

ORIGINAL ARTICLE

Do we need to know about cyberscams in neurorehabilitation? A cross-sectional scoping survey of Australasian clinicians and service providers

Kate Rachel Gould^{1,2*} , Matthew Carolan^{1,2} and Jennie Louise Ponsford^{1,2}

¹Monash-Epworth Rehabilitation Research Centre, Epworth Hospital, 185-187 Hoddle Street, Richmond, VIC, 3121, Australia and ²Turner Institute for Brain and Mental Health, School of Psychological Sciences, Monash University, 18 Innovation Walk, Clayton Campus, VIC, 3800, Australia

*Corresponding author. Email: kate.gould@monash.edu

(Received 19 September 2021; revised 20 February 2022; accepted 23 March 2022; first published online 05 May 2022)

Abstract

Cyberscams, such as romance scams, are prevalent and costly online hazards in the general community. People with Acquired Brain Injury (ABI) may be particularly vulnerable and have greater difficulty recovering from the resultant emotional and financial hardships. In order to build capacity in the neurorehabilitation sector, it is necessary to determine whether clinicians currently encounter this issue and what prevention and intervention approaches have been found effective. This scoping study aimed to explore clinicians' exposure to and experiences with cyberscams in their adult clients with ABI.

Method: Participants were clinicians recruited from multidisciplinary networks across Australia and New Zealand. Eligible participants ($n = 101$) completed an online customised survey.

Results: More than half (53.46%) the participants had one or more clients affected by cyberscams, predominantly romance scams. Cognitive impairments and loneliness were reportedly associated with increased vulnerability. Cyberscams impacted treatment provision and were emotionally challenging for participants. No highly effective interventions were identified.

Conclusions: These findings indicate that cyberscams are a clinical issue relevant to neurorehabilitation providers, with prevalence studies now required. The lack of effective interventions identified underscores the need for the development of evidence-based prevention and treatment approaches to ultimately help people with ABI safely participate in online life.

Keywords: Acquired brain injury; rehabilitation; cybercrime; cross-sectional design; clinicians

Introduction

Picture this: you are a community neuropsychologist assisting Colin to manage the cognitive, psychological and behavioural problems he experiences after severe acquired brain injury (ABI). Colin's wife informs you that he has been embroiled in an online romance scam and defrauded of thousands of dollars. She has cancelled his bank access, but has been unable to convince Colin to stop contacting his fake online lover. What do you do? This real clinical scenario catalysed years of trialling numerous interventions and collaborative investigations, as Colin and author KG learned together about the prevalence and power of romance scams, and worked to untangle him from their herculean grip. As anyone can be scammed, it was unclear whether Colin was targeted or at greater risk because of his ABI. Nevertheless, his memory and executive impairments appeared to interfere with intervention attempts to help him acknowledge the scam

and shift his behaviour of frequent contact with the scammer. There was no available clinical guidance regarding how to support scam recovery, let alone for those with ABI. The aim of this scoping study was to examine whether other clinicians in Australia and New Zealand had encountered cyberscams in clients with ABI, their views as to contributing factors, and the approaches they considered effective in helping clients with ABI avoid and recover from cyberscams.

Cybercrime is predicted to be one of the most significant financial threats to humanity, with \$6 trillion predicted to be lost annually from 2021 (Morgan, 2019). Australians are disproportionately affected as the 5th highest victims of cybercrime worldwide (Internet Crime Complaint Center, 2016). Cyberscams, including romance scams, are online crimes which involve fraudulently obtaining funds, stealing identities, using compromising images for blackmail, or tricking victims into participating in illegal money laundering or goods transfers (Australian Cybercrime Online Reporting Network, 2019). First emerging in 2008, online romance scams are serious crimes in which criminals dupe unsuspecting people into believing they are in romantic relationships using online dating or social media sites, and then defraud victims of significant sums of money (Whitty & Buchanan, 2012). As seen in Colin's dating scam, perpetrators' frequent and exaggeratedly romantic online interactions can become part of daily life for the victim, reinforced through provision of desired companionship (Walther & Whitty, 2021). Based on the Routine Activity Theory, online crimes may occur due to three factors: proliferation of suitable targets with a large proportion of people using the internet; motivated and technically skilled offenders; and an absence of capable personal and community guardianship and threat awareness (Cohen & Felson, 1979; Ross & Smith, 2011). Cyberscammers are increasingly sophisticated and well resourced, utilising large-scale call centres, pre-written scripts, grooming techniques and manipulation to build the trust of their victims (Das & Nayak, 2013; Goel & Raj, 2018). Cyberscams may cause substantial financial losses as well as extreme emotional distress, relationship conflict, loss of trust in others and lowered self-confidence (Whitty & Buchanan, 2016). There are no known interventions which specifically address the unique combination of financial and psychological trauma resultant from cyberscam victimisation.

Whilst anyone can become victim to a scam, demographic, medical and personality characteristics may increase vulnerability to scams. Whitty (2018) identified that romance scam victims were more likely to be 35–54 years old, well-educated women, with higher scores on measures of impulsivity, trustworthiness and addictive disposition and lower scores on kindness. However, findings in the extant literature are mixed, with increased risk to the broader category of consumer fraud found to be associated with lower levels of education and not gender (Lee & Soberon-Ferrer, 1997).

Based on cognitive and psychosocial impairment profiles, clinical experience and a recent qualitative study (Gould, Carminati & Ponsford, 2021), we theorised that history of ABI may increase susceptibility to cyberscams. The few previous studies which have examined cognitive impairment and scam vulnerability provide some support for this contention. In older adults, who are often targeted by financial fraudsters, scam susceptibility has been significantly correlated with reduced cognitive function as well as increased age, lower psychological wellbeing and poorer financial and health literacy (James, Boyle & Bennett, 2014). Furthermore, decreased scam awareness in older adults has been associated with significantly increased risk of mild cognitive impairment (MCI), Alzheimer's dementia and greater Alzheimer disease brain pathology (Boyle, Yu, Schneider, Wilson & Bennett, 2019). Additionally, in 730 older adults with MCI, reduced episodic memory and perceptual speed performance was associated with increased susceptibility to scams (Han, Boyle, James, Yu & Bennett, 2016).

