to feel overwhelmed, confused and fatigued (Brunner *et al.* 2019, 2020). Furthermore, there may be increased vulnerability to online crime victimisation (Kilov *et al.* 2010; Tsaousides *et al.* 2011; Brunner *et al.* 2015, 2019; Gould *et al.* 2023*a*, 2023*b*).

Cyberscams are online crimes involving fraudulent online offers or other deceptive means designed to collect money or personal information (Australian Bureau of Statistics 2008). In Australia, over AU$3 billion was reportedly lost to scams last year (ACCC 2023), with significant emotional impact commonly experienced too (Whitty and Buchanan 2016). A survey of 101 clinicians and service providers found that 53.5% identified having at least one client with ABI who had been scammed (Gould *et al.* 2023*b*). Qualitative interviews with cyberscam survivors with ABI and close others (COs;

e.g. family members, friends) identified a range of risk factors relating to cognitive impairment, lack of scam awareness, feeling 'bored and lonely' and having an overly trusting and generous personality (Gould *et al.* 2023*a*).

To date, purported cyberscam risk factors for people with ABI remain theoretical and require objective investigation. To do so, a valid measure is required to assess risk factors of scams for people with ABI, to enhance our understanding of the frequency of cyberscams and to quantitatively evaluate evidence-based cyberscam interventions. An objective measure may also serve as a screening tool to identify at-risk individuals and support the early identification of potential risk factors that may be addressed through interventions. This is particularly crucial given scam self-discovery for people with ABI is difficult, with detection often dependent on family members or clinicians identifying scam red flags (e.g. family members becoming aware of money sent or of a love interest overseas) and initiating interventions (Gould *et al.* 2023*a*, 2023*b*).

Given the need for a valid measurement of scam susceptibility for people with ABI, our group examined the suitability of existing measures. *The Susceptibility to Scams Scale* is a five-item self-report measure developed to investigate scam risk in older adults without dementia (James *et al.* 2014) and with mild cognitive impairment (Han *et al.* 2016). This scale was piloted with participants with ABI ($n = 7$) and their COs ($n = 6$) as part of a previous qualitative study (Gould *et al.* 2023*a*) to assess suitability within an ABI group due to its brevity and previous use within groups with cognitive impairment. Four adapted items were additionally piloted to reflect ABI specifically (e.g. '*Persons with brain injuries or other disabilities are often targeted by con-artists*'). Participants reported that six of nine items were complex and lengthy, and the seven-point Likert scale options were difficult to differentiate (e.g. between *agree* and *slightly agree*). A disparity between theoretically understanding scam warning signs and behaviourally enacting practical responses to scams was also identified. This dissonance between 'knowing' and 'doing' has been seen in other tasks for people with ABI (e.g. an executive dysfunction task (Jovanovski *et al.* 2012)) and suggests a need for a more ecologically valid assessment.

Recent findings from novel investigations of cyberscam experiences for people with ABI (Gould *et al.* 2023*a*, 2023*b*) suggest that cyberscam risk extends beyond financial decision-making for people with ABI, with a range of psychosocial, cognitive and behavioural risk factors reported. For example, participants reported spending excessive time online due to a lack of work and hobbies (Gould *et al.* 2023*a*). Deficits in decision-making, judgement and theory of mind were also perceived to impact the identification of scammers' inauthentic intentions (Gould *et al.* 2023*a*). Therefore, other measures of financial risk within the general population (e.g. *Financial Exploitation Vulnerability Scale* (Lichtenberg *et al.* 2021) and *Susceptibility to Persuasion Scale* (Modic *et al.* 2018)) may lack appropriate scope. Although differences in cyberscam risk factors for those with and without ABI are not yet conclusive, different scam-type prevalence rates likely support this notion. Romance and dating scams are theorised to be the most common scam affecting people with ABI (Gould *et al.* 2023*a*, 2023*b*) and are likely underpinned by relationship breakdowns and reduced community participation, resulting in loneliness and a desire to seek social connection (Hawthorne *et al.* 2009). This pattern contrasts with financially-driven cyberscams, which make up the most common scam types in the general population and for those aged 65 years and older (e.g. investment scams, phishing, identity theft and threat-based scams) (ACCC 2023).

Taken together, this suggests that although existing scam measures that focus on risky financial decisions assess a proportion of risk factors relevant to people with ABI, important neuropsychological aspects of scam risk for people with ABI are not captured. To address this gap, we aimed to develop and pilot a new measure of vulnerability to cyberscams for people with ABI ('*The CyberABIlity Scale*') by considering existing measures, reviewing literature and developing new items based on ABI-specific scam research (Gould *et al.* 2023*a*, 2023*b*). The term 'cyberability' was coined by Gould and Brokenshire (2017), referring to perspectives of learning and adapting to new and emerging technologies (e.g. using the internet safely and responsibly).

Oftentimes, the systematic development of new measurement tools is not thoroughly and transparently reported on, risking ambiguity around the validity of tools and replicability (Flake and Fried 2020). Further focus must be placed on the way constructs are developed, particularly for new scales (Flake and Fried 2020), with their validity addressed via multiple studies that employ various methodologies systematically (Flake 2021). Pre-testing newly developed measures within a small sample of participants from the target population and those who have expertise in the field is a fundamental step in measure development (Boateng *et al.* 2018; Carpenter 2018), ensuring conceptualised items are meaningful and well-understood prior to larger-scale administration. Early qualitative input into scale development (e.g. through cognitive interviews) allows in-depth evaluation of the thought process of individuals completing the scale (Carpenter 2018), and this is particularly important for individuals with ABI who may have additional cognitive barriers to scale completion (Whiting *et al.* 2015; Miller *et al.* 2022). Unfortunately, a combined qualitative and quantitative approach to measure development is not commonly used or reported on, and a lack of in-depth qualitative pre-testing risks neglecting items that may stem from user and expert feedback as well as lived experiences (Carpenter 2018).

Therefore, this paper provides an in-depth report on the conceptualisation and development of *The CyberABIlity Scale*

through systematic and structured feedback from clinicians and people with ABI. Specifically, this study aimed to:

(1) Develop *The CyberABIlity Scale* based on consideration of existing cyberscam measures and generation of new items,
(2) Evaluate the relevance of the scale to assess face and content validity,
(3) Examine the accessibility of the scale to ensure instructions, items and rating scales are understandable to clinicians and people with ABI, and
(4) Conduct initial item reduction.

Methods

Design

Ethics approval was obtained from the Monash University Human Research Ethics Committee (Project #17984). This study was guided by best practice methods for measure development (Holmbeck and Devine 2009; Mokkink *et al.* 2010; Boateng *et al.* 2018; Carpenter 2018) and was conducted in three phases. In the first phase, items were generated by researchers with early input from people with ABI and their COs through the review of existing scales and the creation of new items. In the second phase, feedback from clinicians was obtained using the Delphi Method (Linstone and Turoff 2002): an iterative process that aims to reach expert consensus on constructs through a series of anonymous surveys. In the third phase, pre-testing with people with ABI was conducted using cognitive interviewing methods (think-alouds and verbal probing), and is presented in accordance with the Cognitive Interviewing Reporting Framework (Boeije and Willis 2013).

