ZARAMUN 2026

“HUMANITAS V : RETROUVER NOTRE HUMANITÉ COMMUNE”

STUDY GUIDE

UNHRC

Protecting the elderly from online economic exploitation: strengthening digital safety and inclusion in aging societies

Eva Saix and Paula Cayuelas

COMMITTEE INTRODUCTION

The United Nations Human Rights Council (UNHRC) is charged with promoting and protecting human rights for all, particularly vulnerable populations. As the global population ages, the number of individuals over 60 is projected to reach 2.1 billion by 2050, creating new challenges in protecting their rights in increasingly digital societies. Older adults often face economic, social, and technological vulnerabilities that expose them to fraud, scams, and manipulation in digital spaces, particularly in contexts where financial and technological literacy is limited.

Digital transformation in financial, healthcare, and social sectors has created unprecedented opportunities but also new ways of exploitation. The rapid growth of online banking, e-commerce, telehealth, and social media has inadvertently increased the risk of online economic abuse, targeting savings, pensions, and personal information. Fraudulent schemes ranging from phishing and fake investment platforms to identity theft and ransomware attacks threaten the financial security and autonomy of elderly populations worldwide.

COMMITTEE OBJECTIVES

Delegates are tasked with addressing these challenges while balancing human rights, autonomy, and protection. The key objectives include:

- Protecting elderly populations from online economic exploitation through legislative, technological, and social measures.
- Promoting digital literacy and inclusion, ensuring seniors can participate safely in digital financial systems.
- Encouraging international cooperation, aligning cross-border regulation, law enforcement, and civil society interventions.
- Developing ethical frameworks, balancing protective measures with respect for autonomy, dignity, and civil liberties.

KEY TERMS

#1 ELDERLY

Elderly are individuals aged 60+. Their vulnerability arises from cognitive decline, social isolation, and limited exposure to digital technologies. Seniors may face barriers in adapting to online financial systems, creating susceptibility to exploitation.

#2 DIGITAL SAFETY

Digital safety are measures protecting individuals online. It includes cybersecurity practices, privacy protections, secure authentication, and awareness of online scams. Requires collaboration between governments, civil society, and private sector platforms.

#3 ONLINE FRAUD

Online fraud are deceptive online schemes for financial gain. It can be perpetrated via phishing, identity theft, investment fraud, tech support scams, or social engineering. Often exploits psychological manipulation and lack of digital literacy.

#4 ONLINE INCLUSION

Online inclusion is the access and participation in digital society. It ensures elderly individuals can engage in online banking, telehealth, e-government services, and social media without undue risk. Digital inclusion is critical for financial independence and social connectivity.

#5 CYBERSECURITY

Protection of digital systems and data

Requires governments, corporations, and individuals to implement secure practices, detect threats, and respond to breaches. Seniors may be particularly targeted due to perceived technical incompetence.

#6 FINANCIAL PROTECTION

Financial protection safeguards against economic harm. It includes consumer protection laws, banking regulations, and oversight mechanisms preventing unauthorized transactions. Often enforced through reporting systems and coordinated fraud prevention strategies.

#7 AUTONOMY

Autonomy is the freedom to make independent decisions. Elderly individuals should maintain control over financial and personal choices while being protected from exploitation. Balancing protection with autonomy is a core ethical and legal challenge.

#8 VULNERABILITY

Vulnerability is the susceptibility to harm. It stems from technological, cognitive, economic, and social factors. Seniors may be isolated, reliant on caregivers, or less aware of online risks.

#9 SCAMS

Scams are fraudulent schemes targeting victims. It includes advance-fee fraud, phishing, tech support scams, fake investment opportunities, and online romance scams. Scammers often exploit emotions such as fear, urgency, or desire for companionship.

#10 LEGISLATION

Legislation are laws and regulations. They are designed to criminalize exploitation, mandate protective measures, regulate platforms, and empower victims to seek redress. Legal frameworks must evolve alongside technological innovation.

#11 ACCESSIBILITY

Accessibility is the ease of using digital tools. It refers to platforms and services being usable for seniors, including those with physical impairments or limited technical experience. Accessibility ensures equitable participation while reducing exposure to scams.

