# 'Don't Fall for This': Communications about Cybersafety from the AARP

NORA MCDONALD, George Mason University, USA
HELENA M. MENTIS, University of Maryland, Baltimore County (UMBC), USA

Older adults face unique risks in trying to secure their online activities. They are not only the frequent targets of scams and fraud; they are the targets of a barrage of cybersafety communiqués whose impact is unclear. AARP, the United States advocacy group focusing on issues facing older adults over the age of 50, is among those educators whose strategies remain underexplored, yet their reach makes it imperative that we understand what they are saying, to whom, and to what effect. Drawing on an analysis of AARP publications about cybersafety and privacy, we sought to better understand their discourse on the topic. We report on findings that AARP's language may have the effect of portraying bad actors ("fraudsters") as individuals, rather than enterprises, which at the target end, personalizes interactions, placing too much onus on individual users to assess and deflect threats. AARP's positioning of, and guidance about, threats may sometimes prompt a thought process that puts users at the center of the narrative and may encourage engagement.[1] Instructing older Americans, or anyone, on the forensics of cyber-sleuthing is enormously difficult. We conclude with a discussion of different approaches to cybersafety, one that involves educating older adults about the rudiments of surveillance capitalism.

CCS Concepts: • **Security and Privacy** ~ Human and Societal aspects of security and privacy

**Additional Key Words and Phrases:** Cybersafety, older adults, cognitive decline, critical discourse analysis

**ACM Reference format:**

Nora McDonald & Helena M. Mentis. 2023. 'Don't Fall for This': Communications about Cybersafety from the AARP. *Proc. ACM Hum.-Comput. Interact,* 7, CSCW2, Article 248 (October 2023), 21 pages, https://doi.org/10.1145/3610039

## 1 INTRODUCTION

Older citizens feel themselves to be at heightened risk of cybersafety fraud [32] and, for a variety of reasons, may potentially be more vulnerable [63], making them a target not only of threats but also of communications about threats. To learn about the public discourse concerning cybersafety education for an aging population, we looked to AARP, an organization serving 38 million members in the U.S. whose mission is to "empower" aging populations, and considered their approach to the mission of cybersafety vigilance [3]. A United States advocacy group for aging adults, the AARP (formerly named the American Association of Retired Persons) is a powerful and influential voice

This is work is supported by the National Science Foundation, under grant CNS-1714514.
Author's addresses: N. McDonald, George Mason University, 4400 University Dr., Fairfax, Virginia, USA; HM Mentis, University of Maryland, Baltimore County (UMBC), 1000 Hilltop Circle, Baltimore, Maryland, USA.


2573-0142/2023/10 – Article#248 … $15.00

https://doi.org/10.1145/3610039

around many issues affecting older adults (50 plus), including internet privacy and security. Given the role that AARP plays as a voice of authority on cybersafety, the methods and content through which they engage with their aging readership about topics of privacy and security are of critical importance. Part of being in command of that discourse means that the AARP communicates to its readers not just what to do, but also how they want their readers to think about themselves and their cybersafety [15]. Willingness to accede to stereotypes of the "older adult" user propagated and fostered by AARP's depiction of cybersafety may affect the user's sense of what constitutes a threat as well as their agency and efficacy in mitigating them.

We analyzed cybersafety and privacy communications from the AARP website, dating back as far as 2004, to understand what types of information and education they provide, and how it is being presented. By examining the discourse strategies of the AARP—the perspectives taken and language used in characterizing cybersafety—we are able to better understand how that threat is defined for older populations and what guidance they are being given to mitigate it. Our study takes a critical stance, drawing on critical discourse analysis (CDA) to look at how the AARP verbally signals cybersafety norms [16]. CDA is a highly useful, disciplined technique for assessing what people are exposed to, and for positing what the effects could be, particularly when the power differential is so stark. We don't know to what extent this discourse influences cybersafety norms or practice, or even user self-perceptions, but in qualitative research, we have become aware of a broader narrative about cybersafety among constituents that is consistent with what AARP communicates. But the semiotics of AARP's cybersecurity warnings and cybersafety training are an important data point in theorizing about existing cybersafety literacy efforts and exploring alternate approaches.

We make several contributions with this work. First, we conduct what is (to our knowledge) the only analysis of AARP (the most-read magazine in the United States as of 2018) communications on cybersafety. We argue that critical approaches are increasingly important in an age when cybersecurity advice is ubiquitous and profitable. Second, we characterize how a sizable number of AARPs' communications portray their reader as victims of very targeted and insidious scams and fraud. Third, we look specifically at a type of communication that exacerbates this conception of user through "click bait" language and narrative that place readers at the solipsistic center—misinforming their audience about the nature of the threats and potentially encouraging active assessment of threats when retreat would be the best course of action. Finally, we use this work, and our methods, to raise concern about the kinds of cybersafety information that is given seemingly unquestioned authority on the web and illustrate how critical approaches can be important to tackle them. We discuss our future work focusing on the development of educational materials and interventions that would emphasize individual context and understanding of the rudiments of surveillance capitalism.

In the next section, we reflect on current practices in cyber-education and aging, and flaws in the concept of cyber-literacy as currently used to imply a skillset that can be achieved through training and advisories from organizations like AARP. We then describe our critical analysis of AARP publications, demonstrating how AARP encourages a reader perspective-taking that could lead, paradoxically, to the adoption of counter-productive strategies, thereby undermining their intended objectives. We conclude with some recommendations for future work to explore best practices in cyber-education with aging communities, particularly among those suffering from memory loss.

## 2 BACKGROUND

### 2.1 The 'scammy' web and digital literacy among older adults

Type "dating scams" into your browser and you might be directed to the Federal Trade Commission (FTC), which provides a bullet point list of the profile and behaviors of "Romance Scammers" and a link to the FTC's most recent research showing that romance scams are rising and that they result in more losses than any other fraud [56]. Or you might be directed to the Federal Bureau of Investigations (FBI) site or the AARP describing "Romance" or "Dating Scams." Search the web for articles about older adults and cybersafety, and you are likely to find numerous anecdotes about dating scams, as well as the notorious "grandparent scam" that is supposedly taking the older adult community by storm. For users with an interest and facility to conduct online searches regarding cybersafety, there is a wealth of well-intended information available both to guide and to alarm. The presumption is that an informed public is a defended public, and that an under-informed public can be given information that will enable them to fend off fraudulent incursions into their lives through the internet. Yet, when the information that is communicated is intended to ignite fear, it's not even clear that this approach is efficacious, as those studying fear based appeals have found [31], and may even have harmful or paradoxical consequences [10].

Conceptions of privacy and its protections are the outer portal in the defense against cybersafety breaches, insofar as "public knowledge" gained about individuals online can be used to target and to personalize various cyber-threats. Considerable study has been done by Human-Computer Interaction (HCI) scholars and those in related fields to measure the "digital literacy" (e.g., [30]) and "privacy literacy" of individuals, including older adults (e.g., [54]) and young children (e.g., [35]), on the internet based on identity characteristics such as age [29], profession [33], and other socio-demographics, as well as numerous studies by applications, such as Facebook (e.g., [4, 8, 22]).

Research has also looked at whether users read privacy policies [46] and whether they understand them [23]. Shoshana Zuboff has inspired skepticism as to whether users should even be expected to read privacy policies given the time and technical knowledge required to interpret them properly—and even beyond that, the futility of expecting people to make thoughtful tradeoffs when the exigencies of functional service may oblige them to relinquish privacy [62]. We are perhaps past the point where we can responsibly say that users even have a choice, making "literacy" a misleading concept in a discussion of people's privacy calculations [38–41, 60]. Internet companies collect vast amounts of data, and offer advertising systems based on "massive surveillance and elaborate personal dossiers" simply to serve up ads [59]. Social network and other companies do this in exchange for free service to which users attach enormous value—platforms from which to search, broadcast, connect, socialize, etc. [11]. These data then become the tools for executing attacks over email, text, websites or social media. In an age of surveillance capitalism when notions of "choice" are illusory, privacy literacy does not usefully describe the way individuals engage with applications.