Phase one: initial scale development

Items were generated using a combination of deductive (e.g. review of relevant literature and existing scam measures) and inductive methods (research identifying domains of interest, e.g. Gould *et al.* 2023*a*, 2023*b*) (Hinkin 1995). Based on ABI and CO participant feedback on *The Susceptibility to Scams Scale* piloted as part of a previous qualitative study (Gould *et al.* 2023*a*), two items were revised and included. Mock scenarios ($n = 10$) for scam types identified as commonly impacting people with ABI were created as a practical and ecologically valid task based on real-life correspondences received from our research team and participants with ABI (Gould *et al.* 2023*a*). Additional items ($n = 48$) were created to address ABI-relevant scam risk factors from our recent qualitative interviews and survey findings (Gould *et al.* 2023*a*, 2023*b*). Collectively, items covered eight theorised risk factors: (1) past scam experience, (2) scam awareness, (3) understanding scam warning signs, (4) cognitive impairment, (5) trusting and generous personality, (6) availability of a trusted person, (7) meaningful engagement and (8) social isolation.

Phase two: clinician feedback

Participants

Twenty-two clinicians and service providers were invited to the study via email and were recruited from professional networks and an existing study database. An expression of interest form was sent to determine eligibility, whereby clinicians were eligible to participate if they were working with adults with ABI within Australasia, had at least 5 years' clinical experience and had self-rated expertise in at least one of the following areas: assessment of people with ABI, intervention/rehabilitation of people with ABI, psychological scale development and impact of cyberscams on people with ABI (see Table 1). Expertise was defined as a self-rating of ≥ 7 for knowledge (10 being high). One individual declined due to time constraints and seven did not respond. All clinicians who expressed their interest ($n = 14$) were eligible for participation. The final panel comprised 14 clinicians, consistent with the recommended sample sizes in Delphi literature (Delbecq *et al.* 1975; Okoli and Pawlowski 2004; Trevelyan and Robinson 2015). As summarised in Table 2, clinician participants were mostly female (86%) aged 32 − 57 years ($M = 44$ years, s.d. = 7.1 years) and worked in a range of disciplines, settings and locations.

Measures

Participant demographics were gathered via a questionnaire.

The pilot version of *The CyberABIlity Scale* comprised two parts. Part One entailed 50 statements regarding risky

Table 1. Clinician participant experience and self-rated expertise ($n = 14$).

	Expertise *n* (%)	Min	Max	Median (IQR)
Experience working with adults with ABI (years)		5	30	15 (10.8)
Knowledge of assessment for people with ABI (self-rating out of 10)	9 (64.3%)	4	9	8 (1.8)
Knowledge of intervention/rehabilitation for people with ABI (self-rating out of 10)	9 (64.3%)	4	9	8 (2.0)
Knowledge of psychological scale development (self-rating out of 10)	3 (21.4%)	3	9	6 (2.0)
Knowledge of cyberscams and how they affect individuals with ABI (self-rating out of 10)	5 (35.7%)	5	9	7 (2.0)

IQR, interquartile range.

Table 2. Clinician participant demographics ($n = 14$).

	n (%)
Gender	
Man	2 (14.3%)
Woman	12 (85.7%)
Residing state	
Victoria	9 (64.3%)
New South Wales	2 (14.3%)
Queensland	2 (14.3%)
South Australia	1 (7.1%)
Highest level of education	
Graduate diploma/certificate	1 (7.1%)
Bachelor's degree	3 (21.4%)
Master's degree	3 (21.4%)
Doctoral degree	7 (50.0%)
Occupation	
Neuropsychologist	4 (28.6%)
Occupational therapist	3 (21.4%)
Speech pathologist	3 (21.4%)
Recreational therapist	1 (7.1%)
Clinical psychologist	1 (7.1%)
Psychologist with endorsement in other area	1 (7.1%)
Social worker	1 (7.1%)
Settings working with adults with ABI[A]	
Solo private practice	5 (35.7%)
Group private practice	3 (21.4%)
Mental health centres	1 (7.1%)
Client's home	6 (42.9%)
Residential facilities/nursing homes	3 (21.4%)
Outpatient rehabilitation centre	4 (28.6%)
Research setting	4 (28.6%)
University training clinic	1 (7.1%)
Community health centres	1 (7.1%)
Schools and other educational/vocational facilities	1 (7.1%)
Practicing locations[A]	
Metro/urban	12 (85.7%)
Rural/remote	4 (28.6%)
Online (e.g. internet or telephone)	10 (71.4%)

[A]Total percentages may be greater than 100% as participants could select multiple options.

online thoughts and behaviours (e.g. '*I think only fools are scammed*') and safe online thoughts and behaviours (e.g. '*I stop and check it's safe before I click on links*'). Response options were on a five-point Likert scale from 1 (*strongly disagree*) to 5 (*strongly agree*). Part Two included examples of a scam ($n = 8$) and genuine correspondences ($n = 2$), for instance emails, text messages, online messages and phone transcripts. Respondents rated scenarios as real or a scam and their confidence in their rating on a five-point Likert scale (1 = *very confident this is a scam*, to 5 = *very confident this is real*).

Clinician feedback on *The CyberABIlity Scale* was collected using online surveys via Qualtrics (https://www.qualtrics.com). Participants were asked to rate aspects of the pilot scale. For example, in the first Delphi round, participants rated the clarity of instructions and the Likert-scale format for Parts One and Two from 1 (*very unclear/inappropriate*) to 5 (*very clear/appropriate*). Participants also rated the clinical relevance (to assess content validity (Mokkink *et al.* 2010)) of each scale item from 1 (*not at all clinically relevant*) to 5 (*very clinically relevant*). Clinical relevance was defined as '*the practical importance of an item. An item that is clinically relevant will have the ability to identify who's at risk of cyberscams and provide ideas on how to address/manage such risk/s*'. Participants provided qualitative feedback if they rated any area ≤3. Feedback was sought regarding additional risk factors that were important to include and the most appropriate timeframe for respondents to consider when rating statements. Participants also provided general feedback on the most appropriate number of items and their preferred scoring method (a cyber risk score and/or cyber safety score; total score or subscale scores). Online surveys were revised at each Delphi round based on scale revisions and clinician consensus.

