Western University
Scholarship@Western

Sociology Publications | Sociology Department

2021

# What Do We Know About Senior Citizens As Cybervictims? A Rapid Evidence Synthesis

Laura Huey
*Western University*, lhuey@uwo.ca

Lorna Ferguson
*Western University*, lfergu5@uwo.ca

Follow this and additional works at: https://ir.lib.uwo.ca/sociologypub

 Part of the Criminology Commons, and the Psychology Commons

Citation of this paper:
Huey, Laura and Ferguson, Lorna, "What Do We Know About Senior Citizens As Cybervictims? A Rapid Evidence Synthesis" (2021). *Sociology Publications*. 53.
https://ir.lib.uwo.ca/sociologypub/53

**What Do We Know about Senior Citizens as Cybervictims?**
**A Rapid Evidence Synthesis**


**Abstract:**

Internet-based victimization of senior citizens is an important potential threat of growing social, economic, and public policy interest. Given this, we sought to examine whether the existing research base could be used to formulate sound public policy in this area. To do so, we conducted a rapid evidence synthesis and assessment of the research literature from 2010-2020 surrounding three central organizing themes: cyber-related harms, responses and strategies, and prevention programs and solutions. Results reveal that there is an insufficient research base, lack of diverse research topics, and shortage of research beyond that of which is exploratory in nature. However, our findings did show promising insights on areas for future research development, such as support for seniors and their caregivers. We conclude with recommendations for future research that can begin to address the vulnerabilities senior citizens face with online victimization and potential policy implications for how to effectively combat this issue and these acts.



**Keywords**: cybervictimization; cybercrime; senior citizens; seniors; prevention; victimization

**What Do We Know about Senior Citizens as Cybervictims?**
**A Rapid Evidence Synthesis**

## Introduction

In 2021, the United States (U.S.) Internet Crime Complaint Center and the Federal Bureau of Investigations (ICCC) released their 2020 report on 'elder fraud.' Of those offenses reported, the estimated cost to American seniors was an estimated $1 Billion in losses, accounting for some 28% of all losses reported to the ICCC (ibid.). Seniors in other countries are hardly immune from cyber-based frauds and other forms of online harm. In the 2009 General Social Survey (GSS) on Victimization, Statistics Canada reported that 64% of older Canadians had experienced a security issue while using the Internet, including viruses, malware, phishing, hacking, and/or adware, among others (Brennan 2009). Financial, identity, and other scams have similarly been reported in China (Lee 2021), India (Tripathi, Robertson, and Cooper 2019), Australia (Cross 2017b), among other countries, leading to untold financial and other losses. Moreover, these reports, we note, focus mainly on fraud and identity theft and thus do not begin to cover the panoply of harms that can occur or are otherwise facilitated through exposure to online environments.

While there is a growing body of research on cybercrime more generally, much of it focused on cybervictimization of younger users, much less is known about Internet-based victimization of senior citizens (defined here as aged 60+[1]). Given the extent to which many countries across the globe are facing the prospect of aging populations, combined with the rapid proliferation of internet-based social, entertainment, information, and other platforms now readily available, we see the potential threat of cybervictimization in this population as an important social, economic and public policy issue. Our goal here is to present an analysis of the relevant

[1] We have opted to use age 60 as our cut-off point for defining 'elderly,' 'senior,' and 'older' for two reasons. First, the retirement age in several countries – including China and Japan – is 60 years of age. Second, as will become evident in the review to follow, this was the cut-off point used by some of the researchers whose work is cited here.

research literature to answer the question, 'Could we use the existing research base to formulate sound public policy in this area?'

To answer this question, we present the results of a rapid review of the relevant published, peer-reviewed literature. In the pages that follow, we map out our results to create a general overview of the breadth and scope of the studies sampled. We then provide a narrative review of the main findings as they relate to three areas of potential interest to public policy-makers: harms, responses, and prevention.

## Method of Inquiry

This rapid review is part of a more extensive programme of evidence assessment and research synthesis. The larger project is centered on improving our understanding of the state of the current research literature on cybercrime in relation to three central organizing themes: cyber-related ***harms***[2], formal and informal types of ***responses*** and strategies, programs and solutions aimed at ***prevention***. Further, as will be recalled, the narrower question that guides this review is the question of whether the current research base on cybervictimization for senior citizens would provide sufficient evidence upon which to develop sound public policy. To these ends, the present research seeks to address four research questions of interest to policy-makers, practitioners, researchers, and others alike:

> RQ1: What is the general nature and scope of published research on senior citizens as actual or potential victims of cybercrime as found within peer-reviewed journals over the past 10 years (2010-2020)?
>
> RQ2: What can we learn from the current research on actual or potential ***harms*** identified in the relevant literature?

[2] We use the term 'harms' rather than 'crimes' to reflect the fact that individuals might be harmed by an activity online that may or may not meet the legal definition of a crime, *per se*. For example, some of the included studies addressed issues related to loss of privacy online, which, depending on the context, may or may not be a criminal offense but can be experienced as a harmful action.