### 2.3 Cybersafety (mis)education

Guidance from trusted sources (from which organizations like the AARP regularly riff) deserve closer examination. A common type of guidance for detecting phishing scams is, for example, to look for grammatical errors and misspellings in URLs, email addresses and content (e.g., [6]). Scholars have found that such "tells" may not be as prevalent as supposed and that, in any case, visual elements (familiar logos, for instance) may be so semiotically powerful that they can elude common sense defenses built up around errors people need to spot [7]. Even though some users can

and do memorize certain signals of risk, they may be unable to extrapolate to specific situations in which their own experiences are not engaged [17]. In their study of non-expert users, Downs et al. finds that individuals are sensitive to risks which they are familiar but tend not to be wary about those they are not. For instance, they might be suspicious of an email from a bank asking for their social security but not from an online store asking for their password [17]. If close reading can easily be undermined by visuals, a Talmudic approach to self-defense, which requires the careful application of detailed rules, is, at best, impractical, and at worst, potentially dangerous.

Putting concerns about this type of potentially misguided guidance aside, HCI researchers have noted something else that has implications for the particular genre we examine in this paper. Detecting phishing in emails is akin to text analysis, whereby the astute user must identify certain literary devices to discern and decode sinister intent [7]. As we will note in our findings, some of these vivid stylistic devices—or similar ones—are also used to capture reader attention by the AARP.

### 2.4 Cybersafety risk and education in aging populations

We use the term "cybersafety" to refer to protections against risk like fraudulent communications that occur over the internet and/or can result in cybersecurity breaches or threats. These breaches often occur with communications from fraudulent bad actors, or when individuals click on links to scams. What is particularly of interest is the sharing of stories of cyberthreat, scams, and fraud that are meant to educate aging populations who have a number of psychosocial and contextual reasons for being more vulnerable to cybersafety threats: e.g., as you grow older your grow more trusting, struggle to detect deception (or fact from fiction) [9]. Older adults are also relatively newer to the internet and may therefore have less experience with clickbait and scams [9]. Perhaps most relevant to our research is that repeatedly showing older adults that a claim is false (the primary practice of government organizations and the AARP in their communications about cybersafety) actually helps them remember it better [57]. The implication is that sites that repeatedly identify anecdotes like "we've heard about romance scammers asking" [61] may indeed be exacerbating the problem. Older adults may also be more susceptible to cybersafety threats because they struggle with their confidence in using technology and with adapting to it—even though, perhaps contrary to stereotypes, they perceive new technology to be a net positive in their lives [47].

One way to think about *cybersafety education* and protections for any group, including older adults, is to think, not about what set of facts people know, ***but how they conceptualize their digital self and how they navigate and reach out to people for support, which requires understanding of their context***—e.g., what structural barriers and community support exist—in addition to categories of vulnerability. Personal importance and children [21], as well as self-efficacy [48] and anxiety [12] play an important role in determining comfort and use among older adults. Research by Kropczynski et al. demonstrates the role that outside experts may have on community collective efficacy among older adults with less self-efficacy or experience [34]. Other research has suggested that trusted cybersecurity advocates may indeed play a key role in overcoming reluctance and negative perceptions of cybersecurity practices [28]. Older adults may be more dependent on family and friends and face-to-face interactions than work colleagues and IT experts [49]. As frequent recipients of hand-me-down devices, older adults may be more often in a position of bypassing expertise that comes with initial and ongoing commercial service support [49].

Unlike their younger counterparts, older adults are more likely to expect that important cybersafety information will grab headlines [49]. Yet another study found, paradoxically, that older adults are also more likely to turn to broadcast news sources, rather than online sources [13]. And other research indicates that age is negatively correlated with seeking out online news source for

security and privacy related threats [13]. Older adults may, in fact, spend more time reading privacy policies [50] although it is actually not clear to what extent current mechanisms for educating the aging public are useful. What we do know is that efforts at education are, unsurprisingly, impacted by familiarity with digital resources [19, 27]. At the same time, one of the institutions that shape older Americans' perspectives on the perils of online life is the AARP (namely their online blog presence), an exceedingly powerful organization with a readership that exceeds celebrity magazines.

### 2.4 Relevance to CSCW

CSCW is increasingly taking up studies of privacy and security among older populations who are perceived to have unique privacy needs. Nicholson et al. finds that older adults tend to prioritize social and accessible resources over expert ones and are more inclined to pay attention to non-internet media sources [49]. Kropczynskiet al. found that older adults tend to gravitate to those in their community with similar expertise [34]. Research of vulnerable populations has similarly found that communities tend to rely on each other for support (e.g., [25]).

While it is important to consider that AARPs audience will evolve to reflect familiarity with internet as well as changes to the internet itself, we believe that some of the same structural problems—e.g., economic models that incentivize click-bate articles—and use of infantilizing content, as opposed to explanations that focus on why and how threats happen will persist in some shape or form. Moreover, research has shown that it is "internet natives" and not older individuals that are more likely to be the victims of internet scams individuals [37].

### 2.5 AARP

The AARP is a US advocacy group that has been carrying out a mission to "empower" individuals as they age for over 60 years [3]. In that time, they have established a commanding online and offline presence. As of 2018, the AARP was the most-read magazine in the United States, reaching over 38 million Americans edging out over People magazine [2, 53]. AARP produces print, blogs, podcasts, local trainings, and other media dedicated to educating aging populations about both their privacy protections and vulnerabilities, and the hazards of offline and online scams and fraud. The AARP also reported that it employs over two thousand staff and over twenty thousand volunteers.

Over the years, AARP's non-profit status has been investigated and challenged based on the scale and scope of its profit-making activities. In 2009, most of its revenue came from the sale of insurance policies, credit cards, and other products [18]. According to their annual report, the majority (roughly 60%) of AARP's revenue in 2018 came from royalties and only nine percent came from publication and advertising (2% from "digital media"). These royalties are branded third-party use of AARP name for primarily healthcare products, followed by financial products, and lifestyle products.

It is understood, particularly by the AARP, that older adults (whom they define as age 50 and older) may be at heightened risk of cybersafety breaches and fraudulent behavior because of their lack of experience with internet technology and the fact that they represent a financially attractive, large target [45, 64]. Yet, the nature and magnitude of older adults' vulnerabilities (or anyone's, for that matter) is not necessarily measured accurately by organizations like the AARP that aim to understand and characterize it. The dubious nature of this measurement may reflect, in part, the absence of valid metrics of cyber-sophistication or vulnerability for any segment of the broader population. For instance, Pew reports that most internet users in the US are not able to answer half of their cybersafety knowledge quiz questions, but there utility or significance to actual user security (definition of a botnet, for instance) are unclear or unproven [51]. Yet, the vast majority can identify

the most secure password from a list [51]. Merely posing these questions implies that a citizen can be called to account for their lack of cybersafety based on insufficient information about the nature of breaches.

In reality, however, the boundary between a user's secure inner space and the "cyberworld" is so porous that commonly devised measures of sophistication can neither measure user risk nor necessarily help to mitigate it [24]. Cybersafety is a daunting challenge for the individual and models that appropriate standards of personal responsibility from other spheres of life may not be apt in the online world [33].