Procedure

Guided by other Delphi studies, it was decided *a priori* to conduct a maximum of three Delphi rounds (Boulkedid *et al.* 2011). If consensus was not obtained following round three, a modified Delphi approach (Fink *et al.* 1984) would be adopted, whereby clinicians would meet to discuss and reach a final consensus in real-time. Clinician participants were sent the online survey link via email and had 3 weeks to complete each survey. Using Microsoft Excel (Microsoft Corporation, https://office.microsoft.com/excel), the frequency of responses at each Likert-scale level was summarised. The two highest (4 or 5) and two lowest (1 or 2) points on the Likert scale were grouped. Expert consensus was defined as 80% or more participants rating in a similar way. This was similar to other Delphi studies (Stanyon *et al.* 2017; Wong *et al.* 2019; Carrier *et al.* 2022) and consistent with a systematic review of Delphi literature identifying a median consensus threshold of 75% (Diamond *et al.* 2014). For items that did not reach consensus, qualitative feedback provided by participants was used to revise the scale. Revised items were included in a follow-up survey sent to participants 3 weeks later. A summary of response

frequencies and de-identified qualitative feedback was sent to participants alongside the follow-up survey. Participants were asked to re-rate areas in consideration of de-identified group feedback. This procedure was repeated for round three, and further revisions were made. The Delphi process was concluded following round three as consensus was reached.

Results

Delphi round one. The instructions and response options for Parts One and Two of *The CyberABIlity Scale* did not reach 80% consensus regarding clarity and appropriateness (71.4–78.6%) and qualitative feedback recommended simplification. Regarding response options, clinicians indicated the need for clearer distinctions between points 1 and 2 (i.e. 'Strongly Disagree' and 'Disagree') and 4 and 5 (i.e. 'Agree' and 'Strongly Agree'). Rating scales were therefore revised to a three-point Likert scale (e.g. 'Don't Agree', 'Somewhat Agree', 'Definitely Agree'). Formatting of the response options to include icons and colours was suggested to improve accessibility.

As summarised in Table 3, of the 50 total items in Part One of *The CyberABIlity Scale* (self-rated statements), 37 items obtained consensus (>80%) regarding clinical relevance, including 13 items obtaining 100% agreement. Of the 13 items that did not reach consensus, nine items were removed, as feedback indicated the relevance of items was unclear or items were too broad or complex. The remaining four items that did not reach consensus were revised based on feedback. For example, for the item '*I jump into things without careful judgement*', feedback to simplify the language and make the item more online specific resulted in the revised item '*I jump into things online without thinking*'. One new item was added to the scale ('*I have loaned money to someone I met online*'). Of the 10 total items in Part Two of *The CyberABIlity Scale* (scam scenarios), there was 100% agreement that items were clinically relevant.

Consensus was not reached regarding the most appropriate timeframe for scale respondents to consider. Clinicians variously indicated preferences for 1 week (21.4%; providing feedback that this was most sensitive to change), 1 month (57.1%; as this was recent enough to support recall whilst allowing for normal variations in time spent online), 3 months (14.3%; reporting some clients to be infrequently online) and no timeframe (7.1%; with feedback that a timeframe added unnecessary complexity).

Delphi round two. Thirteen of the original 14 clinician participants (92.6%) completed round two. In the second Delphi survey, clinicians were asked to re-rate revised instructions and rating scales, five items from Part One (four revised and one new item), and the scale timeframe.

Although the instructions for past scam experience items did not reach consensus regarding clarity (76.9%), the new response options were deemed appropriate (92.3%). Neither the instructions nor the response options for the remainder of Part One (scam risk factors) obtained consensus (69.2% each). Both the instructions and response options for Part Two (mock scam scenarios) reached consensus (100% and 92.3% respectively). Qualitative feedback indicated the low ratings were due to concerns regarding the comprehension abilities of people with ABI completing the scale. The next phase of the study was to directly assess comprehension with people with ABI. Therefore, language was simplified but clinicians were not asked to provide further feedback on these revisions.

As summarised in Table 3, of the five new items proposed in round two, three reached consensus (84.6–100%). The two new items that did not reach consensus were removed from the scale based on qualitative feedback indicating a lack of relevance.

As per round one, consensus was still not met regarding the most appropriate timeframe for scale respondents to consider, with clinicians indicating a preference for 1 month (76.9%), 3 months (15.4%) and no timeframe (7.7%). Similar to round one, clinicians who preferred a 1-month timeframe provided feedback that this timeframe balanced sensitivity to change (due to variations in time spent online) whilst being recent enough to support recall of events. Clinicians endorsing the 3-month timeframe felt 1-month may miss important identifying information should their client infrequently engage in online behaviour.

Delphi round three. Twelve of the original 14 clinician participants completed round three (85.7%). In the third Delphi survey, clinicians were asked to re-rate their preferred timeframe for survey responders to consider. Consensus was reached, with 100% of clinicians indicating a preference for a 1-month timeframe, suggesting this was likely the most appropriate timeframe balancing recency of events with variability in online activities.

Additional feedback. Additional feedback was sought from clinicians regarding scale formatting, length and scoring preferences. Consensus was not sought in these areas as they captured preferences only. Twelve participants requested a digitised scale option. Most clinicians indicated a preference for Part One of the scale to be 10–20 items (84.6%), and Part Two to be 5–8 items (61.5%). Regarding scoring, most clinicians indicated a preference for a separate score for Parts One and Two of the scale (92.9%). Within this, clinicians disagreed regarding their preference for scores to be framed as a cyber safety score (i.e. higher scores indicating higher safety; 7.7%), cyber risk score (i.e. higher scores indicating higher risk; 23.1%) or both a cyber safety and risk score (61.4%). Final decisions regarding scale length and scoring will be guided by future stages of scale development, and the majority clinician preference will be considered.

Table 3. Summary of Delphi consensus of the CyberABIlity scale: Part One items.

Item	Round 1: clinical relevance consensus (%)	Round 1: response to feedback[A]	Round 2: clinical relevance consensus (%)	Round 2: response to feedback[A]
1. I have given money to a stranger online or over the phone	92.9			
2. I have given my personal information (e.g. username, password, date of birth) to a stranger online or over the phone	85.7			
3. I have been in an online romance scam	100			
4. I have given my banking information to a stranger online or over the phone	85.7			
5. I have been scammed online before	100			
6. Someone else has told me that I've been scammed	78.6	Revised for Delphi 2: Others have told me I've been scammed	92.3	
7. I think only fools are scammed	85.7			
8. I know where to find information about staying safe online	78.6	Revised for Delphi 2: I look for information about using the internet safely	61.5	Item removed
9. I think online dating is safe	92.9			
10. The internet is a pretty safe place	92.9			
11. There are dangers to being online	85.7	Rephrased: There are dangers to using the internet.		
12. I believe anyone can be scammed	92.9			
13. Because of my age, background or condition, I am at higher risk of being scammed (Please specify your condition)	64.3	Item removed		
14. People with brain injury/other thinking problems are at higher risk of being scammed	78.6	Item removed		
15. I have a good understanding of what cyberscams are	100			
16. It's possible to be scammed several times	71.5	Item removed		
17. People may not be who they say they are online	92.9			
18. I try to use strong privacy settings online	85.7			
19. I'm interested in learning more about how to stay safe online	92.9			
20. I'm careful when I share personal information online	92.9			
21. I'm suspicious of businesses calling me unexpectedly	92.9			