RQ3: What can we learn from the present body of published studies about ***responses*** to the cybervictimization of older citizens?

RQ4: What can we learn from the current body of peer-reviewed research on ***prevention*** strategies to protect older individuals?

Studies were selected based on the specific inclusion criteria stated below.

### *Inclusion Criteria*

#### *Types of Studies*

We sought primary studies using either primary or secondary data, including quantitative, qualitative, and/or mixed methods. We were open to any type of study design as long as the paper selected had a detailed description of the research methodology employed. Thus, we did not initially exclude any study based on concerns over methodology. Our choice to focus on primary studies, however, meant that systematic or other reviews of the literature were necessarily excluded.

#### *Types of Articles*

We searched for any relevant English language article from a peer-reviewed academic journal, and thus our results include both published and online first articles from across a number of research disciplines. However, the decision to focus on primary research meant that a number of different types of academic articles were excluded, such as commentaries, practice guidelines, and systematic reviews.

#### *Grey Literature*

Early in the process, a decision was made to exclude examples of grey literature and instead focus on peer-reviewed publications in credible academic journals. This decision occurred for two inter-related reasons: quality and time factors. In many research fields, grey literature includes a healthy mix of high, medium, and low-quality research. This is not, however, always the case in

relation to criminology and criminal justice topics, as evidenced by the fact that initial examples of grey literature located for this study were of poor, and sometimes questionable, quality. Attempting to search for, screen, and evaluate the volume of this work produced across the globe – and with the possibility of producing an evidence synthesis of limited value – tipped the decision to exclude this work.

***Search Methods***

We employed Omni, a University library search engine, to conduct a comprehensive search of the 784 databases to which we have access. These databases include ProQuest, PubMed, JSTOR Scopus, and EBSCOHost. To double-check our search results and ensure we had not missed any relevant papers, we then repeated our searches using both Google and Google Scholar. We also focused our search efforts on the period of 2010 to 2020. Initially, our goal was to analyze and present the most current research available; however, as initial exploratory searches of the research databases yielded so few results (n=12), we opted to extend the search period to 2010[3] and collected an additional four (n=4) results.

***Search Strategy***

All searches were conducted using keywords and with the date range set to 2010 to 2020 for the purposes of extracting the most recent insights available in the literature on this matter. Keywords used included iterations and combinations of 'older,' 'elder', 'senior', 'elderly', 'online', 'Internet', 'cyber', 'cybercrime', 'crime', 'fraud', 'scam', 'harm' 'aggression', 'harassment' and 'bullying.'

***Review and Selection of Studies***

[3] To expand our results, we also initially looked for papers from 2001 but located none that were relevant.

To arrive at our final sample, the abstracts of returned results from keyword searches were first read in total, and an initial decision was made as to whether to include or exclude from our sample based on relevancy to the topic under study. After reading the abstract, we chose to err on the side of caution and include the study in our initial sample only if it was unclear whether a paper met the inclusion criteria, as discussed below. We note that each of the combinations of keywords produced thousands of search results. Initially, we made the decision to stop reading beyond the 200$^{th}$ result, as we had found that paper topics became increasingly irrelevant to our search criteria by that point; however, given how few studies we could locate, the cut-off point was subsequently adjusted to 100 search results. Searches beyond this limit proved fruitless, and so it was deemed appropriate to focus our efforts within this range.

Once a decision was made to include an article, it was downloaded in full and stored as a PDF to be carefully read and assessed against the search criteria. As will be recalled, one of the inclusion criteria for our collection was that papers had to be 'peer-reviewed'; thus, we took an additional step by checking the journals in which these studies were accepted and/or published in order to ensure none of the included articles were from predatory journals and that there was a peer-review process for the publication. To note, the rationale behind the decision to exclude articles from predatory journals was made in efforts to reduce the likelihood that the included works had not been subject to formal peer-review and increase the chances that the research was of high quality. To that end, we searched lists of known predatory journals and looked up journal indexing and impact factors. In the end, three (n=3) topically relevant papers were subsequently excluded as they did not meet these criteria.

Final decisions on inclusion were then independently reviewed by another member of the research team for reliability purposes. Our ultimate result of all of the above processes was a total sample of fourteen (n=14) studies included for analysis.

***Data Coding and Analysis***

To answer each of the research questions above, we employed a simple inductive coding scheme using the following categories: title, first author, year of publication, approach (quantitative, qualitative, or mixed methods), methodology (data collection and analysis techniques), and data source. We also employed a manual deductive scheme for coding paper topics that drew upon the list of keywords provided by the authors themselves[4]. Engaging in this first stage of coding allowed us to answer our first research question. To answer the remaining research questions, we then created thematic 'codes' for each relevant topic and sub-topic covered in the paper/report and then recoded our data. We began by setting up codes for our three organizing themes: harms, responses, and prevention. Following this, we used an inductive scheme that relied on manual line-by-line readings of each of the articles, which allowed us to develop new themes, as well as relevant sub-themes that were not necessarily reflected in the keywords provided by authors. See, for example, Table 1 below.