## 3 METHODS

### 3.1 Conceptual framing

The social forces and cultural currents influencing how people view and safeguard their cybersafety have implications for how we design systems that support aging populations. While qualitative work has provided substantial insight into older adults' cybersafety constructs [43, 44, 52], we are interested in how discourse is potentially shaping cybersafety norms among these communities. To do this, we draw on van Dijk's discourse of power [14], a paradigm that deals with differing degrees of power garnered through privileged access. Typically, discourse of power looks at the preferential access granted to media in their propagation of news and opinion. It uses CDA to explore how discourse reifies inequalities and relations of power. Because we are investigating the worldviews of a population made vulnerable by age and its various correlates—removal from the workforce, distance from vectors of technology, decompensation associated with physical limitations, and potential decline in cognitive status—the presence of a powerful channel that monopolizes the conversation is an appropriate focus for our analysis. Specifically, we look at the way that the AARP conceptualizes their readers through language [55] and the implications for their characterization as victims and the limited agency they are conferred, which relates to what strategies are prescribed and which are available.

We use CDA for our content analysis to show how AARP creates a cultural framework around which older adults experience cybersafety. We show how the stories or myths that powerful organizations conceptualize the user as a victim and promulgates enduring fears through stereotypes of scams.

### 3.2 Study design

As background for this research, we reviewed educational materials from other sources like USA.gov, FBI.gov, CISA.gov (the US Cybersafety and Infrastructure Security Agency), and Consumer Reports. The data presented in this paper are the result of a systematic review of cybersafety related content published by the AARP from 2004 to 2020. Our research team has also conducted numerous qualitative studies with older adults about their cybersafety. This project was designed to understand how the most popular publication in the United States is educating aging populations about their cybersafety with the goal of advancing our understanding of how to support and empower this large segment of the population.

### 3.3 Dataset

We conducted a qualitative analysis of articles from 2004 to 2020 on AARP.org. Rather than use a web scraping tool which would have yielded a larger sample from which to sort a larger proportion of non-relevant posts, we took an approach that more closely resembles what someone using the

AARP's search engine might find. We began collecting our dataset by first searching for keywords "cybersafety," "identity theft," "privacy" and found that the majority of articles were concentrated in sections labeled "Scams & Fraud" and "Personal Technology." We collected all articles in these sections using the AARP's site map. "Scams and Fraud" resulted in 913 articles and Personal Technology resulted in 157 articles. We also identified a "Fraud Resource Center" where AARP provides a repository of different kinds of fraud, from which we collected 68 entries. In addition to these sections, we also collected articles from a keyword search for "cybersecurity," which returned 74 entries, "identity theft," (2,775 entries), and "privacy" (36,014 entries), scraping only those articles that were not already listed under the other sections (e.g., "Scams & Fraud," "Personal Technology," and "Fraud Resource Center") or which were not links to discounts or advertisements (which were the vast majority). For the search term "cybersecurity," we collected 40% of the total 74 entries that were not cross-listed with the other sections. For "identity theft," we collected 2,775 entries; but because so many (17 out of a sample of 20 of the first returns) were already filed under Scams & Fraud, we just collected the first 60 entries not in our other sections, which represents 2% of the total returns. For "privacy," so many entries were for discounts that we only collected the first 150 until the returns yielded *only* advertisements and eliminated those cross listed with other sections for a total of 129.

### 3.4 Coding for relevance

Our data collection efforts resulted in a total of 1,356 articles from the AARP site. We conducted a content analysis of each of these articles to determine which ones to include as relevant to our analysis. We coded papers as relevant if they described a cybersecurity or privacy issue, such as a scam, fraud, or theft that can occur through an *internet-connected vector*, which we consider to be any application, data, or other communication over a smartphone or computer. An article would be coded as ***not*** relevant if it did not meet these criteria, which included some articles about fraud or scams that took place in-person or via paper mail.

After the first coder had reviewed a subset of the articles, the research team reviewed and discussed the criteria for relevance. We used inter-rater reliability (IRR) just for coding relevance. Two of the co-authors coded the first 50 articles from Fraud & Scams and achieved 86% agreement. We discussed disagreements and then coded another 50 articles from Fraud & Scams and a random sample of roughly 10% of articles from each of the other categories (a total of 57 articles). We calculated IRR between the two codes using Cohen's kappa. This method yielded an acceptable level of agreement (Cohen's kappa=0.714). There were no disagreements, only reading errors. The co-authors then proceeded to code the remaining dataset. The result was that 518 of the 1,356 (38%) articles published from 2004 to 2020 (80 did not have a date) were relevant.

### 3.5 Relevant dataset

We coded a randomly chosen subset of the 518 relevant articles, roughly 30% from each category, resulting in 162 articles (see Table 1). This is 5 more than were necessary to reach 30% (see "Articles needed for 30%" column in Table 1) for Scams but we settled on 31% to match all other categories, where halves were rounded up (see "% Total dataset coded column in Table 1).

Table 2 shows the distribution of articles across time intervals. The distribution across the years is comparable for the sampled subset and the entire coded set (average differences in the percentage of the total accounted for by any given year is .05%, with a maximum difference of 2.73% (2016)). We see the highest concentration of relevant articles in the last four years and those that are undated (See Table 2).

Table 1. AARP relevant dataset*

| | Total | # relevant | # relevant coded | % relevant coded | % Total dataset coded | Articles needed for 30% |
|---|---|---|---|---|---|---|
| Money: Scams & Fraud | 913 | 414 | 129 | 45.3% | 31% | 124 |
| Personal Technology | 157 | 13 | 4 | 8.3% | 31% | 4 |
| Fraud Resource Center | 68 | 48 | 15 | 70.6% | 31% | 15 |
| Keyword "cybersecurity" | 29 | 9 | 3 | 31.0% | 33% | 3 |
| Keyword "identity theft" | 60 | 21 | 7 | 35.0% | 33% | 7 |
| Keyword "privacy" | 129 | 13 | 4 | 10.1% | 31% | 4 |
| Total | 1,356 | 518 | 162 | 38.2% | 31% | 157 |

### 3.6 Critical discourse analysis (CDA)

This analysis drew on the critical tradition of CDA – specifically in how discourse was being used to construct the user in relationship to the threat and thus control the narrative around what agency is available to the user and how. CDA involves content analysis of a text or set of texts [20]. Ultimately, our method resembled CDA, but with a grounded approach to sampling and coding whereby we remained open to interpretation and only later applied CDA, thinking about how communications contribute to a discourse of control over the user's self-concept.

Coding and CDA was performed by one of the authors who regularly met with the team to discuss codes and findings. The choice of one coder is acceptable, if not preferable, when reliability is sought merely as a matter of agreement through discussion and when the codes are not meant to be replicated in other corpus [42]. The single coder represents an "expert researcher" who emersed themselves in all of the data and accompanying research on cybersafety threats among older adults and the resources they use. This researcher regularly used techniques such as memoing and reflection [42].

For our analysis of relevant articles, we draw on grounded theory methods, treating the types of safety education as areas for selective sampling for the purposes of generating further themes addressing how AARP educates and "empowers" their readers. Building on more recent applications of Strauss and Corbin's [58] grounded theory, e.g., [5, 26], we chose an approach one might deem "lite" in the sense that we used open-coding to generate initial codes, and then used selective coding to focus on the problem of how information was being shared and how readers were being educated. We used theoretical sampling to focus on how information was being used to create a reality in which, for instance, there are shared security threat narratives or tropes that include "veterans," "romance," and "Nigerians." Throughout this process, we constantly compared coding categories against incidences of concepts or codes.

*3.3.1 Article type.* The first author subsequently coded the 162 articles based on two initial categories. The first category of coding was for ***article type***. This coding focused on describing the type of threat described in the article. We generated 16 codes for article type, which were then

consolidated into the following codes: scams, fraud, cybercrime, identity theft, security, and catfishing.

