Elderly Digital Resilience in Responding to Online Fraud

Jumrana[1], Cecep Ibrahim[2]

{jumrana@uho.ac.id[1], cecepibra@gmail.com[2]}

Faculty of Social Science and Political Science, Halu Oleo University
Kendari, 93231[1,2]

Abstract. Digital fraud is one type of crime that is constantly on the rise in cyberspace across many platforms. Anyone of any age can become a victim. The pre-elderly and elderly age groups were shown to be especially susceptible to digital fraud, according to research conducted in February-June 2022. Typically, victims of digital fraud either take no action or are unsure of what to do. This research aimed to provide an overview of the digital resilience of elderly in Kendari City in facing fraud crimes in cyberspace. This type of research is descriptive research with mixed methods, combining surveys and interviews to collect data. The research subjects were elderly and pre-elderly who had taken digital literacy training. The research results showed that some elderly had online resilience, shown by their self-efficacy and confidence in being able to face online fraud by providing active and proactive responses. Active responses include deleting messages, blocking message senders, and reporting, while proactive responses include communication and education.

Keywords: digital fraud, digital resilience, digital literacy, elderly

1 Introduction

Online fraud, also known as digital fraud or cyber fraud, is one of common cybercrimes becoming problem for digital security. This terminology refers to fraud committed via digital communication devices, which is an unethical fraud operation that aims to steal money from or personal information from someone [1].

Some forms of digital fraud often carried out are phishing, lottery scam, video scam, identity theft and scareware [2]. A survey conducted in 2022 throughout Indonesia shows that the type of online fraudulent messages received by the public is gift fraud as much as 91.2%, the second most common type of fraudulent message is illegal online loan fraud, namely 74.8%, next in succession are messages containing malware links 65.2%, fake messages related to family crises 59.8%, illegal investment offer messages 56%, sending fake websites or applications 52.6%, fraudulent buying and selling messages 52.35, and fraudulent messages under the guise of charity 50.6%. Meanwhile, other forms of fraudulent and fake messages, such as fake job vacancies, online social gathering fraud, online identity theft, and fraud under the guise of romance are below 50% [3].

SSIK 2023, September 20, Kendari, Indonesia

DOI 10.4108/eai.20-9-2023.2340976

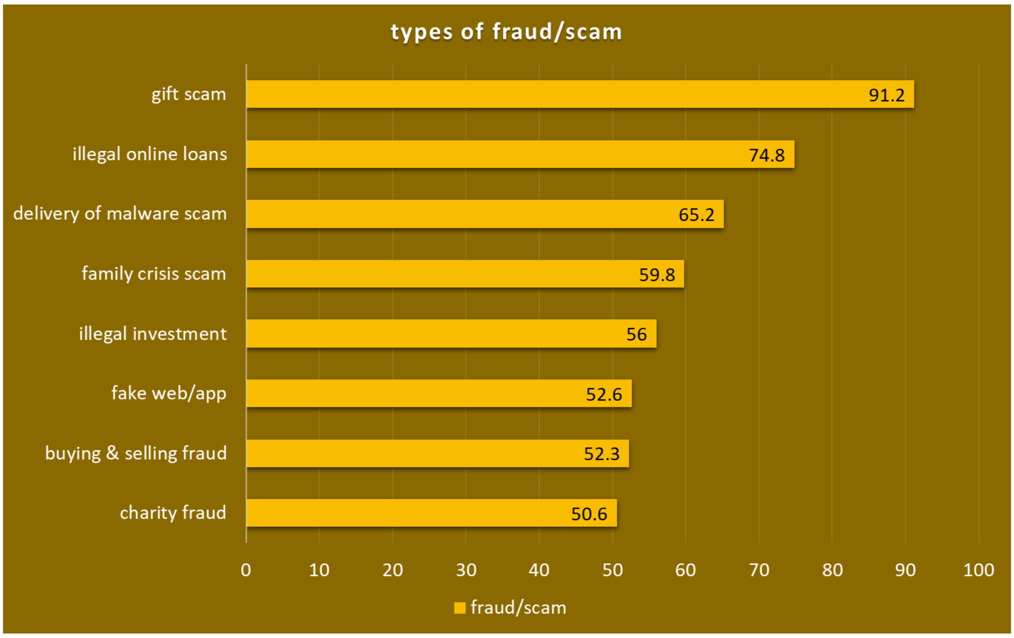


Figure 1. Types of digital fraud
Source: *Penipuan Digital di Indonesia; Modus, Medium, dan Rekomendasi* (Digital Fraud in Indonesia; Mode, Medium, and Recommendations)[3]

From the data description, there is an indication that the digital space is not safe for netizens. Online fraud is rampant and causes losses to society. According to the Directorate General of Technology's report, from 2017 to 2022, the CekRekening.id service from the Ministry of Communication and Information Technology has received approximately 486,000 reports from the public related to information crimes and electronic transactions [4]. Based on OJK data, from January to May 31 2023, the OJK has received complaints related to fraud modes in the form of skimming, phishing, social engineering and sniffing as many as 72,618 (6.5%) of all complaints received of 1,116,175 services. As for illegal investments, losses experienced by the public due to illegal investments from 2018 to 2022 have reached IDR 126 trillion [5].