**Table 1. Major Themes and Sub-Themes**

| **Theme** | **Sub-Themes** | **Code Examples** |
|---|---|---|
| *Harms* | | |
| Identity Theft | Risk Factors | - Cognitive Impairment<br>- Technical Issues |
| Fraud | Causal Attributions | - Loneliness<br>- Greed<br>- Gullibility |
| Cyberbullying | Negative Impacts | - Loss of Information<br>- Financial Loss |
| | Risk Assessments | - Decision-making |

[4] We note that each of the studies had a list of keywords with one exception: Grimes et al. 2010.

| | | |
|---|---|---|
| | Crime Types | - Phishing<br>- Email Scams |
| *Responses*<br>Police<br>Banks<br>Senior Support | <br>Unresponsive Institutions<br>Barriers and Challenges<br>Stigma Against Older Victims | <br>- Impacts<br>- Report Delays |
| *Prevention* | Technical Solutions<br>Personal Strategies | - Lack of Safeguard<br>- Removing Access<br>- Online Decision-making |

We then structured our responses to the second, third and fourth research questions by abstracting relevant content from each article and using it to construct a narrative synthesis. This approach aimed to provide information on what is and is not known based on this literature at this time. Ideally, we would have liked to have been able to engage in a meta-analysis; however, this was not possible because of the heterogeneity of the studies, including differences in methodological approaches and outcomes tested. All coding was independently verified.

***Assessment of Methodological Quality***

The studies in our final sample included eight (n=8) quantitative studies, primarily relying on survey data, and seven (n=7) qualitative, primarily using interview data. Of the nine, three (n=3) were experimental studies, none of which were testing an intervention and thus measuring effect outcomes. As a result, some of the standard social science measures used for evaluating quality in crime-related research – such as the Maryland Scientific Methods Scale (Farrington, Gottfredson, Sherman, and Welsh 2002) or the EMMIE framework (Johnson, Tilley, and Bowers 2015) – were not going to be helpful in this context. Instead, we opted to use two scales developed for evaluating quantitative and qualitative research for use in policy settings: Ratcliffe's (2019) Evidence Hierarchy for Policy Decision-making and Huey's (2021) Qualitative Evidence Hierarchy for Policy Decision-Making. One author undertook an initial rating of the fourteen (n=14) papers

using these two scales, and then they were independently rated by the second author. Discrepancies in reviews were then discussed until consensus on an appropriate score was reached.

## Findings: Overall

In this section, we present an overview of the types and scope of research collected and analyzed for this project. Then, using the scales described above, we also provide an assessment of the quality and thus utility of this research for informing policy and/or practice.

### *Extent and Range of the Literature*

We identified a total of fourteen (n=14) papers that dealt primarily with the issue of cybervictimization of senior citizens persons. As shown in Table 2 below, most identified studies in this area were conducted after 2016. Before that, we could only locate five (n=5) studies meeting our criteria. We also note that the majority of studies in our sample used data from populations in the United States (n=6), followed by four (n=4) studies drawing on Canadian data. Other populations represented in a single study (n=1) included Australia, India, the United Kingdom, and New Zealand.

**Table 2. Year and Number of Works Located (2010-2020)**

| Year | Journal Articles |
|---|---|
| 2010 | 1 |
| 2011 | 0 |
| 2012 | 0 |
| 2013 | 0 |
| 2014 | 1 |
| 2015 | 1 |
| 2016 | 1 |
| 2017 | 3 |
| 2018 | 1 |
| 2019 | 2 |
| 2020 | 4 |
| **Total** | **14** |

While the overall volume of research on cybervictimization of seniors is relatively low, we did observe some diversity in terms of the types of research methods utilized (see also Table 3). There were seven (n=7) qualitative and seven (n=7) quantitative studies, with none (n=0) employing a mixed methodological approach. Qualitative studies relied exclusively on interview data and were primarily descriptive and/or exploratory in nature. Quantitative studies included a mix of experimental (n=3) and survey-based research (n=5) in which the researchers themselves had collected the data. Therefore, most of the sampled studies involve primary instead of secondary data.

**Table 3. Research Methods Employed in the Sampled Studies**

| **Methodology** | **n** |
|---|---|
| Quantitative | |
| Survey | 5 |
| Experimental | 2 |
| Qualitative | |
| Interviews | 7 |

We also sought to determine within which primary research fields each of the articles fell. We considered this an important question to explore, given that researchers within a particular field frequently employ theoretical frameworks, concepts, and methodological and analytical approaches that are largely unique to that field. Thus, a preponderance of papers produced within any one given area could have a potentially limiting effect on what is understood within this area, potentially guiding any policy or prevention strategy developments. Relatedly, scholars, in their particular areas, formulate their understandings through the lens of this area and their research background, which can also influence the empirics, assumptions, conclusions drawn, and any potential recommendations. Lastly, knowing this information can also help direct future research efforts, such as by leaving gaps in the literature base requiring additional study.