The first author made the distinction between ***scams*** and ***fraud*** based on the degree of social engineering and involvement of the adversary. A scam denotes a misleading communication that is not personalized, like a package delivery scam where the victim is sent a malicious link via smartphone or email. This does not require that the adversary put any effort into customizing or speaking with their target. By contrast, we designated something a fraud if it involved direct outreach by the adversary such as, for example, when an adversary uses a pop-up ad, alleging that the target's computer has been infected and offers a number to call and/or has the target wire them money for cybersafety protection. Frauds might involve communication over some period of time, for instance, when a promise to sell a product or service, followed by a request for a wire transfer.

Table 2. AARP relevant dataset by date

| Year | Relevant | % relevant articles | Coded | % coded articles |
|---|---|---|---|---|
| 2004 | 1 | 0.2% | 0 | 0.0% |
| 2005 | 3 | 0.6% | 0 | 0.0% |
| 2006 | 5 | 1.0% | 1 | 0.6% |
| 2007 | 2 | 0.4% | 1 | 0.6% |
| 2008 | 19 | 3.7% | 3 | 1.9% |
| 2009 | 24 | 4.6% | 5 | 3.1% |
| 2010 | 32 | 6.2% | 12 | 7.5% |
| 2011 | 38 | 7.3% | 12 | 7.5% |
| 2012 | 21 | 4.1% | 8 | 5.0% |
| 2013 | 3 | 0.6% | 2 | 1.3% |
| 2014 | 21 | 4.1% | 4 | 2.5% |
| 2015 | 12 | 2.3% | 4 | 2.5% |
| 2016 | 15 | 2.9% | 9 | 5.6% |
| 2017 | 54 | 10.4% | 15 | 8.8% |
| 2018 | 49 | 9.5% | 16 | 9.4% |
| 2019 | 81 | 15.6% | 24 | 15.0% |
| 2020 | 58 | 11.2% | 20 | 12.5% |
| Date not given | 80 | 15.1% | 26 | 16.3% |
| Total | 518 | 100% | 162 | 100% |

While all of these article types might technically be designated ***cybercrime***, we used this code to denote data theft, typically resulting in personal data breaches, theft of passwords or credit card information online, or hacking of banking accounts. Although cybercrime and identity theft are closely related, we reserved the code identity theft for articles that centered specifically on that crime (described below) and which used that language.

***Identity theft*** denotes a particular kind of threat that is covered in the news specifically and is often associated with a prolonged "condition" that requires monitoring and longer-term repair and vigilance. By contrast, the types of breaches associated with cybercrime often lead to hacking of accounts using stolen passwords but do not rise to the level of wholesale triangulation of a person's

information that can produce ongoing vulnerabilities as with "identity theft." In all but one case, these articles included the phrase "identity theft" in their title.

***Security*** covers a range of preemptive-minded article topics focused on banking, smartphones, travel, social media, and internet of things (like robots). We initially coded social media separately but found that it accounted for just three articles, one of which dealt with posting and the remaining two described scams and a security breach.

The first author coded ***catfishing*** (a term used by AARP) as a special case of fraud when someone is led to believe they have developed a relationship with someone only to find that the person is looking for money. These types of fraud play prominently into a narrative of duplicity in which "fraudsters" are depicted as foreigners.

*3.3.2 Cybersafety education.* The first author then coded articles based on the type of cybersafety education they provided. These codes included the following:

**Provide strategy:** Provides guidance or list of "dos" and "don'ts" at the end.

**Top list!:** Describe scams and fraud in a too-detailed way. These articles tend to have sensational names or use "click bait" language" like "Bait-and-Switch Advertising" or "Return Rip-Off's." They are notable often because they provide a play-by-play of how the scam can occur without providing higher level strategy about how to avoid it. Rather, the detail itself is meant to be educational. Many articles fit this profile but were ultimately put in the "provide strategy" category because they also contained a list of strategies for avoiding these scams or frauds—though their accuracy was highly suspect. That is, the majority of AARPs publication contain some element of "click bait" presentation but "pass" off as more helpful because they provide a list of "dos" and "don'ts" much like USA.gov and other supposedly legitimate institutions. We call these articles "top list!" because they borrow from the Web 2.0 era of creating lists of dubious value that contribute to a sense of false importance and heightened attention, anxiety, and suspense through an ordinal format—not to be confused with the dos and don'ts listings of the provide strategy category (described below). Although articles we coded as provide strategy also do this with headlines like "5 Steps to Take If You're a Ransomware Victim," or "Beware of Tech Scammers Who 'Flat-Out Lie'," what sets top list! Apart is both degree or intensity of valence of fear and scarcity (or absence) of strategic guidance. In this section, we talk about the top list! genre and then provide some insights from additional analysis.

**Scam alerts:** A new or relevant scam that users should be on the alert for (e.g., COVID-19 scams).

**Reporting:** Reports from surveys conducted by AARP or other data or sources, usually providing statistics about cybersafety threats in terms of impact and consumer awareness.

**Story:** Tells a story to illustrate how a scam works, for example, how two sisters who advertised their condo on BuyaTimeShare.com were "caught up in a new wave of fraud that has systematically targeted vacation property owners." [2]

**Other:** Includes quizzes and other cybersecurity news related items (e.g., Attorney General "taking on Medicare Fraud"[3]).

## 4 FINDINGS: CLASSIFYING AARP'S APPROACH TO CYBERSAFETY EDUCATION

**Article Type:** We coded each article by type as defined in 3.3.1. AARP dedicates nearly half of its published online communications about cybersafety to scams (46.9%). Fraud accounts for nearly one in five articles (19.1%), followed by cybercrimes (13.0%) (see Table 3).

[2] https://www.aarp.org/money/scams-fraud/info-2017/timeshare-scams-how-they-work.html
[3] https://www.aarp.org/money/scams-fraud/info-2018/jeff-sessions-interview.html

**Cybersafety education:** We coded each of these articles by the type of safety education they offer as defined in 3.3.2 (see Table 4). Just under half of the articles in our dataset provide strategies for dealing with cybersecurity threats (77 articles or 47.5% of articles).
Articles that we coded as "provide strategy" might be talking about general threats (such as "What Should I Do after a Data Breach?" or "10 ways to Protect Yourself from ID Theft") to very specific scams around recent events such as a disaster or health emergency (e.g., earthquakes in Japan, swine flu, COVID-19). We find that many articles in this category provide the same or similar lists provided by government institutions, but that the articles are framed in their urgent and childish manner that is meant to both scare and entertain ("Is your Smart Home Spying on You" or "Beware of Swine Flu Come-Ons" or "When Danger Lurks in 'Heidi Klum'"). In one of several articles about COVID-19 scams, in which the AARP describes everything from "bogus cures" to "phishing," they provide strategies published by the FTC.

Table 3. Article types

| | # articles | % articles |
|---|---|---|
| scams | 76 | 46.9% |
| fraud | 31 | 19.1% |
| cybercrime | 21 | 13.0% |
| identity theft | 17 | 10.5% |
| security | 12 | 7.4% |
| catfishing | 5 | 3.1% |
| Total | 162 | 100% |

Table 4: Type of cybersafety education

| | # articles | % articles |
|---|---|---|
| provide strategy | 77 | 47.53% |
| top list! | 24 | 14.81% |
| scam alert | 19 | 11.73% |
| reporting | 21 | 12.96% |
| story | 14 | 8.64% |
| other | 7 | 4.32% |
| Total | 162 | 100% |

Articles coded as providing a strategy generally reinforce a worldview where the perpetrators of scams are "deceptive scam artists" who are out to trick their targets. Moreover, their titles suggest the content of the article will unlock some knowledge, which exaggerates the promise of cybersafety and creates a misleading view of the threat. For example, 34 of the 77 (44%) provide strategy articles have the word "beware" in the title. But there is subcategory of articles, top list!, that lean heavily on this formula discussed in the next section.