GENERAL OVERVIEW

As populations age, elderly individuals increasingly depend on digital systems for financial transactions, healthcare, and social connection. This dependence intersects with rapid technological change, creating new avenues for exploitation. Online economic abuse may manifest as phishing scams, identity theft, or ransomware attacks, which can cause severe financial loss or social isolation. The global nature of online exploitation complicates enforcement.

Cybercriminals often operate across borders, using anonymity and sophisticated technological tools to evade detection. In addition, older adults in low- and middle-income countries may face compounded vulnerabilities due to limited digital infrastructure, lower literacy rates, and weak consumer protection mechanisms. Governments, NGOs, and the private sector are increasingly recognizing the need for coordinated strategies to protect elderly populations.

Policy interventions must combine legal protections, awareness campaigns, accessible technology, and cybersecurity infrastructure, while respecting the human rights and autonomy of seniors. This is particularly challenging as governments and corporations attempt to strike a balance between protection and empowerment, ensuring seniors can participate fully in digital society without being overprotected to the point of social or financial restriction.

KEY ISSUES

#1 LEGAL AND INSTITUTIONAL RESPONSIBILITY

States bear primary responsibility for protecting elderly citizens from online economic abuse. Many countries, however, lack elder-specific cybersecurity and fraud legislation, leaving gaps in enforcement. Key challenges include:

- Harmonizing cross-border law enforcement to address transnational scams.
- Holding digital platforms accountable for hosting fraudulent activities.
- Ensuring timely victim support, including reporting systems, restitution mechanisms, and digital literacy programs.

#2 DIGITAL INCLUSION AND LITERACY

Older adults often face barriers in understanding or navigating online systems, leaving them vulnerable to scams. Digital literacy initiatives workshops, accessible guides, and community programs can empower seniors while mitigating risk. Countries with successful inclusion programs, such as Japan, South Korea, and Canada, demonstrate measurable reductions in fraud exposure.

#3 BALANCING AUTONOMY AND PROTECTION

A key ethical and policy challenge is safeguarding seniors without undermining autonomy. Excessive intervention, such as mandatory bank freezes, may infringe on individual freedoms. Conversely, insufficient measures leave seniors exposed to scams, often leading to catastrophic financial and psychological consequences.

#4 ETHICAL AND SOCIETAL DILEMMAS

- Platform Responsibility: Should tech companies be legally obligated to implement senior-specific fraud detection measures?
- Government Intervention: To what extent can governments monitor online behavior without infringing privacy rights?
- Resource Allocation: How should resources for awareness, cybersecurity, and victim support be prioritized among different vulnerable populations?

LEGAL FRAMEWORKS & EXISTING INTERNATIONAL AGREEMENTS

UNITED NATIONS GUIDELINES

- UN Principles for Older Persons (1991):

Articles 1–18 emphasize autonomy, participation, and protection against abuse, including economic exploitation.

- Universal Declaration of Human Rights (UDHR):

Articles 3 and 25 provide the basis for protecting seniors' security and economic well-being.

HUMAN RIGHTS TREATIES

- International Covenant on Economic, Social and Cultural Rights (ICESCR):

Guarantees financial security and access to essential resources.

- Convention on the Rights of Persons with Disabilities (CRPD):

Emphasizes digital accessibility, which is relevant to elderly persons with impairments.

REGIONAL AND NATIONAL INITIATIVES

- European Union:

GDPR provides protections against data misuse, while the EU Digital Strategy promotes inclusion.

- Australia:

Elder fraud reporting and digital literacy programs for seniors.

- Canada:

National Strategy for Financial Literacy for Seniors includes collaborative initiatives with banks and NGOs.

ROLES OF MAJOR COUNTRIES AND STAKEHOLDERS

SOURCE AND TRANSIT COUNTRIES

- China, India, Brazil: Some online scams originate from these countries due to high digital connectivity paired with limited oversight.

- Low-income countries: Often lack infrastructure for reporting or tracking cybercrime, leaving seniors especially vulnerable.

DESTINATION COUNTRIES

- United States, Germany, UK: Major financial hubs with high elderly internet usage; face challenges in monitoring transactions across borders.

CIVIL SOCIETY AND NGOS

- HelpAge International, AARP: Provide education, awareness campaigns, and advocacy for elder protection.

- Transparency International: Monitors platforms and governments for gaps in protection.