To determine this, we first looked at the departmental and institutional affiliation of the author. Then, for papers with multiple authors, we looked at the types of departments within which most of the researchers were affiliated. Our results reveal that the majority of papers were produced within the fields of Psychology (n=6) and Criminology (n=4). This was followed by three (n=3) papers from Information Studies and one (n=1) from the Computer Sciences (see also Table 4 below). Knowing the research domains within which the work was produced helps to explain why, for example, several of the papers focus on decision-making and cognitive, emotional, and other related factors that affect decision-making and increase or inhibit risk-taking online – these are topics that typically fall within the field of psychology.

**Table 4. Scholarly Fields in Which the Research was Produced**

| **Research Domain** | **n** |
|---|---|
| Psychology | 6 |
| Criminology | 4 |
| Information Studies | 3 |
| Computer Sciences | 1 |
| **Total** | **14** |

We also sought to undertake assessments of the studies in our analyzed sample. To be clear: these assessments are not evaluations of the quality of the research and/or of the particular methods used, as this would be beyond the scope of this rapid review. However, as a central concern of the present study is to present the strengths and limitations to policy-makers of the current evidence base on cybervictimization of seniors, we felt it worthwhile to conduct assessments of the value of any individual paper to inform policy or practice. Doing so can also offer insight into how much weight should be attached to the body of evidence as a whole. Table 5 presents a synthesis of this assessment. In the instant case, the volume of studies collected was generally exploratory and either descriptive (qualitative) or employing inferential statistics (quantitative). None were testing

an intervention. From a public policy standpoint, the information to be gleaned is useful; however, it does not provide a strong evidence base for moving in any one public policy direction.

**Table 5. Policy value assessments**

| **Ratcliffe Hierarchy[5]** | **n** |
|---|---|
| Quantitative | |
| Level 1 | 7 |
| Level 2 | 0 |
| Level 3 | 0 |
| Level 4 | 0 |
| Level 5 | 0 |
| **Huey Hierarchy[6]** | **n** |
| Qualitative | |
| Level 2 (single method/single data source, small sample, no efforts to reduce sampling or other bias) | 6 |
| Level 3 (single method/single data source, efforts to remove sampling bias, larger, more diverse sample) | 1 |
| Level 4 (mixed methods) | 0 |
| Level 5 (triangulated studies) | 0 |
| Level 6 (quadrangulated studies) | 0 |

When it came to analyzing paper topics, as noted above, for this section of the paper, we drew on the keywords provided by the authors of each study. As will be recalled, we could locate keywords for thirteen of the fourteen papers in our total sample. In those thirteen (n=13) papers, there were thirty (n=30) keywords provided, ranging from topics such as 'aging' and 'elder abuse' to 'fraud' and 'security.'

## Findings: A Narrative Approach

[5] We excluded Level 0 from this hierarchy as our search criteria excluded opinions, commentaries, and commercial documents.
[6] We excluded Levels 0 (non-studies) and 1 (non-academic studies), and 7 (systematic reviews), as our search criteria excluded these types of information sources.

As may be recalled, the goal of the larger programme of research, of which this rapid review forms a part, is to improve our understanding of the strengths and limitations of the relevant research literature on cybersecurity-related issues, with a particular focus on three areas of interest: harms, responses, and prevention. To that end, this section of the paper employs a narrative approach and is organized around the analysis of how the studies sampled address these concerns.

***Harms***

Each of the papers in our sample explored dimensions of one or more online harms that senior and other citizens experience and/or potentially face. Harms identified included: identity theft, advance fee fraud, unauthorized access to personal information, privacy loss, and information misuse, among others. We note that only one (n=1) of the papers focused exclusively on one or more of these subjects. Instead, selected research typically dealt with harms in relation to potential causes and effects, responses to and/or prevention of online harms. This section looks at three major sub-themes to emerge concerning harms: prevalence, risk factors, and impacts.

*Risks: Factors and Behaviours*

The one published journal article we located that provided an in-depth examination of cyber-based harm was Wang and colleagues' (2019) study of cyberbullying in New Zealand and prevalence rates. In particular, what these researchers did was use a national sample to explore differences in exposure to cyberbullying behaviours between young adults (aged 18-25) and senior citizens (aged 66+). What they found was that the latter group typically reported fewer experiences of online harassment (ibid.). They also observed that the slight gender-based differences in rates of bullying decrease in older populations, but that older citizens of Indigenous descent continue to experience some online harassing behaviours (ibid.)

