"Auntie, Please Don't Fall for Those Smooth Talkers": How Chinese Younger Family Members Safeguard Seniors from Online Fraud

Yue Deng
Department of Computer Science and Engineering
The Hong Kong University of Science and Technology
Hong Kong, China
ydengbi@connect.ust.hk

Changyang He*
Max Planck Institute for Security and Privacy
Bochum, Germany
changyang.he@mpi-sp.org

Yixin Zou
Max Planck Institute for Security and Privacy
Bochum, Germany
yixin.zou@mpi-sp.org

Bo Li
Department of Computer Science and Engineering
Hong Kong University of Science and Technology
HongKong, China
bli@cse.ust.hk

Abstract

Online fraud substantially harms individuals and seniors are disproportionately targeted. While family is crucial for seniors, little research has empirically examined how they protect seniors against fraud. To address this gap, we employed an inductive thematic analysis of 124 posts and 16,872 comments on RedNote (Xiaohongshu), exploring the family support ecosystem for senior-targeted online fraud in China. We develop a taxonomy of senior-targeted online fraud from a familial perspective, revealing younger members often spot frauds hard for seniors to detect, such as unusual charges. Younger family members fulfill multiple safeguarding roles, including preventative measures, fraud identification, fraud persuasion, loss recovery, and education. They also encounter numerous challenges, such as seniors' refusal of help and considerable mental and financial stress. Drawing on these, we develop a conceptual framework to characterize family support in senior-targeted fraud, and outline implications for researchers and practitioners to consider the broader stakeholder ecosystem and cultural aspects.

CCS Concepts

• **Human-centered computing → Human computer interaction (HCI)**.

Keywords

older adults, online fraud, family support, anti-fraud, RedNote

*Corresponding Author

1 Introduction

Online fraud is a highly prominent topic in the domains of Human-Computer Interaction (HCI) and Security and Privacy (S&P) [47, 65, 79, 83, 98, 99]. It is increasingly recognized as a critical global issue that impacts communities worldwide [11, 14, 20, 22, 28, 78]. The elderly might be disproportionately targeted and suffer more severe consequences when falling for online fraud, especially when they experience cognitive decline [43, 49], overly trust others [19, 59], are socially isolated [2, 57], or lack knowledge about fraud prevention [8, 30]. In China, 78% of seniors have received scam messages, with fake online shopping and investment being the common schemes, and between 20-30% seniors fall for the scam eventually [69].

To address this global threat, governments, organizations, and researchers worldwide have invested great efforts in safeguarding seniors from fraud. For instance, China enacted the Anti-Telecom and Online Fraud Law of the People's Republic of China to prevent, curb, and penalize online fraud activities in 2022 [72]. China's Ministry of Public Security launched the National Anti-Fraud Center (NAFC) mobile app to detect and report potential telecommunication fraud [104]. The US Federal Trade Commission (FTC) has dedicated advisory groups [22] and Age UK advocated for financial institutions to implement various nudges and frictions in their payment system to safeguard seniors from fraud [96].

Prior academic research has highlighted the significant role *family members* play in safeguarding seniors from fraud [31, 34], such as how family members are often the primary sources of cybersecurity information for the elderly [71]. However, existing studies related to senior-targeted fraud have primarily focused on seniors' perspectives, such as risks and threats faced by older adults [16, 53, 90] and their diverse needs [12, 77]. Little research has empirically and systematically investigated **how family members safeguard seniors from online fraud** in practice.

Focusing on only seniors' perspectives has a potential limitation: underreporting. Prior work has revealed many seniors were hesitant to disclose their experiences of fraud due to self-blame, concerns

about family reputation, and other factors [77, 97]. Additionally, some reports indicated that seniors might not fully grasp how their behaviors could make them vulnerable to fraud [73]. As such, family members can offer a fresh and supplementary perspective in understanding and combating senior-targeted fraud.

Moreover, little is known about what family supportive behaviors are taken in order to counter senior-targeted online fraud and what challenges family members face when assisting older adults. Investigating senior-targeted fraud through the lens of family members has the potential to shed light on the diverse scope and comprehensiveness of senior-targeted fraud, provide novel insights into the actual role of family support in anti-fraud efforts [67], and highlight the design, policy, and educational opportunities against senior-targeted fraud as a sociotechnical problem [87].

In China, the assistance provided by younger family members to the elderly is particularly important. Unlike Western cultures, Chinese society generally views younger family members' support for the elderly as an obligation and responsibility (i.e., filial piety) [107]. Family is usually the primary source of both financial and caregiving support for older adults in China, making family support crucial in the lives of Chinese seniors [109, 110]. By investigating the support ecosystem against senior-targeted online fraud in China from the lens of family members, we also illuminate the social-cultural aspects of fraud prevention and mitigation. Our research centers around the following questions:

- **RQ1**: What vulnerabilities and corresponding senior-targeted online fraud are disclosed by younger family members? **(seniors' vulnerabilities and fraud practice)**
- **RQ2**: What measures do younger family members take to counter senior-targeted online fraud? **(family support behaviors)**
- **RQ3**: What are the challenges when younger family members attempt to assist seniors? **(challenges in family support)**

To answer these questions, we conducted an inductive thematic analysis of 124 posts within 16,872 comments on RedNote (Xiaohongshu),[1] a popular social media platform in China, to explore family support against senior-targeted online fraud. Our findings highlighted how online fraud was crafted to target seniors' vulnerabilities in China, such as by exploiting *seniors' concerns about health and well-being* and *social relationships* (RQ1). Younger family members' supportive behaviors occur throughout the entire anti-fraud process, including *prevention*, *identification*, *persuasion*, *loss recovery* and *education* (RQ2). Nonetheless, younger family members also faced challenges in family support, such as *seniors guarding their information* and *refusal of help*, as well as the *enormous mental and financial stress* they experienced in helping seniors recover from the fraud (RQ3). We discussed our findings' implications and recommendations to counter senior-targeted fraud under the family support ecosystem.

Our work makes the following contributions to HCI.

- We unpack the family support ecosystem against senior-targeted online fraud in China, using the perspectives of younger family members as a novel lens, and show that

the support is a long-term and evolving process including various stakeholders.
- We reflect on how sociocultural factors in China shape the family support ecosystem, leading to tensions between financial autonomy and security for older adults.
- We demonstrate challenges for younger family members to support the elderly. These challenges inform recommendations of interventions to be deployed by platforms, education for older adults, and the support needed for younger family members themselves.

2 Related Work

2.1 Online Fraud and Anti-fraud

Online fraud is defined as "the experience of an individual who has responded through the use of the internet to a dishonest invitation, request, notification or offer by providing personal information or money that has led to a financial or non-financial loss or impact of some kind" by Cassandra Cross [29]. While there are multiple definitions of online fraud, a fundamental aspect is the use of the internet as a means to perpetrate fraudulent activities [52]. The World Economic Forum identifies cyber threats as one of the most significant global risks [38]. Researchers in HCI and S&P explored how to counter fraud from diverse stakeholders' perspectives, such as analyzing victims' experiences to uncover systemic vulnerabilities [47, 98], leveraging experts' insights to advance fraud detection strategies [79, 99], and evaluating the impact of cybersafety communiqué on older adults to develop more effective education solutions [65].

Fraud and anti-fraud efforts are deeply intertwined. A large body of existing works has examined fraud from the attackers' viewpoint by studying their psychological tactics [84], attack intentions [5], and fraudulent techniques [25]. For instance, Mouton et al. introduced a comprehensive framework for social engineering attacks [66]; building on this framework, Razaq et al. investigated the different schemes used by fraudsters [79]. These endeavors provided valuable insights into anti-fraud measures like fraud detection and prevention systems [1, 4, 55]. Additionally, other research has focused on the victims' perspective by investigating why individuals fall for scams [14] as well as their perceptions and experiences [45]. These findings demonstrated victims' anti-fraud strategies and inspired designs for educational and intervention programs [50, 111].

However, according to family systems theory [7], individuals often do not operate in isolation, as they share many material and emotional connections with family members. Moreover, many previous works highlighted the significance of family members in safeguarding seniors from fraud [33, 34]. As such, our research draws from the perspectives of younger family members to enrich the understanding of senior-targeted online fraud, rather than solely focusing on seniors themselves or fraudsters.

2.2 Online Fraud and Seniors

A related study highlighted that an average of 9.1% of adults aged 55 to 64, 7.3% of those between 65 and 74, and 6.5% of individuals over 75 fell prey to consumer fraud in the US [3]. There are numerous challenges in protecting the elderly against online fraud.

---

[1]https://www.xiaohongshu.com/explore

First, factors such as cognitive decline, an overly trusting nature, social isolation, and a lack of knowledge regarding fraud prevention can heighten seniors' vulnerability to online fraud [17, 18, 56, 60, 61, 87]. Second, there is a proliferation of scams specifically targeting older adults. The National Council on Aging in the US reported the top five financial scams aimed at older adults, such as government impersonation scams and grandparent scams [74]. Third, mainstream security mechanisms and application designs often do not adequately consider the needs and perspectives of older adults. For example, older adults might struggle with managing passwords [46], which may amplify potential senior-targeted fraud. Lastly, some older adults may exhibit lower proactive tendencies in avoiding fraud risks. Frik et al. indicated that older adults commonly employed passive strategies, such as limiting or avoiding technology use, while active mitigation strategies were less common [39]. However, Zou et al. found that the elderly applied some active strategies, such as configuring privacy and authentication settings, and selectively disclosing sensitive information [111].

Furthermore, the harm caused by senior-targeted fraud is profound. The most apparent impact is financial loss. Moreover, falling victim to fraud often leads to traumatic experiences with significant physical and mental health repercussions. Victims might suffer from major depression, generalized anxiety disorder, feelings of anger, shame, regret, and various somatic symptoms [13, 40]. The repercussions extend beyond seniors to their families, who may be equally affected by the financial and emotional consequences [6]. In essence, senior-targeted fraud is a pervasive, challenging to combat, and highly detrimental issue.

What makes anti-fraud efforts harder is the under-reporting among older scam victims. While the majority of scams go unreported [13], the reporting rate is even lower when it concerns older adults [76, 97]. Previous work has shown that senior victims were not willing to report crimes or seek assistance from their family or community due to a lack of accessible or sufficient emotional, educational, and technical support [77]. Consequently, it is highly likely that the actual incidence and prevalence of senior-targeted fraud extend far beyond the reported ones.

Prior research on senior-targeted fraud has largely focused on the seniors' perspectives through interviews [80, 85] and surveys [2, 51], etc. However, limited research is from the viewpoint of those close to seniors and aware of their online activities, i.e., *younger family members*, who may provide complementary insights. For example, for the under-reporting issue [77], the disclosures from family members may shed light on the diverse scope of senior-targeted fraud. Moreover, older and younger individuals exhibit different patterns in detecting lies and discerning trustworthy faces in offline contexts [19, 82], which could carry over to the online fraud context. Our work aims to address this gap by exploring the nuances of seniors' vulnerabilities, the various types and channels of fraud, and the tactics used by scammers through the lens of younger family members (RQ1).

