

KA210-ADU Small-Scale Partnership in Adult Education

Empowering Adults: Digital Safety and Fraud Prevention in the Age of Technology | digiSAFE



Project Number:

2025-1-IT02-KA210-ADU-000359787

Transnational Report

Project acronym	digiSAFE
Project title	Empowering Adults: Digital Safety and Fraud Prevention in the Age of Technology
Project number	2025-1-IT02-KA210-ADU-000359787
Duration	Start date: 01-09-2025 End date: 31-08-2027
Sub programme	Small-Scale Partnership in Adult Education
Project website	www.digisafeproject.eu
Date of Delivery	
Status	Version 1.0
Author	UNO
Responsible Author	

Table of Content

1. Introduction.....	4
2. Methodology.....	5
3. National Context.....	6
4. Best Practices.....	15
6. Transnational Analysis.....	52
7. Key Findings.....	56
8. Identified Gaps and Training Needs.....	57
9. Recommendations for Curriculum Development.....	59
10. Conclusion.....	62
Bibliography / References.....	63

1. Introduction

The digiSAFE project – "Empowering Adults: Digital Safety and Fraud Prevention in the Age of Technology" – is an Erasmus+ Small-Scale Partnership in Adult Education (KA210-ADU, Grant Agreement No. 2025-1-IT02-KA210-ADU-000359787) implemented by a transnational consortium comprising three partner organisations: Associazione Italiana Socio-Educatori per la Cooperazione – AISEC APS (Italy, project coordinator), Asociación UNO (Spain), and IKREON (Slovakia). The project runs from 1 September 2025 to 31 August 2027.

Digital transformation is reshaping virtually every aspect of daily life across Europe, from how citizens access public services and manage personal finances to how they communicate and consume information. While digitalisation brings undeniable opportunities, it also generates new and rapidly evolving risks, particularly online fraud, cybercrime, misinformation, and data breaches. Adults aged 45 and over are disproportionately affected by these risks, as they frequently combine high levels of digital engagement with limited cybersecurity awareness and insufficient access to targeted digital safety training.

The digiSAFE project was conceived to address this gap directly. Its core outputs are a Non-Formal Education (NFE) Curriculum focused on digital safety and fraud prevention, and a practical Digital Fraud Prevention Toolkit, both specifically designed for adults aged 45+. To ground these outputs in evidence, the project's first phase involved comprehensive national research across all three partner countries. This Transnational Report synthesises and compares the findings from those national research efforts and represents the main output of Activity A1 (needs assessment phase), providing the evidence base for the development of the curriculum and toolkit.

The present document aims to consolidate and analyse the national research results from Italy, Spain, and Slovakia, and to compare findings across the three countries in order to identify common trends, significant differences, and transnational patterns. It further seeks to identify the specific learning gaps and training needs of adults aged 45+ in relation to digital safety, online fraud prevention, and cybersecurity awareness, while also providing evidence-based recommendations to inform the design of the digiSAFE NFE Curriculum and Digital Fraud Prevention Toolkit.

The primary target group addressed throughout this report consists of adults aged 45 and over, with a particular focus on individuals with low to medium levels of digital skills who are more vulnerable to online risks. This group is increasingly active in digital environments but often lacks the necessary competencies, confidence, and awareness to navigate them safely and autonomously.

In this context, the report aligns with key Erasmus+ and broader European Union priorities, particularly those related to digital transformation, social inclusion, and lifelong learning, by supporting the development of inclusive and accessible educational approaches for adult learners.

2. Methodology

The research underpinning this Transnational Report was conducted simultaneously across all three partner countries during the first phase of the digiSAFE project (late 2025 – early 2026). A shared, harmonised methodology was adopted to ensure the comparability of data and findings across national contexts. This methodology was based on a common research framework developed at project level, with the lead partner of Activity A1 (Asociación UNO) responsible for preparing the research guidelines, which were consistently applied by all partners across the three countries. The research combined two complementary approaches: desk research and a quantitative self-assessment survey.