More frequently, papers in this category focused on exploring risk factors that may increase or decrease exposure to online harms. One such example is a paper by Grilli and colleagues (2020) looking at whether age impacts the ability to detect suspicious emails among 'cognitively normal' adults. To do this, they conducted an experiment in which sixty-five middle-aged to older adults were asked to detect phishing emails, finding that "older age was related to worse discrimination between genuine and phishing emails" (ibid.: 1). A similar result was obtained by James and colleagues (2014) in another study of the susceptibility to online fraud of 639 older adults without cognitive impairments. Taking a multi-dimensional approach, James et al. found that susceptibility was positively correlated to a combination of older age, lowered levels of literacy and cognitive function, as well as decreased psychological well-being (ibid.).

Age as a factor in susceptibility to online frauds and other deceptions was also explored by Ebner et al. (2018) in an experiment that compared results from two categories of seniors (ages 62-74 and 75-89, respectively) and one group of young adults (ages 18-37). In the experiment, researchers sent participants in each group a simulated phishing email to determine if they would access potentially 'risky' content. Their results indicate that "higher susceptibility was associated with lower short-term episodic memory in middle-old users [62-74] and with lower positive affect in young-old [62-74] and middle-old [75-89] users" (ibid.: 522). The fourth study in this cluster compared computer usage and Internet security knowledge between two groups: low-income senior citizens and University students (Grimes, Hough, Mazur, and Signorella 2010). What they found is that older adults sampled were less likely to be using computers, a finding we note may have less to with age than income. Likely a result entirely commensurate with their lower levels of usage, researchers also noted that older participants were less knowledgeable about online security than University students. However, both groups tended to have similar scores when it

came to trusting Internet-based information sources (ibid.). Interestingly, they also observed minimal age-based differences in security awareness between men in either group; however, older women were found to be significantly less knowledgeable about Internet security than those in the university group (ibid.).

A study by Morrison and colleagues (2020) we have also placed in the 'risk' category explores whether transitioning into retirement – a phase they saw as potentially commensurate with changes in loss of status, social interaction, finances, routines, and technological support, among others – increased vulnerability to cyberharms. Based on an analysis of data collected from semi-structured interviews with twelve U.K. seniors, they conclude, "our evidence supports the notion that retirement acts as a major life disruption and one which leads people to seek out … a new lifestyle in which previous technological and social infrastructures are lost and are subsequently replaced with tenuous new structures that can sometimes lead to additional cyber-vulnerabilities" (ibid.: 9). Thus, this study generally finds that retirement presents a risk with respect to Internet-based victimization experiences by seniors, resulting mainly from a break in structure and routine.

Whereas other papers that fell under the sub-theme of 'risk' examined 'risk factors,' papers by both Eleuze and Quan-Haase (2018) and Cross (2017) explored the relationship between 'attitudes' and 'risky behaviours.' The former study looked at how seniors' attitudes towards privacy online variously increased or decreased their willingness to engage in actions that might compromise their privacy online (Eleuze and Quan-Haase 2018). This exploratory study drew on interview data from seniors in Canada to show how "a large number of older adults" in their sample were "marginally concerned" about privacy and security breaches "as they see their online participation as limited and harmless" (ibid.: 1372). Similarly, seniors in an Australian-based study

on cybervictimization related "detailed scenarios where their actions directly compromised their identity, through either a lack of understanding about criminal capabilities or through a lack of understanding of the value of their identification information" (Cross 2017b: 13). As with the Eleuze study, Cross (2017b) observed that victims of phishing often saw the emails and the subsequent provision of their personal information as "harmless" (ibid.: 14). The relationship between age and engaging in risky online behaviours was also a central concern of a paper by Wood and colleagues (2017), who utilized data on risk-taking intentions and behaviours across the lifespan (ages 18-79). By taking this approach, they discovered that risk-taking among individuals in their sample declined with age (ibid.). For example, seniors (60+) were less likely to provide personal information online or to befriend strangers (ibid).

Another paper in the 'risk' category tested self-control theory as a predictor of risky behavior online – in this case, measured as a willingness to purchase online from an unknown vendor – among individuals aged 60 and over (Holtfreter, Reisig, Pratt, and Holtfreter 2015). Perhaps not entirely surprisingly, they found that individuals who exhibit lower levels of self-control were more likely to engage in online transactions triggered by an unsolicited email (ibid.). As Holtfreter and colleagues point out, engaging in risky online purchasing increases one's probability of identity theft (ibid.) and, as we would further add, one's probability of being defrauded through an online shopping scam.

*Impacts of Victimization*

Unfortunately, we were only able to locate one (n=1) study that addressed the impacts of cybercrime and related harms on senior citizens victims. An exploratory study by Tripathi and colleagues (2019) drew upon eleven interviews with seniors and their family members in Mumbai, India, to look at various aspects of cyber-victimization, including the impacts of that experience

for victims. They found that frauds experienced had significant financial and emotional impacts, noting that some victims had lost retirement funds and monies set aside for health and other emergencies (ibid.). These losses, and a lack of supportive responses from police and banks, "led to persistent and unresolved feelings of shame, depression, and anxiety (ibid.: 444). Thus, there appears to be some psychological impacts resulting from Internet-based victimization for seniors.

