Experimental Gerontology 159 (2022) 111678

Contents lists available at ScienceDirect

Experimental Gerontology

journal homepage: www.elsevier.com/locate/expgero

Review

Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review

Alexandra Burton [a,1], Claudia Cooper [b,c,*,1], Ayesha Dar [b], Lucy Mathews [b], Kartikeya Tripathi [d]

[a] Research Department of Behavioural Science and Health, Institute of Epidemiology & Health Care, UCL, UK
[b] UCL Division of Psychiatry, 6th Floor Wing A Maple House, 149-150 Tottenham Court Road, London W1T 7BN, UK
[c] Camden and Islington NHS Foundation Trust, UK
[d] Department of Security and Crime Science, University College London, UK

ARTICLE INFO

Section Editor: Christiaan Leeuwenburgh

Keywords:
Older adults
Fraud
Internet
Crime victims

ABSTRACT

Although older people rarely report being victims of financial cybercrime, there is evidence that older online users are at increased risk. This realist review identified factors leading to older adults' victimisation and reviewed the theory and evidence for interventions to reduce victimisation risks. We developed an initial programme theory from a scoping review and expert stakeholder consultations. We searched electronic databases, references and websites for literature meeting inclusion criteria. We analysed 52 primary and secondary data sources, seeking stakeholder views to develop and refine the programme theory and generate Context-Mechanism-Outcome Configurations (CMOCs) explaining how, why and in what circumstances older adults become financial cybercrime victims; and extrapolated this to consider rational intervention strategies. Our programme theory comprised 16 CMOCs describing how: social isolation, cognitive, physical and mental health problems; wealth status, limited cyber security skills or awareness, societal attitudes and content of scams led to victimisation. Our refined programme theory provides a novel framework to guide future intervention design. Only interventions to enhance older internet users' awareness and skills have been trialled to date. Other theoretically plausible interventions include: offender management programmes, tailored security measures, society-wide stigma reduction and awareness-raising with groups who support older people.

1. Introduction

With the advance of global digitalisation, the incidence of financial cybercrime is increasing rapidly. Over a third of British adults were targeted during the 2020 pandemic (Citizen's Advice Report 2020). Cybercrime is defined as "any criminal activity in which a computer (or networked device) is targeted or used" (Munanga, 2019). Financial cybercrime includes consumer frauds and scams that are designed to obtain financial benefit by deception (Kaldor et al., 2019). Most commonly, phishing (scam) emails or text messages direct users to illicit websites that download viruses, or steal passwords, bank details or other sensitive information.

Adults experiencing mental health problems are at increased risk of cybercrime (Citizen's Advice Report 2020). While older adults are at relatively low risk of frauds, certain groups may be more susceptible, due to increased levels of cognitive and mental health problems, isolation, unfamiliarity with technology, perceived greater wealth and assets, and a reported generational predisposition towards trust of authorities and hesitancy to report crime (DeLiema, 2018). Of the 4 million UK adults who had never used the internet in 2019, over half were aged 75 years and over (Munanga, 2019). One fifth of people aged 65+ experience cognitive impairment, and many of them are online users (Lopez et al., 2007; Cooper et al., 2021). The closure of bank branches, and the Covid-19 pandemic have shifted many transactions online. Though digitalisation can reduce social isolation among older people (DeLiema, 2018; Rabiner et al., 2006), without safeguards and support, it increases exposure to cybercrime victimisation risks, which in cohorts of older adults who are potentially more susceptible, is a concern. In the USA, older adults lost more to fraud in 2020 compared to 2019 (Federal Trade Commission, n.d.). Impacts of financial cybercrime extend beyond financial losses, to reduced trust and online activity (Tripathi et al., 2019; Watson et al., 2018), physical illness (Dong and Simon, 2013;

* Corresponding author at: UCL Division of Psychiatry, 6th Floor Wing A Maple House, 149-150 Tottenham Court Road, London W1T 7BN, UK.
E-mail address: Claudia.cooper@ucl.ac.uk (C. Cooper).
[1] Joint first authors.

https://doi.org/10.1016/j.exger.2021.111678
Received 6 September 2021; Received in revised form 29 November 2021; Accepted 20 December 2021
Available online 30 December 2021

Davidson et al., 2015), emotional distress (Bergmann et al., 2018; Carlson, 2006; Age-UK, 2015) and increased hospital admissions and mortality (Dong and Simon, 2013; Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services, 2019; Age-UK, 2017). Online accessibility, and thus cybercrime prevention are instrumental to healthy ageing in a digital world.

While the concept of financial abuse, as defined by the World Health Organisation is limited to acts occurring within a relationship of trust and excludes "abuse by strangers" (including internet scams and frauds) (Hafemeister, 2003), many of the vulnerability factors and impacts of financial cybercrime in susceptible groups of older adults described above also apply to financial elder abuse (Hafemeister, 2003). Risks of elder abuse, including financial abuse, increase with greater degrees of cognitive impairment and dependency (Cooper et al., 2009; Cooper et al., 2008); this may also be true of cybercrime risks.

A recent report highlighted the need of financial systems to "protect by design" people who due to cognitive or mental illnesses are more vulnerable to fraud, many of whom are in older age groups (Norris et al., 2019). Theoretical points of intervention include attitudes and behaviours of online users, and of family members, friends and professionals in positions to protect vulnerable adults from harm; design of online interfaces and processes, and reporting systems.

The proposed UK Draft Online Safety bill aims to make the UK "the safest place in the world to go online." It strengthens safeguards against hate crimes and harassment, but its scope does not extend to financial cybercrime. Evidence cited in its support suggests that older people are not at greater risk of online fraud, because they are not over-represented among those reporting it (Conway, 2021). This may be explained by the relatively lower rates of older people who are more susceptible to cybercrime, for example due to cognitive decline, who are currently online, and also by hesitancy among older age groups to report.

To inform new approaches to enable older people to benefit safely and equitably from greater digital connectivity, we used a realist theoretical framework to synthesise evidence and stakeholder experience to:

1) Build a programme theory explaining how, why and in what circumstances older adults may be at risk of becoming victims of financial cybercrime.
2) To consider how existing and future interventions might target the mechanisms that explain how older people become victims of financial cybercrime.

2. Methods

Realist evaluation is grounded in the belief that social processes in which we might seek to intervene are complex, and the mechanisms by which outcomes occur depend on and influence their contexts. We based the design of our review of how older people become victims of financial cybercrime (that we defined as cybercrime with the propensity to incur significant financial loss), on Pawson's five stages for realist evaluations (Pawson et al., 2005) and the recommendations of Wong et al. (2016). We followed the 'Realist and Meta-Review Evidence Synthesis: Evolving Standards' (RAMESES) guidelines and standards (Wong et al., 2016). We convened a stakeholder group of content experts (see Results for membership) who we consulted by email throughout the review process and during a half day virtual conference in November 2020, to support us in Programme Theory development and consider its implications for intervention strategies.

2.1. Develop initial programme theory

AB completed an informal scoping search for articles explaining how and why online financial fraud may occur in different contexts. We consulted the stakeholder group to identify key theories and papers and to prioritise topics for further investigation in our systematic literature search. We iteratively consulted stakeholders to develop an initial programme theory to explain why older adults become victims of online financial fraud (Fig. 1a).

2.2. Literature search

We conducted a formal literature search, without limits on dates; this took place between June and August 2020, and was updated in July 2021, to identify evidence to support, refute and refine the stage one initial programme theory. Search terms were informed by stage one and developed with the stakeholder group with input from an information specialist. Search terms were piloted in the Criminal Justice Database and modified as required across the different databases. We searched electronic databases, relevant UK government sites (e.g. Home Office, Ministry of Justice), government and organisational websites for grey literature including third sector (e.g. Age UK) and media reports, key journal publications and conference proceedings, reference lists of relevant articles and we contacted key content experts. See Table 1 for a list of databases and journals searched.

2.3. Study selection

We included grey literature, primary and secondary research studies with potential to inform the development of the programme theory and Context, Mechanism, Outcome Configurations (CMOCs). These configurations delineate different pathways to outcomes of interest. In this instance, they seek to explain the **mechanisms** by which older adults become victims of online financial crime in different **contexts** (environments, populations, life circumstances). Risk factors operate differently in different settings. Understanding how and why (the mechanisms by which) cybercrime occurs in varied circumstances (contexts) can inform development of interventions to produce the desired **outcomes** of reducing and preventing cybercrime. This information was extrapolated from the background, results and/or discussion sections of the identified literature. We included qualitative and quantitative studies investigating online activities (using computers or smart devices), which included a sample or sub sample of older (age 65+) participants. We excluded studies investigating exclusively non-financial cybercrimes e.g. stalking, bullying, sexual victimisation; and non- English language studies.

We screened titles and abstracts and retained relevant articles for full text screening. AD and LM screened and selected studies, with a second reviewer (AB) screening a 10% selection to monitor consistency. Reasons for excluding citations were recorded and inconsistencies discussed to reach consensus. Reviewers followed RAMESES guidelines to consider relevance (whether it can contribute to theory building and/or testing); and rigour (whether the method used to generate that particular piece of data is credible and trustworthy) of articles when determining inclusion (Bunn et al., 2017). The team developed processes to inform these judgements, that involved team discussions; and standard measures to evaluate validity of different types of research (CEBM, 2001).