### 4.1 The anatomy of a Top List! article

We focus the remainder of our analysis on a subset of articles we coded as top list! Articles with this code perform a specific kind of worldmaking in which readers are cast as the central characters—

victims of "scammers" and "fraudsters" who prey as opposed to an article which would highlight cybersafety vulnerabilities of the internet, platforms, and computing infrastructure (e.g., data breaches, password protection, spam filters) or current events, so much as personal vulnerabilities (e.g., veterans, grandparents, moviegoers). It's not clear whether grandparents or moviegoers specifically are a more frequent target, but according to the AARP, veterans are twice as likely as nonveterans to lose money to scams [1]. How frequently certain people like veterans, grandparents, and people who go to the movies are referenced is less important than then what their narratives say about the way that AARP particularizes risk.

**Top list! mythology and the depiction of adversary:** If we look at top list! as a kind of mythology it is instructive because they have certain structures in common—even if AARP is not in the mythmaking business. Myths pass along stable norms and enduring cultural fears. The narratives about scams that are featured in top list! are everchanging, but still perpetuate the normative view of users as having little chance against adversaries. For AARP, being a veteran or being a grandparent is portrayed as a privacy vulnerability, and while we may agree these populations are more at risk, it's not clear who is served by portraying them as easy targets.

The adversaries AARP depicts in top list! execute "dirty tricks." They are cartoonish; and leave one with the impression that scams and fraud are carried out by bad guys whose aim is to lure and ruse for, what almost seems like, the pleasure of the deed. AARP isn't wrong to say that some scams and some fraud are carried out by individuals who know their targets, but these articles suggest adversaries are out to get their readers. In "12 Tools in a Fraudster's Toolbox," AARP depicts adversaries as if they are criminal masterminds whose psychology they have access to:

> "Criminals excel at blarney and use flattery and charm to ingratiate themselves and gain your trust. Alternatively, they may threaten violence to frighten you to act. The goal is the same: to compel you to cough up cash or sensitive data. And the perpetrators are nothing if not persistent." (https://www.aarp.org/money/scams-fraud/info-2020/fraud-tactics.html)

To say that "fraudsters" "excel" at "blarney" and "charm" reinforces a dubious idea that the AARP is well acquainted with the psychology of cyber-criminals—or that there is even a psychology to know. This is dangerous; the entire premise of this blog is to get the reader to consider the cyber-criminal.

**Top list! format of specificity:** Top list! articles also share a format whereby they detail attacks in highly specific ways, guiding people to spot them only by the specific script or ploy, rather than based on some common ground rules. In particularizing storylines, they may divert reader attention from the overarching structure of a scam, making schema development and pattern-matching a more difficult task.

*4.1.1 The epitome of the top list! genre.* Top list! articles could be epitomized by the article about the military-themed scam described in "8 Military-Themed Impostor Scams." The article details the various ways that "fraudsters" manipulate targets by posing as military service members, a plotline used to prey on people's sympathies and sense of obligation:

> "Posting ads on Craigslist and elsewhere, fraudsters claim to be active-duty service members about to be deployed overseas (or as a family member of a service member killed in action) who need to quickly sell a car or other big-ticket item. The price is too good to be true for good reason: There is no item, only a request for upfront payment before the item is delivered — and it won't be." (https://www.aarp.org/money/scams-fraud/info-2017/military-scams-fd.html)

The use of the term "fraudsters" is gratuitously colloquial, and perhaps overfamiliar in a way that adds to the impression that this "person" exists and is meant to be engaged with. This article also fails to point out that the very idea of selling a car on Craigslist, or that an "active-duty service member" is urgently selling a car, should be a red flag discouraging any form of engagement. The phrase a "price [that] is too good to be true" pushes older adults to take a step further than is necessary to avoid the threat.

In "8 Military-Themed Imposter Scams," AARP also detail the "Grandparent Gotchas," a scam that preys on the "loving grandparents" of "military families" when scammers "get word" they are deployed through local news. These scammers pose as grandchildren who need help on "R&R" (presumably, rest and relaxation) that requires "quick cash."

> "Military families are a popular target in this long-running scheme that preys on loving grandparents. Scammers get word of deployed soldiers from local newspaper stories and, posing as the grandchild or relative, they claim a problem while on R&R, such as arrest or hospitalization, to get quick cash from worried elders." (https://www.aarp.org/money/scams-fraud/info-2017/military-scams-fd.html)

In this scam, AARP characterizes the scammers as someone in the reader's midst who uses local news to manipulate "worried elders." The impression one gets is that they have intimate knowledge or local knowledge of these unwitting grandparents, rather than a more obtuse and data-driven registry from which to target. There are other iterations of the "Grandparent Gotchas," like in "Scams by the Season," where AARP's grandparents scam is reloaded for the school summer break.

> "As spring break begins for many college students, con artists behind the notorious Grandparents Scam get to work. You may get a call that a beloved grandchild was arrested, hospitalized or has endured some other hardship that requires your money." (https://www.aarp.org/money/scams-fraud/info-12-2012/scams-by-the-season.html)

In this version of the scam, "thieves" take advantage of the closing school year. AARP frequently casts veterans, as well as military families, as an enduring, specific class of victim. By contrast, AARP specifies an entire nationality, "Nigerians," as a specific class of scam artist depicted in articles like "5 Scams to Watch for in 2012."

While the top list! are not so much different in tone than the articles we coded in other information categories, they are particularly egregious in their contribution to the creation of a worldview that there are cartoonish bad actors in everyone's midst looking to prey on people's emotional weakness and not their security weaknesses. In so doing, they legitimize a view of an ecosystem in which there is always crime and one has to be on the lookout for, rather than simply steer clear of it to protect themselves. While looking for misspellings and email addresses are potentially helpful tactics, we argue that higher level thinking about simply what is legitimate is what AARP should emphasize. The tactics they offer are like decoder rings; if only one had a cypher.

In the next section we distill the components of top list! articles that make them a useful object lesson in cybersafety education premised on personalizing threats potentially resulting in a worrisome education.

*4.1.2 Codifying top list! characteristics.* Top list! have several characteristics that are gratuitously unhelpful in promoting cybersafety that we have codified:

First, they encourage, rather than discourage readers to increase their exposure for the purposes of identifying the threat, dragging out the exposure. An article might describe in detail a scam or fraud where in order to detect the adversarial nature of the communication, one has to answer a call, for

example, in an article titled "3 Scams That Are Driving Everyone Crazy" the victim (apparently) says:

> "'I received a call from 360-203-0375 claiming to be from the IRS and telling me I owed back taxes. It was a recorded message. Knowing I did not owe back taxes, I hung up!!!" (https://www.aarp.org/money/scams-fraud/info-2018/crazy-scam-stories.html)

In this article, the expert, Amy Nofziger, responds: "That's the perfect response! HANG UP! Great job staying safe." Nofziger goes on to recommend that people not pick up calls they don't recognize and download an app that Nofziger says, "warns me when a call comes in, to the legitimacy of the call." This is good advice, but this article still promotes the idea of a phone number as being a way to combat these crimes, when we know that spoofing exists precisely so people will believe the number to be legitimate and is, therefore, rather unique, and therefore, not useful to publish for an audience. Second, the article features a reader's account of following a scam to its finale (thinking about whether they had paid their taxes), rather than identifying the premise of the IRS calling (or a sweepstakes give away, or any other solicitation) as bogus. The implication is that for one to combat scams they must decipher them, and that implies that there is some logic to them. We posit that the more AARP readers feel the villain is out there to get them, the more they will follow the breadcrumbs to their peril.