Cybersafety competency and digital self-efficacy are recognised as important contemporary skills (Nordén, Mannila & Pears, 2017). In one of the few studies investigating the online experiences of people with ABI, Brunner, Palmer, Togher & Hemsley (2019) found that use of social media was popular amongst 13 young people with ABI. In keeping with recognised advantages of computer-mediated communication compared with face-to-face interaction (Walther & Whitty, 2021), participants with ABI benefited from ease of access, time to formulate asynchronous

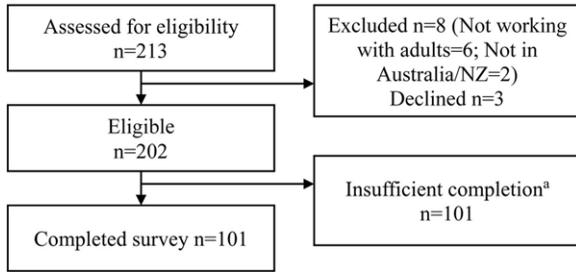


Figure 1. Participation flow chart. Note – ^a Insufficient completion of the survey was defined as only completing eligibility and demographic questions.

responses and ability to hide their disability. However, for people with ABI, a lack of support and supervision in navigating the challenges of social media was reported, including two accounts of online relationship scams (Brunner et al., 2019). Within the neurorehabilitation sector, online technologies are nevertheless increasingly promoted by therapists as part of interventions to support socialisation (Brunner, Hemsley, Palmer, Dann & Togher, 2015), meaningful activities (Jamieson et al., 2020) and social communication (Wong et al., 2017).

It is unclear whether neurorehabilitation clinicians are aware of cybercrime risk and vulnerability factors, are able to recognise scamming of their clients with ABI, and whether they utilise effective prevention or treatment approaches. The perspectives of clinicians and service providers are needed to guide recommendations for professional development and service delivery. Therefore, the aim of the present scoping study was to explore the experiences and perspectives of ABI clinicians with and without cyberscams in their clients, specifically to determine: i) whether clinicians encounter individuals with ABI affected by cyberscams, ii) their views on associated risk factors and impacts and iii) their appraisals of possible approaches to cyberscam prevention and treatment. In regards to aim iii, we hypothesised that cyberscam case experience would be associated with higher ratings of intervention effectiveness based on their lived-expertise of clinical involvement.

Method

An exploratory cross-sectional survey design was used to determine current clinical exposure, experience and capacity of neurorehabilitation clinicians in identifying, preventing and treating individuals with ABI who had been scammed online. Institutional ethics approval was obtained and all participants provided digital consent (Monash University, MUHREC Project ID 17984).

Participants

Participants were a convenience sample of clinicians and community ABI workers from Australia and New Zealand who provided informed consent. Individuals were eligible to participate if they currently or previously worked with adults (aged 18 years or older) living with ABI. There was no requirement for participants to have experience supporting a client with ABI who had been scammed. A total of 101 participants completed the survey. Refer to Figure 1 for the participation flow chart.

Procedure

In order to recruit a broad cross-section of neurorehabilitation clinicians, the study was advertised via multiple means including social media posts by the researchers, emails from the researchers to a mailing list of over 100 colleagues, and distributed to three ABI/neuropsychology list-serves (NPInOz, BRAINSPaN, VicNic). In addition, approximately 40 hospitals, organisations and multidisciplinary networks with large memberships of psychologists, speech therapists and

occupational therapists were asked to distribute the recruitment invitation, for example, professional organisations (e.g. Australasian Society for the Study of Brain Impairment), community advocacy groups (e.g. Brain Injury Australia) and state-based accident insurers (e.g. the Transport Accident Commission in Victoria). Due to the recruitment methodology, the number of individuals approached could not be determined. Prospective participants were emailed the study invitation with an online survey link and explanatory statement. The survey was administered online using Qualtrics and required approximately 30 minutes to complete. All participants completed the eligibility screening and provided digital consent after reviewing the explanatory statement. Participants completed the online survey between May and August 2019.

Materials

Survey development

Due to a lack of suitable extant measures identified from a review of the literature and a need to ensure relevance to individuals with ABI, an online survey was developed by the researchers. Survey items were informed by findings from a concurrent qualitative study (Gould & Ponsford, *In Preparation*), in which 10 clinicians and service providers who had clients with ABI who were scammed were interviewed and analysed using a six-stage iterative thematic analysis (Braun & Clarke, 2006). Emerging themes related to the relationships between the ABI, cyber-scams vulnerability and impacts including cognitive, psychological and behavioural factors, meaningful participation and social relationships, financial access, online competency and the availability of a trusted person (Gould & Ponsford, *In Preparation*). In addition, the survey design was informed by previous studies on romance scams (Buchanan & Whitty, 2014; Whitty, 2018; Whitty, 2019; Whitty & Buchanan, 2012, 2016) and the authors' clinical experiences.

To determine content face validity, the survey was piloted in two rounds by seven community ABI therapists, researchers and university psychology students, with feedback incorporated into the final version. Construct and criterion-related validity were unable to be conducted due to a paucity of existing measures.

Survey design

To address the aims of the study, the survey collected information on participant: 1. Demographics and 2. Cyberscam self-efficacy. Participants were asked whether they had seen a client with ABI who had been scammed. Subsequent survey sections for participants with exposure to a scammed client included 3. Client characteristics, 4. Cyberscam details, 5. Perceived risk factors of clients and scam impact, 6. Perceived efficacy of prevention approaches and 7. Perceived efficacy of intervention approaches. Participants could repeat sections 3 to 7 to provide information for a second client or to describe multiple scams relating to one client. Participants without experience supporting a client with scam exposure were not administered sections 3, 4 or 5 and were asked to complete the survey sections relating to *potential* rather than *perceived* aspects of sections 6 and 7. Most items utilised Likert scales and checklists; participants could also submit their own response using an 'other' item or select 'not applicable'. Survey sections are described in detail below.

1. Demographics

Participants provided demographic information including age, gender, years and highest level of education obtained, occupation and work setting within the ABI sector.