2.1 Desk Research

Each national partner conducted an extensive review of secondary sources, including official statistical data, national policy documents, legislative instruments, European Commission reports, and academic and grey literature, selected based on their relevance and reliability in line with the research guidelines. In addition to mapping the macro-level national context, partners also identified a set of national best practices to inform the development of the project outputs. The desk research aimed to provide a comprehensive overview of each country, including the current state of digital literacy among adults aged 45+, existing regulatory frameworks governing data protection and cybersecurity, and active programmes or initiatives promoting adult digital education and online safety. The sources used are documented in the national reports and consolidated in the bibliography section of this document.

2.2 Self-Assessment Survey

A standardised quantitative self-assessment questionnaire was administered to adults aged 45 and over in each partner country. The same questionnaire was used across all countries to ensure the comparability of results. The instrument used a combination of 5-point scales and multiple-choice questions to assess participants' daily digital habits, self-perceived confidence in online environments, specific digital safety skills, awareness of various types of online threats, direct experience with digital fraud, and perceived training needs. The primary purpose of the survey was to identify digital competencies, levels of risk awareness, and training needs among adults aged 45+.

The survey was distributed online through each partner's networks, using communication channels tailored to reach the target demographic. Data collection took place on a voluntary and fully anonymous basis, in compliance with the General Data Protection Regulation (GDPR). A minimum target of at least 50 valid responses per country, as defined in the project proposal, was established to ensure the reliability of the data and the comparability of results across the three national contexts.

2.3 Participants

Survey data were collected across the three partner countries, with each country contributing a comparable sample size, ensuring a balanced basis for cross-national analysis. In all three samples, women constituted the majority of respondents. Age distribution was concentrated in the 45–54 and 55–64 brackets, with a smaller representation of respondents aged 65 and over. Participants came from a mix of urban, semi-urban, and rural contexts, and displayed diverse educational and employment backgrounds, including employed adults, self-employed individuals, and retired persons. Overall, the sample reflects a diverse group of adults aged 45+, enhancing the relevance and representativeness of the findings.

2.4 Data Analysis

National datasets were analysed independently by each partner using descriptive statistical methods. The analysis focused on frequencies, distributions of responses, and the identification of recurring patterns within each national sample. In particular, partners examined key variables such as levels of digital use, self-perceived confidence, awareness of online risks, experiences with digital fraud, and expressed training needs.

To ensure consistency, a common analytical approach was followed across all countries, allowing for a structured comparison of results. The findings were then examined transnationally through cross-country comparisons, highlighting both similarities and differences in participants' behaviours, perceptions, and vulnerabilities. Particular attention was given to identifying patterns that are relevant for the design of educational interventions, including areas of shared need as well as country-specific challenges.

The present report synthesises these analyses and draws transnational conclusions based on the combined evidence, providing a coherent foundation for the development of the digiSAFE curriculum and toolkit.

3. National Context

This section provides a comparative overview of the digital landscape for adults aged 45+ in each partner country. For each country, the analysis covers the current state of digital

literacy, main challenges faced by the target group, relevant national regulations and policies, and existing programmes and initiatives.

3.1 Italy

Digital Literacy and Main Challenges

Italy presents a notable paradox: while significant progress has been made in digital infrastructure and the roll-out of digital public services, structural gaps in citizens' digital competencies persist, particularly among older adults. According to the European Commission's Digital Decade Country Report 2025, Italy has made advances in connectivity and e-government; however, critical challenges remain in citizens' ability to effectively and safely use digital technologies.

Data from ISTAT confirm this dual trend. In 2024, 86.2% of Italian households had internet access, yet this figure drops to 60.6% among households composed exclusively of elderly individuals. Internet usage varies significantly by age: while 81.9% of the total population aged 6 and over used the internet in the previous three months, only 68.1% of those aged 65–74 did so. Regional disparities further compound this picture, with southern regions lagging behind central and northern Italy in both access and usage.

Digital skill levels among older adults remain a critical concern. In 2023, only 45.9% of individuals aged 16–74 who used the internet possessed at least basic digital skills. The proportion falls to 48.7% among those aged 45–54, 38.5% among those aged 55–64, and a mere 19.3% among those aged 65–74. As a result, many adults in the 45+ group encounter difficulties in independently accessing digital services, evaluating online information, and protecting themselves from online risks.