***Responses***

Two of the issues facing victims of cybercrime and other cyberharms is the question of whether to report victimization and to whom. Three (n=3) of the papers in our sample examined official avenues through which victims might report and access services. These are captured under the theme of 'responses.'

The central focus of two (n=2) papers by Cassandra Cross (2016, 2017a) is the work of the Seniors Support Unit (SSU), a program for senior victims of online crimes provided through the Canadian Anti-Fraud Centre. Seniors, who have been victims of fraud, can contact the SSU to receive peer support from volunteers. The first of these papers explores volunteers' attributions of responsibility for victimization (Cross 2016); the second looks at the emotional and psychological demands on volunteers engaged in supporting elderly victims of fraud (Cross 2017a). While the SSU clearly provides support to individuals who have been victimized online, and the recommendations contained within each paper may have greater salience, we note that neither of these papers is centered exclusively on victimization of seniors from online frauds.

The third paper in this group is Tripathi and colleagues' (2019) exploration of victim experiences of online fraud in India, including having to navigate challenging reporting processes instituted by police and banks. Through interviews with seniors who had been defrauded online, the researchers observed that victims spoke of their frustrations over significant delays in their

ability to report events to local police and have their reports taken seriously. Similar obstacles were reported by victims who attempted to notify banks of fraudulent activity (ibid.).

***Prevention***

We also identified three (n=3) papers in our sample that address the issue of prevention. All three discuss the use of personal strategies for enhancing online safety employed by either senior citizens or their caregivers. Ergo, no strategies exist within the body of literature outside of the individualization of the issue through the study and emphasis on individual tactics to prevent Internet-based victimization of seniors.

The first of these studies draws on in-depth interviews with Canadian seniors to explore different attitudes towards privacy and safety concerns online (Eleuze and Quan-Haase 2018). What these researchers find is that senior Internet users typically fall within one of five categories in terms of their attitudes: 'fundamentalist,' 'intense pragmatist,' 'relaxed pragmatist,' 'marginally concerned,' and 'cynical expert' (ibid.). They note "considerable variability" with respect to how individuals in these groups think and act online, variability that can, in part, be explained by their degree of online activity (ibid.: 1386). However, most of those interviewed felt some degree of concern over security issues, particularly in relation to access to personal information and information misuse (ibid.). It is worth noting that approximately 5% of Eleuze and Quan-Haase's (2018) sample consisted of individuals whose "perception of technology and associated risks created a feeling of impotence about how much they could protect their data, particularly against organizations" (ibid.: 1383). Particularly telling is that individuals within this group did not see age as a factor that predisposed them to increased risks; "rather they saw all users as being at the mercy of organizations" online (ibid.: 1383).

The second paper in this category looked at the decision-making process and subsequent actions taken by caregivers to safeguard their loved ones with mild cognitive impairment (Mentis, Madjaroff, Massey, and Trendafilova 2020). Drawing on interviews with ten families (n=20), these researchers observed that while both sets of participants (caregivers and care recipients) agreed to make joint decisions concerning online usage by the latter, in reality, caregivers were unilaterally taking preventative steps to reduce the potential for online harms. In examining this process more carefully, Mentis and colleagues (2020) concluded that one explanation for this gap between attitude and action is that caregivers are often hampered by a lack of options for managing their loved one's screen time. Without access to easy, affordable, and variable solutions, caregivers felt they had to make a choice between constructing their own personal solutions for reducing cyberthreats or removing access altogether (ibid.). Such efforts, they observed, entail "a significant amount of the [caregiver's] resources, such as time, for them to identify what modification or intervention is available to them" (ibid.: 11).

Much has been written in the criminology literature on the processes by which individuals come to be 'responsibilized' (Garland 1996) into assuming ownership of their own safety and security by the state. Our third paper, by Cross (2017b), draws on data with senior victims of online fraud to explore the problems associated with 'responsibilizing' seniors in relation to cybercrime. In particular, Cross looks at a process by which we expect seniors to become self-educated on the risks they face – with too few supports available – leading to a limited awareness of the risk faced. As Cross (2017b: 1) puts it, "seniors often expose identity information through their actions … [as a result of] flawed assumptions and misguided beliefs over the perceived risk and likelihood of identity crime." For example, they may correctly view some emails as containing fraudulent inquiries; however, given the context of others, they may mistakenly conclude the sender is 'safe.'

Examples of the latter include situations in which individuals responded to phishing attempts by email, sending scammers not only their full names and dates of birth but also banking and passport details (ibid.). Cross (2017b) thus concludes that significantly more educational and other prevention-oriented efforts are required to support seniors in staying safe online.