2. Cyberscam clinical self-efficacy

The survey included definitions of key terms. ‘Cyberscam’ referred to dishonest schemes, or outright fraud initiated online using the internet or social media, including dating and romance scams, investment scams, or attempts to gain personal information, many of which result in financial loss (Australian Criminal Intelligence Commission, 2022; Oxford University Press, 2019). The term ‘CyberAbility’ was coined by Gould and Brokenshire (2017) and referred to technical, cognitive and social-emotional capacity to learn and adapt to current, new and emerging technologies, for example, staying safe online, handling online information and using the internet responsibly for communicating and socialising.

Participants completed 21 self-rated capacity items encompassing their knowledge, skill and confidence in supporting individuals with ABI regarding cyberscams. There were seven items for knowledge, for example, knowledge of potential red flags. Nine items for skill, for example, delivering interventions to help manage emotional impact of cyberscams. Five items related to confidence, for example, in identifying whether an individual with ABI is involved in a cyberscam. These were scored on a Likert scale (1 = *none* to 5 = *high*) and averaged for each capacity and total score.

3. Client characteristics

Participants with experience supporting a client affected by cyberscams provided unidentifiable information on the client’s demographics (e.g. gender, age at time of scam, education) and ABI (e.g. cause, year sustained and severity).

4. Cyberscam details

Data was collected on the number, type and duration of the scam. Participants selected the platform used when the scam was initiated (e.g. online dating, social media, online marketplace). Participants rated their perceived confidence in online safety of the client (Likert rated from 1 = *none* to 5 = *high*), source of identification of the cyberscam (e.g. disclosure by the client, disclosure by family or support service, inferred by participant) and perceived level of awareness of the client that they had been scammed (recorded as a percentage, where 100% reflected complete scam awareness).

5. Perceived risk factors of clients and scam impact

Subjective reports of factors participants considered associated with increased vulnerability to cyberscams were explored across five areas and rated on a Likert scale (1 = *very low* to 5 = *very high*). Emotional and personality attributes such as depression, trust in others, kindness and addictive personality (Whitty, 2018) were measured across 15 items. Cognitive deficits encompassed attention, learning and memory, communication, fatigue and executive functions (e.g. insight, inflexibility, planning and problem-solving) across 10 items. Behavioural items were derived from the Overt Behaviour Scale categories (Kelly, Todd, Simpson, Kremer & Martin, 2006) as well as impulsivity (Whitty, 2019) and irritability (10 items). Social vulnerability factors included unemployment, reduced social and leisure activities, reduced study, increased computer use and accommodation change (seven items). Lack of supervision of online (computer and smartphone/tablet) and financial activities was the final area of vulnerability explored (three items), reflecting the guardianship (protection) aspect of the Routine Activity Theory of crime vulnerability most relevant to clinicians (Reyns, 2015). Participants also rated overall subjective confidence in their clients’ online safety skills before and after a cyberscam event.

Checklists were used to identify psychological, financial and practical impacts of the scam (e.g. reduced trust in others, anger, depression, criminal charges) as well barriers to treatment due to the scam (e.g. disengagement, increased treatment length). Participants could rate overall

psychological and practical impacts from *Low* to *Extreme*. The participants' emotional reactions to addressing the scam were collected via a checklist of 32 possible responses (e.g. angry, empathic, uncertain) derived from the qualitative study findings.

6. & 7. Perceived efficacy of prevention and treatment approaches

Participants rated their perceived self-efficacy in using cyberscam prevention techniques (11 items, e.g. education about staying safe online) and treatment approaches (25 items, e.g. cognitive behaviour therapy), both rated on a Likert scale (1 = *very ineffective* to 5 = *very effective*). These items were generated by the authors on the basis of the qualitative findings and clinical experience.

Data analysis

Data were entered and primarily analysed descriptively using Microsoft Excel 2016 and SPSS Version 25. Visual inspection of histograms of data analysed for each aim by author MC indicated normal distributions of scores and therefore assumptions of normality were met. No individual outliers were identified that significantly affected means or standard deviations. To address aim iii, *t*-tests were used to compare average scores between participants with and without exposure to cyberscam cases regarding prevention and treatment approaches.

Results

Participants

In this paper, the term 'participants' refers to the neurorehabilitation clinicians and service providers who completed the survey, and 'clients' refers to the individuals with ABI described by the participants. As displayed in Table 1, the 101 participants were predominantly female neuropsychologists or occupational therapists in metropolitan community settings in Victoria and Tasmania, with an average of 10 years' experience working with individuals living with ABI. Demographic and occupational characteristics were broadly equivalent between those with and without experience with cyberscammed ABI clients.

Participants with experience supporting individuals with ABI who had been scammed

Over half of the participants ($n = 54$, 53.46%) had a client with ABI affected by cyberscams.

Client characteristics

Participants provided information on 51 clients with ABI who had been cyberscammed. Clients were predominantly male (69.23%), with a mean age of 46 ($SD = 18.18$) and educated to high school. Most clients reportedly had moderate ($n = 16$), moderate-severe ($n = 14$), or severe ($n = 16$) ABI caused by a traumatic brain injury sustained on average 15.32 years ($SD = 12.19$) previously. Participants reported high levels of depression (58.82%) and anxiety (45.1%) in these clients.

Cyberscam details

An average of 1.3 ($SD = 1.79$, range 0-10) cyberscammed clients were reported per participant, with 33% of clients affected by multiple cyberscams. Only one participant provided detailed information on the second scam of their client, resulting in data regarding a total of 52 cyberscam events. Of the 52 cyberscam events, the majority were romance scams (48.08%), buying/selling scams (13.46%) and attempts to gain personal information (11.54%). Average cyberscam duration

Table 1. Participant demographics ($n = 101$)