2.4. Data extraction

We extracted key characteristics of included studies (Tables 2–5). Full texts of included papers were uploaded into NVivo12 and AD/LM coded segments of text that related to i) contexts in which older adults become victims of financial cybercrime, ii) mechanisms and/or associations between contexts, mechanisms and relevant outcomes. We used inductive and deductive approaches to create a coding framework: pre-existing codes informed by the initial programme theory were created before data extraction, and new codes were added to represent the data in included studies. The initial programme theory was tested and refined based on the emerging coding framework and data from included studies was revisited as the theory developed.

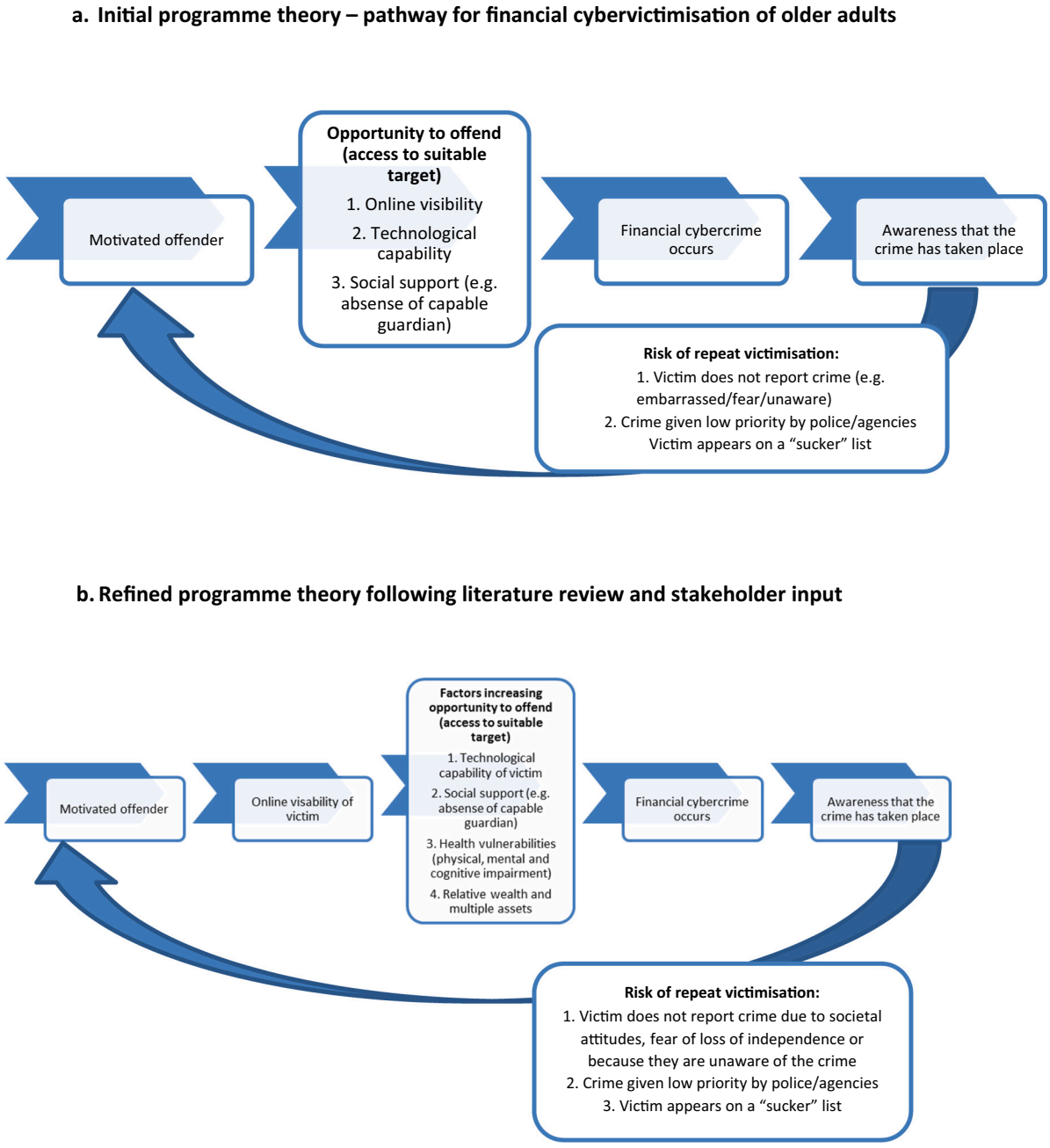

Fig. 1. a. Initial programme theory – pathway for financial cybervictimisation of older adults.
b. Refined programme theory following literature review and stakeholder input.

2.5. Data synthesis

Data were analysed and synthesised using accepted methods (Wong et al., 2016). We assessed the relevance of each segment of text to the development of the programme theory, whether it provided information that could be interpreted as a partial or complete Context, Mechanism Outcome Configuration (CMOC); and determined whether the data was credible and trustworthy enough to influence the CMOC and/or programme theory.

2.6. Refine and test the programme theory

During data analysis, we iteratively refined the programme theory through discussion between authors and with the wider stakeholder group. We consulted stakeholders by email and at a remote workshop held on 26th November 2020, where we refined and finalised the CMOCs, exploring how they aligned with their professional and lived experiences. At the workshop, AB introduced the initial programme theory, and stage two review findings. The stakeholder group discussed these CMOCs in small groups, followed by whole group discussions. The group examined if each CMOC configuration was supported by empirical evidence and compared it to their own experiences. We considered patterns emerging from CMOCs and used these to refine our programme theory and to consider how interventions to reduce victimisation of older people by financial cybercrime might work across different contexts.

3. Results

3.1. Stakeholder group membership

We recruited a broad stakeholder group, comprising 21 members. The group included academics, social researchers, members of the UK Police Service and English Home Office, third sector, financial sector, cybersecurity experts, NHS and social care workers for older adults, government policy advisors and local councillors; and representatives of older people's advocacy organisations. At the workshop the members were divided into three smaller groups for consultation. Each sub-group represented the diversity of stakeholders to facilitate broad discussions.

3.2. Initial programme theory (Fig. 1a)

Developed in stage one (above), this hypothesised that for a financial cybercrime to occur there needed to be 1. a motivated offender and 2. factors present that enabled access to the victim including i) online visibility, ii) technological capability of the victim and iii) absence of social support. This was primarily modelled on Routine Activity Theory (Cohen and Felson, 1979) which relates offending to everyday patterns of social interaction. It situates crime as dependent on opportunities to offend, and requiring: a motivated offender, opportunity to offend (e.g. suitable targets), and absence of a capable guardian. While this theory was originally derived to explain crimes involving physical contact between offenders and victims, it can also apply when motivated offenders