(*Continued on next page*)

Table 3. (*Continued*)

Item	Round 1: clinical relevance consensus (%)	Round 1: response to feedback[A]	Round 2: clinical relevance consensus (%)	Round 2: response to feedback[A]
22. It's unusual to be asked to pay for a bill with a gift voucher	85.7			
23. It's normal for someone I'm talking to online to not have a bank account	78.6	Item removed		
24. I go with my gut feeling when I think something online is not quite right	71.4	Item removed		
25. I find it difficult to remember new information I have learnt about online safety	78.6	Item removed		
26. I might think something is a scam, but I still go along with it anyway	78.6	Revised for Delphi 2: I might think something is a scam but I keep going	84.6	Rephrased: I might think something is a scam but I keep going with it anyway.
27. If I think something is a scam, I stop being involved	78.6	Item removed		
28. If something sounds too good to be true, it's probably not true	78.6	Item removed		
29. I often seek new, exciting experiences	71.4	Item removed		
30. I stop and check it's safe before I click on links	92.9			
31. I click on links and emails without thinking	92.9			
32. I jump into things without careful judgement	78.6	Revised for Delphi 2: I jump into things online without thinking	76.9	Item removed
33. I have quite a trusting personality	100	Rephrased: I trust people easily		
34. I am suspicious of strangers online	92.9			
35. I find it hard to say no to a stranger when they ask for my help	100			
36. If I make a mistake online, I'm usually too embarrassed to tell anyone about it	100			
37. If something doesn't look right, I check with someone first	85.7	Rephrased: If something doesn't look right online, I check with someone first		
38. I have someone I trust to ask for help with online safety	100			
39. I feel comfortable asking someone for help to check if something is safe online	92.9			
40. I spend a lot of time online	92.9			

(*Continued on next page*)

Table 3. (*Continued*)

Item	Round 1: clinical relevance consensus (%)	Round 1: response to feedback[A]	Round 2: clinical relevance consensus (%)	Round 2: response to feedback[A]
41. I have close friends who I talk to and see in person on a regular basis	78.6	Item removed		
42. I don't have many close friends who I regularly talk to or see in person	92.9			
43. I have hobbies, special interests or belong to a club	92.9			
44. My night times are usually spent online	100			
45. I feel lonely	100	Rephrased: I often feel lonely		
46. I use online dating sites	100	Rephrased: I regularly use online dating sites		
47. I enjoy chatting to strangers online	100			
48. I actively look for strangers to chat to online	92.9			
49. I often use online dating sites to look for relationships	100	Rephrased: I use online dating sites to look for relationships		
50. Most of my friends are online friends who I haven't met in real life	100			
		New item: I have loaned money to someone I met online	100	

[A]Items with no outcome listed were unchanged.

Phase three: ABI participant feedback

Participants

Eight participants with ABI were recruited via an existing project database ($n = 5$), an ABI support organisation ($n = 1$) and referrals from clinicians ($n = 2$). Participants with ABI were eligible if they were aged ≥18, living within Australia, had a non-degenerative ABI (any time post-injury) and were fluent in English. As summarised in Table 4, participants with ABI were five men and three women, between 25 and 65 years of age ($M = 44$, s.d. = 14.30) who had sustained a moderate to severe ABI of various causes 3–39 years prior ($M = 13.75$, s.d. = 12.50). The sample size was consistent with cognitive interviewing recommendations of 5–15 interviews (Beatty and Willis 2007) and aimed to capture a range of scam experiences (participants who had and had not experienced cyberscams). All participants provided either written or audio-recorded informed consent.

Measures

Participant demographics were gathered via a questionnaire.

A semi-structured interview schedule was developed to guide cognitive interviews with people with ABI. Participants were instructed to verbalise their thought process aloud whilst completing *The CyberABIlity Scale* and were given general prompts as required (e.g. '*Can you tell me why you chose that answer?*'). Probing questions (see Supplementary Appendix A) were generated and used where further detail was required. Probing questions were developed based on Tourangeau's *et al.* (2000) four-stage model describing cognitive processes of responding: (1) comprehension (assessing accurate understanding and comprehension of items), (2) retrieval (participants' ability to recall information as relevant to the item), (3) decision (participants deciding on a response with appropriate mental effort) and (4) response (participants' understanding of the rating scale and ability to map their decision onto the provided responses). Participants were also asked to provide general feedback on the scale, including assessing face validity (e.g. '*What do you think this survey is measuring?*'), overall feedback (e.g. likes and dislikes of the scale, opinion on the scale length) and their experience in completing the scale (e.g. whether items triggered discomfort).

Procedure

Cognitive interviews were conducted between March and May 2022 and were between 50 and 72 minutes in duration ($M = 57.63$ min). Participants took part in one individually conducted interview. The interviewer (JC) was a doctoral student in clinical neuropsychology who was trained in interviewing. Interviews were conducted via videoconference, audio recorded and externally transcribed ($n = 5$) or transcribed by JC ($n = 3$). Identifying information was removed from transcripts. The interviewer maintained a reflective journal with interview observations.

Table 4. ABI participant demographics ($n = 8$).

	n (%)	*M*	s.d.	Range
Age at interview (years)		44	14.30	25–65
Gender				
Man	5 (62.5%)			
Woman	3 (37.5%)			
Residing state				
Victoria	8 (100.0%)			
Living situation				
Living alone	2 (25.0%)			
Living with spouse/ family	5 (62.5%)			
Share house	1 (12.5%)			
Highest level of education				
Year 9	1 (12.5%)			
Year 11	1 (12.5%)			
Completed high school	2 (25.0%)			
Graduate diploma/ certificate	3 (37.5%)			
Bachelor's degree	1 (12.5%)			
Years of formal education		15.13	3.44	10–19
Cause of ABI				
Hypoxic brain injury	1 (12.5%)			
TBI – motor vehicle accident	3 (37.5%)			
TBI – fall	1 (12.5%)			
Illness	1 (12.5%)			
Substance-related	1 (12.5%)			
Unknown	1 (12.5%)			
Estimated Injury severity				
Moderate	3 (37.5%)			
Severe	5 (62.5%)			
Years since injury		13.75	12.50	3–39
Current funding				
NDIS	5 (62.5%)			
TAC	3 (37.5%)			
Scam experience by type				
No scam experience	2 (25.0%)			
Near-scam experience	1 (12.5%)			
Dating/romance scam	3 (37.5%)			
Remote access scam	4 (50.0%)			
Sexual extortion	1 (12.5%)			

ABI, acquired brain injury; TBI, traumatic brain injury; NDIS, National Disability Insurance Scheme; TAC, Transport Accident Commission.