	Participant experience with scammed ABI clients		Total (n)
	Yes (n)	No (n)	
Highest level of education	54	47	101
Doctoral degree	13	9	22
Master's degree	11	13	24
Graduate diploma / certificate	7	5	12
Bachelor's degree with honours	3	8	11
Bachelor's degree	13	8	21
Diploma	2	0	2
Certificate 3 / 4	0	1	1
High school	3	3	6
Primary school	1	0	1
Other	1	0	1
Gender	54	47	101
Female	47	43	90
Male	7	4	11
NDIS Registration	54	47	101
Yes	19	10	29
No	30	33	63
No, but planning to register	5	4	9
State			
Victoria	25	18	43
Tasmania	19	10	29
New South Wales	4	9	13
New Zealand	3	3	6
Queensland	2	6	8
South Australia	1	0	1
Western Australia	0	1	1
Other: New Zealand	3	3	6
Years of Age M (SD, range)	43.00 (11.42)	40.13 (9.59)	41.68 (10.66, 23–68)
Years' clinical experience M (SD, range)	10.33 (6.93)	9.60 (7.43)	10.00 (7.14, 1–26)
Work location(s)*	71	63	144
Metro / Urban	48	41	89
Rural / Remote	23	18	41
Telehealth/Online	10	4	14
Work setting(s)*	111	97	208
Client's home	19	17	36

(Continued)

Table 1. (Continued)

	Participant experience with scammed ABI clients		Total (<i>n</i>)
	Yes (<i>n</i>)	No (<i>n</i>)	
Residential facilities / nursing homes	14	10	24
Outpatient rehabilitation centre	8	13	21
Inpatient rehabilitation centre	8	11	19
Group private practice	9	9	18
Solo private practice	9	9	18
Inpatient hospital	7	10	17
Research settings	6	5	11
Outpatient hospital	3	6	9
Schools and other educational / vocational facilities	5	2	7
Community health centre	5	1	6
Mental health centre	6	0	6
Other	12	4	16
Role(s)*	67	54	121
Clinical neuropsychologist	15	11	26
Occupational therapist	11	14	25
Other	17	8	25
Case manager	10	3	13
Support worker	2	7	9
Speech pathologist	5	3	8
Clinical psychologist	0	5	5
Psychologist with no endorsement	3	2	5
Advocate	2	0	2
Mental health nurse	1	0	1
Psychiatrist	0	1	1
Recreational therapist	1	0	1

Note. Participants could select multiple clinical roles, work settings and work locations. Years of experience: the number of years the participant has spent working with people with ABI.

was 5.37 months ($SD = 6.72$, Range 1-30). Cyberscams were predominantly initiated over social media ($n = 21$), telephone calls ($n = 12$) and non-dating online chatrooms ($n = 9$).

Cyberscam identification

Participants rated only seven clients as 100% aware of the cyberscam, with the majority estimated as less than 50% aware (Mdn = 41.5%, IQR = 27.75 % to 68.25%). Most clients were made aware that they were being scammed by a clinician/service provider (31.37%) or a family member (23.53%) and only 21.57% self-identified the cyberscam according to the participants.

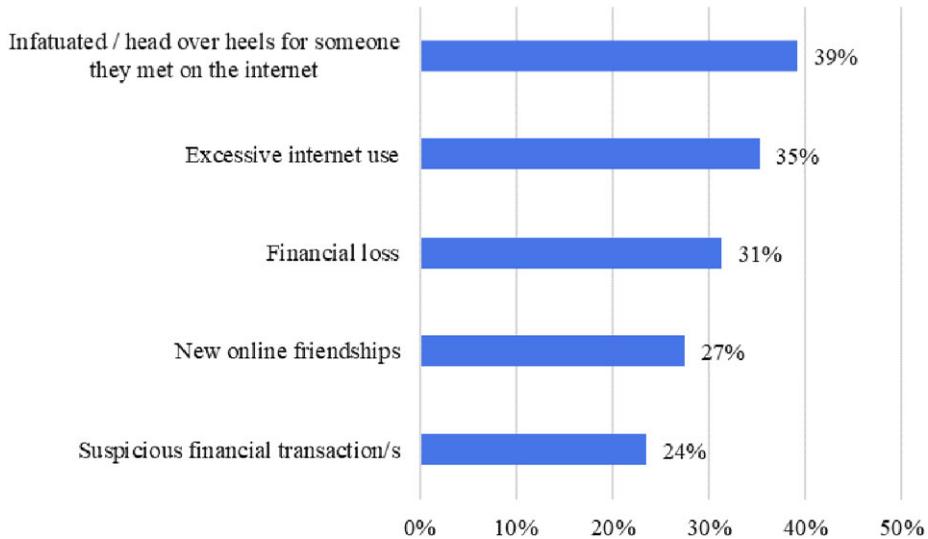


Figure 2. Top five cyberscam red flags identified by participants with cyberscam experience ($n = 51$). Note: Participants could select multiple red flags.

Participants' most common cyberscam red flags were noticing their clients were infatuated with someone online, excessive internet use and reported financial loss (Fig 2).

Factors increasing vulnerability to cyberscams

Participants whose clients had been scammed rated cognitive, social, psychological, behavioural and supervision factors that were considered to increase their client's vulnerability to cyberscams (see Appendix). The highest ranked of these were cognitive factors, including lack of insight and awareness ($M = 4.17$, $SD = 0.96$) and reduced planning and problem-solving abilities ($M = 4.11$, $SD = 0.85$). This was closely followed by social factors including loneliness ($M = 4.06$, $SD = 1.22$) and a strong desire for a relationship ($M = 3.85$, $SD = 1.53$). Psychological factors identified included tendency to place high trust in others ($M = 3.87$, $SD = 0.96$) and openness/agreeableness ($M = 3.78$, $SD = 1.11$). Behaviourally, impulsivity ($M = 3.81$, $SD = 1.15$) was the dominant feature, with inappropriate sexual behaviour ($M = 1.59$, $SD = 1.09$) not considered to increase vulnerability to cyberscams. Unsupervised use of smartphones ($M = 3.80$, $SD = 1.04$) and computers ($M = 3.70$, $SD = 1.10$) were also considered risk factors. On average, participants with cyberscam experience had 'minimal' confidence in their clients' online safety skills (i.e. *cyberability*) both before ($M = 1.72$, $SD = 0.99$) and after ($M = 2.09$, $SD = 0.99$) the cyberscam.