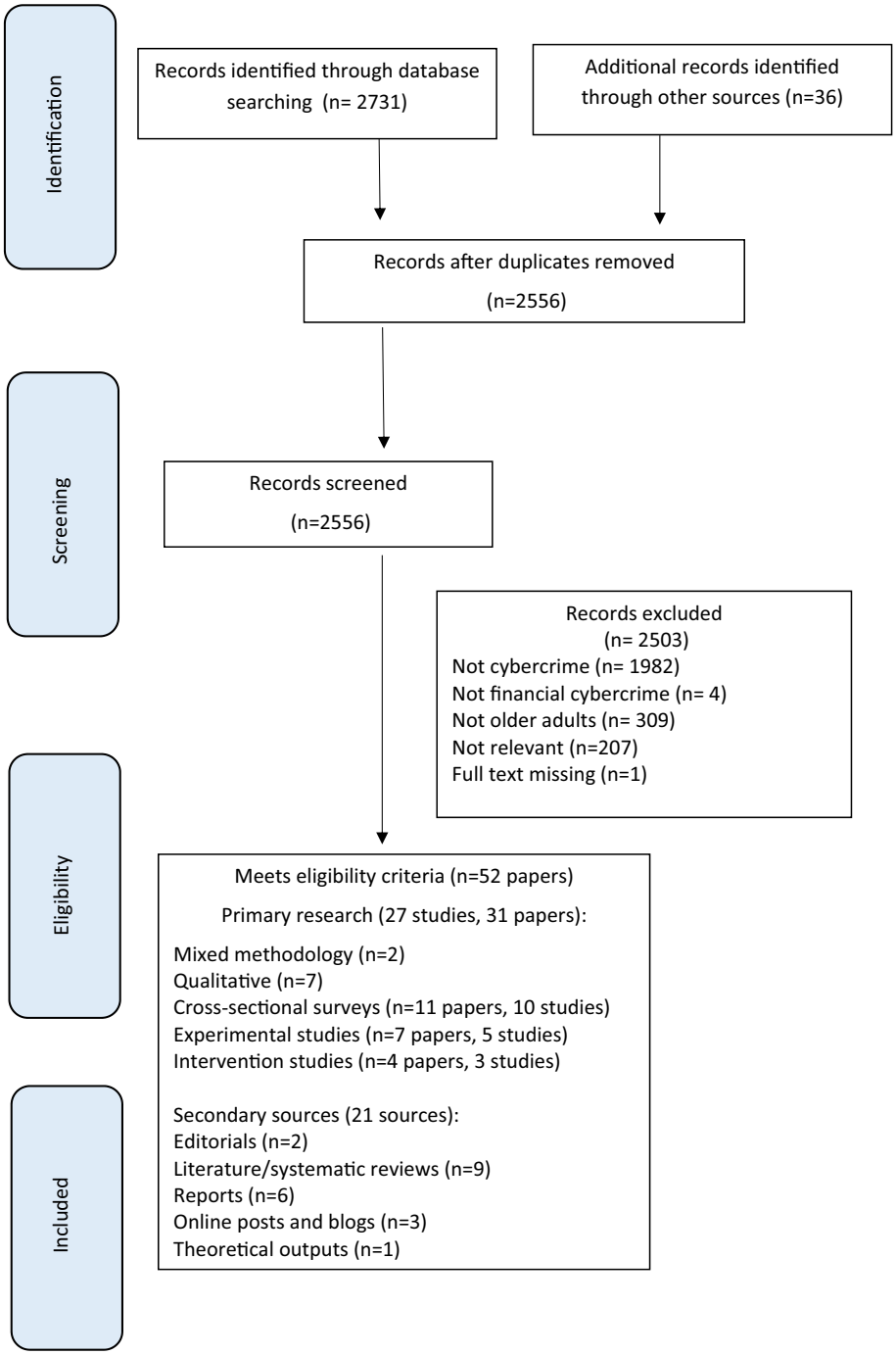

Fig. 2. Diagram of study selection (adapted from Moher et al., 2009).

and likely victims converge in cyberspace (Reyns, 2011; Leukfeldt and Yar, 2016; Pratt et al., 2010).

3.3. Formal literature search and synthesis

Fig. 2 shows our diagram for selection of studies for inclusion. We included 49 papers from our main search, and an additional 3 from our updated search in July 2021, yielding a total of 52 reports and articles

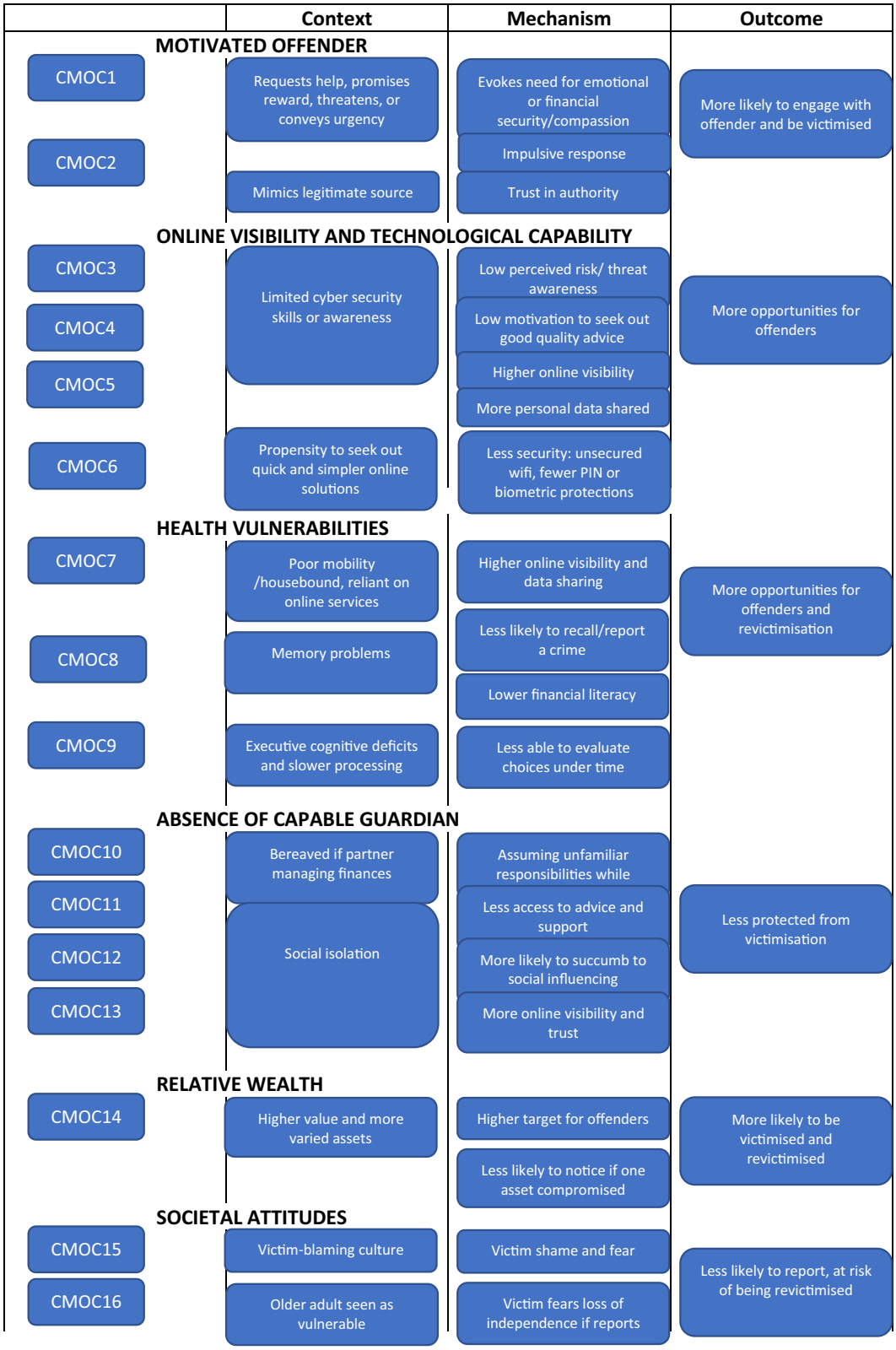

Fig. 3. Mid-range programme theory illustrating 16 CMOCs.

(Moher et al., 2009).

3.3.1. Description of included sources

27 studies (31 papers) reported primary research findings. Seven of these used qualitative (Tripathi et al., 2019; Mentis et al., 2019; Nicholson et al., 2019; Morrison et al., 2020; Bailey et al., 2021; Cross, 2016; Cross, 2015) methods, 10 were cross-sectional survey (reported in 11 papers) (Bergmann et al., 2018; Chia et al., 2017; Han et al., 2016; Muscat et al., 2002; Judges et al., 2017; Whitty, 2019; Whitty, 2018; Jones et al., 2019; Kolimi et al., 2012; O'Connor et al., 2021; Grigoryeva, 2014) and two mixed methods (Bolimos and Choo, 2017; Skidmore et al., 2020) design to explore prevalence, experiences, or correlates of financial cybercrime in older adults. Five studies (reported in 7 papers) were experimental (Ebner et al., 2020; Lin et al., 2019; Oliveira et al., 2017; Nino et al., 2017; Morgan et al., 2019; Alwanain, 2020; Sarno et al., 2020), evaluating whether older adults could distinguish between genuine and fraudulent emails; and three studies (reported in 4 papers) tested the effectiveness of cyber security training (Blackwood-Brown et al., 2019; Nicholson and McGlasson, 2020; Garg et al., 2012; Blackwood-Brown et al., 2018). For full characteristics of primary studies see Tables 2–5. We also included 21 secondary data sources: editorials (Munanga, 2019; Saariluoma, 2016), literature/systematic reviews (Watson et al., 2018; Davidson et al., 2015; Carlson, 2006; Norris et al., 2019; Kane, 2015; Lee, 2018; UK, 2015; Crosby et al., 2007; Lippert and K., 2017), reports (Her Majesty's Inspectorate of Constabulary and Fire &amp and Rescue Services, 2019; Rosenorn-Lanng et al., 2019; AVIVA, 2020; Gloag et al., 2019; Karagiannopoulos et al., 2019), online posts and blogs (Kirchheimer, 2012; USA, 2019) and theoretical outputs (Myojin and Babaguchi, 2018).

3.3.2. Summary of findings

Fig. 1 illustrates how our initial programme theory (Fig. 1a) was developed, using findings from our systematic review and discussions with stakeholders, to make a refined programme theory (Fig. 1b). Comparing Fig. 1a and b shows how we developed our programme theory, to include a broader range of factors conferring opportunities to offend. We describe below how we synthesised and used review findings to develop theory. We created 16 CMOCs configurations during this process. These sought to provide an explanatory account of why, how and in what contexts older adults may become victims of online financial crime (Fig. 3). We organised them into three overarching risk factors: i) scam content (developed by a motivated offender), ii) opportunities to offend and iii) societal responses to financial cybercrime and older people and used them to refine our programme theory.

3.3.2.1. Scam content (developed by a motivated offender). The presence of a motivated offender is an essential first step in the pathway to financial cybercrime (Cohen and Felson, 1979). The tactics employed by offenders to increase success are multi-fold.