According to Bambang Tri Santoso, Head of the Digital Literacy Team for the Education Sector of the Ministry of Communication and Information Technology, digital literacy is crucial for ensuring that the general public is aware of the different types of online fraud so they can be vigilant and anticipate if there are indications of fraud [4]. In addition to educating the public about different types of fraud, digital literacy teaches digital safety skills, including protecting data and accounts, accessing and conducting transactions safely, avoiding and reporting online fraud, and others. The aim of digital literacy is not only to increase awareness and change behavior but also to encourage people to become resilient online.

Online resilience refers to the concept of how people cope with stressful, harmful, and risky situations in cyberspace [6]. According to a different viewpoint, online resilience is the ability to handle challenges, avoid harms when exposed to risks, and deal with problems [7].

Online resilience, according to both perspectives, is the capacity of an individual to deal effectively with unpleasant, risky, and harmful information and messages in cyberspace to prevent impact detrimental, including online fraud.

Reivich and Shatte described a number of factors affecting resilience, including emotional management, impulse control, optimism, causal analysis, empathy, and self-efficacy [8]. However, of these seven aspects, there are five aspects that can influence online resilience. These five aspects are the emotional regulation aspect in the form of the ability to remain calm and be able to control stressful situations when facing online risks, the impulse control aspect in the form of the ability to regulate emotions so as not to lose control of oneself when exposed to harmful things from cyberspace, the optimistic aspect is self-confidence in facing and controlling situations when facing online crime, the causal analysis aspect in the form the ability to identify the cause of an event (this aspect can prevent someone from making mistakes or detrimental conditions in cyberspace), and self-efficacy in the form of an individual's self-confidence to be able to face and solve online crime problems.

The pre-elderly and elderly age groups are among those most at risk of falling victim to online fraud. According to a survey done in 2022 by the Center for Digital Society (CfDS), 67% of pre-elderly and 72.6% of senior people had fallen victim to online fraud. In addition to fraud disguised as a family emergency and messages with malware links, nearly half of them were deceived by messages purporting to be gifts [3]. Therefore, this research aimed to analyze online resilience of pre-elderly and elderly in Kendari City to understand how respond to and deal with online fraud.

2 Method

The research used a mixed-method approach by combining a quantitative approach using survey methods and a qualitative approach using interviews to collect data. The combined method scenario in this research tends to combine both methods by using quantitative methods to develop qualitative research [9]. This mixed method can explain various online fraud phenomena by using basic data from survey data analysis developed in interviews to explore informants' experiences in dealing with online fraud. Mixed methods attempt to describe precisely the values of a phenomenon accurately through observations from different methodological viewpoints [10].

This research was conducted from March to July 2023, with a series of research divided into several stages, namely: (a) Literature Study; (b) Preparation of survey questionnaires; (c) Testing the questionnaire; (d) Analysis of survey trial data; (e) Refinement of the survey questionnaire; (f) Survey of respondents; (g) Process and analyze survey data; (h) interviews with 12 informants selected from respondents to deepen online fraud data (i) processing and analysis of interview data; and (j) preparation of reports.

The survey method was carried out by selecting respondents using non-probability sampling on 98 pre-elderly and elderly aged 45 - 88 years old who had taken part in digital literacy training in Kendari City. From this sampling method, the respondents were 12 pre-elderly and 86 elderly people, consisting of 31 men and 67 women. Apart from considering having attended digital literacy training and age range, the selected respondents actively use SMS, phone call, conversation applications and social media.

3 Results and Discussion

Personal communication tools are increasingly necessary due to the requirement for interaction, discussion, and quick information dissemination. The development of personal digital communication media, such as mobile phones, has led to an increased number of users. Mobile devices connected in Indonesia are 353.8 million (128% of the total population) [11] since some people in Indonesia have more than one mobile device. Mobile devices like smartphones are channels often used to spread fraudulent messages.

The platforms most used in Indonesia are WhatsApp 92.1%, Instagram 86.5%, Facebook 81.3% and Tiktok 63.1%, all of which show an increase in the number of users [11]. The platforms frequently used to spread fraudulent messages received by pre-elderly and elderly are conversation applications (WhatsApp and Messenger) 38.8%, SMS/phone call 29.6%, social media (Facebook and Instagram) 18.4%, e-commerce applications (Tokopedia, Shopee, local marketplace) 9.2%, and email 4.1%. The more users there are, the more likely the platform is to be used to spread fraudulent messages.