Impact of cyberscams

Participants estimated cyberscams had a moderate impact on clients' psychological wellbeing ($M = 2.85$, $SD = 0.78$) and everyday functioning ($M = 3.02$, $SD = 0.93$). Commonly reported impacts of the cyberscams were depression (41.18%), family/relationship conflict (31.37%), self-blame (31.37%), financial distress (29.41%), anxiety (25.49%) and agitation/irritability (25.49%). The cyberscam impacted support services; More than a third (35%) of participants identified that addressing the cyberscam became the treatment focus at the expense of other goals. The cyberscam also increased treatment duration (18%), with some clients refusing to discuss the scam (16%), disengaging (8%) or refusing treatment (4%). Addressing the cyberscam was emotionally difficult for many participants, resulting in frequently feeling worried (45.1%), challenged

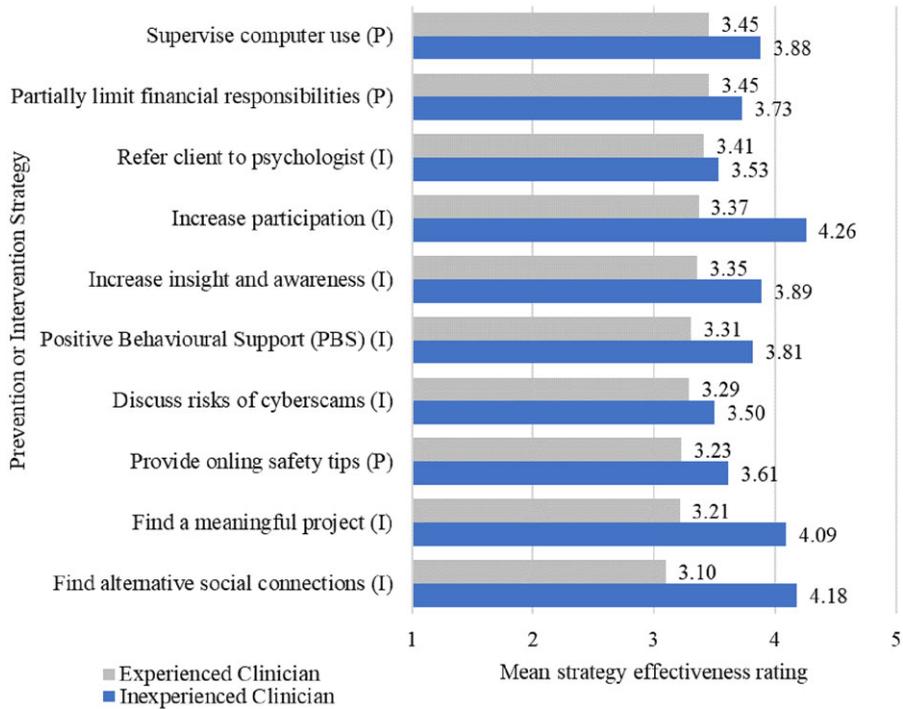


Figure 3. The 10 most effective prevention and intervention strategies as rated by clinicians with and without experience of working with a person with ABI who had been cyberscammed. *Note: Effectiveness was rated from 1 = very ineffective to 5 = very effective; P = Prevention strategy; I = Intervention treatment strategy.*

(43.14%), empathic (41.18%), frustrated (33.34%) and sad (27.45%) about their client’s experience.

Participant capacity to support clients with ABI affected by cyberscams

Participants rated their overall capacity in supporting individuals with ABI affected by cyberscams at 2.53 out of 5 (SD = 0.60), equivalent to ‘minimal’ to ‘adequate’ ratings, with similar findings across subscales relating to their knowledge (M = 2.46, SD = 0.75), skill (M = 2.41, SD = 0.76) and confidence (M = 2.74, SD = 0.76).

Effectiveness of prevention and treatment strategies

Both participants with and without experience supporting an individual with ABI who had been cyberscammed provided their perspectives on intervention options. There were no highly effective prevention or treatment strategies identified by participants (Fig 3). Prevention strategies rated as having ‘average’ effectiveness were supervising computer use, partially limiting financial responsibilities and providing online safety tips. Treatment strategies rated as having ‘average’ effectiveness included referring the client to a psychologist, increasing participation in activities and supporting insight development. Compared with participants inexperienced with scams, participants with experience supporting a scammed client gave significantly lower ratings of prevention strategy effectiveness (M = 3.06, SD = 0.72 c.f. M = 3.45, SD = 0.46, $t(84) = 3.01, p < 0.01, d = 0.66$, “large”) and treatment strategy effectiveness (M = 3.05, SD = 0.72 c.f. M = 3.44, SD = 0.49, $t(84) = 3.01, p < 0.01, d = 0.66$, “large”).

Discussion

Cyberscams represent a growing worldwide threat to which people with ABI may be particularly vulnerable. This potentially represents an important clinical issue for ABI rehabilitation providers. This scoping study surveyed 101 Australasian clinicians and service providers to determine their experiences in identifying and treating cyberscams in adults with ABI. Approximately half of the participants had identified at least one client with ABI who had been cyberscammed, suggesting that this is of relevance to neurorehabilitation. Participants subjectively appraised that awareness of the scam by clients with ABI was low and it was generally someone in the client's support network who recognised that the cyberscam had occurred. Accordingly, there may be cyberscam cases which remain undetected by clinicians and service providers or unreported by the person with ABI due to their lack of scam awareness. In the general community, cybercrimes may not be formally reported by up to two thirds of victims due to shame, concern about being blamed and pessimism regarding the outcome of reporting (Cross, Richards & Smith, 2016; Smith, 2008). In the case of romance scams, acknowledging the scam has occurred not only entails accepting that they were deceived and the improbability of recouping financial losses, but also the loss of the relationship with someone with whom they have developed a deep emotional attachment, called a "double-hit" (Buchanan & Whitty, 2014).

Cyberscam warning signs frequently reported by participants included noticing infatuation in an online relationship, excessive internet use and financial losses. To a certain extent, these observations represent clinically helpful indicators of cyberscam victimisation. However, by the time these behaviours are recognised, the scam may have substantially progressed, rendering intervention more difficult. Rather than being acute events, the reported cyberscams were generally protracted, with the average duration more than five months and some as long as two and a half years. During this time, romance scammers may engage in grooming, enticing the person with declarations of love and detailed dramatic stories, to which the person being scammed can heroically respond by providing financial assistance. This grooming and sharing of seemingly personal stories renders disengaging more difficult (Kopp, Layton, Sillitoe & Gondal, 2016; Whitty, 2013). Based on the finding of low self-rated capacity, clinicians and service providers may benefit from efforts to increase their knowledge, skills and confidence in identifying cyberscam vulnerability and warning signs. The development of validated screening tools for susceptibility to cyberscams currently being undertaken by our team may provide a practical means of earlier scam identification and enable timely instigation of preventative approaches such as conversations about online safety.