CMOC1. If the content of an online financial scam contains a threat, request for help or promises reward (C) this provokes an emotional response in the user (M) increasing the likelihood they will respond to the offender's request (O).

Persuasive techniques are designed to evoke emotional, visceral responses by appealing to compassion for others and needs for financial and emotional security (companionship). Scam emails often imply threats of negative consequences (Nino et al., 2017; Garg et al., 2012; Rosenorn-Lanng et al., 2019). Phishing emails increase anxiety about not responding; e.g. 'If you do not contact us on the following, your account may be closed' (Garg et al., 2012). Befriending or grooming techniques, such as identification with victim characteristics appear most effective in older adults who are socially isolated (Age-UK, 2015; Her Majesty's Inspectorate of Constabulary and Fire &amp and Rescue Services, 2019; Bolimos and Choo, 2017). Emotional responses can encourage impulsive decisions, and thus a greater likelihood of responding to scams, especially where they demand a rapid response (Sarno et al., 2020; Rosenorn-Lanng et al., 2019), for example emails entitled '*Urgent assistance needed*' (Crosby et al., 2007).

CMOC2. If an online financial scam appears to be from a legitimate source (C), due to their relative greater trust in authority (M), older users may be more likely to respond to the request (O).

Older adults were more likely to respond to communications from apparently legitimate sources, for example reputable businesses or official institutions, and this appeared to be due to a greater trust in authority (Age-UK, 2015; Bolimos and Choo, 2017; Kane, 2015; Lee, 2018; Rosenorn-Lanng et al., 2019; Kirchheimer, 2012). Scammers impersonated organisations, including banks, police or government departments to extract personal or financial information, for example by alleging issues with payment, account security or an outstanding refund (Rosenorn-Lanng et al., 2019).

3.3.2.2. Online visibility and technological capability. **CMOC3**. If older adults have limited cyber security skills or awareness (C), then their perception of victimisation risk will be low, and they will lack motivation to seek out cybersecurity protection information (M) resulting in increased opportunities for offenders (O).

Older adults may have limited cyber security skills or awareness due to fewer years of exposure to technology (Sarno et al., 2020; Blackwood-Brown et al., 2019; Kane, 2015). People who had previously used computers at work were found to have better cyber security skills and more motivation to learn new skills (Nicholson et al., 2019; Saariluoma, 2016). Limited technological capability was associated with reduced awareness of one's vulnerability online and thus motivation seek protection; and with lower capability to seek out cyber security information; and identify illegitimate sources of communication (Chia et al., 2017).

CMOC4. If older adults have limited cyber security awareness (C) then their perception of victimisation risk will be low, and their online visibility may be high (M) resulting in increased opportunities for offenders to target them (O).

A low perception of risk or lack of understanding of security threats may lead to more unguarded technology use, increased online visibility and sharing of personal details (Davidson et al., 2015; Nicholson et al., 2019; Kane, 2015). Criminals often target social network websites, where novice users are more likely to post personal information due to a lack of awareness of dangers of disclosures (Kane, 2015). For example, they may leave Wi-Fi and Bluetooth turned on permanently, and thus personal information exposed (Chia et al., 2017). In one study, older adults were aware of phishing, but unaware of their own susceptibility and how their own behaviours may put them at risk (Nicholson et al., 2019).

CMOC5. If older adults have limited cyber security skills (C) then they will be unfamiliar with online security language and jargon and less likely to identify illegitimate sources/emails (M) resulting in increased risk of victimisation (O).

Lack of familiarity with online security language and jargon may lead to use of unsecured Wi-Fi networks and provide offenders with easy access to devices (Nicholson et al., 2019; Kane, 2015). This is not universal – one study reported greater propensity of older people to detect fraudulent emails, and greater caution in considering emails may be fraudulent (O'Connor et al., 2021).

CMOC6. If older adults are more likely to seek out quick and simpler solutions to accessing online services (C) then they may be more likely to use unsecure Wi-Fi networks, seek advice from people in their networks with limited expertise, and be less likely to adopt PIN or biometric

protections (M) resulting in increased opportunities for offenders to target them (O).

Older adults have reported to be more likely to seek out informal support to achieve quick and simple solutions to online access (Nicholson et al., 2019; Chia et al., 2017), potentially leading to risky decision making. This may include seeking local or easily accessible advice, even where they have access to greater IT expertise. Motivated by ease of accessing services, older adults are less likely to adopt PIN or biometric protections (Nicholson et al., 2019; Chia et al., 2017). In a small survey, 43.6% of older smart phone users did not lock their devices (Chia et al., 2017). One report suggested that half of global smartphone owners do not set a password, install antivirus software, or create backup files (Grigoryeva, 2014).

3.3.2.3. Health vulnerabilities. **CMOC7**. If an older adult experiences declining health and mobility (C) they may rely more on online banking, shopping, health care and social media services, sharing personal details more frequently, resulting in increased online visibility (M) and risk of victimisation (O).

One response to declining health and mobility, heightened by the pandemic, is to use online services, increasing the risk of identity theft (Blackwood-Brown et al., 2019). The purchase of some health-related products or services may identify them to offenders as being more vulnerable (Garg et al., 2012; Blackwood-Brown et al., 2018).

3.3.2.4. Cognitive decline. **CMOC8**. If an older adult has memory problems (C) they may find it difficult to recall information about a crime or be unaware that a crime has taken place (M) leading to a lack of reporting and investigation of the crime and risk of repeat victimisation (O).

Memory loss may reduce awareness or understanding that a crime has occurred and ability to recall details of the crime or offender (Nino et al., 2017; Gloag et al., 2019). It may only be a third party such as a family member who notices the deception (Gloag et al., 2019). Memory loss may reduce financial literacy if users cannot recall or act on signs of a potential scam (Mentis et al., 2019; Han et al., 2016). Scammers may attempt to fill gaps in memory with information that enables frauds to be committed (Han et al., 2016). People with Mild Cognitive Impairment (MCI) were less able to recognize scams such as email phishing, compared with healthy controls in one study (Mentis et al., 2019); though in the early stages of cognitive decline, users may develop strategies to compensate for memory loss, including more cautious decision making (Sarno et al., 2020).

CMOC9. If an older adult is experiencing executive cognitive deficits (impaired judgement or impulsivity) and/or reduced perceptual speed (C) they are less able to understand and evaluate potential choices, particularly under time pressure (M), increasing their risk of victimisation (O).

Cognitive decline may result in the user being less able to understand and evaluate choices, particularly under time pressure (Nicholson et al., 2019). This may relate to difficulties with divided attention tasks (Mentis et al., 2019; Morgan et al., 2019); or reduced processing speed, as in one study with people with MCI (Han et al., 2016). Changes in the ventromedial prefrontal cortex are associated with increased gullibility and suggestiveness in people with cognitive decline (Judges et al., 2017); and with age-related changes in risky decision making (Judges et al., 2017). These deficits may decrease likelihoods of following recommended security measures (Mentis et al., 2019). Being interrupted by a pop-up may increase susceptibly to scams, due to the increased cognitive load that divided attention demands (Morgan et al., 2019).

3.3.2.5. Absence of a capable guardian. Social isolation is common in older populations, who are more likely to have smaller social networks, be bereaved of a partner or live alone. It increases the risk of victimisation, due to the absence of protective social networks, or as termed in Routine Activation Theory, "a capable guardian" (Cohen and Felson, 1979); as well as the impact of the fraud on the victim (Skidmore et al., 2020).

CMOC10. If an older adult is bereaved of a partner who was responsible for financial matters (C) then assuming new and unfamiliar financial responsibilities at a time of stress and grief (M) may impair their ability to identify scams and increase their risk of victimisation (O).

Social isolation limits opportunities to discuss concerns or doubts about the legitimacy of financial email or internet requests, and, those who live alone cannot rely on others to identify or intercept scams (Nicholson et al., 2019; AVIVA, 2020). People who are recently bereaved may feel out of control of issues that were previously dealt with by their partner (Age-UK, 2015). This may make it easier to make mistakes (Gloag et al., 2019).

CMOC11. If an older adult is socially isolated (c) then they are at an increased risk of victimisation (O) because they have limited opportunities to discuss potential scams and seek advice from others (M).

Nicholson and McGlasson (2020) found that older adults with relatively weak social ties and/or poor digital literacy are less likely to learn from peers, and to assess the quality of advice. In their report on cybercrime in the pandemic, AVIVA (2020) noted that one fifth of the UK population were targeted by suspicious communications (e.g. emails, texts and phone calls) mentioning coronavirus. Isolated older people are less likely to be aware of their rights and know where to turn for help (Age-UK, 2015).

CMOC12. If an older adult is lonely (C) then the use of social influence methods such as identifying with victim characteristics or befriending/grooming techniques (M) increase the likelihood that older users will respond to the scam/offender and be victimised (O).

CMOC13. If an older adult is lonely (C), then their online visibility and trust in strangers may increase as they seek out connections with others online (M) leading to increased risk of financial cybercrime victimisation (O).