2.3 Family Dynamics in Safeguarding Seniors from Fraud

Research on fraud against the elderly has increasingly underscored the significance of extending anti-fraud efforts from seniors to their family members [34, 77]. For example, DeLiema encouraged the involvement of family members in financial decision-making processes and the implementation of legal and financial safeguards to protect the assets of older adults [33]. Scammers also noticed the potentially protective role of family members in countering fraud, so they exploited social isolation to manipulate targets to hide information from family members [33]. In addition to the benefits that come with family involvement, there might be tensions and challenges during the support process. Younger family members might become overly paternalistic in their efforts to protect older adults, leading to what is known as "family surveillance" [68]. Moreover, Parti et al. demonstrated that in the realm of online fraud, US older adults were often hesitant to disclose their experiences of fraud to their family members due to self-blame, concerns about losing family status, particularly among younger family members, and trust issues [77].

The cultural, economic, and technological contexts in China have a profound influence on the family's role in anti-fraud efforts. The high regard for filial piety within Chinese society shapes the cultural norm that the younger generation should care for and protect their elders [107]. Additionally, traditional parenting and family relationships in Chinese families give parents an authoritative or authoritarian position [21]. This internal power structure within families might pose obstacles for the younger generation to intervene and prevent fraud. Economically, younger family members often offer financial care to parents within Chinese families [88, 109]. Unlike in the US, where government assistance such as Medicaid is available for elderly adults who have exhausted their funds for long-term care, in China, family members represent the last line of financial security [110]. In this context, the financial support and education provided by the younger family members are crucial for preventing senior-targeted fraud.

Prior research has examined family support in the context of older adults' technology use and finances, such as family's support in financial technology onboarding [93], family's account sharing for digital inclusion [44] and general online security and privacy support [68]. Our study extends this work by shedding light on family support in safeguarding seniors from online fraud. Existing research on senior-targeted fraud primarily focuses on the perspectives of the seniors themselves [53, 77], while sporadically mentioning the important role of family members, such as encouraging family members in assisting older adults with financial issues [33] or indicating that family members are one of the information sources of S&P news [31]. However, a systematic investigation of how younger family members engage in online fraud safeguarding remains underexplored. Moreover, family support in senior-targeted fraud within the non-Western context of China remains unknown. As such, our research aims to fill the research gap by examining the family support ecosystem. We explore younger family members' supportive behaviors (RQ2) and the challenges (RQ3) they face, as well as provide implication insights for better mitigating senior-targeted online fraud.

3 Method

To systematically understand how younger family members safeguarded seniors from fraud, we collected discussions related to

seniors' online fraud on social media and conducted thematic analysis [9] to discover meaningful patterns about online fraud targeted seniors perceived by younger family members (RQ1), their support behaviors (RQ2), and challenges (RQ3). The overall analytical flow is shown in Figure 1.

3.1 Data Source

We chose social media platforms as our data source, where younger family members shared their experiences about senior-targeted fraud. This method provides the following advantages: (1) Discussions there occurred in a natural setting, unlike in interviews or surveys where responses might be influenced by social desirability bias and the Hawthorne effect [64]. (2) Social media platforms provide access to extensive data, which addresses the limitations of small sample sizes that are typical in qualitative studies. (3) The interactive features on social media (e.g., comments, likes, and shares) can foster ongoing discussions that yield deeper insights.

We focused on discussions related to senior-targeted online fraud on RedNote (Xiaohongshu). RedNote, often referred to as the Chinese Instagram, is a Chinese life-sharing platform [103]. Users of RedNote often share personal life experiences and opinions through text, photos, and videos, which aligns with our everyday context of senior-targeted online fraud. By 2020, RedNote had over 450 million registered users, and more than 121 million monthly active users [91, 92]. Many prior work has explored user-generated content on experience sharing on RedNote [15, 35, 94]. We also looked through the related content on other popular social media platforms in China such as Weibo [102] and WeChat [100], but content about senior-targeted online fraud on these platforms tends to be more focused on news and official advice rather than personal stories. RedNote, similar to Instagram, has a threaded discussion structure where each initial post is followed by a series of subsequent comments over time. This structure allows for the observation of discourse and interaction dynamics among users. A screenshot of RedNote's interface is shown in Figure 2.

3.2 Data Collection

Before collecting data, we studied the search mechanism of RedNote. We discovered that searching a keyword does not only bring up content containing that exact keyword but also surfaces content related to the keyword, suggesting that RedNote's search algorithm returns posts based on contextual similarity rather than specific queried words. For our study, the population featured was seniors, our context was online environments, and our focus was fraud. Therefore, we set our search keywords to "seniors" AND "online" AND "fraud" to gather content pertinent to our research topic. We employed data crawling assisted by MediaCrawler tool based on these keywords [81]. The search also yielded posts associated with "parents," "grandparents," "mobile," "internet" and other words related to our keywords, which ensured the richness of our data.

Furthermore, RedNote has a personalized content recommendation algorithm that tracks users' interactions, such as clicks, viewing time, and likes, to tailor content recommendations [86, 105]. Therefore, to mitigate the influence of previous usage records on our data collection, we created unused accounts for crawling data, a common practice recommended in previous research on crawling

social media data [41, 70]. When creating new accounts on RedNote, the selection of gender and age could also impact the recommended content. To ensure a diverse data collection, we established eight different accounts, corresponding to male and female users aged 21, 30, 40, and 52 years. These ages were based on median values derived from the age distribution of RedNote's adult user profile [32]. We did not select older age for user accounts, considering the possibility of older members being victims themselves, which may introduce noise to the dataset. We adopted the default search sort of RedNote and collected all types of data including texts, videos, and images. Each search returned around 200 posts. The limited size of search results on RedNote prevented us from creating a comprehensive dataset. Nonetheless, the search mechanism of RedNote based on contextual similarity and our collection strategies with diversified identities ensured the representativeness and randomness of collected data. Ultimately, we completed our data collection in January 2024, and we retrieved 2,288 posts with 393,197 comments.

3.3 Data Processing

After removing duplicated cases, we had a collection of 747 posts with 148,614 comments. However, the dataset, even after deduplication, still contained some unrelated entries, such as anti-fraud advertisements, public awareness campaigns, and personal stories of being scammed.

To filter out these irrelevant contents, the first and second authors independently coded all the posts with the inclusion criteria that focused on data related to younger family members disclosing experiences of seniors being deceived. The two coders reached high inter-rater reliability (Cohen's kappa=0.91). Following this, the two coders engaged in discussions to resolve any discrepancies and reach a consensus on all the annotations. After the filtering process, our final dataset contained 124 posts with 16,872 comments ranging from May 2020 to January 2024 [54, 58], specifically related to the disclosures by younger family members about the online fraud experiences of seniors. We also collected user profiles for each user, including user ID, gender, IP locations, and age. These posts were created by 124 unique users and comments were created by 12,383 unique users. The users' IP locations covered all provinces in China. The median age was 26 and the average age was 28, with the 25th percentile at 22 and the 75th percentile at 32.[2]

3.4 Data Analysis

We applied inductive thematic analysis [9], a qualitative method that entails searching across a dataset to identify, examine, and report repeated patterns, to thoroughly explore three research questions focusing on seniors' vulnerabilities and online fraud practices (RQ1), the supportive behaviors of younger family members (RQ2), and their challenges (RQ3). Initially, two authors independently performed open coding [26] on a random sample of 50 posts and their comments to generate preliminary codes (e.g., *the elderly did not tell the scammed amount*" and *"arguments with seniors"* related

---

[2]We found only 3,161 users (25.47%) disclosed their ages, and some reported unrealistic ages such as 2023 years old. After removing such outliers, we got the statistical data of ages. But note that our data analysis was based on the content of the posts and comments rather than on age, and the ages listed in profiles might be fabricated [63]. Therefore, these ages should not be considered as accurate representations of users' actual ages but rather as reference data, which we have acknowledged in limitations.
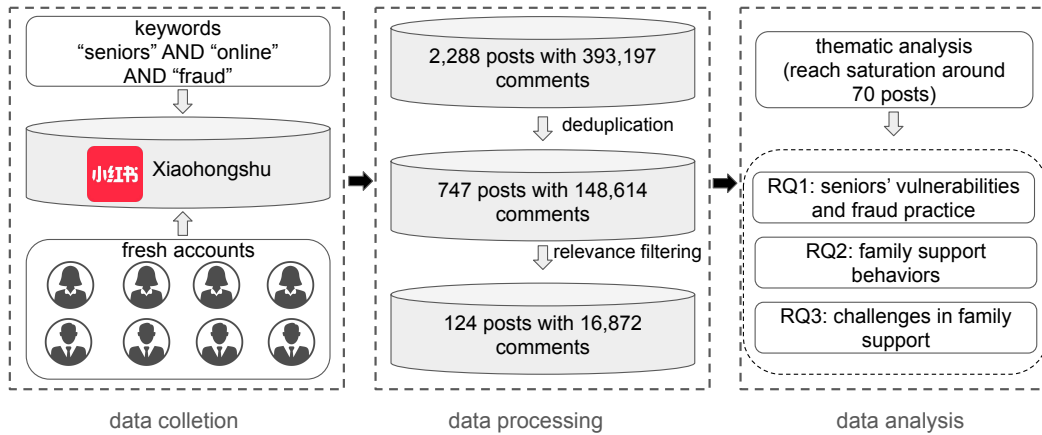
Figure 1: The analytical flow to understand younger family members' safeguarding against senior-targeted fraud.
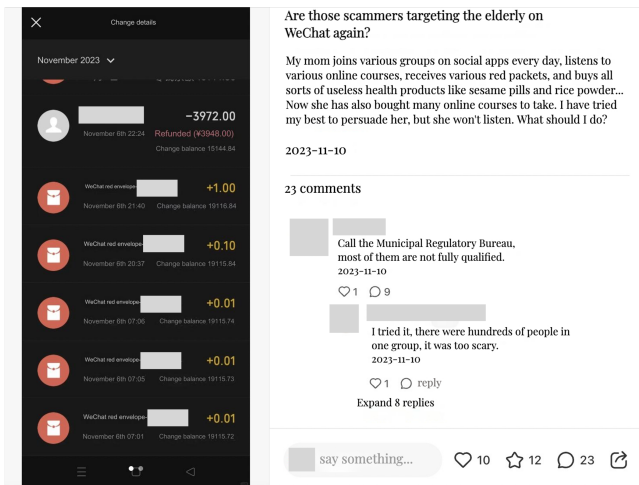

Figure 2: An interface example of RedNote (translated from Chinese).

to RQ3 about challenges). This stage directly reflected insights derived from the data. Subsequently, we discussed and reconciled our codes to ensure a unified understanding and constructed a codebook. Then we evaluated our codebook by applying it to additional posts and comments and documenting newly merged codes. We repeated the process, where we revisited and refined our codebook in weekly meetings. This iterative coding process continued until saturation was reached when approximately 70 posts with more than 12,000 comments were coded. Then axial coding [26] was employed to identify connections between these codes, fostering the development of broader themes. For example, the codes *"the elderly did not tell the scammed amount"* and *"younger family members did not know the fraud"* were linked under a broader theme of *"guarding information."* This thematic connection indicated a behavior pattern among seniors regarding their experiences with fraud.