An example of this is in an article titled, "12 Tools in a Fraudster's Toolbox" where AARP defines "phishing":

> "So-called 'phishing' emails, calls, texts and letters try to trick you into sending cash or disclosing personal information. Or, the correspondence aims to allow a bad actor to infiltrate your computer device and steal sensitive information. Microsoft, for example, has warned that cybercrooks send phishing emails from rnicrosoft.com—note the 'r' and 'n' were combined to appear at a glance as an 'm.' The word phishing — which dates to 1996 — combines 'fishing' and 'phreaking,' the latter a term for using an electronic device to avoid paying for phone calls, says Merriam-Webster." (https://www.aarp.org/money/scams-fraud/info-2020/fraud-tactics.html)

In their definition, they illustrate a specific attack detected through misspelling of the name Microsoft, where mere generalization would do and foster extrapolation. It's rather odd that AARP defines the portmanteau in this context, suggesting decipherability of text as the key to detecting and decoding a scam. It's not untrue that misspellings can be flag for cybercrime, but the emphasis should be on emails that are *not for you—which should be summarily dismissed instead of scanned for meaning*. By defining the term phishing with such specificity, using philology, AARP goes too far and there is some suggestion that their audience can be a good detective, too. This is inconsistent with mainstream cybersecurity guidance, which is to not engage with suspicious emails and, when impersonation is suspected, to find other means of contacting that person.

Second, and relatedly, top list! articles provide examples that may be too specific to help readers deduce and remember patterns, thus limiting their value as guidance. They provide specific scenarios, rather than a roadmap that might empower users across scenarios. For example, in an article titled, "6 Scams to Dodge in 2020," the reader is told how "Scammers pretend to be Amazon representatives, taking advantage of the fact that the company sent more than 3.5 billion packages

last year."[4] AARP could alternatively provide categories of scams that were not company specific, which have the advantage of both alerting people to a known scam and also reenforcing that scams are not particular; rather they are constantly shifting in order to thwart this very type of detection. This tactic of enumerating lists of things is certainly used around the web, but AARP does it with such specificity as to make it unproductive as argued. AARP also uses references to time and times of the year to create urgency and relevance (see Table 5).

Table 5: Framing Tactics used in TopList! Article

| **Framing tactic** | **Examples** | **% articles** |
|---|---|---|
| Enumeration | e.g., "12 Tools In A Fraudster's Toolbox"; "3 Scams That Are Driving Everyone Crazy"; "9 Things The 2020 Census Won't Ask You" | 38% (9) |
| Use of time, date or season | e.g., "6 Scams to Dodge in 2020"; "Scams by the Season" | 38% (9) |

Third, top list! articles use language and syntax that is cartoonish and demeaning, and which serve to perpetuate metaphor of social intermediation. In Table 6, we catalogue some of the linguistic tactics that contribute to this pastiche and their frequency. AARP top list! articles use alliteration (e.g., "Sweepstake Swindles") in half of their articles. One in five of top list! articles use wordplay like "Facebook Unfriendlies." Top list! article's use of wordplay place scams and fraud in a familiar social context, reinforcing a notion of scams and fraud as the product of social intermediation and personal engagement, which require users resists them or defend against them on those same terms. Both the alliteration and the wordplay trivialize the scam with use of childish communication; and, in the latter, additionally personalizes the adversary by using language that makes them seem as a known adversary, someone simply who is "unfriendly." AARP top list! gratuitous cataloging reminds us of all the ways scam and fraud outreach occurs (e.g., "Facebook Unfriendlies") but never attempt to depersonalize it.

Table 6: Linguistic Tactics used in TopList! Articles

| Linguistic tactic | Examples | % articles |
|---|---|---|
| Alliteration | Sweepstakes Swindles, Devilish Diagnoses, Grandparent Gotchas, Gossip Gotchas, Diet Duplicity, Romance Rookery | 50% (12) |
| Wordplay | Pay Us" Play, Facebook Unfriendlies, Prime Time for Fraudsters, Bait-and-Switch Advertising, "Dialing for Diabetics" Diversion | 21% (5) |

## 5 DISCUSSION

Because scams and fraud are, themselves, stories, the AARP articles (particularly those we coded toplist!) are like anthologies. Beyond that, these stories may even function deceptively as myths, but they fall critically short. Myths present people with a "theory of the world" in which they live, and

[4] https://www.aarp.org/money/scams-fraud/info-2020/beware-scams-2020.html?intcmp=AE-FRDSC-MOR-R2-POS3

they also instruct them in the consequences of failing to interpret certain events and behaviors correctly. AARP might try to inoculate people against the idea that whatever strangers might seem to know or want is an illusion, but it's not clear that the "myths" AARP tells are functioning that way—that they provide structure and clear rules for digital living. These articles (particularly these lists of scams and fraud) do not have the structure that myths have, leaving their users to weave together a moral from a broad mesh.

We should be concerned about the efficacy of the anthology of myths approach. The social forces and cultural currents that influence how older adults understand their susceptibility to threats and also from whom they accept help with their cybersafety are, we have to assume, very much influenced by AARP, given their reach.

We have been conducting research aimed at empowering those experiencing memory loss associated with aging through the design of technology application guardrails [anonymous for review]. While our focus is on supporting couples in collaborative management of their internet security, we also wanted to understand how and what the populations we study are learning about cybersafety risks and threats and the strategies they are being given to prevent them. This research has led us to some insights about how we and others in this community might offer assistance.

### 5.1 Cybersafety education

This guidance specifically takes up AARPs tendency to promote personalization and thus force engagement. Cybersafety education should focus on finding ways to prevent harmful links and texts from invading people's technology. A good place to start would be **prevention:** educating people about ways to *block ads and report spam,* to limit the amount of data that is out there about them. In addition, cybersafety education should emphasize *avoiding communications and products users didn't ask for*, such as a package, loans, or gifts. Cybersafety education should not engage in the same literary tactics as used in phishing emails [7]. Finally, we argue for educating individuals about **data capitalism**: the way that their data is mined, monetized, and extracted—so that they can better depersonalize what seems familiar or serendipitous. In the next section, we elaborate on how this might be taken up in our future work.

### 5.2 Future work

Future work should, of course, explore the degree of influence of AARP on older adult cybersafety education as well as explore alternatives. Below we touch on key components of cybersecurity tools and guidance to consider.

*5.2.1. Prevention.* Future research should explore cybersafety tools that focus on prevention—on blocking harms through technical interventions—such as blocking ads, reporting spam and limiting one's digital footprint—that mitigate the need for social engineering training in the first place. Indeed, future work should explore ways of reconceptualizing older adult users not as victims, but as agents capable of better censoring their lives. Of course, there is no entertainment value in the mythological character that is not drawn in to the fray and there is obviously an advertising model with "free" incentives to combat [36]. The extent to which the very systems that are educating internet users are bound up in the same advertising logics is, perhaps, unavoidable. Yet the AARP, as we demonstrate, seems to employ the very tactics of those they are supposedly protecting their readers from.

*5.2.2. Rethinking Social Engineering.* Future work on education should interrogate structures. For example, let's challenge a premise: should one really ever address a communication from someone they don't know over email? The answer is almost always, no. But the AARP does often convey the

opposite advice—that one should engage—or at least puts their constituents in the interior of these dilemmas and thus casts them in that role, as negotiating rather than blocking harms. AARP readers are, in a way, depicted like the gullible characters of mythology, easily drawn into the story for a lesson but in the case of cybersafety, the "story" or "myth" is the poisoned apple, and they the pawns of the mythological conceit. We argue that publications like the AARP's lead older adults in the wrong direction by having them memorize a series of rules and particularize threats, rather than instructing them in the importance of context. Older adults should be reminded that their own context, behaviors and relationships are all that matter—not the stories that the AARP tells, or for that matter that our digital footprint tell.