INTERGOVERNMENTAL ORGANIZATIONS

- OECD: Publishes guidance for consumer protection and digital literacy initiatives.

- UNHRC: Monitors violations and encourages cooperation between states to prevent elder abuse online.

CRISIS SCENARIO

A transnational online scam targets elderly citizens across multiple continents, using fake pension notifications and fraudulent bank communications. Thousands report financial losses within days, overwhelming banking institutions. Delegates must coordinate an immediate response, including:

- Cross-border information sharing and law enforcement collaboration.

- Emergency victim support, including freezing fraudulent transactions and reimbursement programs.

- Long-term preventive strategies such as awareness campaigns, digital literacy programs, and platform regulations.

ASPECTS TO CONSIDER

AUTONOMY VS SAFETY

- Should banks intervene in transactions suspected of fraud, potentially restricting the elderly's financial autonomy?

AGE-SPECIFIC PROFILING

- Is monitoring by age discriminatory, or is it justified to protect vulnerable populations?

PLATFORM RESPONSIBILITY

- Should private companies be legally mandated to prevent elder exploitation online?

RESOURCE ALLOCATION

- How should funding for digital literacy and cybersecurity programs for older adults be prioritized?

DIGITAL LITERACY GAPS

- How should societies address inequalities in digital skills that make older adults more vulnerable to scams?

PRIVACY VS SURVEILLANCE

- To what extent should monitoring tools track online activity to prevent fraud without infringing on personal privacy?

LEGAL REMEDIES AND ACCESS TO JUSTICE

- Are existing legal frameworks sufficient to protect elderly victims of online scams, and how accessible is recourse for them?

EMERGING THREATS

- How should policy adapt to new scams (AI-driven fraud, deepfakes, phishing) targeting older adults specifically?

INTERGENERATIONAL RESPONSIBILITY

- What role should family members or caregivers play in supervising online financial activities, and how can support be balanced with respect for the elder's independence?

TECHNOLOGICAL BARRIERS

- How do usability issues and poorly designed interfaces affect older adults' ability to safely use online financial services?

CASE STUDIES

PHISHING SCAMS IN EUROPE

In countries like Germany and Italy, phishing scams have increasingly targeted older adults by impersonating government agencies, health insurers, or public health programs. Scammers use emails, SMS messages, and phone calls to trick victims into providing personal information, banking details, or clicking malicious links, often under the guise of tax refunds, pension adjustments, or health updates. These scams exploit trust in official institutions and disproportionately affect vulnerable populations.

Efforts to counter these scams rely on collaboration between government bodies, consumer protection groups, and cybersecurity NGOs. Initiatives include public awareness campaigns, streamlined reporting systems, and rapid takedown of fraudulent websites. These coordinated actions have led to a reported 15% decline in phishing incidents over the past three years, demonstrating the effectiveness of cross-sector cooperation and targeted education, particularly for protecting older adults.