Elderly typically connect and interact online via WhatsApp app, SMS, and phone call, but they do not use Messenger or email. This age group is unfamiliar with social media and solely uses Facebook and Instagram. They rarely upload and share content on Facebook since they use it to obtain information and entertainment. Meanwhile, Instagram is occasionally used to share content in the form of images. Compared to big marketplaces like Shopee and Tokopedia, they prefer to shop in local marketplaces. In contrast to the elderly, the pre-elderly group engages in online communication and interaction more frequently using WhatsApp app, phone call, Messenger, and email. Typically, they are active social media users on Facebook and Instagram. They like to share their activities and opinions on social media and actively interact with people on their friend list. Therefore, the pre-elderly and elderly are more vulnerable to online fraud.

Table 1. Types of fraud and distribution media

Types of online fraud	**Distribution media**
Gift scam	SMS
Illegal loans	Facebook, WhatsApp
Delivery of malware link	WhatsApp, Messenger, Facebook
Social gathering fraud	WhatsApp, Phone call
Buying & selling fraud	E-commerce applications, Instagram, Facebook
Family crisis scam	Phone Call
Identity fraud	What’s App, Facebook
Charity fraud	Email, Facebook, WhatsApp
Job vacancy fraud	Email, WhatsApp, SMS

Love scam	Messenger

Source: Analysis of research results on online fraud among the elderly and pre-elderly in Kendari 2023

The large number of mobile cellular users is not accompanied by the ability to protect personal data and accounts on online media. According to the data, 12.2% of elderly and pre-elderly only know how to create passwords, while 25.5% know to create passwords and routinely update them. Only 27.6% of elderly and pre-elderly are aware of personal data and how to keep it private online, compared to 34.7% of those who are knowledgeable about password creation, password changes, and personal data and keep it private, as well as understand two-step authentication. The pre-elderly and elderly have uneven levels of knowledge about basic digital security, which limits their ability to protect their online accounts and personal information.

The variety of online frauds that are often found by the pre-elderly and elderly in Kendari City shows that fraud disguised as gifts is the most common type of online fraud, followed by applying illegal loans online. The types of fraudulent messages frequently received by elderly and pre-elderly include viral link messages (malware), social gathering fraud messages, buying and selling fraud, family crisis fraud, personal identity theft, fraud under the guise of charity, job vacancy fraud, and fraud under the guise of romance.

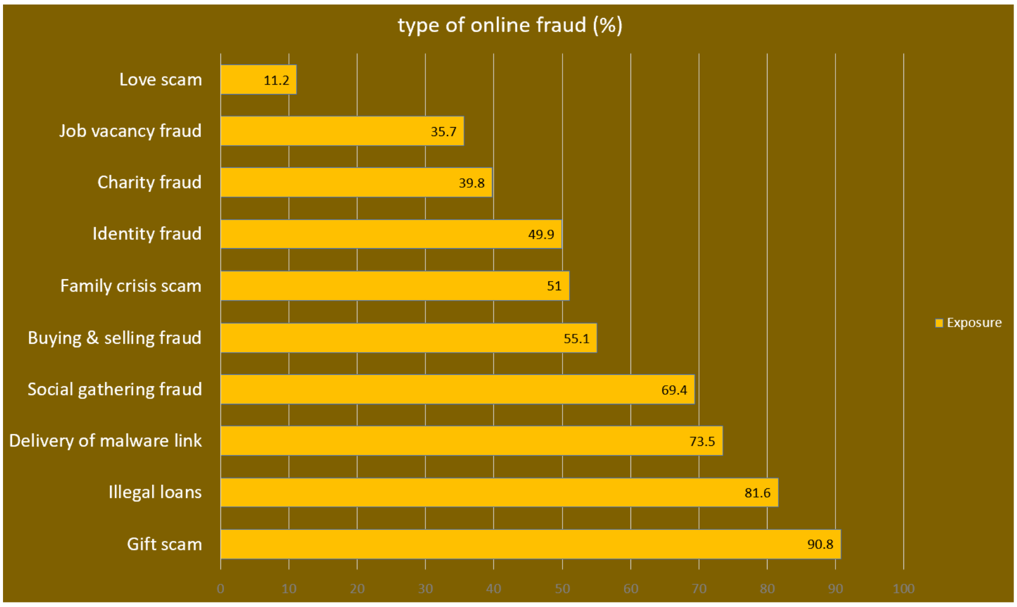
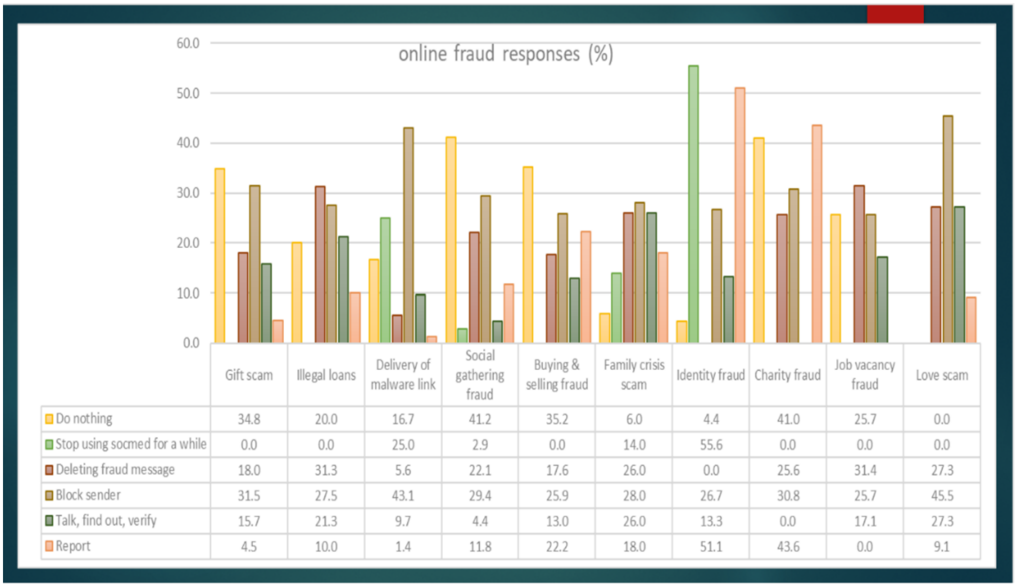