3.5 Ethics Statement

Our study received approval from our Institutional Review Board (IRB). When collecting and analyzing users' public data for research purposes, it's still essential to carefully consider the potential risks, benefits, and harm involved [36]. We believe this research provides significant benefits by highlighting seniors' vulnerabilities to fraud and fraud practice, exploring family support behaviors, and identifying challenges in providing support. Our intention is not to expose individual fraud experiences or single supportive behavior and challenge but to uncover broader patterns in collective online behaviors. To minimize the risk of linking quotations back to specific users, we implemented several measures. First, we removed all usernames when presenting data. Second, all quotes were translated from Chinese to English using Google Translate and then paraphrased to further reduce searchability. The final translations were reviewed and refined by the first author to ensure accuracy. Moreover, collecting data from the perspective of younger family members on social media avoids direct contact with seniors and their families, thereby preventing the ethical concerns of retraumatizing them by recounting distressing experiences [23, 24].

4 Findings

Our findings contribute a rich understanding of how younger family members safeguard seniors from online fraud. We first report on seniors' vulnerabilities and corresponding senior-targeted online fraud disclosed by younger family members in §4.1 (RQ1). We then demonstrate the supportive behaviors of younger family members in §4.2 (RQ2). We finally reveal the challenges faced by younger family members during their assistance process in §4.3 (RQ3).

4.1 RQ1: Senior-Targeted Online Fraud

Our work added more nuances to prior research that systematically examined online senior-targeted fraud, including the vulnerabilities targeted, fraud types, fraud channels, and fraudsters' strategies. Our findings were drawn from the perspectives of younger individuals, but this did not imply that their viewpoints were definitive. Previous work also indicated perceptual differences between seniors and

young regarding lies and trust [19, 82]. Instead, the perspectives of younger individuals provide a new lens for understanding the complex nature of elderly fraud. The complete taxonomy is shown in Table 1.

Vulnerabilities of seniors. We identified various types of fraud and how they target seniors' vulnerabilities. Seniors' **concerns for health and well-being** made them easy targets for online frauds involving *false advertising of health products*, *purchases of fraudulent health and lifestyle courses*, and *purchases based on superstition*. Additionally, seniors' **financial expectations** might lead them to fall prey to *investment fraud*, *false advertising of collectibles*, and *purchases of fraudulent money-making courses*. **Overreliance on authority** could be exploited by scammers *impersonating authorities*. Furthermore, **social isolation** might open doors for *romance fraud*, and **caring about the younger generations** could sometimes be manipulated by *family member impersonation fraud*. Moreover, **low digital literacy** potentially hindered seniors from recognizing signs of fraud. For instance, seniors might *not notice charges deducted from their bank accounts*. Some seniors working as street vendors could also be deceived by *fake payments* when they were told the money had been paid, but it was not. Each of these vulnerabilities contributed to the risk profile of seniors and put them in a dire situation when online fraudsters also use sophisticated channels and strategies.

Unrecognized fraud schemes among seniors. By examining online fraud from the perspectives of younger family members, our research revealed some frauds that seniors might overlook, demonstrating the critical role of intergenerational insights in protecting seniors from online fraud. For instance, seniors were often enticed by the fabricated but compelling stories presented in live-streaming, which led them to believe in the high value of collectibles. As a younger family member pointed out,

> *"My elderly family members got hooked on live-streams and spent a lot of money buying a bunch of so-called antiques, paintings, gold jewelry … We even took these items to museums for expert appraisal, only to find out that they were all fake. But they still have unwavering trust in the live-stream host."*

Another example was *unnoticed charges*. These often remained overlooked until younger family members noticed unusual charges on the seniors' bills. Some online short videos or novels require payment to continue viewing after an initial free portion. Seniors, sometimes due to low digital literacy or password-free payment settings, would inadvertently make money transfers while engaging with these platforms, not fully realizing the financial commitments involved. As one younger family member explained,

> *"My dad was maliciously deducted a lot of money from reading novels before, 100 yuan at a time. I asked my dad and he said that all the novels he reads were free, and he did not know about the deductions."*

Diversity of fraud channels and exploitation of social relationships. Fraudsters used various channels to target seniors. Some channels were straightforward, such as *purchase links in live-streaming* and *fraudulent QR codes* to be scanned in physical electronic payments. Other tactics were more deceptive and harder to notice, such as *fake pop-up ads* designed to trick users

into making unwanted purchases. Particularly, *the exploitation of social relationships on social apps* served as a breeding ground for numerous fraud types. In one case about *fraudulent money-making courses*, a younger family member found that a salesperson added her mother on WeChat (a popular social app in China) to trick her mother into purchasing courses.

> *"I discovered my mom was tricked into buying courses worth thousands of yuan. The salesperson who added her on WeChat kept promising that people in their 60s could earn a thousand yuan a day. He constantly pretended to care and showered my mom with attention."*

Additionally, scammers even utilized the calling feature in social apps to establish stronger connections with the elderly. Another young person shared, *"The teacher called my dad on WeChat every day to ask him to attend class."*

Common strategies used by fraudsters. Although the vulnerabilities and types of fraud varied, there were common strategies employed by scammers. For example, the strategy of *offering rewards for referrals* was utilized in three kinds of fraud types. Furthermore, for *false advertising of health products* and *fraudulent health and lifestyle courses*, scammers often sent small amounts of money in *red packets* on social apps to increase the engagement of elderly individuals. *Red packets* on social apps were based on the Chinese tradition of lucky money, where money could be given to others as a gift [101]. These strategies worked out well when the seniors targeted were too trusting or had a strong desire for small gains. Furthermore, scammers sometimes crafted their strategies to exploit seniors' vulnerabilities specifically. For seniors with an *overreliance on authority*, scammers *posed as officials offering help*. Exploiting *seniors' care for the younger generations*, fraudsters might impersonate younger family members to request money.

4.2 RQ2: Supportive Behaviors

In the section, we show the family support behaviors from the aspects of *prevention* (§4.2.1), *identification* (§4.2.2), *persuasion* (§4.2.3), *loss recovery* (§4.2.4), and *education* (§4.2.5).

4.2.1 Prevention: The Involvement of Controlling Behaviors. To safeguard seniors from online fraud, younger family members used a diverse set of preventive measures. These included *restricting online payments*, *managing tasks for seniors*, *monitoring*, *selective blocking* and *setting up anti-fraud defenses*. The common theme was that younger individuals tried to control seniors' online activities to mitigate the risk of fraud.

Online payment restriction. Some younger family members restricted online payment of seniors, such as restricting online spending and not allowing seniors to link their bank cards to mobile phones. As a younger family member explained, *"We do not allow them to link cards to mobile phones and only give them cash."*

Managing tasks for seniors. Younger family members would take on the responsibility of performing online tasks on behalf of the seniors, such as registering online accounts and doing online shopping. A daughter said,

> *"My mom always asks me to teach her how to link her bank card for payments, but I refuse and tell her to let me know what she needs and I'll purchase it for her."*

Table 1: Vulnerabilities and online senior-targeted fraud disclosed by younger family members. "Fraud Channel" refers to the crucial steps for money outflow, while "Fraud Strategy" denotes the tactics employed by fraudsters. * means there are other types of fraud utilizing the same fraud channel or strategy.

Vulnerability	Fraud Type	Fraud Channel	Fraud Strategy
health and well-being concern	false advertising of health products	C1*: transactions built through social relationships on social apps[3]	S1*: offering rewards for referrals
			S2*: leveraging expert endorsements for promotion
			S3*: sending red packets on social app
		C2*: live-streaming purchase links	S4*: creating benefit illusion (free gifts/insider price)
			S5: amplifying seniors' guilt
	purchase induction of fraudulent health and lifestyle courses	C1*: transactions built through social relationships on social apps	S2*: leveraging expert endorsements for promotion
			S3*: sending red packets on social app
			S4*: creating benefit illusion (free trial/insider price)
		C2*: live-streaming purchase links	S6: affirming seniors
			S7: disparaging medicine for self-promotion
	purchase induction based on superstition	C3: live-streaming virtual gifts	S8: blessing for families
financial expectation	investment	C4: investment app/website	S1*: offering rewards for referrals
			S2*: leveraging expert endorsements for promotion
		C1*: transactions built through social relationships on social apps	S9*: luring with high profits
			S10: pretending to be helpless
			S11: disguise the project as national
	false advertising of collectibles	C2*: live-streaming purchase links	S12: highlighting collectible value
			S13: presenting compelling stories
	purchase induction of fraudulent money-making courses	C1*: transactions built through social relationships on social apps	S1*: offering rewards for referrals
		C2*: live-streaming purchase links	S9*: luring with high profits
overreliance on authority	authority impersonation	C5: transactions instructed through video calls	S14: pretending to be authorities to offer assistance
			S15: educating fraud knowledge to decrease suspicion
social isolation	romance	C1*: transactions built through social relationships on social apps	S16: exploiting intimacy to deceive for money or information
generational affection	family member impersonation	C1*: transactions built through social relationships on social apps	S17: pretending to be family members in urgent need of money
low digital literacy	unnoticed charges	C6: password-free payment	S18: exploiting unintentional enrollment to deduct money
		C7: auto-renewal service subscription	
		C8: pop-up ads with fake/transparent close buttons	S19: popping up red packets to induce clicks
		C9: fake red packets redirecting to payment pages	
	fake payment	C10: fraudulent QR code scanning	S20: falsely claiming to have paid

Monitoring. Another strategy employed by younger family members is to monitor seniors' online activities and be prepared to eliminate any risks as soon as they detect anomalies. As one younger family member recalled,

> *"I directly logged into my dad's Kuaishou account (a live-streaming platform). When I saw something strange, I immediately refunded items without waiting for delivery."*

Selective blocking. Some younger individuals employed technical methods to limit seniors' access to specific applications. For example, one person provided suggestions on how to block certain applications, *"Hey guys, you can log in to the router and block access to TikTok and TikTok live-streaming in our home. You can find the domain names online for reference."*

Setting up anti-fraud defenses. Some younger family members might assist the elderly in setting up patterns on mobile phones or

downloading anti-fraud applications. A younger individual told her setting, *"Set the seniors' phones to reject calls from unknown numbers. Disable features that allow strangers to like, follow, or send private messages."*

Most of these preventative measures involved controlling behaviors. While these approaches might enhance online security for seniors, they also introduced issues, such as conflicts between seniors' autonomy and the control exercised by younger family members, as we elaborated in §4.3.1.

4.2.2 Identification: A Three-Phase Process. An essential component of younger family members' efforts to protect seniors was to suspect and confirm incidents of fraud. This identification typically unfolded in a three-stage process, including *initial contacts*, *collecting evidence*, and *making the judgment*.

Stage I: initial contacts. This meant the stage where younger individuals first became aware of the scam, which might be different from when the elderly person first encountered it. For example, seniors might invite their children to participate in some supposedly profitable activities, and it was during this participation that the younger individuals recognized the fraudulent nature of these activities. This corresponded to fraud strategies like *S4: offering rewards for referrals* in Table 1, i.e., when fraudsters claim that seniors could receive red packets for adding more people to a group on social apps. Additionally, younger individuals sometimes caught a clue when seniors asked for help with their financial accounts. One young person mentioned,

> *"My mom asked me to look at her WeChat account because she thought there was something wrong. When I checked, I found out she signed up for an online course that cost 2900 yuan."*

There were also instances where potential risks were identified through prevention behaviors like *monitoring*, allowing younger family members to intervene and prevent further development of the scam.