Loneliness can provide the initial motivation for older people to meet people online, and therefore lead to increased visibility to offenders (Bolimos and Choo, 2017). It also provides the means through which offenders can establish a relationship with victims (Cross, 2015). Fraudsters commonly attempt to establish rapport with victims, creating a sense of trust that increases their willingness to act on fraudulent guidance or advice (All-Party Parliamentary Group on Financial Fraud and Scamming 2019). 'Grooming' or befriending is common in investment fraud (Age-UK, 2015). It is also central to romance scams, which Whitty (2019, 2018) has described as "a 'double hit'–a financial loss and the loss of a relationship". These relationships of trust are associated with greater financial losses (Bolimos and Choo, 2017).

3.3.2.6. Relative wealth. **CMOC14**. If older adults have high value, varied assets (C) they may be more likely to be targeted and less likely to notice financial loss (M) and to report a crime, and thus are at risk of repeat victimisation (O).

Older people can be a favoured target as they are more likely to have a higher credit limit, and less likely to check their balance online between statements (Age-UK, 2015); they may also have greater variety of assets than younger adults, such as property, life savings (Tripathi et al., 2019; Bolimos and Choo, 2017; Lin et al., 2019), inheritance (All-Party Parliamentary Group on Financial Fraud and Scamming 2019) and good credit scores. People with multiple assets may be less likely to notice and therefore report a crime (Age-UK, 2015; Nino et al., 2017).

3.3.2.7. Societal response to financial cybercrime and older people.

CMOC15. When financial cybercrime is not perceived as serious by society and prevailing attitudes blame the victim (C) older adults experience embarrassment, shame and fear of not being taken seriously (M) and are less likely to disclose victimisation, making them at increased risk of repeat victimisation (O).

Pervasive societal attitudes blame the victim for gullibility or greed (Carlson, 2006; Age-UK, 2015; Han et al., 2016; Kane, 2015; Karagiannopoulos et al., 2019; The RAMES Projects 2013), leading to victim embarrassment, shame or fear of not being taken seriously and therefore non-reporting and repeat victimisation (Age-UK, 2015). Victims may fear not being heard or feel unable to seek out information on whether and how to report the crime. These victim-blaming attitudes are pervasive and, for many individuals, exacerbate the impact of the crime, inhibit disclosure and are a barrier to accessing support (Cross, 2016). Any negative response to reporting fraud makes victims feel blamed and foolish; this may contrast with the relationship they developed with the fraudster (Age-UK, 2015).

CMOC16. When older adults are perceived as vulnerable by society (c) they are less likely to disclose they have been a victim of crime making them at increased risk of repeat victimisation (o) because they fear a reduction or loss of their independence (m).

Older people may fear that disclosing financial cybercrime will be interpreted as a decline in their capacity or ability to selfcare, resulting in a loss of independence (Cross, 2016). They may be less inclined to report fraud because of concern that their relatives will lose confidence in their abilities to manage their own financial affairs (USA, 2019).

3.4. How should we intervene?

Most existing evidence addresses CMOC 3–6, digital awareness and skills of the victim, which secondary research has extrapolated to contexts of 'health vulnerability' (Fig. 3). We found three primary studies evaluating interventions to protect older adults from cybervictimisation (Table 2). All aimed to increase knowledge, awareness and peer support for older people without cognitive impairment, to reduce risks. Secondary sources have considered how training materials might be tailored to people, including those with cognitive impairment, for example video messages could be more accessible than text material (Garg et al., 2012), and real-life scenarios relevant to older people may increase impact of messages (Blackwood-Brown et al., 2018). Other authors have suggested a solutions-based approach - "this is how you resolve the issue" rather than "you are at risk" (Kane, 2015); and "If in doubt leave it out" – slogans that reinforce key messages, such as not to open suspicious-looking emails (Nicholson and McGlasson, 2020). Multiple training sessions, peer-based learning and branding to appeal to older people are suggested (Blackwood-Brown et al., 2018). Bolimos and Choo (2017) advise explicitly informing older people about common frauds. For example, a simple intervention to raise awareness of phishing through demonstration of what an attack is like (in an email directing users to a website with a warning message) reduced the risk of clicking on an illegitimate link subsequently (Alwanain, 2020).

In areas where there was no primary research evidence regarding intervention strategies, stakeholder group lived and clinical experiences suggested a number of potential options. No intervention study has intervened directly with offenders (i.e. addressed CMOC 1 and 2, the motivated offender). Experts in crime (police and academic) suggested that behavioural management programmes, aimed at reducing repeat offending may promote reflection on victim impact of crimes, which can be easily minimised due to the remoteness of cyber victims.

The group considered that a successful intervention to safeguard people with cognitive impairment (CMOC 7–9) would combine training in cybercrime detection and prevention for health and social care, third sector and other public workers such as librarians, with Artificial Intelligence (AI) approaches. These might include enhancing usability of security software for people with cognitive impairment; for example, use of biometrics that do not require password recall, or provide warnings when online visibility is high. To address low rates of cybercrime reporting by older people, the group suggested information campaigns about online and offline reporting options.

Information campaigns targeting workers and family members who support older online users, could usefully include strategies for detecting and managing incidents of cybercrime, including situations where victims are unaware of frauds. These would address CMOC 10–13, by reducing risks from absence of a "capable guardian". The group commented that older people who have appointed a family member or friend as Lasting Power of Attorney, may be at risk of financial abuse within this relationship. Though overseen in England by the Court of Protection, management of affairs of the donor may be subjected to few checks if no concerns are reported.

At a societal level (CMOC 15 and 16), the group prioritised changing victim blaming discourses, through providing education and communication skills training to those supporting victims of online fraud (police, charity workers, health, and social workers), and positive campaigns from financial institutions. Use of national media to mainstream messages around online financial fraud was suggested (Nicholson et al., 2019; Lippert and K., 2017).

4. Discussion

We have elucidated mechanisms explaining cybercrime risk factors in older people and considered potential theory and evidence-based intervention strategies. Our CMOCs encompass seven factors: social isolation, health vulnerabilities, memory loss; wealth, limited cyber security skills or awareness, societal attitudes and scam content. Only interventions to enhance the awareness and skills of potential older victims have been tested to date. Targeting offender motivation, and redesign of security software to increase usability by older people are rational, as yet untested interventions. With greater awareness of cybercrime risks and prevention, professionals and family members may be empowered to support potentially more susceptible older online users to continue engaging online safely, and signpost them to appropriate IT support. A shift in societal attitudes, conveying positive messages, of older people's rights to be safely active online, is needed too. Negative ageist discourse blames the victim (gullible, greedy, culpable, stupid, suckers) and relates cybercrimes to victim deficits (lack of friends, family, common sense, cognition, decline, deterioration) which in turn discourage reporting of the crime (Cross, 2016; Cross, 2015).

While we hypothesise that interventions to target identified mechanisms will protect susceptible older people against cybercrime, future research is needed to develop and test theory and evidence-based, multidisciplinary interventions. Our work can inform these. Training programmes targeting older adults, or their supporters should be deliverable by a range of professionals for greatest reach; and be co-designed with end users to ensure that if they are useful, they are acceptable and used (Burton et al., 2019).

We suggest that stronger legal safeguards could reduce opportunities for financial cybercrime, to protect older people, the fastest growing group of internet users. The omission of fraud from the new UK Online Safety Bill, which plans to strengthen legal sanctions against hate crimes, harassments and threats is a concern, especially as this appears to be based on an erroneous belief that older people are not at greater risk of cybercrime than younger people (Conway, 2021). This is not supported by the evidence presented here which suggests that there are specific social, cognitive and health related factors that need to be considered for older people to navigate online spaces safely and to be supported and encouraged to report financial cybercrime where it occurs.

4.1. Strengths and limitations

This realist review is the first to explore the theoretical basis for interventions to reduce risks of cybercrime in older populations. A persistent problem with previous research on cybercrime prevention has been that it treats victims as a homogenous category, and therefore suggests very broad prevention measures (Karagiannopoulos et al., 2021). Through developing a framework for conceptualising this risk across different contexts, our novel contribution is to develop a refined programme theory that can guide future plans to develop and implement more targeted interventions to reduce the risk of financial cybercrime in older adults. We adhered to established guidelines and included a broad range of stakeholders. As well as representing diversity in perspectives and experience, there was also diversity in research, clinical and lived expertise. We considered this a strength but it also presented challenges in ensuring that all stakeholders were supported to participate in and influence the review. We focused on the UK context and our findings may not be generalisable to other jurisdictions. While we have extrapolated findings and used expert opinion to consider intervention approaches most likely to be effective, we found only one randomised controlled study. We did not exclude any studies wholly on grounds of rigour, in part due to this paucity of robust trial evidence, and the robustness of our evidence is inherently limited by that of the evidence from which it is derived.

5. Conclusions

Societal, structural protections are needed to enable us all to continue being as digitally active as we would like, safely in older age. While direct intervention with older people appears to reduce cybercrime risks in small studies, measures to change societal attitudes, reduce offending and increase protections are also needed. We support calls for legal changes to enhance online protections against financial frauds.