Figure 2. Graph of types of fraudulent messages received by the elderly and pre-elderly
Source: Analysis of survey data on online fraud among the elderly and pre-elderly in Kendari 2023

Many elderly and pre-elderly still rely on cell phones. Although smartphones with more robust applications and capabilities are becoming more common, mobile messaging (SMS) is often a tool for receiving messages under the guidance of gifts and fraudulent job vacancies. Meanwhile, conversation applications (WhatsApp and Messenger) have become a medium for spreading illegal online loan messages, links containing malware, fraud under the guise of social gatherings, charity and job vacancies, and personal identity theft. Specifically, fraudulent messages under the guise of romance are most often sent to elderly via Messenger.

Apart from these two types of media, social media (Facebook and Instagram) are also targets for spreading fraudulent messages. Elderly and pre-elderly often receive fraudulent online loan messages, malware link messages, buying and selling fraud, personal identity theft, and fraud under the guise of charity through these two social media. Besides, marketplaces are a means of spreading messages about buying and selling fraud, and phone calls are a means of spreading family crisis fraud and fraud under the guise of social gatherings.



	Gift scam	Illegal loans	Delivery of malware link	Social gathering fraud	Buying & selling fraud	Family crisis scam	Identity fraud	Charity fraud	Job vacancy fraud	Love scam
🟨 Do nothing	34.8	20.0	16.7	41.2	35.2	6.0	4.4	41.0	25.7	0.0
🟩 Stop using socmed for a while	0.0	0.0	25.0	2.9	0.0	14.0	55.6	0.0	0.0	0.0
🟥 Deleting fraud message	18.0	31.3	5.6	22.1	17.6	26.0	0.0	25.6	31.4	27.3
🟫 Block sender	31.5	27.5	43.1	29.4	25.9	28.0	26.7	30.8	25.7	45.5
🟩 Talk, find out, verify	15.7	21.3	9.7	4.4	13.0	26.0	13.3	0.0	17.1	27.3
🟧 Report	4.5	10.0	1.4	11.8	22.2	18.0	51.1	43.6	0.0	9.1

Figure 3. Graph of response to online fraud
Source: Analysis of survey data on online fraud received by the elderly and pre-elderly in Kendari 2023

The data in Figure 3 shows that in several types of online fraud messages received via online media, elderly and pre-elderly did not do anything or just ignored it. The percentage of allowing fraudulent messages is quite high in fraudulent messages under the guise of social gatherings (41.2%), charity (41%), buying and selling (35.2%), gifts (34.8%), fake job vacancies (25.7%), and online loans (20%), while the remaining percentage of omissions is for the type of other fraudulent messages (under 20%). A high percentage of fraudulent messages are ignored because they are considered harmless, such as messages under the guise of social gatherings, charity, gifts, fake job vacancies and online loans. The way for elderly and pre-elderly not to get caught in this type of fraud is by not replying to messages and not clicking on any links attached to messages. Generally, they already know about this type of fraud. There are 22.5% of elderly and pre-elderly who do not do anything or allow fraudulent messages online.