*5.2.3. Data capitalism*: To make effective, consistent use of security guidance and tools, older adults need to be armed with theory of the online world that educates them about the rudiments of surveillance capitalism. For example, in future work, we will attempt to explore how to educate older adults about how data can be used to create context, and the distinction between algorithmic context (e.g., knowing things about you based on what you have done) versus personal context (e.g., knowing that you have a relationship with the person or business who is contacting you). This would involve teaching people to view their online selves as reconstructions made out of data that do not represent real relationships or patterns of behavior that represent a legitimate frame of reference or a relationship. One question this research will explore is how challenging it might be for people to imagine themselves as separate from the data they generate, and to recognize that their online lives (what they see) are influenced by algorithms that analyze and act on that data. We hypothesize that older adults are capable of embracing this mindset, learning that it's best to ignore the communications, for example, in their email that reflect "selves" they don't recognize. We contend that if given the right support, people may very well understand how their data and algorithms are shaping a reality—how the economy of data that uses algorithms predict online behavior. Future research efforts should include older adults in refining this type of guidance and experimenting with the impact of such an intervention.

### 5.3 Limitations

Our analysis has limitations in that we do not know how these communications by the AARP are received by older adults and how they shape behavior. We used CDA to articulate what people are exposed to and thus posit how it might shape their worldview. More research is needed to empirically understand the influence of the AARP and similar prominent sources and find ways to counteract their teaching. We need to explore how to better educate older populations (in particular about the rudiments of data capitalism) and to evaluate how effective those types of programs might be. Instructing older Americans, or anyone, on the forensics of cyber sleuthing is enormously difficult. Our research is meant to encourage a systematic, self-critical approach to much-needed public education on a subject of great importance.

## 6 CONCLUSIONS

We used CDA to show what types of narratives the AARP is endorsing on its blog that may exacerbate the very problem they are presumably trying to solve. We build, in part, on previous research on the "illusion of truth" which suggests that repeated false claims are remembered better and as true [57]. We also note that in an era where attention is monetized, the format of their online blog and business model of AARP are relevant and require more research into how clicks and data flows serve their bottom line [36]. We may need to radically rethink cybersafety and AARP provides an instructive case study in where it has gone off the rails. AARP's communications do, indeed,

convey that they want to influence how their users see themselves and their security risks, but they do so often by depicting them as victims and easy targets, ripe for interpersonal manipulation. Moreover, they depict scam and fraud stories as teaching users something that they need to understand about their adversary on personal terms, rather than delivering them structure and interpretive tools that emphasize avoidance. AARPs narrative of empowerment is about people overcoming adversaries who seem intent on manipulating them. They act as if they are in the business of mythmaking when their aim should be providing users with guidance about how to avoid the myths they tell.

## REFERENCES


[1] AARP Widens Its Lead as America's Most-Read Magazine: 2018. *https://www.foliomag.com/aarp-widens-its-lead-as-americas-most-read-magazine/*. Accessed: 2020-05-12.

[2] AARP's Mission, Vision, Advocacy, Community Service & Products: *http://www.aarp.org/about-aarp/*. Accessed: 2020-05-12.

[3] Acquisti, A. and Gross, R. 2006. Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *Privacy Enhancing Technologies* (Jun. 2006), 36–58.

[4] An Encounter with Grounded Theory: Tackling the Practical and Philosophical Issues: 2001. *www.igi-global.com/chapter/encounter-grounded-theory/28261*. Accessed: 2020-05-14.

[5] Avoiding Social Engineering and Phishing Attacks | CISA: *https://www.cisa.gov/uscert/ncas/tips/ST04-014*. Accessed: 2022-04-07.

[6] Blythe, M., Petrie, H. and Clark, J.A. 2011. F for fake: four studies on how we fall for phish. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (New York, NY, USA, May 2011), 3469–3478.

[7] boyd, danah and Hargittai, E. 2010. Facebook privacy settings: Who cares? *First Monday*. 15, 8 (2010).

[8] Brashier, N.M. and Schacter, D.L. 2020. Aging in an Era of Fake News. *Current Directions in Psychological Science*. 29, 3 (Jun. 2020), 316–323. DOI:https://doi.org/10.1177/0963721420915872.

[9] Cho, H. and Salmon, C.T. 2006. Fear Appeals for Individuals in Different Stages of Change: Intended and Unintended Effects and Implications on Public Health Campaigns. *Health Communication*. 20, 1 (Jun. 2006), 91–99. DOI:https://doi.org/10.1207/s15327027hc2001_9.

[10] Confessore, N., LaForgia, M. and Dance, G.J.X. 2018. Facebook's Data Sharing and Privacy Rules: 5 Takeaways From Our Investigation. *The New York Times*.

[11] Czaja, S.J., Charness, N., Fisk, A.D., Hertzog, C., Nair, S.N., Rogers, W.A. and Sharit, J. 2006. Factors predicting the use of technology: Findings from the center for research and education on aging and technology enhancement (create). *Psychology and Aging*. 21, 2 (2006), 333–352. DOI:https://doi.org/10.1037/0882-7974.21.2.333.

[12] Das, S., Lo, J., Dabbish, L. and Hong, J.I. 2018. Breaking! A Typology of Security and Privacy News and How It's Shared. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery. 1–12.

[13] van Dijk, T.A. 2008. *Discourse and Power*. Palgrave.

[14] van Dijk, T.A. 1996. Discourse, power and access. *Texts and Practices: Readings in Critical Discourse Analysis*. Routledge. 84–104.

[15] van Dijk, T.A. 2001. Multidisciplinary CDA: A Plea for Diversity. *Methods of Critical Discourse Analysis*. Sage. 95–120.

[16] Downs, J.S., Holbrook, M.B. and Cranor, L.F. 2006. Decision strategies and susceptibility to phishing. *Proceedings of the second symposium on Usable privacy and security* (New York, NY, USA, Jul. 2006), 79–90.

[17] Eggen, D. 2009. AARP could benefit from the health insurance reforms it advocates.

[18] Eynon, R. and Helsper, E. 2011. Adults learning online: Digital choice and/or digital exclusion? *New Media & Society*. 13, 4 (Jun. 2011), 534–551. DOI:https://doi.org/10.1177/1461444810374789.

[19] Fairclough, N. 1995. *Critical Discourse Analysis*. Longman.

[20] Fausset, C.B., Harley, L., Farmer, S. and Fain, B. 2013. Older adults' perceptions and use of technology: a novel approach. *Proceedings of the 7th international conference on Universal Access in Human-Computer Interaction: user and context diversity - Volume 2* (Berlin, Heidelberg, Jul. 2013), 51–58.

[21] Fiesler, C., Dye, M., Feuston, J.L., Hiruncharoenvate, C., Hutto, C.J., Morrison, S., Khanipour Roshan, P., Pavalanathan, U., Bruckman, A.S., De Choudhury, M. and Gilbert, E. 2017. What (or Who) Is Public?: Privacy Settings and Social Media Content Sharing. *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (New York, NY, USA, 2017), 567–580.

[22] Fiesler, C., Lampe, C. and Bruckman, A.S. 2016. Reality and Perception of Copyright Terms of Service for Online Content Creation. *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (New York, NY, USA, 2016), 1450–1461.

[23] Frank, D. AARP Survey Finds Veterans Are Frequent Scam Victims. *AARP*.

[24] Gandy, O.H. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Westview Press.

[25] Geeng, C., Harris, M., Redmiles, E. and Roesner, F. 2022. "Like Lesbians Walking the Perimeter": Experiences of {U.S}. {LGBTQ+} Folks With Online Security, Safety, and Privacy Advice. (2022), 305–322.