Funding

This work was supported by the Dawes Trust, which funds the UCL Dawes Centre for Future Crime. The funder had no role in study design; collection, analysis and interpretation of data; in the writing of the report; or the decision to submit the article for publication.

Declaration of competing interest

None.

Appendix A. Additional tables

Table 1
Database and journal search sources.

Databases
Criminal Justice Database (ProQuest)
IBSS: International Bibliography of the Social Sciences (ProQuest)
ACM Digital Library
Engineering Village
Web of Science
IEEE Xplore Digital Library
Scopus
PsycINFO

Journals
Computers & Security
Computers in Human Behavior
Procedia Computer Science
Computer Law and Security Review
International Journal of Advanced Computer Science and Applications
Journal of Theoretical and Applied Information Technology
Digital Investigation
Journal of Information Security Applications (JISA)
Transactions on Privacy and Security (TOPS)
Transactions of Information, Forensics and Security (TIFS)

Conference proceedings
USENIX Security
Annual Computer Security Applications Conference (ACSAC)
Computers and Communication Systems (CCS)
Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
Conference on Human Factors in Computing Systems (CHI)
The Network and Distributed System Security Symposium (NDSS)
Conference on Computer-Supported Cooperative Work and Social Computing (CSCW)

Table 2
Studies evaluating interventions to reduce the risk of cybercrime.

Study	Study design	Population	Intervention/control	Findings
Blackwood-Brown et al. (2019); Blackwood-Brown et al. (2018)	Single group, mixed methods	254 USA people aged 60+, accessing internet for 1 year+	Intervention: 1 × 2-hour face-to-face cybersecurity awareness training	Cybersecurity skills to take mitigating actions against cyberattacks increased; qualitative interviews suggested longer sessions needed to process information and multiple rather than a single session helpful
Nicholson and McGlasson (2020)	Single group, mixed methods	14 computer-users aged 55–80 from England unselected for IT skills, trained as Cyber-guardian	Intervention: 3 × 3 interactive workshops on University premises, with presentations, videos, live demonstrations, (e.g. password cracking) and hands on activities (e.g. phishing tests). Topics identified by the group and existing literature	Participants interacted with on average 9 people after their training, in role of Cyber-guardian; flexible training materials that can be adapted by CyberGuardians for sharing with peers were most helpful.
Garg et al. (2012)	Randomised study	249 USA people aged 65+ recruited to be representative of older population	Intervention (n = 136): Participants shown two videos – where an older man was persuaded to give out personal information (physical representation of phishing), and a caller gained entry to covertly place a device on his telephone (malware representation); Control (n-113): Similar information provided in text form	For phishing – no significant difference in ratings of attitudes to risk or predicted behaviour (rated on Likert scales); for malware, video group perceived the risk as greater after intervention relative to control (p = 0.03)

Table 3
Studies exploring cybercrime in older people, through qualitative interviews or mixed methods.

	Aim	Population/data sources	Findings related to older people and cybercrime
Qualitative interview studies			
Mentis et al. (2019)	To determine how a person with MCI and their caregiver respond to cybersecurity incidents	6 USA people with MCI and their carers	Themes: 1) Experiences of dyad with technology 2) caregivers limiting unsupervised online interactions or keeping a minimal check 3) lack of forethought and planning for supporting online engagement
Cross (2016)	To explore two discourses: 1. older victims are weak & vulnerable; 2. fraud victims generally positioned as greedy and gullible	21 Canadian volunteers aged 60+ at telephone support line for older fraud victims	Volunteers overwhelmingly perceive fraud to occur out of loneliness and isolation of the victim, and actively resist victim blaming narratives towards these individuals.
Cross (2015)	To explore discourses that surround victims who experience online fraud and how it is discussed	85 Australians aged 50+ who had received a fraudulent email request	Victim-blaming discourse is overwhelmingly powerful and controlling discourse; humour can reinforce this discourse by isolating victims and impacting disclosure
Nicholson et al. (2019)	To explore cybersecurity information seeking behaviours, to understand what lifestyle and digital literacy factors affect ability to obtain/assess information and advice	22 UK older internet users	Participants lacked confidence using the internet to find security information, some older users cannot articulate their problems or understand the information on offer. Tended to seek help from family members or friends, using opportunistic rather than strategic approach.
Morrison et al. (2020)	To explore interactions with online and offline technology changes, and how these are associated with cybersecurity vulnerabilities	12 UK adults who retired in last 5 years, with experience using technology	Themes: 1. Renewing Social Interaction, and vulnerabilities arising from: 2. Losses of social interaction, 3. financial changes, 4. loss of sense of purpose, 5. loss of day-to-day routine, 6. loss of perceived competence, 7. losing support
Tripathi et al. (2019)	To explore vulnerability factors for cybercrime among older people in Mumbai, and its impact	6 adults aged 60+ who have been victims of cybercrime, 7 experts	1. Unresponsive institutions, 2. Lack of data protection and privacy safeguards, 3. lack of proximal family support, 4. relative affluence, 5. impact on older people
Bailey et al. (2021)	To investigate the impact of scams on individuals	80 UK participants aged 50+ in a Mass Observation project	Themes: 1. Exposure, 2. Anxiety, 3. Censure, 4. Protective behaviours
Mixed methods studies			
Bolimos and Choo (2017)	Quantitative: To test hypothesis that "Older people are more prone to being victims of online fraud" in national data; qualitative: To explore how to best apply resources to combat online fraud	Quantitative: 7383 incidents of online fraud reported in Australian national crime data 2008–13. Qualitative: 3 agency electronic crime investigators	Quantitative: reports decreased in younger people but increased with time in people aged 61+; proportion of all reports in 61+ age group increased from 9% in 2008–2009, to 13% in 2012–2013; 41–60 year olds reported greatest financial losses. Qualitative: relative wealth, living alone, internet/computer inexperience vulnerability factors
Skidmore et al. (2020)	To explore the meaning of vulnerability in the context of fraud	Quantitative: national crime data (n = 61,902), qualitative: interviews with practitioners (n = 107) & survey of strategic lead police officers (n = 32).	Quantitative: Greater vulnerability associated with greater impact of fraud; qualitative: lack of clarity across practitioners and organisations in their understanding of vulnerability and the way it informed the police response to fraud, and a lack of resources and capability for identifying it.

Table 4
Surveys investigating cybercrime in older people.

Study	Topic of survey	Population	Findings
Chia et al. (2017)	Security and privacy risks experienced	55 Singaporean Chinese smart mobile device users aged 45+, 10% aged 65+; Convenience sample	32.7% experienced difficulty understanding information accessed; 38.2% said they were unlikely to read information before downloading an app; and 87.3% reported insufficient understanding of phishing
Muscat et al. (2002)	Consumer fraud victimisation	2005 Australian Crime Victims Survey respondents in 2000: probability sample of aged 16+ national population; 1026 people aged 65+ asked about victimisation in detail	People aged 65+ were less likely than younger adults to be fraud victims, and more likely to report fraud if also victims of personal crime and report going out in the evening at least weekly
Han et al. (2016)	Susceptibility to scams	738 older adults (aged 58–100) from a USA community research study.	People with MCI self-report higher susceptibility to scams than those without MCI; episodic memory and perceptual speed were associated with susceptibility
Judges et al. (2017)	Fraud victimisation	151 Canadian community-dwelling adults, convenience sample, aged 60–90, without cognitive impairment or neurological disorder diagnosis, managing own finances.	Victims were significantly less honest and humble and conscientious and had lower cognitive scores than non-victims. For generalised trust there were no significant relationship with victimhood
Grigoryeva (2014)	Content of computer and internet courses for older people	8 courses, in Belarus, Russia, Lithuania and Denmark: conveniences sample	5 discussed cybercrime; 3 use of anti-virus software, 1 security risks of Internet communication, and 2 E-commerce risks
Whitty (2019); Whitty (2018)	Romance scam victimisation	11,780 UK participants (aged 18–93); random sample from a panel of research volunteers	728 were one-off victims, 329 repeat victims of cyber-frauds; victims were older, scored higher on addictive and impulsivity measures and engaged more frequently in routine, risky activities than non-victims. There was little difference between one-off and repeat victims. Most romance scam victims were middle-aged
Kolimi et al. (2012)	Attitudes to information privacy	Convenience sample of students aged 17–33 from previous survey; and older group (Leukfeldt and Yar, 2016; Pratt et al., 2010; Mentis et al., 2019; Nicholson et al., 2019; Morrison et al., 2020; Bailey et al., 2021; Cross, 2016; Cross, 2015; Chia et al., 2017; Han et al., 2016; Muscat et al., 2002; Judges et al., 2017; Whitty, 2019; Whitty, 2018; Jones et al., 2019; Kolimi et al., 2012; O'Connor et al., 2021; Grigoryeva, 2014; Bolimos and Choo, 2017; Skidmore et al., 2020; Ebner et al., 2020; Lin et al., 2019; Oliveira et al., 2017; Nino et al., 2017; Morgan et al., 2019; Alwanain, 2020; Sarno et al., 2020; Blackwood-Brown et al., 2019; Nicholson and McGlasson, 2020; Garg et al., 2012; Blackwood-Brown et al., 2018; Saariluoma, 2016; Kane, 2015; Lee, 2018; UK, 2015; Crosby et al., 2007; Lippert and K., 2017; Rosenorn-Lanng et al., 2019; AVIVA, 2020) who were students' parents, co-workers, guardians, friends	For 21/26 identity elements, older participants were significantly more likely than younger adults to rate them 'extremely important' to keep private
Jones et al. (2019)	The words people associate with cyber security	Convenience sample of 503 respondents, aged 11–18 (n = 146) recruited from schools, working age adults from social media (n = 211), and aged 60+ from community groups (n = 146)	Older adults used less positive and social process-related language, and more anxiety-related words
Bergmann et al. (2018)	Cyber offence victimisation	Random sample of 26,665 Internet users in two in German states, aged 16–97	16.6% report at least one cybercrime: 11.5% malware, 3.6% a ransomware infection, and 5.3% misuse of personal data. Older people less likely to experience personal data loss
O'Connor et al. (2021)	Ability to detect fraudulent email activity	100 email users aged 18–26 years; and 96 adults aged 60–90 years who managed their own finances	Older adults more accurately detected fraudulent e-mail (83%) compared to younger adults (71%); and more frequently mistook legitimate e-mails as fraudulent (40% vs 26% of the time)