Apart from not doing anything and allowing fraudulent messages, some elderly and pre-elderly decide to stop using social media and the internet for a moment, especially when they often receive messages indicating personal identity theft and containing links to malware or viruses, or have received family crisis calls and avoid fraudulent messages under the guise of social gathering. The reason they stopped using social media and the internet for a moment was because some of them had experienced personal identity theft, were worried about clicking the wrong link containing malware, were traumatized by fraudulent family crisis calls and did not want to receive messages and persuasions to join online social gatherings. In general, 9.7% of elderly and pre-elderly have decided to stop using social media and the internet for a while because they often receive fraudulent messages online. The behavior of not doing anything or allowing fraudulent messages online and stopping using social media and the internet are passive responses shown by netizens when facing a crisis and receiving negative messages in cyberspace. This is related to low impulse control when receiving fraudulent messages, especially family crisis messages, or poor emotion regulation when receiving fraudulent messages under the guise of gifts and other fraudulent messages.

The majority of elderly and pre-elderly responded differently to fraudulent messages by deleting them from their devices after receiving them. There are 31.4% of them deleting fake job offers, 31.3% deleting illegal online loan messages, 27.3% deleting fraud under the guise of romance, 26% deleting family crisis messages, 25.6% deleting frauds under the guise of charity, and 22.1 % eliminating fraud under the guise of social gathering. Meanwhile, under 20% of fraudulent messages under the guise of gifts, buying and selling, and containing malware/virus link messages were deliberately deleted. Cleaning the message directory, not wanting to be bothered, and not wanting to read the messages are a few reasons why the delete or hide the fraudulent messages.

Another different response shown by the elderly and pre-elderly is to block the telephone number or social media account that sent the fraudulent message. The majority admitted to utilizing this technique, particularly when dealing with fraudulent messages posing as romantic 45.5%, malware/virus link messages 43.1%, gifts fraud 31.5%, social gathering fraud 29.4%, and family crisis fraud 28%. Blocking was also done on the phone numbers and accounts that post other fraudulent messages at a smaller percentage. They blocked them because they didn't want to receive fraudulent messages from them, despite the fact that some elderly and pre-elderly said they frequently received the same fraudulent messages from several phone numbers and accounts.

One form of very positive response made by the elderly and pre-elderly is reporting when they find fraudulent messages online. They reported messages related to personal identity fraud (51%), charity fraud (43.6%), buying and selling frauds (22.2%), and other forms of fraudulent messages with a smaller percentage (below 20%). In general, they mostly report on platforms, marketplaces, content complaint channels of Ministry of Communication and Information Technology, and cekrekning.id. Their hope is that with this reporting, there will be efforts to deactivate the fraudster's number, trace and freeze the fraudster's account number, and ban the fraudster's account on social media. The pre-elderly and elderly typically do not report online scams to the authorities because they believe the lengthy, time- and effort-intensive process is not worthwhile given the modest amount of money lost.

From the explanation above, it is found that apart from a passive response, some elderly and pre-elderly people also performed an active response when faced with online fraudulent messages by deleting fraudulent messages, blocking telephone numbers/WhatsApp and social media accounts that sent fraudulent messages and reporting fraud. The active response shown by the pre-elderly and elderly is resilience to face negative things in online experiences. They do not feel disadvantaged and are able to handle problems without feeling disturbed; d'Haenens et al. [7] calls this high-level resilience. This contrasts with the passive response, in which people decide to ignore or temporarily cease using social media and the internet after being mentally disturbed.

Elderly and pre-elderly frequently use telling problem, finding out, or verifying to make sure the information they got is accurate. For example, 26% who received a family crisis fraud asked for help from others, and 21.3% who received messages about illegal loans sought other people's opinions. Meanwhile, the others did the same when they received fraudulent messages from other sources. Almost all pre-elderly has received fraudulent messages under the guise of romance. Two people almost became victims, but this incident could be avoided because they shared it with their families. One of them said that he had received a telephone call saying that his child admitted to hospital due to an accident, was about to undergo surgery, and was being asked for money. Under a stressful situation, he took the initiative to ask his neighbor's opinion, who told him that this was a form of fraud so that he could avoid this. Another elderly immediately sought information for clarification at the nearest bank branch after receiving a fraudulent message about a transaction deduction, which he had to confirm via a certain number in the name of the bank where he received his pension salary. However, some elderly said they experienced anxiety and worry when they received fraudulent messages with no one around them to ask because they didn't know how to respond to such messages, which are mainly family crisis messages, fraud under the guise of gifts, and link messages containing malware or viruses.