Microsoft Excel (Microsoft Corporation, https://office.microsoft.com/excel) was used to summarise the descriptive statistics for participant demographics. Interview transcripts were managed using NVivo (ver. 12.5.0, QSR International, https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home) whereby participant responses were summarised descriptively to capture the performance for each of the four stages of Tourangeau's *et al.* (2000) model. For example, comprehension errors or difficulty choosing a response option were identified and grouped based on common meaning. Five of the total eight interviews were first completed, and identified errors were discussed between all authors with relevant revisions made to the scale. The remaining three of the total eight interviews were then conducted, and again, revisions were made. The study ceased following a total of eight interviews as no new feedback was reported by participants.

Results

Cognitive interviews: round one. In the first round of cognitive interviews ($n = 5$), seven comprehension errors, one retrieval error and four response errors were identified. Table 5 summarises identified errors and resulting revisions to the scale and includes representative participant quotes. Comprehension difficulties related to terms such as 'bill', 'online dating site' and 'online romance scam'. There was some confusion regarding whether a near-scam experience was classified as being scammed and whether smartphone applications were classified as online or over-the-phone activities. Participants were sometimes unsure whether to consider their answers specific to online or face-to-face interactions.

Overall, participants were able to appropriately recall information from the past month as relevant to scale items and provide examples of thoughts/behaviours leading to their response. Some participants answered outside of the 1-month timeframe on several items; however, after reminders, this difficulty was no longer observed. Several participants recalled further scam experiences throughout the scale completion that were not recalled at the interview outset; however, in all instances, this only provided further evidence of prior scam experience and did not change ratings of previously completed items.

Participants occasionally displayed difficulty understanding the response options; however, this was resolved with further explanation. Some participants answered items in an inverse manner (e.g. endorsing the behaviour but responding with 'disagree') but appropriately self-corrected their response with further time or after prompting. Participants deemed several items not personally relevant and therefore displayed difficulty answering these items. Participants understood scale instructions and had no difficulty completing scam scenario items. Participants were able to appropriately identify and explain potential warning signs for each mock scam scenario (e.g. P1: '*Anything to do with Bitcoin…is like a red flag straight away*'). Participants were able to map their responses onto the Likert scale appropriately and differentiate responses between, for example, 'Somewhat Agree' and 'Definitely Agree'.

Cognitive interviews: round two. The remaining three of eight participants were interviewed in round two. Three comprehension errors and one response error were identified. As summarised in Table 5, comprehension errors affected terms such as 'online', 'privacy settings' and 'connection'. Participants six and seven did not display any difficulty mapping their responses onto the three-point Likert scale and provided positive feedback regarding the response options: '*Choice of three was…really good because it was a yes, no, or maybe, whereas a lot of surveys are a choice of five and you sometimes get stuck between three and four*' (P7). Although participant eight was able to appropriately respond to all items, he reflected that three Likert-response choices were potentially too limiting to the way he would have preferred to answer items: '*I would tend to answer things in a slightly more granular style than the three answers*' (P8). No other challenges were reported or observed; participants understood scale instructions, responded appropriately within the 1-month timeframe and interpreted items as intended.

General feedback. All participants with ABI were able to explain in their own words what the scale intended to measure, confirming face validity: '*For me, it's like, do I understand what a scam is, and am I vulnerable to them?*' (P1). Participants were forthcoming in answering questions and reportedly experienced only mild discomfort for some items (e.g. '*I feel lonely*'). All participants were nonetheless agreeable to answer all items. Based on qualitative observations recorded in the interviewer's journal, participants were observed to put in sufficient effort in answering scale items and did not appear to answer in a socially desirable manner. This was indicated by participants sharing personal and sensitive explanations of their responses.

Three participants had a preference to complete the scale digitally, three by paper and pen, and two participants had no preference. Two participants noted that they would like support from their carers when completing the scale. Six participants reflected that the current length of the scale was appropriate, and two participants recommended shortening the scale but were not able to suggest any specific number of items or preferred amount of time required to complete the scale.

Discussion

This study described the conceptualisation and development of a novel and tailored measure of cyberscam vulnerability, *The CyberABIlity Scale,* with feedback from clinicians and people with ABI. Through five rounds of item development

Table 5. Summary of cognitive interview feedback of the CyberABIlity scale.

Error/difficulty description	Example from participant interview	Reported by	Response to feedback
Comprehension errors			
Interpreted 'bill' as any required payment, rather than an invoice as intended.	'*Unless it's from that shop that you buy it with then maybe you can use that [gift voucher] to cheapen the price a bit.*' P3	P1, P3	Added specific examples to item: '*It's unusual to be asked to pay for a bill (e.g. internet, electricity, taxes) with a gift voucher*'
Confusion regarding whether a social networking site (e.g. Facebook) used with the intention of dating was classified as an online dating site.	'*I suppose I'd have to agree with that 'cause I'm on one on Facebook so, but not online dating sites anymore.*' P5	P5	Revised wording to capture social networking site use with the intention of dating: '*I use online sites for dating or social connection*'
Required clarification that 'others' referred to 'other people'. Did not consider family members as part of 'others'.	*Item: … Others have told me I've been scammed.* *P3: 'No'.* *Interviewer: 'Has someone in your family told you that you've been scammed?'* *P3: 'Mum, yes.'*	P1, P3	Added specific examples to item: '*Other people (e.g. family members, friends, therapists, the bank, Police)*'
Considered a near-scam experience as a scam.	*Item: I have been in an online romance.* *P5: 'Someone's tried it, but I didn't fall for it'.* *Interviewer: 'What answer best represents your experience?'* *P5: 'Well, I guess I have been.'*	P5	Item revised to measure a more specific behaviour: '*I have formed a connection with someone in a romance or friendship scam*'.
Considered smartphone usage as 'over-the-phone' rather than 'online'.	'*It's on the phone but I guess – how do you class it? I'm on the sites and often we come off the…dating site, and then we go on the social media site, like WhatsApp.*' P1	P1, P5	Wording of multiple items revised to include '*online or over the phone*'.
Unsure whether to interpret items as specific to online or face-to-face behaviours.	*Item: I trust people easily.* *P4: 'Online I don't, but in personal face-to-face I somewhat agree, but disagree online.'*	P3, P4, P5	Revised wording of relevant items to capture behaviours broadly (both online and face-to-face): e.g. '*I trust people easily in everyday life*'
Confusion regarding whether a platonic relationship (involving sending money) was considered an online romance scam.		P2	Wording revised ('…*romance or friendship scam*') to capture both relationship types.
'Privacy settings' Misinterpreted privacy settings (adding extra security features to accounts) as safe behaviours or being careful online (e.g. not handing out passwords).	*Item: I try to use strong privacy settings on online accounts like social media or banking.* *P6: 'Often…I just never hand out my details to anyone…'*	P6	Item revised to include examples of privacy settings (…'e.g. *using strong and different passwords for each account, making social networking accounts private, 2-factor authentication*…')
'Connection'	In item 'I have formed a connection with someone in a romance or friendship scam', connection was viewed as a practical connection (i.e. being contacted) rather than an emotional connection as intended.	P7	Item revised to more specifically address emotional connection ('*I have formed an emotional connection with someone in a romance or friendship scam*').
Retrieval process difficulty			
Answering outside of the 1-month timeframe	Item: *I might think something is a scam, but I keep going with it anyway.* *P5: 'Oh, I agree, like I've done that before.'* *Interviewer: 'Has that happened to you within the last month…?'* *P5: 'Not the last month.'*	P2, P4, P5	Instructions emphasised and repeated more frequently to remind respondents of the timeframe.