Stage II: collecting evidence. In this phase, younger people used multiple approaches to gather concrete evidence. Some would use their wisdom to obtain information. For instance, they initially affirmed their parents and encouraged them to share more details, as some parents might hesitate to discuss their situations with their children due to a fear of criticism or a desire to save face. One child said, *"My dad really cares about his reputation and would never admit he's been scammed. To get to the bottom of it, I started by affirming him positively. Then he sent me his TikTok account and the links to the classes he's been taking."*

In other cases, younger people even joined the group on social apps created by fraudsters to gather firsthand information about the ongoing scams. For example, a young person suggested to other young people, *"If the elderly ask us to join the group again, we must be proactive and report it to prevent seniors from getting deeper and deeper."* Except for taking evidence by strategy, some utilized a direct approach, such as examining their parents' financial footprints by checking their payment histories on mobile devices.

Stage III: make the judgment. After collecting evidence, family members might synthesize the evidence to make a judgment. They usually evaluated the legitimacy of the business model, identified obvious misinformation, and compared costs with standard market prices. However, sometimes they were not certain whether a case was a scam, so they would turn to the internet to validate their suspicions. Social media platforms provided a useful venue where younger individuals could inquire if others thought it was a scam and obtain detailed information such as similar fraud experiences, the specific amounts lost, and the names of fraudulent organizations.

4.2.3 Persuasion: Younger Family Members Rack Their Brains to Convince Seniors. To convince seniors about the dangers of ongoing scams, younger family members developed a set of persuasive strategies. These efforts were crucial in addressing the often stubborn disbelief among seniors who might not easily accept that they were being scammed. By *presenting direct evidence* and *involving third parties*, younger individuals worked diligently to protect their elderly family members from further exploitation.

Presenting the direct evidence. To persuade the elderly about ongoing scams, younger family members developed a set of approaches. Typically, they *provided evidence or shared similar cases of fraud* to demonstrate to the seniors that what they were experiencing was indeed a scam. For example, one daughter recounted,

> *"I exposed the truth to my mom tonight. The financial company she invested in has been revoked, but she still believes it. I'm really at my wit's end."*

Involving third parties. Despite their efforts, seniors often remained in denial, insisting they were not deceived. In such cases, younger people resorted to *involve other stakeholders for the persuation*, such as other family members, the police, and broader communities on social media. For instance, a young person leveraged the "@" feature to mention seniors in social media posts so that other users could help to persuade this older person,

> *User1: @ [one older person], please take a look at this.*
> *User2: "Auntie, please don't fall for those smooth talkers. My grandparents are fully convinced that the scammers are looking out for them, and now they think the rest of us are the enemies. It's giving me daily headaches and insomnia."*

When it comes to communication styles used for persuasion, some tried to understand, resonate, and discuss how to avoid fraud with seniors. Others directly scolded the elderly or even threatened to call the police to prevent them from falling into fraud, especially when more gentle methods failed. While some persuasion efforts successfully protected seniors from further scams, these also had many negative results. Seniors might respond by *guarding information* or *refusal of help and intervention*, and persuasion might also contribute to strained family relationships, which we elaborate in §4.3.

4.2.4 Loss Recovery: Dual Burden of Financial Assistance and Emotional Care. We observed that younger family members frequently engaged in two key types of support: *financial assistance* and *emotional care*. This dual approach encompassed both tangible financial interventions to recuperate losses and strategies to support the emotional and psychological well-being of their affected loved ones.

Financial assistance. *Helping seniors repay their debts* was a common form of support. For instance, one child shared,

"I'm planning to transfer 30,000 yuan to my mom to cover half of her losses. It hurts to see her suffer, and it's equally painful to part with my money."

Another approach was to *help seniors reclaim money lost*. This included filing complaints and reporting fraudulent activities to relevant authorities, as well as processing refunds and returns on behalf of the elderly.

Emotional care. In addition to *financial assistance*, younger family members also took on the role of soothing the emotions of the elderly. They often *provided more companionship*, as one younger family member mentioned, *"I comfort her every day . . . We talk things through, and it helps her let off some steam."*

Moreover, some young people suggested using *white lies* to alleviate the emotional burden on the elderly, e.g., *"How about just tell mom we've gotten the money back? Maybe get a friend to put on a little show for her. After all, we can always make the money back."*

4.2.5 Education: Active Involvement in Fraud Education. We found that fraud education provided by younger family members to seniors involves *raising awareness of specific fraud schemes*, *informing general attitudes* needed to protect oneself against fraud, and *providing practical advice*. This education spanned the entire fraud process, including before, during, and after the fraud occurred.

Raise awareness. Younger family members hoped to educate their parents or grandparents to raise their awareness of fraud prevention. In addition to *basic finance knowledge*, they also shared knowledge about *specific instances of fraud* with seniors, often by forwarding fraud cases on social apps or mentioning recent fraud examples. The younger generation themselves also deepened their understanding of fraud when paying attention to these cases. One person commented, *"This is the first time I've heard about this type of fraud. I will quickly inform my parents. Thank you for sharing."*

An interesting approach to raising awareness involves *simulating fraudsters* to alert seniors to potential fraud. For example, a daughter tested her father,

"I directly messaged them on WeChat, saying, 'Dad, lend me some money,' and my father didn't ask any questions and transferred the money."

Inform general attitudes. Younger individuals also informed seniors about the general attitudes to keep in mind against fraud, such as the *importance of always communicating with the younger generation before decision making*. Moreover, they educated seniors to *establish a value system against greed*, emphasizing principles such as *"there is no such thing as a free lunch"* and *"there is no such thing as a risk-free investment."*

Provide practical advice. The younger generation engaged in practical instructions as well, such as teaching their parents about *how to resist or ignore scammers* in certain situations. As a young individual shared, *"I make it clear to my parents that no matter who calls and asks them to perform any actions related to their bank cards, they should ignore them completely. Especially when they receive messages requiring them to reply for subscriptions or click on websites for information, they should disregard them entirely."*

4.3 RQ3: Challenges in Providing Support

From §4.2, we observed younger individuals implemented various supportive measures to safeguard seniors from fraud. However, they also encountered various challenges during the assistance process. First, there was resistance from seniors towards the help provided by younger family members as seniors *guard their information* and *refuse to get help*, as shown in §4.3.1 and §4.3.2. Second, §4.3.3 describes *dark patterns in online payment systems*, which potentially exacerbated the likelihood of seniors falling victim to scams. Furthermore, §4.3.4 demonstrates *a lack of consumer protection* when younger people advocate for seniors' losses. Finally, §4.3.5 documents the *mental and financial stress as well as strained family relationships* experienced by younger family members.

4.3.1 Guarding Information. Although younger family members made lots of efforts to assist seniors from fraud, we found that the elderly did not always accept their help and resisted in their own ways, echoing existing studies [77]. In this section, we described the practice of *guarding information* among seniors. The phenomenon of seniors holding back critical fraud-related information with younger family members permeated various supportive behaviors.

Seniors might prevent young people from accessing suspicious information from the *initial contact phase*. For example, one young person shared,

"From the time she signed up for the courses until now, I had no idea. She didn't talk about it, not just with me, but also didn't mention it to my dad or anyone else, until I came home for winter break and checked her phone."

Furthermore, even when younger individuals noticed something unusual, they often encountered resistance from the elderly during the *evidence collection phase*. One person recounted,

"My mom started following some I Ching courses and secretly paid a lot of money, not telling any of us. When I asked her, she was as reluctant . . . to tell me anything. She wouldn't say how much she spent or what exactly she learned. When pressed further, she would just dismiss it with 'Oh, it's not what you think.'"

When younger family members sought to persuade seniors about the fraud's existence, some seniors might deceitfully reassure their children that they understood the warnings and would not fall for scams again, only to secretly maintain contact with scammers. One child expressed profound regret,

"I sent countless messages and made phone calls, warning her she'd been scammed and needed to stop the loss in time. But she never told the truth, while claiming that she understood and I had let my guard down. Now, looking back, I should stayed home and watched over her. I deeply regret it."

Moreover, our findings in §4.2.3 about persuasive behaviors highlighted that some younger people opted for an intense communication style, like scolding. This might lead to parents withholding information after being scolded, potentially increasing the risk of being deceived multiple times. For example, one person shared, *"After my mother was scammed for over 10,000 yuan, I scolded her, and now she keeps everything hidden from us."*

Young people also speculated potential reasons for seniors' guarding of information. The first might be a fear of being blamed. Many elderly were afraid of being reprimanded, leading them to withhold information about scams. A granddaughter revealed, *"My grandmother didn't dare tell anyone at home and only told me when I came home for a vacation after she lost several hundred."* Some elderly individuals might lie about the amount they were scammed to avoid criticism, e.g., *"My mother-in-law had actually invested over 20,000 yuan but lied to us that she only put in 1,000 yuan."*

Another reason could be seniors' regard of their own superiority. Some seniors believed they were more knowledgeable or experienced than their children and completely disregarded their advice. One child expressed, *"They always say that they have lived more years than us, so they know better. They are not willing to listen to you because they think you lack experience."*

Lastly, manipulations by scammers might also play a role in seniors' guarding of information. Scammers preemptively instructed elderly individuals not to discuss their activities with their children, brainwashing them to trust only themselves. One younger individual shared, *"After telling my mother that she was being deceived, she responded, 'my teacher said not to tell the children and to believe in my own efforts!'"* Seniors' guarding of information might also explain why some younger family members resorted to more forceful measures, such as *monitoring* in §4.2.1, to prevent online fraud among the elderly.

4.3.2   Refusal of Help and Interventions. In addition to *guarding information*, seniors rejected their children's interventions in various ways. Psychologically, they expressed *distrust* by believing scammers over their own family. Behaviorally, they *grilt-tripped* younger family members using the concept of filial piety. Cognitively, there was also *a conflict between seniors' autonomy and younger family members' desire to control*, as seniors sought to maintain independence and make their own decisions.

Distrust. Seniors often firmly believed the words of scammers while distrusting their own family members and even official institutions such as hospitals and the police. For instance, one individual shared,

> *"My mom spent 50,000 on a mattress advertised by a known scam reported in the news. No matter how much we tried to convince her, she chose to trust the scam over her own children. She didn't even consider a visit to the hospital, insisting on trusting these deceivers over established science."*

Additionally, we found that elderly people would protect scammers in front of the police. For example, a daughter was extremely helpless when her mother lied to the police,

> *"After confronting her, she still wanted to invest more. I asked the police to intervene, but she told them she hadn't made any transfers, still firmly believing in the scam. The police told me they couldn't help if she didn't admit to being a victim."*

When the seniors themselves were not aware of the scam, seeking redress became an even more difficult task. Moreover, seniors might also suspect that their family members tried to seize their assets, leading to significant frustration and disappointment among younger family members who feel disinclined to intervene further. A younger person said,

> *"All my grandfather's money went to a high-risk company. When I asked him to reclaim it, he thought I was trying to take his money. He'd rather trust an obvious scam than his own granddaughter. I've given up now, and he might as well end up begging once he realizes he's been scammed."*

Seniors' distrust could originate from real concerns, as financial exploitation by family members is a common type of fraud encountered by the elderly [33]. Furthermore, seniors would demean their family members and doubt their capabilities, as one individual shared, *"My mom thinks I have no right to criticize her because she believes I wouldn't know any better either. Our conversation tonight ended unpleasantly, and it really made me cry."* This behavior not only facilitated the scam but also severely damaged family relationships, a point we elaborated in §4.3.4.