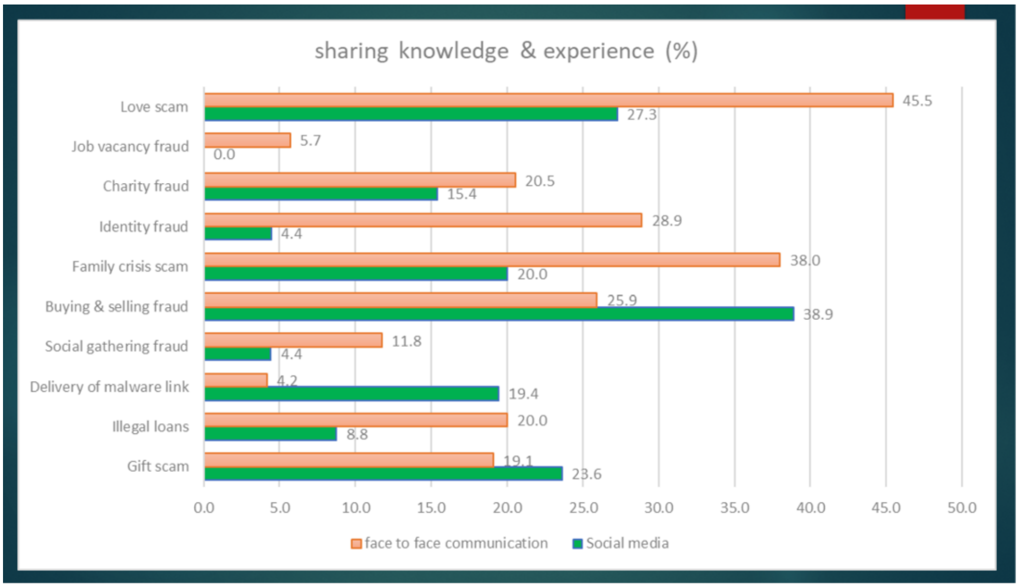


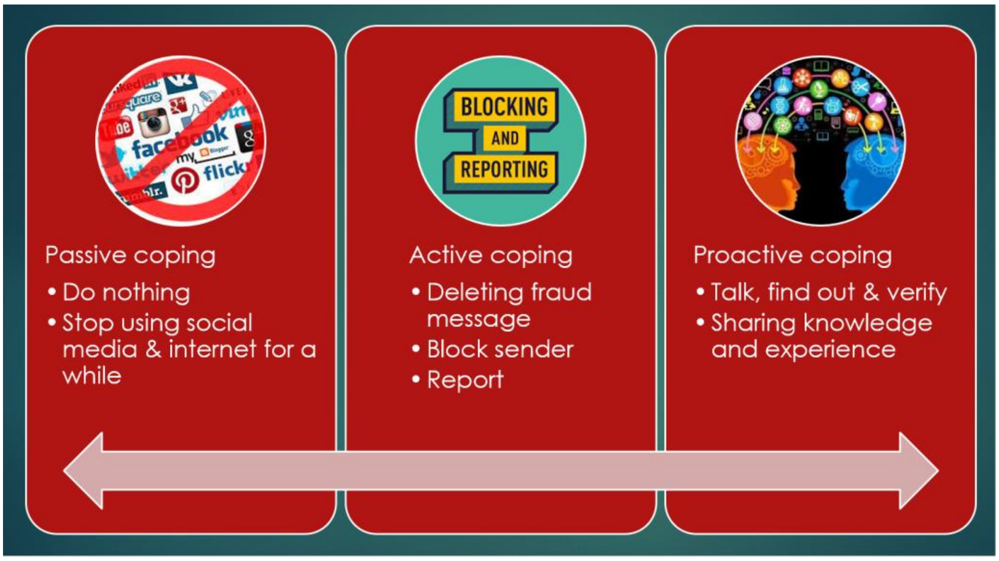
Figure 4. Graph of Percentage of Sharing Knowledge and Experience of elderly and pre-elderly regarding online fraud
Source: Analysis of survey data on online fraud received by the elderly and pre-elderly in Kendari 2023

It was found that 37.8% of the pre-elderly and elderly had the willingness and ability to share knowledge and experience regarding online fraud through conversation applications and direct communication in the form of face-to-face conversations, although in a limited scope.

Sharing knowledge and experiences regarding online fraud aims to educate the people around them. According to Figure 4, elderly and pre-elderly more often share their experiences and knowledge about fraud under the guise of romance 45.5%, family crises fraud 38%, personal identity theft 28.9%, charity fraud 20.5%, and illegal online loans fraud 20% through direct communication with the people around them (family, relatives and friends). However, they also share it via WhatsApp application. However, in this conversation application, the elderly and pre-elderly tend to share more knowledge and experience regarding buying and selling fraud 38.9%, fake links containing malware/viruses 19.4%, and fraud under the guise of gifts 21.6%. Although experiences of fraud under the guise of romance are mostly shared through face-to-face communication, 27.3% also share them via WhatsApp.