The majority of cyberscams reported by participants that impacted people with ABI in this study were romance and dating scams. Whilst acknowledging the secondary source of this finding, it is noted that this is in contrast with the most frequently reported scams in Australia, namely phishing, threats to life or arrest and identity theft (ACCC, 2019). Whether this reflects a difference in scam profiles between these populations would require larger, representative data sets using validated measures. Consistent with the greater proportion of romance scams, seeking out companionship and loneliness were identified by participants in the current study as factors that reportedly increased vulnerability to scams in their clients with ABI. Rather than loneliness representing a specific vulnerability to being scammed, it may be the impetus for desiring a relationship, with online daters in a large European sample noted to be lonely, regardless of whether or not they were scammed. (Buchanan & Whitty, 2014). Social isolation and relationship breakdown are common after ABI, with loss of employment, rejection by peers, fractured families and reduced leisure activities all more prevalent than in the general community and contributing to feelings of loneliness (Hawthorne, Gruen & Kaye, 2009). According to Williams, Beardmore & Joinson (2017), social isolation and loneliness create vulnerability to online grooming, and this need for attention is exploited by offenders. Resisting influence to potential scams is a cognitively effortful task (Williams et al., 2017), potentially compounded by ABI-related attentional

difficulties. For people with ABI, the combination of wanting a relationship, loneliness, reduced attention and cognitive fatigue may explain increased vulnerability specifically to romance scams. Further research is required to verify this contention. Understanding the mechanisms of vulnerability to romance scams for people with ABI is also needed in order to design interventions addressing these factors.

In addition to the natural desire for a relationship, increased susceptibility to cyberscams was reported by participants in this study to be associated with executive impairments and impulsivity in their clients. Whilst we did not have direct evidence of cognitive impairments in these predominantly moderate to severely injured clients, executive dysfunction due to ABI commonly results in errors in judgement, decision-making and impulsivity (Cotrena *et al.*, 2014). Indeed, cognitive impairments, albeit relating to reduced speed and episodic memory, were found in scam-susceptible adults with MCI (Han *et al.*, 2016). Similarly, longer response time when deciding whether an online dating profile was genuine or fraudulent was associated with poorer accuracy in a UK sample of 261 adults (Whitty, 2019). Conversely, greater self-reported impulsive behaviour was associated with better scam detection accuracy, with Whitty suggesting that following one's initial instincts of distrust may be beneficial, rather than ignoring these feelings or directly challenging the scammer. To address the cognitive-executive and psychological factors in individuals with ABI associated with online risk-taking behaviour, clinicians and service providers may consider preventative approaches which improve online safety skills, normalise open discussion of potential scams and promote least restrictive approaches to computer independence and financial responsibilities such as supervising or limiting access to potentially hazardous online sites.

Despite romance scams being the most frequently documented cyberscam type, participants in this study endorsed social media as the most common means of scam initiation for their clients rather than online dating platforms. Accordingly, individuals with ABI may be at risk of online dating scams even if they do not formally use internet dating sites. Furthermore, individuals with ABI commonly use social media (Baker-Sparr *et al.*, 2018) and many report that they initiate and use social media without support from rehabilitation professionals, instead relying on a "trial and error" approach (Brunner *et al.*, 2019). Taken together, neurorehabilitation professionals should ensure that online activities, and social media competencies in particular, are routinely assessed.

In this study, clinicians considered that most clients with ABI who were scammed experienced a range of negative psychological and practical impacts of the cyberscam including depression, anxiety, agitation and irritability, family and relationship conflict, self-blame and financial distress. Whilst these issues are similar to those experienced by scam victims in the general population (Whitty, 2018; Whitty & Buchanan, 2012), for people with ABI they may occur against a background of concurrent ABI-related difficulties, further compounding their psychosocial challenges. Furthermore, some clinicians reported that the scam interfered with treatment goals, duration and engagement. This may have financial implications due to increased therapy costs and potentially additional burden on natural support networks.

Participants had low confidence in the cybersafety skills of their clients with ABI and did not identify any preventative or treatment strategies deemed to be highly effective. Prevention strategies considered to have *average* effectiveness included supervising computer use, partially limiting financial responsibilities and providing online safety tips. Interestingly, and contrary to our hypothesis, participants with actual clinical experience were more guarded in their endorsement of these prevention approaches than participants without experience on which to base their ratings. Whether this finding reflects disapproval of the specific prevention approaches suggested, or a more generalised pessimism towards risk reduction, is unclear. Additional qualitative investigation may shed some light on the reasons for low ratings of commonly available approaches and may support the need for the creation of tailored prevention programmes.

The Australian government recently established several agencies to improve cybersafety through community awareness and online resources (e.g. Australian Cyber Security Centre, eSafety Commissioner, StaySmartOnline). Recognising that training designed for school-aged

children, seniors and adults in the workforce may not be appropriate for adults with disabilities such as ABI, existing digital citizenship education programmes could be adapted or created specifically to compensate for common brain-injury-related deficits such as attention, memory and executive impairments. Although tailored prevention resources are now emerging for people with disability (Gould & Brokenshire, 2017; ThinkUKnow, 2019), their effectiveness requires evaluation. Whilst the evidence base is developing, potential interim cybersafety prevention approaches for neurorehabilitation professionals could include routinely discussing online risks to increase awareness and normalisation, discussing risk tolerance with the individual and their support network, providing hands-on and practical support for the specific social media and online activities relevant to the individual, encouraging and praising exhibited cybersafety behaviours and establishing trusted support people to assist if difficulties are encountered (Gould et al., 2021; Third, Forrest-Lawrence & Collier, 2014). As well as increasing the cybersafety of the individuals with ABI, clinicians and carers are akin to teachers in school settings who act as online safety role models, and as such also require early and ongoing cybersafety skill development (Walsh, Wallace, Ayling & Sondergeld, 2020). For individuals with ABI who become victim to a scam, treatment approaches recommended by experienced clinicians to have *average* likely effectiveness were referral to psychology, increased participation and increase insight and awareness. As described in the case of Colin, it remains challenging to identify specific, psychological approaches to help someone recognise and recover from a cyber-scams. The lack of evidence-based interventions and guidelines for psychological recovery from cyber-scams highlights a need for further clinical research in this field.