Guilt trip. To "assist" scammers in deceiving themselves, seniors would impose moral pressure on their children, frequently invoking the concept of *filial piety*, which is profound in Chinese culture [48]. Being accused of unfilial behavior carried a significant social stigma and moral burden in China, as filial piety was not merely a personal virtue but a pivotal societal expectation [75]. This cultural value could strongly influence younger family members, who might feel compelled to comply with their elders' wishes. For instance, one child expressed their dilemma,

> *"It's incredibly real. Whenever you try to convince them with logic and facts, they hit you with accusations of being unfilial or remind you of all the money they spent raising you to manipulate you with guilt. It's truly infuriating."*

Beyond such moral manipulation, seniors also tried to evoke their children's empathy, as one individual shared, *"My dad says that buying those fake ceramics is his heartfelt wish in his old age, and he enjoys it using his own money, should I really stop him? He spends thousands from his salary every month anyway."* This behavior undoubtedly placed children in a difficult position, thereby softening their stance against intervening in scams.

Moreover, children would compromise to maintain family harmony and ensure their parents' happiness, despite their better judgment, as in the following example:

> *"My mom told me she wanted to buy something today, so I did some research and found there's no scientific basis for it. But to avoid any arguments, I went along with her decision. After all, she's unhappy if she doesn't buy it. I just told her not to use it every day and treated it like an occasional health supplement."*

Conflicts between seniors' autonomy and younger family members' control. Some elderly individuals had a strong sense of ownership and autonomy over their own affairs. When younger family members provided supportive behaviors, the elderly might feel that their independence was being challenged. For example, a young person said that her dad did not allow her to delete anything from his devices: *"It's already great that your parents let you help*

uninstall things. My dad's attitude is very hostile, he doesn't permit me to delete anything."

Furthermore, this sense of autonomy also drove the elderly to refuse younger people's attempts at fraud intervention, using phrases such as *"It's my money, you don't get to manage it. I'm willing to be scammed."* When seniors exhibited strong independence, younger individuals might choose to reduce their control to avoid potential arguments. As one younger individual shared, *"She's fiercer than anyone. 'Am I spending your money? Why do you care!' So, I just don't dare to speak up anymore."*

4.3.3 Dark Patterns in Online Payment Systems. Although some spending by seniors appeared minor and legally permissible, specific features in online payment systems could facilitate dark patterns. Many mechanisms made payments especially easy, such as password-free payments and "buy now, pay later" options. One young person mentioned,

> *"Many elderly people are induced to enable password-free payments. Orders under 100 yuan don't even show a payment page, and it just places the order directly. Unscrupulous merchants deliberately price items at 99 yuan to skirt the rules."*

Moreover, important information was often minimized or hidden in a way that made it difficult to notice, as one young individual commented, *"The option to enable password-free payments is in fine print, which the elderly can hardly see."* Platforms also facilitated seamless transitions from one app to the other. One younger person described the experience,

> *"Typically, seniors are lured by short videos on platforms like Douyin. It gets cut off at the key moment, and then it jumps to the WeChat payment page. Although watching is free, the rest of the content requires a paid subscription. Elderly people end up paying without realizing it."*

For seniors with low digital literacy, the issue was more severe. This situation raised the question of whether these overly convenient payment methods were genuinely user-friendly or cleverly designed traps. Indeed, young individuals shared their observation that some businesses were exploiting the low digital literacy of the elderly. One person commented,

> *"It's infuriating to see posts about merchants heartlessly exploiting the elderly, who are unfamiliar with online shopping. They display prices like 9.9 yuan, but the payment page shows 99 yuan. Many don't even realize how much they've spent, and if they do find out, they don't know how to seek redress."*

In addition, closing ads could be a challenge with invisible or fake close buttons designed to force accidental purchases. One individual described such features, *"As soon as you open the page, the first thing that appears is an ad with an almost invisible close button in the top right corner, which many older people can't see and end up inadvertently making payments."*

Red packets, traditionally given as monetary gifts during special occasions, have evolved into online formats like WeChat Red Packets [106]. However, these digital adaptations have also been commonly abused as a fraud strategy. These cultural tokens are manipulated through various digital forms, such as *fake and click-baiting red packets* that redirect the user to payment pages, causing older individuals to mistake fraudulent schemes for legitimate online transactions. For example, one young person recounted, *"My mom was just watching a video and suddenly paid for a membership through a red packet link. Older people think it's like the red packets we send on WeChat, so they just click and end up paying unexpectedly."*

4.3.4 Limited Consumer Protections. §4.2.4 showed how some younger individuals took on the responsibility of recovering losses for the elderly. In this process, they encountered multiple challenges in helping the seniors protect their rights.

Lack of knowledge of reporting channels. Many young people did not know how to seek redress for unconscious consumption. A common trend observed in our dataset was young people sought help through social media, either by posting for advice or commenting on similar cases for guidance. For instance,

> **Post (Help seeking):** *"My mom is not very good at using a mobile phone. I just discovered that there were inexplicable deductions last month. I can't find the public account or anything that the deductions were made to, and the records show no information . . . I checked her identity information and there was no theft or unauthorized subscriptions, so I don't know if I can get this money back."*
>
> • **Comment1 (Solution):** *"I just went through almost the same thing. Just file complaints with each service; most will refund directly, some might ask you to contact customer service via WeChat and provide order numbers."*
> • **Comment2 (Help seeking):** *"Just discovered my elderly family member also had mysterious deductions by [merchant name] while watching a series. No idea how to get a refund, what do I do?"*
> • **Comment3 (Update from post author):** *"Thanks for the help, everyone. I've filed complaints on all transactions via WeChat Pay, waiting for further updates."*

Whether in posts or comments, many young people did not know the specific steps to seek redress. Social media partly filled the knowledge gap as it enabled younger family members to collectively brainstorm and find appropriate redress channels, as well as share progress and solutions.

Difficulties in seeking redress. Even when young people knew possible avenues to lodge complaints, they often faced hurdles such as unresponsive customer service or false contact details. One young person vented,

> *"Aside from recovering less than a quarter of the amount yesterday, other complaints are either ignored, or they provide fake numbers and fake WeChat customer service accounts that can't be searched, or they just say the service has been used and tell off the complainers.".*

4.3.5 Enormous Mental and Financial Stress. The supportive behaviors described in §4.2 suggested that such assistance required young people to invest significant time and effort. These processes

created a dual burden of external and internal pressures for the younger generation.

External pressures include shouldering the family's financial losses and preventing the elderly from being defrauded again. The financial burden alone could be crushing, as one young person complained,

> *"The money is in their hands, and no matter what I say, they won't listen. In the end, I have to clean up the mess. I've already helped them pay back over 1 million yuan. What else can I do? From now on, I won't take responsibility for them anymore. I can't keep dealing with this."*

Internally, strained family relationships were another major source of significant stress. Many younger family members disclosed feelings of helplessness and disappointment when dealing with this issue. One young person even described these challenges as torturous,

> *"I've been tormented for years. I felt utterly helpless and disappointed. Most of our fights have revolved around these issues. My mom is stubborn. She won't listen to me, acts irrationally towards scammers with complete trust, and becomes impatient and aggressive when discussing these matters with me. She refuses to reveal details or admit she's been scammed and even lashes out at me for calling out the scammers."*

In severe cases, the elderly might threaten to cut off relationships, as one individual cried for help, *"What do I do? My mom wants to cut off our mother-daughter relationship!"* The strained family relationships had a profound psychological blow to the young generation. Moreover, young people faced a moral dilemma between adhering to social norms such as filial piety and being firm about protecting seniors from fraud. This internal conflict could also significantly contribute to younger family members' mental stress. The stress further led to insomnia (*"I can't sleep. I'm having trouble sleeping."*) or a sense of exhaustion and resignation (*"I'm tired of it, I won't let them make me pay the money anymore."*)

5 Discussion

In summary, our work provides insights into senior-targeted online fraud, younger family members' support and challenges based on a comprehensive analysis of posts and comments in RedNote. In this section, we situate our findings in prior literature, reflect on the whole support ecosystem against senior-targeted online fraud, and propose implications and recommendations for safeguarding seniors from online fraud.

5.1 Situating Findings within the Literature

5.1.1 Unique help enabled by younger family members. Our findings revealed that younger family members could help identify diverse fraud types faced by older adults. Aligning with prior work, we identify common types of scams targeting seniors, such as *investment fraud* [12, 95], *romance fraud* [10, 27] and *fake payment* [44] shown in Table 1. Beyond these similarities, we extend prior work by revealing fraud types that older adults struggle to recognize, such as *unnoticed charges* and *false advertising of collectibles*

in §4.1. Moreover, younger family members support recognizing various fraud details. Previous work showed older adults often did not fully understand how their behaviors might expose them to risks [71, 73]. We found that younger family members unveiled the specific channels and strategies used by fraudsters, such as *exploitation of social relationships* (e.g., tricking seniors via building connections on WeChat in §4.1) and *dark patterns* in online payment systems (e.g., *fake red packets* mentioned in §4.3.3). These complicated and manipulative mechanisms can be challenging for the elderly to detect on their own. This provides empirical evidence supporting previous work that many victims may not realize they have been scammed for a long time, and it is often family members who see through the deception [42, 89]. To this end, we suggest future research take a holistic view to examine older adults' online security, recognizing the sociocultural contexts including the support and influence of family models.

5.1.2 Strong family bonds in Chinese sociocultural contexts. Filial piety [48] is an important concept in Chinese culture, which sets up the expectations for children to care, respect, and show obedience to older family members. Filial piety contributes to closer ties between family members in Chinese families compared to those in Western countries [93]. Tang et al. found that filial piety helped seniors feel comfortable seeking help from younger family members in technology support, viewing their protection as beneficial rather than disempowering [93]. However, our findings revealed filial piety functioned as a double-edged sword in online fraud. While it served as a foundation for family support in anti-fraud efforts, seniors leveraged filial piety to compel younger family members to accommodate scammers' requests in 4.3.2, causing enormous pressure on younger family members. Moreover, when seniors trusted scammers over their families, it could disappoint younger members and halt their support in §4.3.2. Given this, we suggest future anti-fraud educational campaigns fostering a balanced understanding of filial piety to encourage mutual respect and communication within families and raise awareness about its potential misuse in facilitating online fraud.

5.1.3 Tension between financial security and autonomy. Financial autonomy, beyond access, has become a crucial factor in financial inclusion [67]. However, our work cautions against the possibility of reduced financial autonomy when older adults are exposed to online fraud and family members take strict paternalistic approaches such as *online payment restriction* and *monitoring* in §4.2.1. Different from Murthy et al.'s study on family support in general online security and privacy, which found that older adults are generally open to family members managing their devices and accounts [68], our findings reveal that in the context of online fraud, older adults often exhibit behaviors such as *guarding information* and *refusing help and intervention* in §4.3.1 and §4.3.2. We encourage future research to propose approaches to balance financial autonomy with financial security when designing anti-fraud intervention systems.