(*Continued on next page*)

Table 5. (*Continued*)

Error/difficulty description	Example from participant interview	Reported by	Response to feedback
Response process difficulty			
Difficulty understanding rating scale for 'past scam experience' items	'*I probably gotta read it over quite a few times, one, yes in the last month and two, yes at any time.*' P1	P1, P2, P3	Rating scale simplified.
Answering inversely	Item: *If something doesn't look online, I check with someone first.* *P1*: '*No, I definitely never do that, so I definitely agree.*'	P1, P4	A new rating scale was made for behavioural items (never – sometimes – often) to address difficulty in rating agreement to behaviours.
Unsure how to respond to an item as it was not personally relevant.	Item: *I try to use strong privacy settings on online accounts like social media or banking.* *P3*: '*I don't have social media…for banking, I'm not too sure 'cause I don't control my own account.*'	P1, P3, P4	Instructions revised to encourage respondents to choose the nearest response ('If you are not sure of your answer, choose the closest response.')
Responding to mock scam scenarios as relevant to their own, personal experience only	'*If I got that [text], it would be definitely [a scam] 'cause I don't lodge tax returns.*' P4	P2, P4, P5	Participants were able to answer an item appropriately when encouraged to consider the scenario hypothetically.
Frequently responding with the middle Likert option when unsure.	'*I've sat in the middle on a bunch of ones which I would then go and figure it out*' P8	P8	Participants benefitted from encouragement to choose the closest response when unsure.

and scale feedback, revisions were made to the scale to improve accessibility and clinical relevance. Overall, participants supported the face and content validity of *The CyberABIlity Scale*, and participants with ABI showed evidence of appropriate scale completion across the four stages of Tourangeau's *et al.* (2000) model of cognitive processes of survey responding.

Using a combined approach of feedback from clinicians and participants with ABI to pre-test *The CyberABIlity Scale* is in keeping with recommended measure development processes (Mokkink *et al.* 2010; Boateng *et al.* 2018; Carpenter 2018). Particularly for 'cyberability', a newly conceptualised latent variable, scale development must be conducted through multiple studies and using various qualitative and quantitative methods of assessing validity (Flake 2021). Throughout this paper, we reported on the detailed process of developing a new measure through a combination of deductive and inductive approaches. Importantly, ensuring scale instructions, items and Likert-scale response options are clear for clinicians and people with ABI assists in the minimisation of measurement error that can occur due to misinterpreted items, leading questions or vague response choices (Carpenter 2018), particularly in the context of cognitive impairment that may impact scale completion for people with ABI (Whiting *et al.* 2015; Miller *et al.* 2022). Pre-testing *The CyberABIlity Scale* with a small sample of participants proved to be highly beneficial in ensuring items were meaningful and well-understood prior to larger-scale administration. This initial qualitative evidence of validation enables psychometric evaluation, which is currently underway.

The feedback provided in the current study was consistent with a recent cognitive interview study by Miller *et al.* (2022) regarding valued living, in which participants with ABI also had difficulty orientating to the timeframe specified in the scale instructions and rating items deemed personally irrelevant. Potentially, some people with ABI may require additional support in completing scales even if it has been designed and adapted to accommodate cognitive impairments (Miller *et al.* 2022). Although *The CyberABIlity Scale* has been developed for use within an ABI population, the accessibility of items and relevance to cognitive impairment may suggest suitability for other populations, for example various forms of dementia or neurodevelopmental conditions. Given the novelty of research on cyberscams and ABI, we have focussed first on non-degenerative ABI and encourage ongoing validation in other high-risk groups, as well as expansion to the general population using a universal design approach.

Development of *The CyberABIlity Scale* addresses the lack of existing measures assessing theorised unique risk factors to cyberscams for people with ABI in an accessible format. Whether these factors are unique to people with ABI or present similarly in other vulnerable groups or the general population, will be able to be explored once this measure is psychometrically validated.

The response patterns of participants underscore the need for this measure; several participants with ABI in the current study recalled further scam experiences throughout scale completion that were not recalled at the interview outset. This suggests that directly asking someone with ABI if they have been scammed online might be unreliable due to factors such

as poor free recall or lack of insight. Individuals with ABI typically display less difficulty in memory retrieval when provided with cues (i.e. recognition memory) as it relies less on strategies for information organisation and retrieval (Vakil *et al.* 2019). Potentially, scale items acted as a cue for recalling specific aspects of online behaviour and scam experiences.

In terms of feasibility, this measure was acceptable to participants with ABI who did not experience any discomfort or distress. *The CyberABIlity Scale* may provide a means to explore scam vulnerability in a non-confronting manner, mitigating the psychological distress and shame reported to be associated with discussing scam experiences (Gould *et al.* 2023*a*).

Limitations and future directions

Clinician participants involved in the Delphi method phase of this study were invited based on their known occupation and expertise within the ABI sector and were predominantly female (85.7%). Eleven clinician participants had been involved in previous aspects of the wider research program, and the remaining three clinician participants were known to the researchers based on their expertise. Clinician participants were all based in Australia. The clinician sample may have therefore been biased, for example by being familiar with types of scams that are common in Australia or have been addressed in our previous cyberscam research.

The appropriateness of *The CyberABIlity Scale* for populations outside of English-speaking Australians cannot be assumed from this study alone. Although there is limited research on cultural and geographical differences between cyberscams, there is some indication that cyberscam risk is perhaps different between groups. For example, within Australia, culturally and linguistically diverse communities were over-represented in reports of certain scam types (e.g. threats to life arrest or other; ACCC 2023). The reasons for this are unknown but may reflect different cross-cultural risk factors, for example, documented cultural differences in internet use (Li and Kirkup 2007; Laconi *et al.* 2018)

The sample of participants with ABI in the current study aimed to include participants with and without scam experience, as it was important to capture the perspectives of persons who may not personally relate to scale items. However, most of the sample had prior scam experience. At recruitment, one participant with ABI disclosed no prior scam experience; however, during the cognitive interview, recalled being scammed. Likely, persons with ABI who had previously been victims of cyberscams were more inclined to volunteer for our cyberscam research and this probably underpinned the very high scam frequency reported. Although the scale may be limited in its generalisability to people with ABI without scam experiences, further validation work that is currently underway will allow for psychometric evaluation of the scale in a larger sample of people with ABI who have and have not been scammed.