Limitations and strengths

Several methodological limitations of this study require acknowledgement. Relying on the perspective of clinicians and service providers limited direct inferences about the experiences of people with ABI, and as such the findings regarding the factors which increase vulnerability and the impacts should be interpreted with caution. Nevertheless, this methodology did enable investigation of clinicians' awareness of the occurrence and impact of scams within their clients, their management approaches and their training needs. The study methodology prohibited generation of prevalence data of cyber-scams within the ABI population due to potential recruitment bias, whereby people with an *a priori* interest in scams could be more likely to participate. The findings are also tempered by the modest sample size, reliance on secondary sources of information; subjective ratings of cognitive impairment; lack of construct and criterion validity analyses; 50% incomplete surveys, and possible overlap in cases between clinicians. A potential recruitment bias is exemplified by the high response rates in Victoria and Tasmania, where the authors and our collaborators have been conducting awareness raising campaigns in the ABI sector. Whilst the response rate was not able to be estimated due to the recruitment method of convenience via snowballing, participants represented a broad range of disciplines and professional settings, half of whom did not identify any scams within their clients. First-person prevalence studies, validated self-report and objective measures of cyber-scams vulnerability, and representative data collection protocols are needed to address these shortcomings.

Strengths of this scoping study included the investigation of a novel clinical practice issue to increase awareness, provide an introductory understanding and guide the direction of future targeted studies in cyber-scams after ABI. These findings will inform the development of planned quantitative and qualitative studies to investigate cyber-scams vulnerability and impact from the perspectives of people with ABI and their close others, as well as the development of tailored intervention programmes. A further strength of this study was the piloting of a new survey measure.

Conclusions

This study found that cyber-scams vulnerability and victimisation is of relevance to neurorehabilitation clinicians, with half of respondents identifying cyber-scams of their clients with ABI,

particularly romance scams. Cyberscams were reported to interfere with treatment provision, and participants lacked effective prevention and intervention strategies, experiencing personal distress and concern about their scammed clients. The findings suggest that clinicians would benefit from education and evidence-based resources to assist them in identifying vulnerable clients, and access to tailored interventions which help clients avoid, disengage and psychologically recover from cyberscams. These initial scoping findings call for further methodologically rigorous research and validated self-report measures to quantify the frequency and vulnerabilities of cyberscams in the ABI population.

Acknowledgements. Thank you to the participants for your time and efforts in completing the study, and the students, staff and colleagues of MERRC in assisting with the piloting of the survey.

Financial support. This work was supported by the 2018 Allen Martin Research Scholarship awarded to Dr Kate Gould by the Summer Foundation with the support of Rotary Kew and Robinson Gill Lawyers.

Conflicts of interest. The authors report no conflicts of interest.

Ethical standards. 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.

References

- ACCC. (2019). *Targeting scams: Report of the ACCC on scams activity 2018*. Canberra, ACT: Commonwealth of Australia, Retrieved from <https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2018>.
- Australian Criminal Intelligence Commission (2022). *Cybercrime*, <https://www.acic.gov.au/about/priority-crime-themes/cybercrime>.
- Australian Cybercrime Online Reporting Network (2019). *What is cybercrime?*. ReportCyber, Retrieved 26 April 2022 from, <https://www.cyber.gov.au/acsc/view-all-content/threats/scams>.
- Baker-Sparr C., Hart T., Bergquist T., Bogner J., Dreer L., Juengst S., & et al. (2018). Internet and social media use after traumatic brain injury: A traumatic brain injury model systems study. *Journal of Head Trauma Rehabilitation*, 33(1), E9–E17. doi: 10.1097/HTR.0000000000000305
- Boyle P. A., Yu L., Schneider J. A., Wilson R. S., & Bennett D. A. (2019). Scam awareness related to incident Alzheimer dementia and mild cognitive impairment: A prospective cohort study. *Annals of Internal Medicine*, 170(10), 702–709. doi: 10.7326/m18-2711
- Braun V., & Clarke V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. doi: 10.1191/1478088706qp063oa
- 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) [Review]. *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 and Communication Disorders*, 54(2), 221–233. doi: 10.1111/1460-6984.12405
- Buchanan T., & Whitty M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime and Law*, 20(3), 261–283. doi: 10.1080/1068316X.2013.772180
- Cohen L. E., & Felson M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. doi: 10.2307/2094589
- Cotrena C., Branco L. D., Zimmermann N., Cardoso C. O., Grassi-Oliveira R., & Fonseca R. P. (2014). Impaired decision-making after traumatic brain injury: The iowa gambling task. *Brain Injury*, 28(8), 1070–1075. doi: 10.3109/02699052.2014.896943
- Cross C., Richards K., & Smith R. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice*, 518, 1–14. <https://eprints.qut.edu.au/98343/>
- Das S., & Nayak T. (2013). Impact of cyber crime: Issues and challenges. *International Journal of Engineering Sciences & Emerging Technologies*, 6(2), 142–153. <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.429.548>