The response of the elderly and pre-elderly who want to tell the problem, to do research, and to verify the fraudulent messages they receive is measurable communication behavior. Meanwhile, the actions of the elderly and pre-elderly in sharing knowledge and experiences are educational efforts. Both communication and education are proactive responses. Proactivity is action that is more active and braver in taking the initiative to do something. Telling problem, finding out and verifying the right sources is one way to get a solution when you find fraudulent content online. Telling the problem to the people closest to you and the right people can help find alternative opinions, suggestions and input that provide solutions. In the online resilience framework [12], it is stated that individuals need to recognize and manage the risks they face when socializing, browsing or working online, and this can be done by confiding in other people they trust.

The various data presented above show four methods used by the elderly and pre-elderly in dealing with online fraud, consisting of passive methods by not doing anything and stopping for a moment in using social media and the internet, active methods by deleting messages, blocking the number and account of the message sender/post spreader, and reporting it, communication by telling problems, finding out and verifying, and education by sharing experiences and knowledge with others. According to d'Haenens et al. [7], this method is called coping strategy, where a person has thoughts and behavior to adapt to disturbing situations. This strategy is an effort to become online resilient. However, the findings of this study are different from those of d'Haenens et al. [7], which only created three categories of coping, namely fatalistic or passive coping, communication coping, and overcoming or proactive coping. The coping used by the elderly and pre-elderly is not just to remain silent and let the problem of fraud resolve itself but also to take action against fraud by cutting off access so as not to connect with fraudsters, deleting messages, and reporting them as a solution to dealing with online fraud. Some of them also actively build communication with people around them when they find or receive fraudulent messages. Some elderly and pre-elderly have shown good online resilience skills by participating in educating people in their environment to prevent victims of online fraud.



Passive coping

- Do nothing
- Stop using social media & internet for a while

Active coping

- Deleting fraud message
- Block sender
- Report

Proactive coping

- Talk, find out & verify
- Sharing knowledge and experience

Figure 5. Coping strategies in online resilience of the elderly and pre-elderly

This research shows that the elderly and pre-elderly have active and proactive behavior. One of the active and pro-active behaviors is formed by self-efficacy [7]. There are four dimensions of self-efficacy, which encourage the formation of active and pro-active behavior, including cognition, motivation, affection and selection [13]. Active response (deleting messages, blocking message senders, and reporting messages) and pro-active responses (communication and education) are driven by cognition to plan appropriate actions in dealing with online fraud and motivation to take action to resolve and stop the problem of online fraud that befalls him and the people around him.

Active responses (deleting messages and blocking message senders) are driven by affection, the desire to overcome negative emotions and feelings caused by fraudulent messages [8] [13], which is an aspect of emotional regulation and impulse control [13]. This can prevent them from being exposed to fraudulent messages. Meanwhile, pro-active communication response is an effort to identify fraudulent messages so that it is easy to make decisions in responding to online fraud. This aspect of causal analysis [8] is also a way to learn to protect yourself when receiving similar negative messages in cyberspace.

Pro-active communication response aims to choose the right behavior and decisions in responding to online fraud. Suggestions from other people, the results of finding out and verification will help choose the right action. Apart from that, choosing to carry out education is considered a further action to achieve the goal.

Sharing knowledge and experiences with others for educational purposes shows that some elderly and pre-elderly have self-efficacy in playing roles with pro-active responses. Self-efficacy is belief in one's own abilities [14], self-confidence, motivation, affection, and selectiveness to face and solve online crime problems [8] [13]. This is not only obtained through learning, but the main thing is subsequent experience reflected in online challenges [12]. Self-efficacy is an important aspect of online resilience, which is an individual's self-confidence to be able to face and solve crime problems [8].

Resilience against online fraud is the ability to control oneself, determine motivation, choose the right actions, successfully avoid and overcome the challenges of online fraud, and determinedly share knowledge and experience with the people around them. Resilience is demonstrated by successfully facing adversity and getting through it in an extraordinary way [15]. For the elderly and pre-elderly, achieving digital resilience is a challenge because digital resilience is a continuous process. First challenge is having knowledge about digital fraud and security but lacking skills in implementing digital security. Another challenge is the lack of opportunities and efforts to improve digital knowledge and skills. Digital resilience requires continuous efforts to keep up with and easily access technological innovations and digital security strategies. Unsupportive digital environment can also be a challenge. Family and people around them are digital technology users but do not have good digital literacy. The last challenge is low impulse control in dealing with fraud and several types of online crime.