## 5.2 Theoretical Insights into the Support Ecosystem against Senior-Targeted Online Fraud

Combating senior-targeted fraud involves efforts beyond the victim [6, 34, 71, 77]. The family systems theory [7] suggests that when addressing a crisis, individuals cannot be fully understood in isolation, but rather as components of a family unit. In the context of online fraud, our findings provided empirical evidence, demonstrating that family members indeed played multiple roles, from somewhat controlling behaviors to prevent the fraud to identifying and persuading seniors about the fraud's existence, providing both financial and emotional support in the recovery process and educating the elderly about fraud (§4.2). Our empirical findings in §4.2 and §4.3 inform a conceptual framework of family support in safeguarding seniors against online fraud, as outlined in Figure 3. Except for these basic elements, family support also displays three important characteristics:

(1) *long-term and evolving*. Our findings reveal that family support for seniors in online fraud scenarios is prolonged and evolving. For example, the three-phase identification process in §4.2.2, the years-long persuasion efforts described in §4.3.5, and daily emotional care shown in §4.2.4 highlighted the sustained nature of such support. Seniors may also fall victim to fraud multiple times, requiring repeated family support as described in §4.3.5. Furthermore, younger family members adapt and refine their support behaviors over time. For instance, they may seek new redress solutions by leveraging advice from social media users in §4.3.4 or update their educational materials in response to emerging fraud cases in §4.2.5. Given this long-term and evolving feature, we call for future work to explore the longitudinal dynamics of family support, such as the evolution of supportive behaviors.

(2) *multiple stakeholders*. Younger family members often serve as mediators, bridging the family with various external stakeholders involved in anti-fraud efforts. For example, younger family members may turn to the police for assistance in persuading older adults, as shown in §4.2.3. §4.3.4 highlighted the difficulties in seeking redress through customer service, and social media provided a platform for younger family members to seek help and discuss possible solutions. These examples depicted younger family members as the primary mediators in obtaining support from other stakeholders. Future work should explore strategies to better equip younger family members with resources and tools to facilitate their mediation role effectively while also examining how other stakeholders can collaborate more seamlessly within this support ecosystem.

(3) *latency in support*. There may be a mismatch in timing between the support provided and the occurrence of the fraud. For instance, by the time younger family members recognize the fraud, financial losses may have already occurred, as described in §4.2.2, necessitating post-fraud recovery efforts. This latency is further exacerbated by seniors' *guarding of information* shown in §4.3.1. Therefore, future work could explore ways to conduct timely interventions from family members, reducing losses and alleviating the subsequent burden on younger family members.

Our conceptual framework provides a novel perspective of family support on senior-targeted fraud. We encourage future work to empirically validate and expand upon this framework.
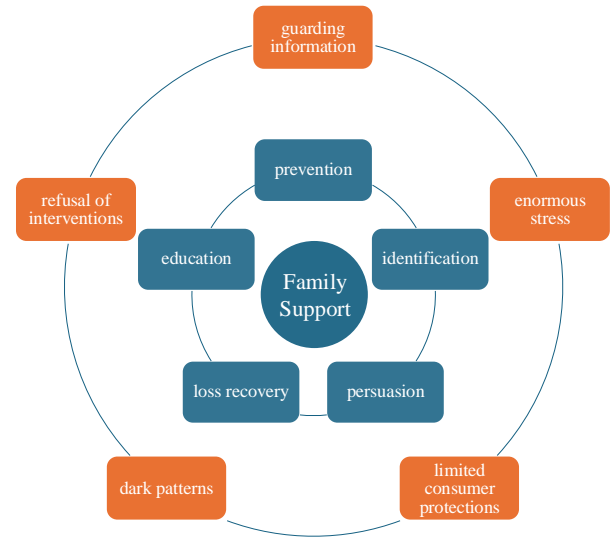
Figure 3: The conceptual framework of family support against senior-targeted fraud. The supportive behaviors are highlighted with the blue color and the challenges are showcased with the orange color.

5.3 Practical Implications and Recommendations

5.3.1 Platform interventions. In §5.1, we discussed the necessity of balancing online autonomy with financial security. Moreover, our findings revealed sometimes older adults actively sought assistance from younger family members, such as asking their children to check their accounts, as shown in §4.2.2. Given this, designers can develop mechanisms that empower seniors to easily request help when needed, satisfying seniors' need for financial autonomy. One potential approach is to integrate a built-in tool on seniors' mobile phones that facilitates seeking advice from family members. For instance, older adults encountering financial security concerns could click the tool to automatically capture screenshots, highlight possible problematic areas, generate concise descriptions of the potential issue, and revise under the tool's guidance if the content is inaccurate by using advanced technologies (e.g., generative AI). The summarized information could then be forwarded to a chat interface (e.g., WeChat) for family members to review and respond. Alternatively, with the senior's consent, younger family members could remotely access the device to take necessary actions or demonstrate solutions through the tool. Such a built-in tool has the potential to enhance online safety for seniors while also reducing tensions between seniors and younger family members.

However, our findings also revealed that sometimes older adults were reluctant to share their online activities and guarded their information in §4.3.1, which indicates that an older adult-initiated approach may not always work effectively. Additionally, §5.2 highlighted *the latency in support*, emphasizing the importance of timely

intervention from younger family members for better protection. To this end, designers could consider developing a system that automatically alerts younger family members to intervene promptly under specific circumstances, ensuring timely support while maintaining a balance between autonomy and security. One feasible solution could involve a collaborative approach where older adults and their younger family members set a predefined monetary threshold for interventions. When a payment exceeds this threshold, the system could trigger different actions depending on different payment stages. For instance, before payments, it could actively prompt older adults, asking whether they wish to discuss the payment with a younger family member, summarize payment details (e.g., product descriptions, payment links) and share them through a chat interface for discussion. During transactions, the tool could require explicit verification from younger family members, temporarily blocking the transaction until approval is granted. After payments, it could send notifications of transactions beyond the threshold to younger family members, enabling them to follow up as necessary. For specific designs, we call for future research to focus on co-designing such support models through workshops or participatory design, involving older adults, their families, and other stakeholders like caregivers and communities to identify older adults' needs for flexible support models while ensuring online autonomy and financial security. Generalization of design implications to other countries may require consideration of family dynamics within the local sociocultural context.

In addition to the intergenerational support model, there are other design implications worth considering. For instance, §4.3.3 highlighted the presence of *dark patterns*, such as *overly convenient password-free payment options, fake close buttons*, etc. Relevant policies should explicitly address these issues to promote accountability. Additionally, we observed that *red packets* were exploited in various fraud types, indicating their significant appeal to seniors (Table 1). A possible design solution is a warning message in interfaces involving red packets to alert seniors. We suggest researchers and designers systematically evaluate how fraud-checking nudges in online payments could prompt seniors to think carefully before proceeding.

5.3.2 Education for older adults. Drawing on our findings about older adults' *guarded behavior* and *refusal of intervention* in §4.3, educational materials should highlight the critical role of family members in anti-fraud. In the Chinese context, where filial piety and the authoritative or authoritarian position of seniors are ingrained [21], educational efforts should challenge superiority-based perspectives that undermine younger family members' roles in recognizing and preventing online fraud. For example, new anti-fraud guidelines could explicitly showcase that *distrusting* family members and *guarding information* from younger family members shown in §4.3.1 and §4.3.2 are the common brainwashing tactics used by scammers. Prior research also noted that US older adults were often unwilling to disclose fraud experiences to family members due to concerns about losing family status, trust issues and others [77], indicating that this implication might hold value for other contexts as well.

Additionally, an interesting phenomenon was observed in §4.2.5 that younger family members simulated fraudsters to raise seniors'

awareness of potential fraud. Existing research has also explored fraud simulation as a method to directly capture the behavioral response to attempted fraud "in the wild" [62], providing an immersive and realistic experience. Inspired by this, future work could explore simulating real-life fraud scenarios through customized education tools tailored to various fraud types, channels, and strategies based on §4.1, enhancing seniors' comprehensive fraud prevention literacy. Future designers could consider potential simulation formats, such as gamified fraud simulations or AI-based real-life simulations. For example, *exploitation of social relationships*, a common fraud tactic mentioned in §4.1, often involves interactive relationship-building, which could be simulated using AI to educate seniors. However, designers must consider ethical issues. For instance, explicitly labeling it as an education tool might reduce its effectiveness, as older adults could develop preemptive awareness, while not disclosing this could create artificial stress or be perceived as deceptive, even if deception has been used in previous work [62]. The use of AI introduces another crucial question regarding whether and how to disclose its involvement. Future research should also pay attention to whether prolonged interactions might lead older adults to over-engage with or believe the false narratives created by these simulations.

5.3.3 Support needed for younger family members. In §4.3, we found that the supportive process involves numerous challenges faced by younger family members. Our findings in §4.3.4 showed younger family members could discover potential solutions on social media. Additionally, social media allows them to gather new fraud cases, which could be used to educate seniors about emerging threats mentioned in §4.2.5. Therefore, facilitating the use of social media to seek help and discuss online fraud-related solutions might benefit more families. To this end, future designers could consider creating a dedicated discussion space on social media specifically for senior-targeted anti-fraud, allowing information to be more centralized and accessible. Platforms may consider how to prevent discussions from being exploited by scammers, such as implementing robust authentication mechanisms, to ensure a secure and trustworthy environment.

Furthermore, we call for the participation of more stakeholders in the discussion space on social media. As highlighted in §4.2.5, one notable challenge younger family members face is strained family relationships, particularly when efforts to persuade seniors result in conflict. A compelling example from §4.2.3 involved a younger family member "@" the older adult in a discussion thread, prompting another user to assist in persuasion. To alleviate the emotional stress on younger family members, inviting more stakeholders, such as police representatives, community members or psychologists, to join the conversations might make it easier to convince seniors and probably foster harmonious family relationships. Additionally, the participation of policymakers and law enforcement officials could also be beneficial. For instance, as illustrated in §4.3.4, family members faced significant challenges when seeking external help—e.g., filing a report was not accepted by the police if the elderly did not acknowledge being scammed. Policymakers could use related insights from social media discussions to address practical challenges and develop human-centric strategies. While

specific discussions on social media are rooted in the unique cultural and policy context of China, these design implications, such as the dedicated discussion space on social media and the participation of more stakeholders, could be adapted to benefit other regions.

5.4 Limitations

First, younger family members may selectively highlight roles or actions that are more favorably perceived by their audience, potentially influenced by social desirability bias [37]. Additionally, our data may not include all viewpoints, such as those of seniors, local communities, and official departments. We advocate for future research to adopt a multi-stakeholder approach, incorporating diverse perspectives and data sources to better understand younger family members' roles and seniors' experiences with fraud. Second, while we utilized social media to gather a diverse range of viewpoints, our sample might not be fully representative of all older adults in China. We call for future work to validate and cross-compare our findings by exploring a larger corpus of data through quantitative or computational methods. Third, while the perspectives of younger family members provide valuable supplementary insights into senior-targeted fraud, it is important to clarify that this approach is not necessarily superior to direct interviews with older adults. Rather, it offers an alternative lens to enrich our understanding with different nuances. Fourth, as our research was conducted on a Chinese platform, some findings might not generalize globally. Fifth, our dataset shares common limitations with all analyses based on social media data. We cannot fully ensure the credibility of each post and user profile. If the posts contain false or exaggerated information or users fill in fake profiles, we might not be able to detect it. Moreover, due to potential changes in dataset collection stemming from RedNote's contextual similarity-based search mechanism, the repeatability of this research cannot be guaranteed. However, our findings are based on a thematic analysis of the entire dataset rather than conclusions from individual posts, which helps mitigate the credibility issue and ensure the representativeness of the findings. We hope future work will validate these findings through more empirical methods, such as interviews and surveys. Finally, the demographic characteristics of RedNote's users, predominantly young and female [32], could have influenced the findings reported in our study.