The need for developing *The CyberABIlity Scale* was based on previous qualitative and survey research (Gould *et al.* 2023*a*, 2023*b*). Although we acknowledge the importance of anecdotal and living experience findings, we further acknowledge the lack of objective research on cyberscams and ABI as a basis for developing this measure. Purported risk factors do remain theoretical, and although there are likely potential differences in scam profiles for those with ABI compared with the general public and/or other high-risk groups, whether this reflects different types of vulnerabilities or similar vulnerabilities to a different degree remains unclear and requires exploration. An initial way of measuring 'cyberability' must be developed before it can be studied empirically, and developing *The CyberABIlity Scale* to address risk factors beyond financial vulnerability will allow for such investigation. A valid measure will also enable future evidence-based cyberscam interventions to be quantitively evaluated.

Conclusion

This study outlined the development and validation of a novel and tailored measure of cyberscam vulnerability, *The CyberABIlity Scale*. We highlight the importance of transparent reporting of systematic and in-depth measure development approaches, particularly when developing new measures of latent constructs to demonstrate early validity. Expert feedback from clinicians and participants with ABI revealed comprehension errors and opportunities for scale simplification, scale reduction, the addition of new items and a revised Likert-scale format. Overall, the face and content validities of the resultant scale were verified, and feedback was provided to assist in the further development and distribution of the scale, enabling psychometric validation to proceed. Once finalised, *The CyberABIlity Scale* has the potential to be an effective screening measure of online risk for persons with ABI, and in the future, other cohorts. This study advances our ability to close a significant societal and research gap in understanding and reducing cybercrime for vulnerable populations.

Supplementary material

Supplementary material is available online.

References

ACCC (2023) Targeting scams Report of the ACCC on scams activity 2022. (Australian Competition and Consumer Commission)

Australian Bureau of Statistics (2008) 'Personal fraud in Australia.' (Australian Institute of Criminology) Available at https://www.aic.gov.au/publications/cfi/cfi180

Beatty PC, Willis GB (2007) Research Synthesis: The Practice of Cognitive Interviewing. *Public Opinion Quarterly* **71**(2), 287–311. doi:10.1093/poq/nfm006

Boateng GO, Neilands TB, Frongillo EA, Melgar-Quiñonez HR, Young SL (2018) Best Practices for Developing and Validating Scales for Health, Social, and Behavioral Research: A Primer. *Frontiers in Public Health* **6**, 149. doi:10.3389/fpubh.2018.00149

Boeije H, Willis G (2013) The Cognitive Interviewing Reporting Framework (CIRF): Towards the harmonization of cognitive testing reports. *Methodology: European Journal of Research Methods for the Behavioral and Social Sciences* **9**(3), 97–95. doi:10.1027/1614–2241/a000075

Boulkedid R, Abdoul H, Loustau M, Sibony O, Alberti C (2011) Using and Reporting the Delphi Method for Selecting Healthcare Quality Indicators: A Systematic Review. *PLoS One* **6**(6), e20476. doi:10.1371/journal.pone.0020476

Brunner M, Hemsley B, Palmer S, Dann S, Togher L (2015) Review of the literature on the use of social media by people with traumatic brain injury (TBI). *Disability and Rehabilitation* **37**(17), 1511–1521. doi:10.3109/09638288.2015.1045992

Brunner M, Palmer S, Togher L, Hemsley B (2019) 'I kind of figured it out': the views and experiences of people with traumatic brain injury (TBI) in using social media—self-determination for participation and inclusion online. *International Journal of Language & Communication Disorders* **54**(2), 221–233. doi:10.1111/1460-6984.12405

Brunner M, Palmer S, Togher L, Dann S, Hemsley B (2020) "If I knew what I was doing on Twitter then I would use it more": Twitter experiences and networks of people with traumatic brain injury (TBI). *Brain Impairment* **21**(1), 1–18. doi:10.1017/BrImp.2019.12

Brunner M, Hemsley B, Togher L, Dann S, Palmer S (2021) Social Media and People With Traumatic Brain Injury: A Metasynthesis of Research Informing a Framework for Rehabilitation Clinical Practice, Policy, and Training. *American Journal of Speech-Language Pathology* **30**(1), 19–33. doi:10.1044/2020_AJSLP-20-00211

Carpenter S (2018) Ten Steps in Scale Development and Reporting: A Guide for Researchers. *Communication Methods and Measures* **12**(1), 25–44. doi:10.1080/19312458.2017.1396583

Carrier SL, Wong D, Lawrence K, McKay A (2022) Preliminary validation of a new competency tool for evaluating assessment skills in professional psychology trainees. *Training and Education in Professional Psychology* **16**(2), 166–172. doi:10.1037/tep0000394

Charters E, Gillett L, Simpson GK (2015) Efficacy of electronic portable assistive devices for people with acquired brain injury: a systematic review. *Neuropsychological Rehabilitation* **25**(1), 82–121. doi:10.1080/09602011.2014.942672

Delbecq AL, Van de Ven AH, Gustafson DH (1975) 'Group techniques for program planning: a guide to nominal group and delphi processes.' (Scott Foresman) Available at https://eduq.info/xmlui/handle/11515/11368

Diamond IR, Grant RC, Feldman BM, Pencharz PB, Ling SC, Moore AM, Wales PW (2014) Defining consensus: a systematic review recommends methodologic criteria for reporting of Delphi studies. *Journal of Clinical Epidemiology* **67**(4), 401–409. doi:10.1016/j.jclinepi.2013.12.002

Fink A, Kosecoff J, Chassin M, Brook RH (1984) Consensus methods: characteristics and guidelines for use. *American Journal of Public Health* **74**(9), 979–983. doi:10.2105/AJPH.74.9.979

Flake JK (2021) Strengthening the foundation of educational psychology by integrating construct validation into open science reform. *Educational Psychologist* **56**(2), 132–141. doi:10.1080/00461520.2021.1898962

Flake JK, Fried EI (2020) Measurement Schmeasurement: Questionable Measurement Practices and How to Avoid Them. *Advances in Methods and Practices in Psychological Science* **3**(4), 456–465. doi:10.1177/2515245920952393

Gould KR, Brokenshire C (2017) Scams and brain impairment: a clinician's treatment recommendations and a survivor's perspective. *Brain Impairment* **18**, 395. doi:10.1017/BrImp.2017.24

Gould KR, Carminati JJ, Ponsford JL (2023*a*) "They just say how stupid I was for being conned". Cyberscams and acquired brain injury: a qualitative exploration of the lived experience of survivors and close others. *Neuropsychological Rehabilitation* **33**(2), 325–345. doi:10.1080/09602011.2021.2016447

Gould KR, Carolan M, Ponsford JL (2023*b*) Do we need to know about cyberscams in neurorehabilitation? *Brain Impairment* **24**, 229–244. doi:10.1017/BrImp.2022.13

Han SD, Boyle PA, James BD, Yu L, Bennett DA (2016) Mild Cognitive Impairment and Susceptibility to Scams in Old Age. *Journal of Alzheimer's Disease* **49**(3), 845–851. doi:10.3233/JAD-150442