4 Conclusion

Digital resilience of the elderly and pre-elderly requires a supporting ecosystem, primarily easy access to learning opportunities and increasing digital skills, humanistic communication using a peer- to-peer communication model, and people around who have digital skills and are good discussion partners.

Elderly and pre-elderly who have self-efficacy, or self-confidence that they can overcome the challenges they experience with online fraud, can develop digital resilience. As a result, there are three coping strategies that they can use to deal with online fraud: passive response (doing nothing and pausing from using social media), active response (deleting messages, blocking senders, and reporting), and pro-active response (communication and education). Active and pro-active responses are used in effective coping mechanisms. Only the elderly and pre-elderly who have self-efficacy—the self-confidence to take action to overcome problems—can perform these two responses.

The limited digital literacy of the elderly and pre-elderly in Kendari City encourages them to try to avoid and fight online fraud in ways considered the safest. However, within these limitations, some of them are able to carry out simple education by sharing their knowledge and experience with the people around them.

References

[1] M. Button and C. Cross, "Cyber Frauds, sCams and their ViCtims," 2017.

[2] P. K. Puram, M. Kaparthi, A. Krishna, and H. Rayaprolu, "ONLINE SCAMS: TAKING THE FUN OUT OF THE INTERNET," 2011.

[3] N. Kurnia -Rahayu -Engelbertus, W. Zainuddin, M. Z. Monggilo -Acniah, D. Dewa, A. Diah, and A.-F. Qurratu'ain Abisono, "MODUS, MEDIUM, DAN REKOMENDASI PENIPUAN DIGITAL DI INDONESIA," Yogyakarta, Aug. 2022.

[4] Admin Aptika, "Upaya Kominfo Berantas Aksi Penipuan Transaksi Online," *Direktorat Jenderal Aplikasi Informatika*, Sep. 15, 2022.

[5] Admin OJK, “Waspada Modus Penipuan Gaya Baru,” *https://www.ojk.go.id/ojk-institute/id/capacitybuilding/upcoming/2746/waspada-modus-penipuan-gaya-baru*, Sep. 15, 2023.

[6] A. K. Przybylski, A. Mishkin, V. Shotbolt, and S. Lininngton, “A shAred responsibility building children’s online resilience,” 2014. Accessed: Sep. 13, 2023. [Online]. Available: https://www.knowsleyclcs.org.uk/wp-content/uploads/2015/02/VM-Resilience-Report.pdf

[7] L. d’Haenens, S. Vandoninck, and V. Donoso, “How to cope and build online resilience?,” 2013. [Online]. Available: www.eukidsonline.net

[8] P. W. Widiarti, M. L. Endarwari, G. L. Adikara, A. L. Pradipta, and A. Sukmawati, “RESILIENSI (KETANGGUHAN DIRI) ONLINE SISWA SMP DITINJAU DARI GAYA KOMUNIKASI GURU DAN REGULASI MORAL SISWA PADA MASA PANDEMI COVID DI KOTA YOGYAKARTA,” Yogyakarta, May 2020. Accessed: Sep. 05, 2023. [Online]. Available: https://simppm.drpm.uny.ac.id/uploads/8636/laporan_akhir/laporan-akhir-8636-20201214-100838.pdf

[9] A. Tashakkori and C. Teddlie, *Mixed Methodology, Combining Qualitative and Quantitative Approaches*, vol. 46. Thousand Oaks London New Delhi: Sage Publications, 1998.

[10] M. Henn, M. Weinstein, and N. Foaerd, *A Short Introduction to Social Research*. Thousand Oaks London - New Delhi: Sage Publication, 2006.

[11] S. Kemp, “DIGITAL 2022: INDONESIA,” *https://datareportal.com/reports/digital-2022-indonesia*, Feb. 12, 2022.

[12] UK Council, “Digital Resilience Framework,” London, 2020. Accessed: Sep. 13, 2023. [Online]. Available: https://www.gov.uk/government/publications/digital-resilience-framework

[13] I. B. Weiner and Craighead W. Edward, Eds., *The Corsini Encyclopedia of Psychology, Volume 3, 4th Edition*, 4th ed., vol. 3. Oxford: John Wiley, 2010.

[14] D. Stipek and P. Byler, “Academic achievement and social behaviors associated with age of entry into kindergarten,” *J Appl Dev Psychol*, vol. 22, no. 2, pp. 175–189, Mar. 2001, doi: 10.1016/S0193-3973(01)00075-2.

[15] A. M. Pidgeon, N. F. Rowe, P. Stapleton, H. B. Magyar, and B. C. Y. Lo, “Examining Characteristics of Resilience among University Students: An International Study,” *Open J Soc Sci*, vol. 02, no. 11, pp. 14–22, 2014, doi: 10.4236/jss.2014.211003.