Table 5
Experimental studies (all uncontrolled apart from one) exploring vulnerability to cybercrime or interventions to reduce susceptibility to cybercrime.

Study	Sample	Experimental condition	Findings
Nino et al. (2017)	Swedish nursing home residents aged 65+ without dementia who used internet regularly, and members of a Swedish older people's forum (convenience sample)	Participants asked to distinguish fraudulent from genuine emails, and select reasons for decision from pre-determined list	Participants identified the following factors correctly as indicative of fraudulent email: grammatical errors (identified by 40%), spelling errors (25%), unprofessional design (35%); sender requesting fast reply (19%), appears threatening (34%), request seems unnecessary (23%), too good to be true (68%); address (27%) or links looked unreliable (17%)
Lin et al. (2019) Ebner et al. (2020) Oliveira et al. (2017)	100 younger (Hafemeister, 2003; Cooper et al., 2009; Cooper et al., 2008; Norris et al., 2019; Conway, 2021; Pawson et al., 2005; Wong et al., 2016; Bunn et al., 2017; CEBM, 2001; Cohen and Felson, 1979; Reyns, 2011; Leukfeldt and Yar, 2016; Pratt et al., 2010; Mentis et al., 2019; Nicholson et al., 2019; Morrison et al., 2020; Bailey et al., 2021; Cross, 2016; Cross, 2015; Chia et al., 2017), 41 young-old (62–74 years), and 16 middle-old	Participants were sent one simulated phishing email a day, and researchers observed whether they clicked on it; on final study day (day 21), they were sent 21 emails and asked to rate likelihood they would click on them, to assess awareness of behaviour	No age group differences in susceptibility or susceptibility awareness; though older women most vulnerable group. Higher susceptibility was associated with worse memory in middle-old users and lower mood in young-old and middle-old users. Greater susceptibility awareness was associated with better verbal fluency in middle-old users and better mood in young and middle-old users.

(*continued on next page*)

Table 5 (*continued*)

Study	Sample	Experimental condition	Findings
	(75–89 years) regular internet users, convenience community sample from Florida, USA		
Morgan et al. (2019)	Convenience sample of 29 UK computer-users aged 60+ who scored 26+ on the Montreal Cognitive Assessment test.	Participants asked to distinguish between genuine, mimicked, and low authority pop-ups: (1) during serial recall memory trials; (2) with no interference/time constraints	Users were significantly more likely to accept pop-ups in phase one, and there was a main effect for message authority, with genuine emails relatively more likely than mimicked emails to be accepted in phase 2.
Sarno et al. (2020)	10 Florida University students and 10 adults aged 65+ from local community scoring 23+ on MMSE	Participants asked to distinguish 50 fraudulent from 50 genuine emails, with and without a time pressure	No age differences were observed in overall classification accuracy between age groups
Alwanain (2020)	20 adults from Saudi Arabia aged 60–75 years	Participants were sent a WhatsApp message with a hyperlink to a legitimate website (n = 10), or a website where they were notified this was a phishing attack (n = 10). 2 months later, all were sent link to phishing website	The number of users in the group sent the phishing link on both occasions decreased, indicating improvement in phishing and security awareness.

References

Age-UK, 2015. Only the tip of the iceberg: fraud against older people. In: Evidence Review.

Age-UK, 2017. Older People, Fraud and Scams. Age UK.

All-Party Parliamentary Group on Financial Fraud and Scamming, 2019. The Impact of Frauds and Scams on Vulnerable People.

Alwanain, M., 2020. Phishing awareness and elderly users in social media. Int. J. Comput. Sci. Netw. Sec. 20, 5.

AVIVA, 2020. The Aviva Fraud Report. Available from. Aviva.

Bailey, J., Taylor, L., Kingston, P., Watts, G., 2021. Older adults and "scams": evidence from the mass observation archive. J. Adult Prot. 23 (1), 57–69.

Bergmann, M.C., Dreissigacker, A., von Skarczinski, B., Wollinger, G.R., 2018. Cyber-dependent crime victimization: the same risk for everyone? Cyberpsychol. Behav. Soc. Netw. 21 (2), 84–90.

Blackwood-Brown, C., Levy, Yair, D'Arcy, John, Wang, Ling, 2018. An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills. ProQuest Dissertations and Theses.

Blackwood-Brown, C., Levy, Y., D'Arcy, J., 2019. Cybersecurity awareness and skills of senior citizens: a motivation perspective. J. Comput. Inf. Syst. 61 (3), 195–206.

Bolimos, I.A., Choo, K.-K.R., 2017. Online fraud offending within an Australian jurisdiction. J. Financ. Crime 24 (2), 277–308.

Bunn, F., Goodman, C., Reece Jones, P., Russell, B., Trivedi, D., Sinclair, A., et al., 2017. What works for whom in the management of diabetes in people living with dementia: a realist review. BMC Med. 15 (1), 141.

Burton, A., Ogden, M., Cooper, C., 2019. Planning and enabling meaningful patient and public involvement in dementia research. Curr. Opin. Psychiatry 32 (6), 557–562.

Carlson, E., 2006. Phishing for elderly victims: as the elderly migrate to the internet fraudulent schemes targeting them follow. Elder Law J. 14, 423–452.

CEBM, 2001. Levels of Evidence and Grades of Recommendation. Available from. Centre of Evidence Based Medicine website [Internet]. http://www.pdptoolkit.co.uk/Files/ebm/cebm/Doing%20ebm/levels_of_evidence.htm#notes.

Chia, C., KKR, Choo, Fehrenbacher, D., 2017. In: How Cyber-savvy are Older Mobile Device Users?, pp. 67–83.

Citizen's Advice Report, 2020. Prevalence of Scams in Lockdown.

Cohen, L.E., Felson, M., 1979. Social change and crime rate trends: a routine activity approach. Am. Sociol. Rev. 44 (4), 588–608.

Conway, L., 2021. Consumer Protection: Online Scams. House of Commons Library, London.

Cooper, C., Selwood, A., Livingston, G., 2008. The prevalence of elder abuse and neglect: a systematic review. Age Ageing 37 (2), 151–160.

Cooper, C., Maxmin, K., Selwood, A., Blanchard, M., Livingston, G., 2009. The sensitivity and specificity of the modified conflict tactics scale for detecting clinically significant elder abuse. Int. Psychogeriatr. 21 (4), 774–778.

Cooper, C., Mansour, H., Carter, C., Rapaport, P., Morgan-Trimmer, S., Marchant, N.L., et al., 2021. Social connectedness and dementia prevention: pilot of the APPLE-tree video-call intervention during the Covid-19 pandemic. Dementia (London) 14713012211014382.

Crosby, G., Clark, A., Hayes, R., Jones, K., Lievesley, N., 2007. The Financial Abuse of Older People. A Review From the Literature. Centre for Policy on Ageing on Behalf of Help the Aged.

Cross, C., 2015. No laughing matter: blaming the victim of online fraud. Int. Rev. Vict. 21, 187–204.

Cross, C., 2016. They're very lonely': understanding the fraud victimisation of seniors. Int. J. Crime Justice Soc. Democr. 5, 60–75.

Davidson, S., Rossal, P., Hart, S., 2015. Financial abuse evidence review. In: Age UK Research.

DeLiema, M., 2018. Elder fraud and financial exploitation: application of routine activity theory. Gerontologist 58 (4), 706–718.

Dong, X., Simon, M.A., 2013. Elder abuse as a risk factor for hospitalization in older persons. JAMA Intern. Med. 173 (10), 911–917.

Ebner, N.C., Ellis, D.M., Lin, T., Rocha, H.A., Yang, H., Dommaraju, S., et al., 2020. Uncovering susceptibility risk to online deception in aging. J. Gerontol. B Psychol. Sci. Soc. Sci. 75 (3), 522–533.