Hawthorne G, Gruen RL, Kaye AH (2009) Traumatic Brain Injury and Long-Term Quality of Life: Findings from an Australian Study. *Journal of Neurotrauma* **26**, 1623–1633. doi:10.1089/neu.2008.0735

Hinkin TR (1995) A Review of Scale Development Practices in the Study of Organizations. *Journal of Management* **21**(5), 967–988. doi:10.1177/014920639502100509

Holmbeck GN, Devine KA (2009) Editorial: an author's checklist for measure development and validation manuscripts. *Journal of Pediatric Psychology* **34**(7), 691–696. doi:10.1093/jpepsy/jsp046

James BD, Boyle PA, Bennett DA (2014) Correlates of Susceptibility to Scams in Older Adults Without Dementia. *Journal of Elder Abuse & Neglect* **26**(2), 107–122. doi:10.1080/08946566.2013.821809

Jovanovski D, Zakzanis K, Ruttan L, Campbell Z, Erb S, Nussbaum D (2012) Ecologically Valid Assessment of Executive Dysfunction Using a Novel Virtual Reality Task in Patients with Acquired Brain Injury. *Applied Neuropsychology: Adult* **19**(3), 207–220. doi:10.1080/09084282.2011.643956

Kilov AM, Togher L, Power E, Turkstra L (2010) Can teenagers with traumatic brain injury use Internet chatrooms? A systematic review of the literature and the Internet. *Brain Injury* **24**(10), 1135–1172. doi:10.3109/02699052.2010.490511

Laconi S, Kaliszewska-Czeremska K, Gnisci A, Sergi I, Barke A, Jeromin F, Groth J, Gamez-Guadix M, Ozcan NK, Demetrovics Z, Király O, Siomos K, Floros G, Kuss DJ (2018) Cross-cultural study of Problematic Internet Use in nine European countries. *Computers in Human Behavior* **84**, 430–440. doi:10.1016/j.chb.2018.03.020

Li N, Kirkup G (2007) Gender and cultural differences in Internet use: a study of China and the UK. *Computers & Education* **48**(2), 301–317. doi:10.1016/j.compedu.2005.01.007

Lichtenberg PA, Tocco M, Moray J, Hall L (2021) Examining the Validity of the Financial Exploitation Vulnerability Scale. *Clinical Gerontologist* **44**(5), 585–593. doi:10.1080/07317115.2021.1954124

Linstone, HA, & Turoff, M (2002). The Delphi Method: Techniques and Applications. Journal of Marketing Research, 13, 317

McDonald S, Togher L, Code C (2013) 'Social and Communication Disorders Following Traumatic Brain Injury.' (Psychology Press)

Miller H, Lawson D, Power E, das Nair R, Sathananthan N, Wong D (2022) How do people with acquired brain injury interpret the Valued Living Questionnaire? A cognitive interviewing study. *Journal of Contextual Behavioral Science* **23**, 125–136. doi:10.1016/j.jcbs.2022.01.003

Modic D, Anderson R, Palomäki J (2018) We will make you like our research: The development of a susceptibility-to-persuasion scale. *PLoS One* **13**(3), e0194119. doi:10.1371/journal.pone.0194119

Mokkink LB, Terwee CB, Knol DL, Stratford PW, Alonso J, Patrick DL, Bouter LM, de Vet HC (2010) The COSMIN checklist for evaluating the methodological quality of studies on measurement properties: A clarification of its content. *BMC Medical Research Methodology* **10**(1), 22. doi:10.1186/1471-2288-10-22

Okoli C, Pawlowski SD (2004) The Delphi method as a research tool: An example, design considerations and applications. *Information & Management* **42**(1), 15–29. doi:10.1016/j.im.2003.11.002

Ponsford JL, Downing MG, Olver J, Ponsford M, Acher R, Carty M, Spitz G (2014) Longitudinal Follow-Up of Patients with Traumatic Brain Injury: Outcome at Two, Five, and Ten Years Post-Injury. *Journal of Neurotrauma* **31**(1), 64–77. doi:10.1089/neu.2013.2997

Stanyon MR, Goldberg SE, Astle A, Griffiths A, Gordon AL (2017) The competencies of Registered Nurses working in care homes: a modified Delphi study. *Age and Ageing* **46**, 582–588. doi:10.1093/ageing/afw244

Tourangeau R, Rips LJ, Rasinski K (2000) 'The Psychology of Survey Response.' (Cambridge University Press)

Trevelyan EG, Robinson PN (2015) Delphi methodology in health research: How to do it? *European Journal of Integrative Medicine* **7**(4), 423–428. doi:10.1016/j.eujim.2015.07.002

Tsaousides T, Matsuzawa Y, Lebowitz M (2011) Familiarity and prevalence of Facebook use for social networking among individuals with traumatic brain injury. *Brain Injury* **25**(12), 1155–1162. doi:10.3109/02699052.2011.613086

Vaccaro M, Hart T, Whyte J, Buchhofer R (2007) Internet use and interest among individuals with traumatic brain injury: a consumer survey. *Disability and Rehabilitation: Assistive Technology* **2**(2), 85–95. doi:10.1080/17483100601167586

Vakil E, Greenstein Y, Weiss I, Shtein S (2019) The Effects of Moderate-to-Severe Traumatic Brain Injury on Episodic Memory: A Meta-Analysis. *Neuropsychology Review* **29**(3), 270–287. doi:10.1007/s11065-019-09413-8

Whiting DL, Deane FP, Ciarrochi J, McLeod HJ, Simpson GK (2015) Validating measures of psychological flexibility in a population with acquired brain injury. *Psychological Assessment* **27**(2), 415–423. doi:10.1037/pas0000050

Whitty MT, Buchanan T (2016) The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice* **16**(2), 176–194. doi:10.1177/1748895815603773

Wong D, Grace N, Baker K, McMahon G (2019) Measuring clinical competencies in facilitating group-based rehabilitation interventions: development of a new competency checklist. *Clinical Rehabilitation* **33**(6), 1079–1087. doi:10.1177/0269215519831048

Data availability. The data that support this study cannot be publicly shared due to ethical or privacy reasons and may be shared upon reasonable request to the corresponding author if appropriate.

Conflicts of Interest. The authors report no conflicts of interest and do not financially profit from the publication of *The CyberABIlity Scale*.

Declaration of funding. Author J.C. is supported by an Australian Government Research Training Program Scholarship.

Ethics standard. The authors assert that all procedures contributing to this work comply with the ethical standards of the relevant national and institutional committees on human experimentation and with the Helsinki Declaration of 1975, as revised in 2008.

Acknowledgements. The authors would like to acknowledge and thank the generosity, time and effort of all participants involved.

Author affiliations

[A]Turner Institute for Brain and Mental Health, School of Psychological Sciences, Monash University, Clayton, Vic. 3800, Australia.

[B]Monash-Epworth Rehabilitation Research Centre, Epworth Healthcare, Richmond, Vic. 3121, Australia.