6 Conclusion

Family support is a significant component in senior-targeted online fraud. This work makes the first attempt to investigate the younger family members' roles in safeguarding seniors from online fraud. To achieve this, we conducted a thematic analysis of 124 posts with 16,872 comments related to family support against senior-targeted fraud on RedNote, one of the largest life-sharing platforms in China. Our results highlight seniors' vulnerabilities in online fraud, younger family members' supportive behaviors across different stages, and challenges in family support. To conclude, we propose a conceptual framework of family support in senior-targeted online fraud and suggest actionable implications for senior's online security within the multi-stakeholder ecosystem.

References

[1] Aisha Abdallah, Mohd Aizaini Maarof, and Anazida Zainal. 2016. Fraud detection system: A survey. *Journal of Network and Computer Applications* 68 (2016), 90–113.
[2] Linda M Alves and Steve R Wilson. 2008. The effects of loneliness on telemarketing fraud vulnerability among older adults. *Journal of elder abuse & neglect* 20, 1 (2008), 63–85.
[3] Keith B. Anderson. 2013. Consumer Fraud in the United States, 2011: The Third FTC Survey. https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf. Accessed: 2024-05-20.
[4] Emilie Lundin Barse, Hakan Kvarnstrom, and Erland Jonsson. 2003. Synthesizing test data for fraud detection systems. In *19th Annual Computer Security Applications Conference, 2003. Proceedings.* IEEE, 384–394.
[5] Debalina Bera, Obi Ogbanufe, and Dan J Kim. 2023. Towards a thematic dimensional framework of online fraud: An exploration of fraudulent email attack tactics and intentions. *Decision Support Systems* 171 (2023), 113977.
[6] Kenneth V Berry. 2013. *The effect of elder fraud and ways to prevent it.* Ph.D. Dissertation. Utica College.
[7] Murray Bowen. 1993. *Family therapy in clinical practice.* Jason Aronson.
[8] Patricia A Boyle, Lei Yu, Robert S Wilson, Eisuke Segawa, Aron S Buchman, and David A Bennett. 2013. Cognitive decline impairs financial and health literacy among community-based older persons without dementia. *Psychology and aging* 28, 3 (2013), 614.
[9] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
[10] David Buil-Gil and Yongyu Zeng. 2022. Meeting you was a fake: investigating the increase in romance fraud during COVID-19. *Journal of Financial Crime* 29, 2 (2022), 460–475.
[11] Mark Button. 2012. Cross-border fraud and the case for an "Interfraud". *Policing: An International Journal of Police Strategies & Management* 35, 2 (2012), 285–303.
[12] Mark Button, Chris Lewis, and Jacki Tapley. 2009. A better deal for fraud victims: Research into victims' needs and experiences. (2009).
[13] Mark Button, Chris Lewis, and Jacki Tapley. 2014. Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal* 27 (2014), 36–54.
[14] Mark Button, Carol McNaughton Nicholls, Jane Kerr, and Rachael Owen. 2014. Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand journal of criminology* 47, 3 (2014), 391–408.
[15] Haoxian Cai and Wei Duan. 2022. Changing perceptions and uses of "companion animal" public and pseudo-public spaces in cities during COVID-19 pandemic: The case of Beijing. *Land* 11, 9 (2022), 1475.
[16] Eric L Carlson. 2006. Phishing for elderly victims: as the elderly migrate to the Internet fraudulent schemes targeting them follow. *Elder LJ* 14 (2006), 423.
[17] Laura L Carstensen. 2006. The influence of a sense of time on human development. *Science* 312, 5782 (2006), 1913–1915.
[18] Laura L Carstensen and Joseph A Mikels. 2005. At the intersection of emotion and cognition: Aging and the positivity effect. *Current directions in psychological science* 14, 3 (2005), 117–121.
[19] Elizabeth Castle, Naomi I Eisenberger, Teresa E Seeman, Wesley G Moons, Ian A Boggero, Mark S Grinblatt, and Shelley E Taylor. 2012. Neural and behavioral bases of age differences in perceptions of trust. *Proceedings of the National Academy of Sciences* 109, 51 (2012), 20848–20852.
[20] Internet Crime Complaint Center. 2023. Federal Bureau of Investigation Internet Crime Report 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf. Accessed: 2024-05-20.
[21] Susan S Chuang, Jenny Glozman, David S Green, and Sarah Rasmi. 2018. Parenting and family relationships in Chinese families: A critical ecological approach. *Journal of Family Theory & Review* 10, 2 (2018), 367–383.
[22] Federal Trade Commission. 2022. FTC brings together advisory group to combat scams against older adults. https://consumer.ftc.gov/consumer-alerts/2022/09/

ftc-brings-together-advisory-group-combat-scams-against-older-adults. Accessed: 2024-05-30.

[23] Marie-Therese Connolly. 2010. Where elder abuse and the justice system collide: Police power, parens patriae, and 12 recommendations. *Journal of Elder Abuse & Neglect* 22, 1-2 (2010), 37–93.

[24] Laura Consalter. 2024. Technology-Facilitated Gender-Based Violence: The Case of Couchsurfing. com.

[25] Gregory Conti and Edward Sobiesk. 2010. Malicious interface design: exploiting the user. In *Proceedings of the 19th international conference on World wide web*. 271–280.

[26] Juliet Corbin and Anselm Strauss. 2014. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications.

[27] Cassandra Cross. 2016. 'They're very lonely': Understanding the fraud victimisation of seniors. *International Journal for Crime, Justice and Social Democracy* 5, 4 (2016), 60–75.

[28] Cassandra Cross. 2022. Meeting the challenges of fraud in a digital world. In *The handbook of security*. Springer, 217–238.

[29] Cassandra Cross, Russell G Smith, and Kelly Richards. 2014. Challenges of responding to online fraud victimisation in Australia. *Trends and issues in crime and criminal justice* 474 (2014), 1–6.

[30] Olivia DaDalt. 2016. Older adults and fraud: Suggestions for policy and practice. *Journal of Economic & Financial Studies* 4, 03 (2016), 38–44.

[31] Sauvik Das, Joanne Lo, Laura Dabbish, and Jason I Hong. 2018. Breaking! A typology of security and privacy news and how it's shared. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. 1–12.

[32] Qiangua Data. [n. d.]. 2024 Research Report on "Active Users" (RedNote Platform). https://www.qian-gua.com/blog/detail/2898.html. Accessed: 2024-05-20.

[33] Marguerite DeLiema. 2018. Elder fraud and financial exploitation: Application of routine activity theory. *The Gerontologist* 58, 4 (2018), 706–718.

[34] Marguerite DeLiema, Yiting Li, and Gary Mottola. 2023. Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type. *International Journal of Consumer Studies* 47, 3 (2023), 1042–1059.

[35] Lai Fan and Dayu Zhang. 2023. Study on the hotspots of urban tourism spaces based on Instagram-Worthy locations data: Taking Beijing as an example. *Environment and Planning B: Urban Analytics and City Science* 50, 7 (2023), 1822–1837.

[36] Casey Fiesler. 2019. Ethical considerations for research involving (speculative) public data. *Proceedings of the ACM on Human-Computer Interaction* 3, GROUP (2019), 1–13.

[37] Robert J Fisher. 1993. Social desirability bias and the validity of indirect questioning. *Journal of consumer research* 20, 2 (1993), 303–315.

[38] World Economic Forum. 2024. The Globle Risks Report 2024. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf. Accessed: 2024-05-20.

[39] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In *Fifteenth symposium on usable privacy and security (SOUPS 2019)*. 21–40.

[40] Linda Ganzini, Bentson H McFarland, and David Cutler. 1990. Prevalence of mental disorders after catastrophic financial loss. *The Journal of nervous and mental disease* 178, 11 (1990), 680–685.

[41] Minas Gjoka, Maciej Kurant, Carter T Butts, and Athina Markopoulou. 2011. Practical recommendations on crawling online social networks. *IEEE Journal on Selected Areas in Communications* 29, 9 (2011), 1872–1892.

[42] Andrew Gloag and Polly Mackenzie. 2019. Protected by Design. *Demos* (2019).

[43] S Duke Han, Patricia A Boyle, Bryan D James, Lei Yu, and David A Bennett. 2016. Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease* 49, 3 (2016), 845–851.

[44] Changyang He, Lu He, Zhicong Lu, and Bo Li. 2023. "I Have to Use My Son's QR Code to Run the Business": Unpacking Senior Street Vendors' Challenges in Mobile Money Collection in China. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1 (2023), 1–28.

[45] Franziska Herbert, Steffen Becker, Annalina Buckmann, Marvin Kowalewski, Jonas Hielscher, Yasemin Acar, Markus Dürmuth, Yixin Zou, and M Angela Sasse. 2022. Digital Security–A Question of Perspective. A Large-Scale Telephone Survey with Four At-Risk User Groups. *arXiv preprint arXiv:2212.12964* (2022).

[46] Dominik Hornung, Claudia Müller, Irina Shklovski, Timo Jakobi, and Volker Wulf. 2017. Navigating relationships and boundaries: Concerns around ICT-uptake for elderly people. In *Proceedings of the 2017 CHI conference on human factors in computing systems*. 7057–7069.

[47] Adele E. Howe, Indrajit Ray, Mark Roberts, Malgorzata Urbanska, and Zinta Byrne. 2012. The Psychology of Security for the Home Computer User. In *2012 IEEE Symposium on Security and Privacy*. 209–223. doi:10.1109/SP.2012.23

[48] Charlotte Ikels. 2004. *Filial piety: Practice and discourse in contemporary East Asia*. Stanford University Press.

[49] Bryan D James, Patricia A Boyle, and David A Bennett. 2014. Correlates of susceptibility to scams in older adults without dementia. *Journal of elder abuse & neglect* 26, 2 (2014), 107–122.

[50] Pascal Jansen and Fabian Fischbach. 2020. The social engineer: An immersive virtual reality educational game to raise social engineering awareness. In *Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play*. 59–63.

[51] Rebecca A Judges, Sara N Gallant, Lixia Yang, and Kang Lee. 2017. The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in psychology* 8 (2017), 248182.

[52] Joakim Kävrestad. 2014. Defining, categorizing and defending against online fraud.

[53] Steven Kemp and Nieves Erades Pérez. 2023. Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health* 20, 7 (2023), 5404.

[54] Yubo Kou, Sam Moradzadeh, and Xinning Gui. 2024. Trading as Gambling: Social Investing and Financial Risks on the r/WallStreetBets Subreddit. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–17.

[55] Varun Badrinath Krishna, Carl A Gunter, and William H Sanders. 2018. Evaluating detectors on optimal attack vectors that enable electricity theft and DER fraud. *IEEE Journal of Selected Topics in Signal Processing* 12, 4 (2018), 790–805.

[56] Lin Kyi and Elizabeth Stobert. 2022. "I don't really give them piece of mind": User Perceptions of Social Engineering Attacks. In *2022 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 1–13.