Federal Trade Commission. Data and Visualizations 2020. Available from. https://www.ftc.gov/enforcement/data-visualizations.

Garg, V., Camp, L.J., Connelly, K., Lorenzen-Huber, L. (Eds.), 2012. Risk Communication Design: Video vs. Text. Springer Berlin Heidelberg, Berlin, Heidelberg.

Gloag, A., Mackenzie, P., Atay, A., 2019. Protected by Design. New Fraud Protections for People at Risk. DEMOS.

Seniior citizen in the internet - cybersecurity risks. In: Grigoryeva (Ed.), 2014. SGEM International Multidisciplinary Scientific Conferences on Social Sciences and Arts.

Hafemeister, T., 2003. Financial abuse of the elderly in domestic setting. In: WR, Bonnie R.J. (Ed.), National Research Council (US) Panel to Review Risk and Prevalence of Elder Abuse and Neglect. National Academies Press (US), Washington, USA.

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. J. Alzheimers Dis. 49 (3), 845–851.

Her Majesty's Inspectorate of Constabulary and Fire &amp, Rescue Services, 2019. The poor relation. In: The Police and CPS Response to Crimes Against Older People.

Jones, S.L., EIM, Collins, Levordashka, A., Muir, K., Joinson, A., 2019. In: What is 'Cyber Security'?, pp. 1–6.

Judges, R.A., Gallant, S.N., Yang, L., Lee, K., 2017. The role of cognition, personality, and trust in fraud victimization in older adults. Front. Psychol. 8, 588.

Kaldor, L., Klippan, L., Svejkar, D., Wong, J., 2019. Report for the NSW Department of Justice. Designing Out Crime, UTS Design Innovation Research Centre. https://static1.squarespace.com/static/57bbee1829687fe2a564ba75/t/6032ea137806406cda769a05/1613949477350/CAOP_Report_WEB.pdf.

Kane, D., 2015. Security Awareness Training of the Elderly: Means, Methods, Discovery, Safety, and Security..

Karagiannopoulos, V., Sugiura, L., Kirby, A., 2019. The Portsmouth Cybercrime Awareness Clinic Project: Key Findings and Recommendations. Institute of Criminal Justice Studies, University of Portsmouth.

Karagiannopoulos, D.V., Kirby, D.A., Oftadeh-Moghadam, S., Sugiura, D.L., 2021. Cybercrime awareness and victimisation in individuals over 60 years: a Portsmouth case study. Comput. Law Secur. Rev. 43, 105615.

Kirchheimer, S., 2012. 5 schemes and scams you may find hard to resist. Available from. In: Con Artists Target Older Victims. https://www.aarp.org/money/scams-fraud/info-06-2012/scams-targeting-older-victims.html.

Kolimi, S., Zhu, F., Carpenter, S., 2012. Is Older, Wiser?: An Age-specific Study of Exposure of Private Information.

Lee, N.M., 2018. Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom. Commun. Educ. 67 (4), 460–466.

Leukfeldt, E.R., Yar, M., 2016. Applying routine activity theory to cybercrime: a theoretical and empirical analysis. Deviant Behav. 37 (3), 263–280.

Lin, T., Capecci, D.E., Ellis, D.M., Rocha, H.A., Dommaraju, S., Oliveira, D.S., et al., 2019. Susceptibility to spear-phishing emails: effects of internet user demographics and email content. ACM Trans. Comput. Hum. Interact 26 (5).

Lippert, R.K.W., K., 2017. Funnelling through foundations and crime stoppers: how public police create and span inter-organisational boundaries. Policing and Society 27, 16.

Lopez, O.L., Kuller, L.H., Becker, J.T., Dulberg, C., et al., 2007. Incidence of dementia in mild cognitive impairment in the cardiovascular health study cognition study. Arch. Neurol. 64 (3), 416–420.

Mentis, H.M., Madjaroff, G., Massey, A.K., 2019. In: Upside and Downside Risk in Online Security for Older Adults With Mild Cognitive Impairment, pp. 1–13.

Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., The PRISMA Group, 2009. Preferred Reporting Items for Systematic Reviews and Meta Analyses: The PRISMA Statement. PLoS Med 6 (7), e1000097. https://doi.org/10.1371/journal.pmed1000097.

Morgan, P.L., Williams, E.J., Zook, N.A., Christopher, G. (Eds.), 2019. Exploring Older Adult Susceptibility to Fraudulent Computer Pop-up Interruptions. Springer International Publishing, Cham.
Morrison, B.A., Coventry, L., Briggs, P., 2020. Technological change in the retirement transition and the implications for cybersecurity vulnerability in older adults. Front. Psychol. 11, 623.
Munanga, A., 2019. Cybercrime: a new and growing problem for older adults. J. Gerontol. Nurs. 45 (2), 3–5.
Muscat, G., James, M., Graycar, A., 2002. Older people and consumer fraud. Australian Institute of Criminology, Canberra.
Myojin, S., Babaguchi, N., 2018. A logical consideration on deceived person's thinking. Artif. Life Robot. 24 (1), 114–118.
Nicholson, J., McGlasson, J., 2020. In: CyberGuardians: Improving Community Cyber Resilience Through Embedded Peer-to-peer Support. DIS' 20 Companion: Companion Publication of the 2020 ACM Designing Interactive Systems Conference; Eindhoven, Netherlands, pp. 117–121.
Nicholson, J., Coventry, L., Briggs, P., 2019. "If it's important it will be a headline": cybersecurity information seeking in older adults. In: CHI '19: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, pp. 1–11.
Nino, J.-R., Enström, G., Davidson, A.R., 2017. In: Factors in Fraudulent Emails That Deceive Elderly People, 10297, pp. 360–368.
Norris, G., Brookes, A., Dowell, D., 2019. The psychology of internet fraud victimisation: a systematic review. J. Police Crim. Psychol. 34 (3), 231–245.
O'Connor, A.M., Judges, R.A., Lee, K., Evans, A.D., 2021. Can adults discriminate between fraudulent and legitimate e-mails? Examining the role of age and prior fraud experience. J. Elder Abuse Negl. 33 (3), 181–205.
Dissecting spear phishing emails for older vs young adults: on the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In: Oliveira, D., Rocha, H., Yang, H., Ellis, D., Dommaraju, S., Muradoglu, M., et al. (Eds.), 2017. CHI '17: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Denver, CO, USA.
Pawson, R., Greenhalgh, T., Harvey, G., Walshe, K., 2005. Realist review–a new method of systematic review designed for complex policy interventions. J. Health Serv. Res. Policy 10 (Suppl. 1), 21–34.
Pratt, T.C., Holtfreter, K., Reisig, M.D., 2010. Routine online activity and internet fraud targeting: extending the generality of routine activity theory. J. Res. Crime Delinq. 47 (3), 267–296.
Rabiner, D.J., O'Keeffe, J., Brown, D., 2006. Financial exploitation of older persons. J. Aging Soc. Policy 18 (2), 47–68.
Reyns, B.W., 2011. Online routines and identity theft victimization. J. Res. Crime Delinq. 50 (2), 216–238.
Rosenorn-Lanng, E., Corbin-Clarke, S., Lee, S., Forster, S., Maskall, P., 2019. Cyber Fraud and Scamming Guidance and Advice. The National Centre for Post-Qualifying Social Work and Professional Practice, Bournemouth University.
Saariluoma, P., 2016. Cybersecurity for old people. Gerontechnology 14, 1.
Sarno, D.M., Lewis, J.E., Bohil, C.J., Neider, M.B., 2020. Which phish is on the hook? Phishing vulnerability for older versus younger adults. Hum. Factors 62 (5), 704–717.
Skidmore, M., Goldstraw-White, J., Gill, M., 2020. Vulnerability as a driver of the police response to fraud. J. Criminol. Res. Policy Pract. 6, 49–64.
The RAMES Projects 2013. Available from: http://www.ramesesproject.org/.
Tripathi, K., Robertson, S., Cooper, C., 2019. A brief report on older people's experience of cybercrime victimization in Mumbai, India. J. Elder Abuse Negl. 31 (4-5), 437–447.
UK, A., 2015. Only the Tip of the Iceberg: Fraud Against Older People. Age UK, London.
USA, Elder Fraud, 2019. Federal Bureau of Investigation. Available from. https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud.
Watson, J.M., Salmon, P.M., Lacey, D., Kerr, D., 2018. Continuance in online participation following the compromise of older adults' identity information: a literature review. Theor. Issues Ergon. Sci. 19 (6), 637–657.
Whitty, M.T., 2018. Do you love Me? Psychological characteristics of romance scam victims. Cyberpsychol. Behav. Soc. Netw. 21 (2), 105–109.
Whitty, M.T., 2019. Predicting susceptibility to cyber-fraud victimhood. J. Financ. Crime 26 (1), 277–292.
Wong, G., Westhorp, G., Manzano, A., Greenhalgh, J., Jagosh, J., Greenhalgh, T., 2016. RAMESES II reporting standards for realist evaluations. BMC Med. 14 (1), 96.