## Discussion

We began this exercise in knowledge synthesis with the question of 'could we use the existing research base to formulate sound public policy in this area?' Unfortunately, the simple answer is no.

First, as our review makes evident, there is an insufficient evidence base in any one area of the literature upon which to inform sound policy or practice. There is clearly a significant need to not only grow the volume of research on cybervictimization of seniors, but also to diversify the range of research topics beyond phishing and identity theft. For example, there is emergent literature on topics such as non-consenting distribution of sexual images, romance scams, online harassment, doxing, and an increasing range of other harmful online activities that are not exclusive to young or middle-aged persons. We know little about the prevalence and reporting rates of such harms among older citizens, nor about their financial, emotional, psychological, and other impacts. Given that the victimological scholarship has well-researched and established that there are a range of socio-emotional and other impacts stemming from such instances of victimization more generally, understanding the array of impacts of Internet-based victimization for seniors and beyond is likely to bring about critical insights on needed supports, services, and programs alike.

Next, we also note that the quality of available studies is suitable for exploratory research. However, there is a notable lack of research aimed at innovating and testing interventions that

might tell us ‘what works’ in terms of developing policies or practices aimed at producing accessible prevention education and tools and/or improving responses to victimization. The most studied areas in the area of prevention pertain to personal strategies (by senior and/or caregiver) to manage and tackle this issue. That is, in terms of what has been researched, onus for this issue has been largely individualized or attributed as a personal problem rather than a social and public policy issue that requires broader, more extensive support and efforts by government, social services, and policy-makers, among others. This is not to say that the issue has been individualized more generally (i.e., in the policy realm), but any future efforts to draw upon research for public policy development would likely be steered to these aims, given this focus in the existing literature.

We are, however, fortunate to be able to identify some specific areas in which the research in this area might continue to be developed. For example, one insight gleaned from work by Eleuze and Quan-Haase (2018) is the need to look more closely at beliefs and attitudes towards online decision-making rather than focusing solely on demographic and/or cognitive risk factors. Enhanced knowledge of risk-based decision-making among this and other demographic groups could be greatly useful for shaping future prevention strategies. We also note the need for greater research on victimization and, in particular, how best to support not only seniors but also their caregivers. Work by Mentis and colleagues (2020) suggests a critical need for equipping caregivers with tools to help them more efficiently and effectively manage loved ones’ online activities. Similarly, as greater numbers of seniors are 'aging in place,' Cross' (2017b) work highlights the need for research into educational and other prevention-oriented efforts aimed at supporting seniors in staying safe online. Lastly, we also note that the Ebner and Tripathi studies remind us – albeit in different ways – of the need to develop an improved understanding of resiliency in this

population and how best to support senior victims in positive, affirming ways that allow for increased growth and understanding of risks and how to reduce them.

### *Limitations*

No study is without limitations, and ours is no exception. We acknowledge that our choice to utilize a rapid review approach that drew exclusively on peer-reviewed publications likely resulted in the exclusion of some relevant information sources, such as dissertations, theses, and reports by non-profits and other groups. This is also the case with respect to our decision to vet the academic journals in which studies were published, which led to the post-selection exclusion of three papers published in journals appearing on lists of predatory journals. The decision to limit our selection to English language publications may also have played a role in the low volume of results achieved from our searches. If we had access to highly reliable translation software suitable for academic publications, we would have gladly expanded our searches to include non-English research from across the globe.

## References


Brennan, S. 2009. 'Victimization of Older Canadians.' Statistics Canada report catalogue. No: 85-002-X. Available at: https://www150.statcan.gc.ca/n1/en/pub/85-002-x/2012001/article/11627-eng.pdf?st=GuoG2JeB.

Farrington, D., Gottfredson, D., Sherman, L., and Welsh, B. 2002. 'The Maryland Scientific Methods Scale,' in Sherman, L., Farrington, D., Welsh, B. and MacKenzie, D. (eds.). *Evidence-Based Crime Prevention*. New York: Routledge. https://www.taylorfrancis.com/chapters/edit/10.4324/9780203166697-7/maryland-scienti%EF%AC%81c-methods-scale-david-farrington-denise-gottfredson-lawrence-sherman-brandon-welsh

Garland, D. 1996. 'The Limits of The Sovereign State: Strategies of Crime Control in Contemporary Society.' *The British Journal of Criminology*, 36(4): 445–471. https://doi.org/10.1093/oxfordjournals.bjc.a014105

Huey, L., Mitchell, R., Kalyal, H., and Pegram, R. 2021. *Implementing Evidence Based Research: A How-to Guide for Police Organisations.* Bristol, UK: Policy Press.

Internet Computer Crime Center (ICCC) and Federal Bureau of Investigation (FBI). 2021. 'Elder Fraud Abuse 2020.' Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3ElderFraudReport.pdf.