[57] Mark S Lachs and S Duke Han. 2015. Age-associated financial vulnerability: An emerging public health issue. 877–878 pages.

[58] Jingjie Li, Kaiwen Sun, Brittany Skye Huff, Anna Marie Bierley, Younghyun Kim, Florian Schaub, and Kassem Fawaz. 2023. "It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2850–2866.

[59] Tianyuan Li and Helene H Fung. 2013. Age differences in trust: An investigation across 38 countries. *Journals of Gerontology Series B: Psychological Sciences and Social Sciences* 68, 3 (2013), 347–355.

[60] Peter A Lichtenberg, Laurie Stickney, and Daniel Paulson. 2013. Is psychological vulnerability related to the experience of fraud in older adults? *Clinical gerontologist* 36, 2 (2013), 132–146.

[61] Peter Alexander Lichtenberg, Michael A Sugarman, Daniel Paulson, Lisa J Ficker, and Annalise Rahman-Filipiak. 2016. Psychological and functional vulnerability predicts fraud cases in older adults: Results of a longitudinal study. *Clinical Gerontologist* 39, 1 (2016), 48–63.

[62] Tian Lin, Daniel E Capecci, Donovan M Ellis, Harold A Rocha, Sandeep Dommaraju, Daniela S Oliveira, and Natalie C Ebner. 2019. Susceptibility to spear-phishing emails: Effects of internet user demographics and email content. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26, 5 (2019), 1–28.

[63] Walid Magdy, Yehia Elkhatib, Gareth Tyson, Sagar Joglekar, and Nishanth Sastry. 2017. Fake it till you make it: Fishing for Catfishes. In *Proceedings of the 2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining 2017*. 497–504.

[64] Jim McCambridge, John Witton, and Diana R Elbourne. 2014. Systematic review of the Hawthorne effect: new concepts are needed to study research participation effects. *Journal of clinical epidemiology* 67, 3 (2014), 267–277.

[65] Nora McDonald and Helena M Mentis. 2023. 'Don't Fall for This': Communications about Cybersafety from the AARP. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW2 (2023), 1–21.

[66] Francois Mouton, Louise Leenen, and Hein S Venter. 2016. Social engineering attack examples, templates and scenarios. *Computers & Security* 59 (2016), 186–209.

[67] Srihari Hulikal Muralidhar, Claus Bossen, and Jacki O'neill. 2019. Rethinking financial inclusion: From access to autonomy. *Computer Supported Cooperative Work (CSCW)* 28 (2019), 511–547.

[68] Savanthi Murthy, Karthik S Bhat, Sauvik Das, and Neha Kumar. 2021. Individually Vulnerable, Collectively Safe: The Security and Privacy Practices of Households with Older Adults. 5, CSCW1, April: 1–24.

[69] China Central Television (CCTV) News. 2024. Focused on the 'old and young'! 77.7group have received fraud information (translated from Chinese). https://news.cctv.com/2024/02/05/ARTIIAcXLj1zwC29Ik7UtNN2240205.shtml. Accessed: 2024-05-30.

[70] Reuben Ng and Nicole Indran. 2022. Not too old for TikTok: How older adults are reframing aging. *The Gerontologist* 62, 8 (2022), 1207–1216.

[71] James Nicholson, Lynne Coventry, and Pamela Briggs. 2019. "If It's Important It Will Be A Headline" Cybersecurity Information Seeking in Older Adults. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–11.

[72] The State Council of the People's Republic of China. 2022. Anti-Telecom and Online Fraud Law of the People's Republic of China. https://www.gov.cn/xinwen/2022-09/02/content_5708119.htm. Accessed: 2024-05-01.

[73] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. 2017. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing.

In *Proceedings of the 2017 chi conference on human factors in computing systems*. 6412–6424.

[74] National Council on Aging. 2023. The Top 5 Financial Scams Targeting Older Adults. https://www.ncoa.org/article/top-5-financial-scams-targeting-older-adults. Accessed: 2024-05-01.

[75] Patricia O'Neill. 2015. *Chinese daughters negotiating contemporary norms and traditional filial obligation*. Ph. D. Dissertation. Oxford University, UK.

[76] Karla Pak and Doug Shadel. 2011. AARP Foundation National Fraud Victim Study. https://assets.aarp.org/rgcenter/econ/fraud-victims-11.pdf. Accessed: 2024-05-20.

[77] Katfalin Parti and Faika Tahir. 2023. "If We Don't Listen to Them, We Make Them Lose More than Money:" Exploring Reasons for Underreportifng and the Needs of Older Scam Victims. *Social Sciences* 12, 5 (2023), 264.

[78] PYMNTS. 2024. FBI: More Than \$12 Billion Lost to Online Fraud in 2023. https://www.pymnts.com/news/security-and-risk/2024/fbi-more-than-12-billion-lost-to-online-fraud-in-2023/. Accessed: 2024-05-20.

[79] Lubna Razaq, Tallal Ahmad, Samia Ibtasam, Umer Ramzan, and Shrirang Mare. 2021. " We Even Borrowed Money From Our Neighbor" Understanding Mobile-based Frauds Through Victims' Experiences. *Proceedings of the ACM on human-computer interaction* 5, CSCW1 (2021), 1–30.

[80] Michael D Reisig and Kristy Holtfreter. 2013. Shopping fraud victimization among the elderly. *Journal of Financial Crime* 20, 3 (2013), 324–337.

[81] Relakkes. 2023. MediaCrawler. https://github.com/NanmiCoder/MediaCrawler. Accessed: 2024-05-20.

[82] Ted Ruffman, Janice Murray, Jamin Halberstadt, and Tina Vater. 2012. Age-related differences in deception. *Psychology and aging* 27, 3 (2012), 543.

[83] Stuart E. Schechter, Rachna Dhamija, Andy Ozment, and Ian Fischer. 2007. The Emperor's New Security Indicators. In *2007 IEEE Symposium on Security and Privacy (SP '07)*. 51–65. doi:10.1109/SP.2007.35

[84] Marc Schmitt and Ivan Flechais. 2023. Digital Deception: Generative artificial intelligence in social engineering and phishing. *arXiv preprint arXiv:2310.13715* (2023).

[85] Michal Segal, Israel Doron, and Sagit Mor. 2021. Consumer fraud: Older people's perceptions and experiences. *Journal of Aging & Social Policy* 33, 1 (2021), 1–21.

[86] Virda Setyani, Yu-Qian Zhu, Achmad Nizar Hidayanto, Puspa Indahati Sandhyaduhita, and Bo Hsiao. 2019. Exploring the psychological mechanisms from personalized advertisements to urge to buy impulsively on social media. *International Journal of Information Management* 48 (2019), 96–107.

[87] Jingjin Shao, Qianhan Zhang, Yining Ren, Xiying Li, and Tian Lin. 2019. Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse & Neglect* 31, 3 (2019), 225–243.

[88] Xuewen Sheng and Barbara H Settles. 2006. Intergenerational relationships and elderly care in China: A global perspective. *Current Sociology* 54, 2 (2006), 293–313.

[89] Sinthujan Sivagumaran. 2023. Challenges of Online Security for Senior Citizens.

[90] Herut Soffer. 2023. Old Age and the Potential for Web Fraud: An In-Depth Analysis. *Available at SSRN 4602538* (2023).

[91] Statista. [n. d.]. Number of monthly active users of Xiaohongshu app in China from December 2020 to September 2023. https://www.statista.com/statistics/1327421/china-xiaohongshu-monthly-active-users/. Accessed: 2024-05-20.

[92] Statista. [n. d.]. Number of registered users of Xiaohongshu in China from 2015 to 2020. https://www.statista.com/statistics/1053577/china-xiaohongshu-user-number/. Accessed: 2024-05-20.

[93] Xinru Tang, Yuling Sun, Bowen Zhang, Zimi Liu, RAY Lc, Zhicong Lu, and Xin Tong. 2022. " I Never Imagined Grandma Could Do So Well with Technology" Evolving Roles of Younger Family Members in Older Adults' Technology Learning and Use. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (2022), 1–29.

[94] Shuoyu Tao and Yang Xi. 2023. Social Media and Lifestyle: The Lifestyle Integration Path for Brand Communication. In *Proceedings of the 2nd International Conference on Bigdata Blockchain and Economy Management, ICBBEM 2023, May 19–21, 2023, Hangzhou, China*.

[95] Age UK. 2015. Only the tip of the iceberg: Fraud against older people. https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_april15_only_the_tip_of_the_iceberg.pdf. Accessed: 2024-05-30.

[96] Age UK. 2018. Applying the brakes: Slowing and stopping fraud against older people. https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_mar18_applying_the_brakes.pdf. Accessed: 2024-05-30.

[97] Judy Van Wyk and Karen A Mason. 2001. Investigating vulnerability and reporting behavior for consumer fraud victimization: Opportunity as a social aspect of age. *Journal of contemporary criminal justice* 17, 4 (2001), 328–345.

[98] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True" The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction* 2, CSCW

[99] Rick Wash. 2020. How experts detect phishing scam emails. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2 (2020), 1–28.

[100] Wikipedia. [n. d.]. WeChat. https://en.wikipedia.org/wiki/WeChat. Accessed: 2024-08-20.

[101] Wikipedia. [n. d.]. WeChat red envelope. https://en.wikipedia.org/wiki/WeChat_red_envelope. Accessed: 2024-05-20.

[102] Wikipedia. [n. d.]. Weibo. https://en.wikipedia.org/wiki/Weibo. Accessed: 2024-08-20.

[103] Wikipedia. [n. d.]. Xiaohongshu. https://en.wikipedia.org/wiki/xiaohongshu. Accessed: 2024-05-20.

[104] Wikipedia. 2021. National Anti-Fraud Center. https://en.wikipedia.org/wiki/National_Anti-Fraud_Center. Accessed: 2024-05-01.

[105] Qunfang Wu, Zitong Huang, Yaqi Zhang, and Chung-Chin Eugene Liu. 2018. Auditing Personalized Recommendation Algorithms Through Spontaneous Click-Based User Interaction. (2018).

[106] Ziming Wu and Xiaojuan Ma. 2017. Money as a social currency to manage group dynamics: Red packet gifting in chinese online communities. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. 2240–2247.

[107] Yuebin Xu. 2001. Family support for old people in rural China. *Social Policy & Administration* 35, 3 (2001), 307–320.

[108] Yusi Xu. 2021. The "Lucky Money" That Started It All—The Reinvention of the Ancient Tradition "Red Packet" in Digital Times. *Social Media+ Society* 7, 3 (2021), 20563051211041643.

[109] Xiaodong Yue and Sik Hung Ng. 1999. Filial obligations and expectations in China: Current views from young and old people in Beijing. *Asian Journal of Social Psychology* 2, 2 (1999), 215–226.

[110] Heying Jenny Zhan, Zhanlian Feng, Zhiyu Chen, and Xiaotian Feng. 2011. The role of the family in institutional long-term care: cultural management of filial piety in China. *International Journal of Social Welfare* 20 (2011), S121–S134.

[111] Yixin Zou, Kaiwen Sun, Tanisha Afnan, Ruba Abu-Salma, Robin Brewer, and Florian Schaub. 2024. Cross-Contextual Examination of Older Adults' Privacy Concerns, Behaviors, and Vulnerabilities. *Proceedings on Privacy Enhancing Technologies* (2024).