FINANCIAL FRAUD IN NORTH AMERICA

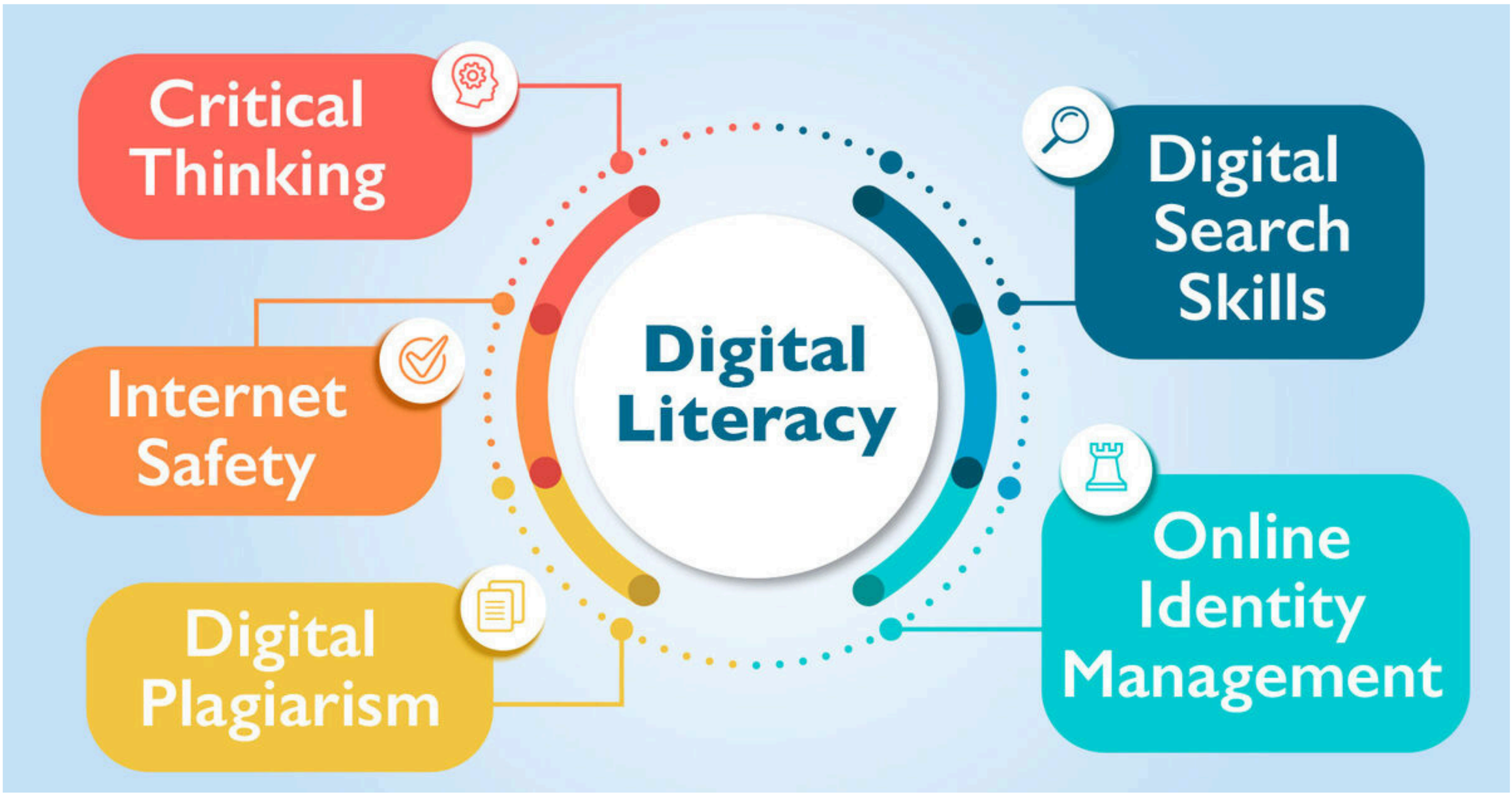
In the U.S. and Canada, online investment fraud has become a major threat, particularly to seniors. Scammers pose as financial advisors or legitimate investment platforms to promote fake cryptocurrency schemes, high-yield bonds, or retirement opportunities, exploiting trust and limited digital familiarity. Victims often suffer substantial financial losses due to these manipulative tactics.

Banks and financial institutions have responded with proactive measures such as behavioral analytics to detect suspicious transactions, temporary transaction holds, and direct customer verification. Institutions also provide victim support services and collaborate with law enforcement to track emerging fraud patterns. These steps have improved early detection and recovery, underscoring the importance of institutional accountability and coordinated responses in tackling large-scale financial fraud.

DIGITAL LITERACY PROGRAMS IN ASIA

In Japan and South Korea, governments focus on preventing fraud through digital literacy programs targeted at seniors. Recognizing that limited digital confidence increases vulnerability, these programs teach practical skills such as identifying phishing attempts, verifying information online, using secure payments, and managing privacy settings.

Community centers, libraries, and local governments host hands-on workshops supported by volunteers, tech companies, and younger digital mentors. Training is tailored to real-world scenarios like online banking, e-commerce, and e-government services. By empowering seniors with digital competence, these programs aim to reduce fraud risk and build long-term resilience against online threats.



FURTHER RESOURCES

- UN PRINCIPLES FOR OLDER PERSONS
- OECD DIGITAL SECURITY FOR SENIORS
- AARP FRAUD WATCH NETWORK
- HELPAGE INTERNATIONAL
- UNHRC REPORTS ON HUMAN RIGHTS OF OLDER PERSONS