Johnson, S., Tilley, N. and Bowers, K. 2015. 'Introducing EMMIE: An Evidence Rating Scale To Encourage Mixed-Method Crime Prevention Synthesis Reviews.*' Journal of Experimental Criminology,* 11(4): 459–73. https://doi.org/10.1007/s11292-015-9238-7.

Lee, C. 2021. 'Online Fraud Victimization in China: A Case Study of Baidu Tieba.' *Victims & Offenders,* 16(3): 343-362. https://doi.org/10.1080/15564886.2020.1838372

Ratcliffe, J. 2019. *Reducing Crime: A Companion for Police Leaders*, Routledge: New York. https://www.taylorfrancis.com/books/mono/10.4324/9781351132350/reducing-crime-jerry-ratcliffe.

## Appendix: List of Studies


Cross, C. 2016. 'They're Very Lonely': Understanding the Fraud Victimisation of Seniors. *International Journal for Crime, Justice and Social Democracy*, 5(4): 60-75. DOI:10.5204/ijcjsd.v5i4.268.

Cross, C. 2017a. '"I've Lost Some Sleep Over It": Secondary Trauma in The Provision Of Support To Older Fraud Victims.' *Canadian Journal of Criminology and Criminal Justice,* 59(2): 168–197. DOI: 10.3138/cjccj.2016.E11.

Cross, C. 2017b. '"But I've Never Sent Them Any Personal Details Apart from My Driver's Licence Number...": Exploring Seniors' Attitudes Towards Identity Crime.' *Security Journal*, 30(1): 74-88. https://doi.org/10.1057/sj.2015.23.

Ebner, N., Ellis, D., Lin, T., Rocha, H., Yang, H., Dommaraju, S., Soliman, A., Woodard, D., Turner, G., Spreng, R., and Oliveira, D. 2020. 'Uncovering Susceptibility Risk to Online Deception in Aging.' *Journal of Gerontology, Series B*, 75(3):522-533. https://doi.org/10.1093/geronb/gby036.

Elueze, I. and Quan-Haase, A. 2018. 'Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin's Privacy Attitude Typology Revisited.' *American Behavioral Scientist*, 62(10):1372-1391. https://doi.org/10.1177/0002764218787026.

Grilli, M., McVeigh, K., Hakim, Z., Wank, A., Getz, S., Levin, B., Ebner, N., and Wilson, R. 2020. 'Is This Phishing? Older Age Is Associated with Greater Difficulty Discriminating Between Safe and Malicious Emails.' *The Journals of Gerontology: Series B*, online first. https://doi.org/10.1093/geronb/gbaa228.

Grimes, G., Hough, M., Mazur, E., and Signorella, M. 2010. 'Older Adults' Knowledge of Internet Hazards.' *Educational Gerontology*, 36(3): 173-192. https://doi.org/10.1080/03601270903183065.

Holtfreter, K., Reisig, M., Pratt, T. and Holtfreter, R. 2015. 'Risky Remote Purchasing And Identity Theft Victimization Among Older Internet Users.' *Psychology, Crime & Law*, 21(7): 681-698. https://doi.org/10.1080/1068316X.2015.1028545.

James, B., Boyle, P., and Bennett, D. 2014. 'Correlates of Susceptibility to Scams In Older Adults Without Dementia.' *Journal of Elder Abuse and Neglect*, 26(2): 107-122. https://doi.org/10.1080/08946566.2013.821809.

Mentis, H., Madjaroff, G., Massey, A., and Trendafilova, Z. 2020. 'The Illusion of Choice in Discussing Cybersecurity Safeguards Between Older Adults with Mild Cognitive Impairment and Their Caregivers.' *ACM Human-Computer Interaction*, 4(2): 1-19. https://doi.org/10.1145/3415235.

Morrison, B., Coventry, L. and Briggs, P. 2020. 'Technological Change in the Retirement

Transition and the Implications for Cybersecurity Vulnerability in Older Adults.' *Frontiers in Psychology*, 11(1): 1-13. https://doi.org/10.3389/fpsyg.2020.00623.

Tripathi, K., Robertson, S., and Cooper, C. 2019. 'A Brief Report on Older People's Experience of Cybercrime Victimization in Mumbai, India.' *Journal of Elder Abuse & Neglect*, 31(4-5): 437-447. https://doi.org/10.1080/08946566.2019.1674231.

Wang, M., Yogeeswaran, K., Andrews, N., Hawi, D., and Sibley, C. 2019. 'How Common Is Cyberbullying Among Adults? Exploring Gender, Ethnic, and Age Differences in the Prevalence of Cyberbullying.' *Cyberpsychology, Behavioral and Social Networking*, 22(11): 736-741. https://doi.org/10.1089/cyber.2019.0146.

White, C., Gummerum, M., Wood, S. and Hanoch, Y. 2020. 'Internet Safety and the Silver Surfer: The Relationship Between Gist Reasoning and Adults' Risky Online Behavior.' *Journal of Behavioral Decision Making*, 30(6): 819-827. https://doi.org/10.1002/bdm.2003.