[26] Glaser, B. and Holton, J. 2007. Remodeling Grounded Theory (Reprinted from FQS-Forum Qualitative Sozialforschung, vol 5). *Historical Social Research / Historische Sozialforschung*. (Jan. 2007), 47–68.

[27] Grimes, G.A., Hough, M.G., Mazur, E. and Signorella, M.L. 2010. Older Adults' Knowledge of Internet Hazards. *Educational Gerontology*. 36, 3 (Feb. 2010), 173–192. DOI:https://doi.org/10.1080/03601270903183065.

[28] Haney, J.M. and Lutters, W.G. 2018. "It's Scary…It's Confusing…It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security. (2018), 411–425.

[29] Hargittai, E. 2010. Digital Na(t)ives? Variation in Internet Skills and Uses among Members of the "Net Generation." *Sociological Inquiry*. 80, 1 (2010), 92–113.

[30] Hargittai, E. 2005. Survey Measures of Web-Oriented Digital Literacy. *Social Science Computer Review*. 23, 3 (2005), 371–379.

[31] Hastings, G., Stead, M. and Webb, J. 2004. Fear appeals in social marketing: Strategic and ethical reasons for concern. *Psychology & Marketing*. 21, 11 (2004), 961–986. DOI:https://doi.org/10.1002/mar.20043.

[32] Hoofnagle, C.J., King, J., Li, S. and Turow, J. 2010. *How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?*. Technical Report #ID 1589864. Social Science Research Network.

[33] Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S. 2015. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. *Eleventh Symposium On Usable Privacy and Security SOUPS'15* (Ottawa, 2015), 35–52.

[34] KropczynskiJess, AljalladZaina, Jeffrey, E., LipfordHeather and J, W. 2021. Towards Building Community Collective Efficacy for Managing Digital Privacy and Security within Older Adult Communities. *Proceedings of the ACM on Human-Computer Interaction*. (Jan. 2021). DOI:https://doi.org/10.1145/3432954.

[35] Kumar, P., Naik, S.M., Devkar, U.R., Chetty, M., Clegg, T.L. and Vitak, J. 2017. "No Telling Passcodes Out Because They're Private": Understanding Children's Mental Models of Privacy and Security Online. *Proceedings of the ACM on Human-Computer Interaction*. 1, CSCW (Dec. 2017), 64:1-64:21. DOI:https://doi.org/10.1145/3134699.

[36] Landwehr, M., Borning, A. and Wulf, V. 2019. The High Cost of Free Services: Problems with Surveillance Capitalism and Possible Alternatives for IT Infrastructure. (Jun. 2019), 1–10.

[37] Lieber, R. 2021. The Young Fall for Scams More Than Seniors Do. Time for a Warning. *The New York Times*.

[38] Madden, M. 2017. *Privacy, Security, and Digital Inequality*. Data & Society.

[39] Madden, M., Gilman, M., Levy, K. and Marwick, A. 2017. Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans. *Washington University Law Review*. 95, 1 (Jan. 2017), 053–125.

[40] Marwick, A., Fontaine, C. and boyd, danah 2017. "Nobody Sees It, Nobody Gets Mad": Social Media, Privacy, and Personal Responsibility Among Low-SES Youth. *Social Media + Society*. 3, 2 (Apr. 2017).

[41] McDonald, N. and Forte, A. 2020. The Politics of Privacy Theories: Moving from Norms to Vulnerabilities. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, Apr. 2020), 1–14.

[42] McDonald, N., Schoenebeck, S. and Forte, A. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction*. 3, CSCW (Nov. 2019), 72:1-72:23. DOI:https://doi.org/10.1145/3359174.

[43] Mentis, H.M., 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. *Proceedings of the ACM Conference on Computer-Supported Cooperative Work & Social Computing* (2020).

[44] Mentis, H.M., Madjaroff, G. and Massey, A.K. 2019. Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, 2019), 343:1-343:13.

[45] Miller, M. 2020. Scammers step up efforts to target older Americans during pandemic. *The Hill*.

[46] Milne, G.R. and Culnan, M.J. 2004. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing*. 18, 3 (Jan. 2004), 15–29. DOI:https://doi.org/10.1002/dir.20009.

[47] Mitzner, T.L., Boron, J.B., Fausset, C.B., Adams, A.E., Charness, N., Czaja, S.J., Dijkstra, K., Fisk, A.D., Rogers, W.A. and Sharit, J. 2010. Older Adults Talk Technology: Technology Usage and Attitudes. *Computers in Human Behavior*. 26, 6 (Nov. 2010), 1710–1721. DOI:https://doi.org/10.1016/j.chb.2010.06.020.

[48] Mitzner, T.L., Rogers, W.A., Fisk, A.D., Boot, W.R., Charness, N., Czaja, S.J. and Sharit, J. 2016. Predicting Older Adults' Perceptions about a Computer System Designed for Seniors. *Universal Access in the Information Society*. 15, 2 (Jun. 2016), 271–280. DOI:https://doi.org/10.1007/s10209-014-0383-y.

[49] Nicholson, J., Coventry, L. and Briggs, P. 2019. "If It's Important It Will Be A Headline": Cybersecurity Information Seeking in Older Adults. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (New York, NY, USA, May 2019), 1–11.

[50] Oeldorf-Hirsch, A. and Obar, J.A. 2019. Overwhelming, Important, Irrelevant: Terms of Service and Privacy Policy Reading among Older Adults. *Proceedings of the 10th International Conference on Social Media and Society* (Toronto, ON, Canada, Jul. 2019), 166–173.

[51] Pew Research Center 2017. *What the public knows about cybersecurity*.

[52] Piper, A.M., Cornejo, R., Hurwitz, L. and Unumb, C. 2016. Technological Caregiving: Supporting Online Activity for Adults with Cognitive Impairments. (May 2016), 5311–5323.

[53] PR Newswire 2017. AARP The Magazine Has the Highest Readership of All U.S. Magazines, MRI Finds. *AARP-Magazine-ranking*. (Dec. 2017).

[54] Quan-Haase, A. and Elueze, I. 2018. Revisiting the Privacy Paradox: Concerns and Protection Strategies in the Social Media Experiences of Older Adults. *Proceedings of the 9th International Conference on Social Media and Society* (New York, NY, USA, Jul. 2018), 150–159.

[55] Rogers, R., Malancharuvil-Berkes, E., Mosley, M., Hui, D. and Joseph, G.O. 2005. Critical Discourse Analysis in Education: A Review of the Literature. *Review of Educational Research*. 75, 3 (2005), 365–416.

[56] Romance scams take record dollars in 2020: 2021. *https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020*. Accessed: 2021-04-15.

[57] Skurnik, I., Yoon, C., Park, D. and Schwarz, N. 2005. How Warnings about False Claims Become Recommendations. *Journal of Consumer Research*. 31, (Feb. 2005), 713–724. DOI:https://doi.org/10.1086/426605.

[58] Strauss, A.C. and Corbin, J.M. 1990. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. Sage Publications, Inc.

[59] Vaidhyanathan, S. 2018. *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. Oxford University Press.

[60] West, S.M. 2019. Data Capitalism: Redefining the Logics of Surveillance and Privacy. *Business & Society*. 58, 1 (Jan. 2019), 20–41. DOI:https://doi.org/10.1177/0007650317718185.

[61] What You Need to Know About Romance Scams: 2019. *https://www.consumer.ftc.gov/articles/what-you-need-know-about-romance-scams*. Accessed: 2021-04-15.

[62] Zuboff, S. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.
[63] 2019. *Consumer Sentinel Network*. Federal Trade Commission.
[64] 500. Scams Targeting Older Adults Are On The Rise. *HuffPost*.

Received July 2022, revised January 2023, accepted March 2023.