- Goel V., & Raj S. (2018). That virus alert on your computer? scammers in India may be behind it. *New York Times*, 28 November 2018. <https://www.nytimes.com/2018/11/28/technology/scams-india-call-center-raids.html>
- Gould K. R., & Brokenshire C. (2017). Scams and brain impairment: A clinician's treatment recommendations and a survivor's perspective [Conference abstract]. *Brain Impairment*, 18(3), 395. doi: <https://doi.org/10.1017/BrImp.2017.24>
- Gould K. R., Carminati J.-Y. J., & Ponsford J. L. (2021). 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*, 1-21, [10.1080/09602011.2021.2016447](https://doi.org/10.1080/09602011.2021.2016447)
- Gould K. R., & Ponsford J. A qualitative exploration of cyberscam discovery and treatment after acquired brain injury from the perspective of clinicians in the community. Monash University (In Preparation).
- Han S. D., Boyle P. A., James B. D., Yu L., & Bennett D. A. (2016). Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's disease : JAD*, 49(3), 845–851. doi: [10.3233/JAD-150442](https://doi.org/10.3233/JAD-150442)
- Hawthorne G., Gruen R. L., & Kaye A. H. (2009). Traumatic brain injury and Long-Term quality of life: Findings from an Australian study. *Journal of Neurotrauma*, 26, 1623–1633, <http://www.liebertonline.com/doi/pdf/10.1089/neu.2008.0735?cookieSet=1>
- Internet Crime Complaint Center. (2016). *Internet crime report*. Retrieved from https://www.ic3.gov/media/annualreport/2016_IC3Report.pdf.
- James B. D., Boyle P. A., & Bennett D. A. (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](https://doi.org/10.1080/08946566.2013.821809)
- Jamieson M., Jack R., O'Neill B., Cullen B., Lennon M., Brewster S., & Evans J. (2020). Technology to encourage meaningful activities following brain injury. *Disability and Rehabilitation: Assistive Technology*, 15(4), 453–466. doi: [10.1080/17483107.2019.1594402](https://doi.org/10.1080/17483107.2019.1594402)
- Kelly G., Todd J., Simpson G., Kremer P., & Martin C. (2006). The overt behaviour scale (OBS): A tool for measuring challenging behaviours following ABI in community settings. *Brain Injury*, 20(3), 307–319. doi: [10.1080/02699050500488074](https://doi.org/10.1080/02699050500488074)
- Kopp C., Layton R., Sillitoe J., & Gondal I. (2016). The role of love stories in romance scams: A qualitative analysis of fraudulent profiles. *International Journal of Cyber Criminology*, 9(2), 205–216. doi: [10.5281/zenodo.56227](https://doi.org/10.5281/zenodo.56227)
- Lee J., & Soberon-Ferrer H. (1997). Consumer vulnerability to fraud: Influencing factors. *The Journal of Consumer Affairs*, 31(1), 70–89, <http://www.jstor.org/stable/23859598>
- Morgan S. (2019). *Official annual cybercrime report*. Retrieved from <https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/>.
- Nordén L., Mannila L., & Pears A. (2017, 18-21 Oct. 2017). Development of a self-efficacy scale for digital competences in schools. In: 2017 IEEE Frontiers in Education Conference (FIE).
- Oxford University Press. (2019). *Definition of scam in English*. Oxford University Press, Retrieved 26 April 2022 from, <https://www.lexico.com/definition/scam>.
- Reyns B. W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, 22(4), 396–411. doi: [10.1108/JFC-06-2014-0030](https://doi.org/10.1108/JFC-06-2014-0030)
- Ross S., & Smith R. G. (2011). Risk factors for advance fee fraud victimisation. *Trends and Issues in Crime and Criminal Justice*(420), 1–6. doi: [10.3316/agispt.20114328](https://doi.org/10.3316/agispt.20114328)
- Smith R. G. (2008). Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change*, 49(5), 379–396. doi: [10.1007/s10611-008-9112-x](https://doi.org/10.1007/s10611-008-9112-x)
- ThinkUKnow. (2019). *A guide for staying safe online: Easy read version*. Retrieved from <https://thinkuknow.org.au/index.php/resources/guides/guide-staying-safe-online-easy-read-version>.
- Third A., Forrest-Lawrence P., & Collier A. (2014). *Addressing the cyber safety challenge: From risk to resilience*. Telstra Corporation Limited/University of Western Sydney, 32 pages, <https://researchdirect.westernsydney.edu.au/islandora/object/uws:28267/>
- Walsh K., Wallace E., Ayling N., & Sondergeld A. (2020). *Best practice framework for online safety education*. e. Commissioner. Retrieved from https://www.esafety.gov.au/sites/default/files/2020-06/Best%20Practice%20Framework%20for%20Online%20Safety%20Education_0.pdf.
- Walther J. B., & Whitty M. T. (2021). Language, psychology, and new new media: The hyperpersonal model of mediated communication at twenty-five years. *Journal of Language and Social Psychology*, 40(1), 120–135. doi: [10.1177/0261927x20967703](https://doi.org/10.1177/0261927x20967703)
- Whitty M. T. (2013). The scammers persuasive techniques model. *British Journal of Criminology*, 53(4), 665–684. doi: [10.1093/bjc/azt009](https://doi.org/10.1093/bjc/azt009)
- Whitty M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, Behavior, and Social Networking*, 21(2), 105–109. doi: [10.1089/cyber.2016.0729](https://doi.org/10.1089/cyber.2016.0729)
- Whitty M. T. (2019). Who can spot an online romance scam? *Journal of Financial Crime*, 26(2), 623–633. doi: [10.1108/JFC-06-2018-0053](https://doi.org/10.1108/JFC-06-2018-0053)

- Whitty M. T., & Buchanan T.** (2012). The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior, and Social Networking*, 15(3), 181–183. doi: [10.1089/cyber.2011.0352](https://doi.org/10.1089/cyber.2011.0352)
- Whitty M. T., & Buchanan T.** (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial[Article]. *Criminology and Criminal Justice*, 16(2), 176–194. doi: [10.1177/1748895815603773](https://doi.org/10.1177/1748895815603773)
- Williams E. J., Beardmore A., & Joinson A. N.** (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, 72, 412–421. doi: <https://doi.org/10.1016/j.chb.2017.03.002>
- Wong D., Sinclair K., Seabrook E., McKay A., & Ponsford J.** (2017). Smartphones as assistive technology following traumatic brain injury: a preliminary study of what helps and what hinders. *Disability and Rehabilitation*, 39(23), 2387–2394. doi: [10.1080/09638288.2016.1226434](https://doi.org/10.1080/09638288.2016.1226434)

Cite this article: Gould KR, Carolan M, and Ponsford JL (2023). Do we need to know about cyberscams in neurorehabilitation? A cross-sectional scoping survey of Australasian clinicians and service providers. *Brain Impairment* 24, 229–244. <https://doi.org/10.1017/BrImp.2022.13>