Online fraud and cybercrime represent a growing and concrete concern. ISTAT estimates that approximately 1.7 million individuals – corresponding to 3.3% of internet users – experienced online fraud or scams in the 12 months preceding the 2022–2023 survey. Cases of financial fraud through online banking increased by 74% compared to 2015–2016. In 2024, the Commissariato di PS Online platform recorded around 3 million visits, over 82,000 reports, and approximately 23,000 requests for assistance related to phishing and online scams.

These data indicate that for adults aged 45+, the issue is no longer access alone but the quality and autonomy of digital use.

National Regulations and Policies

Italy has developed a comprehensive regulatory and policy framework for digital safety. Data protection is governed by the GDPR (EU 2016/679), implemented nationally through Legislative Decree No. 196/2003 as amended, with oversight provided by the Italian Data

Protection Authority (Garante per la protezione dei dati personali). The Digital Administration Code establishes citizens' digital rights in interactions with public administrations, while the Agency for Digital Italy (AgID) promotes digital citizenship and violation reporting. Cybersecurity is coordinated through the National Cybersecurity Strategy 2022–2026, managed by the National Cybersecurity Agency (ACN). Italy has also transposed the NIS2 Directive through Legislative Decree No. 138/2024 and implemented the Digital Operational Resilience Act (DORA) in the financial sector.

Existing Programmes and Initiatives

Alongside regulatory measures, Italy has developed a wide range of programmes and initiatives to support digital inclusion and education among adults. A central role is played by Repubblica Digitale, a national initiative led by the Department for Digital Transformation, which coordinates the National Strategy for Digital Skills and promotes collaboration among public institutions, private sector actors, and civil society organisations. Within this framework, the Digital Facilitation Network aims to reach two million citizens by 2026 through 4,000 physical access points (Punti Digitale Facile), providing support in accessing digital services and improving online safety.

Additional initiatives include the Servizio Civile Digitale and targeted funding programmes such as Dritti al Punto, which support training activities focused on cybersecurity awareness, critical use of information, and safe access to public digital services. In parallel, labour market policies such as the GOL Programme (Garanzia di Occupabilità dei Lavoratori) aim to involve three million beneficiaries, with a strong emphasis on digital skills development.

Adult education is further supported by the Centres for Adult Education (CPIA), which serve as key territorial hubs for lifelong learning. These centres provide both formal and non-formal education opportunities and play a crucial role in reaching vulnerable groups, including older adults with low levels of education or digital skills. Their function is embedded within broader policies promoting lifelong learning and skills development across the population.

Finally, a wide range of institutional and sectoral actors contribute to raising awareness and promoting safe online behaviour. The Agency for Digital Italy (AgID) and the National Cybersecurity Agency (ACN) support the dissemination of digital and cybersecurity skills, while the Postal Police provides prevention and assistance services. The Data Protection Authority promotes awareness of privacy rights, and financial institutions such as the Bank of Italy, together with initiatives like I Navigati, contribute to educating citizens about online fraud and financial cybersecurity risks.

Overall, the Italian context highlights a significant gap between the rapid digitalisation of services and the actual capacity of adults (particularly those aged 45 and over) to use these tools safely and effectively. While the regulatory and institutional framework is well

developed, the key challenge remains ensuring that all citizens, especially older adults, acquire the necessary skills to participate fully and securely in the digital society.

3.2 Spain

Digital Literacy and Main Challenges

Spain has experienced rapid digital transformation over the past decade, reshaping the ways in which citizens interact with public services, financial institutions, healthcare systems, and communication platforms. The widespread adoption of online banking, e-government platforms, digital health services, and social media has significantly increased digital connectivity across the population, improving both accessibility and administrative efficiency.

However, despite this overall progress, a persistent digital divide remains in Spain. This divide is strongly associated with age, educational background, and socio-economic conditions. Adults aged 45 and over, and particularly those above 55, tend to report lower levels of digital confidence and more limited familiarity with digital security practices. Many individuals in this age group did not acquire digital skills during their formal education or professional careers, which makes adaptation to rapidly evolving digital environments more complex and often slower.

This generational gap is further reflected in patterns of digital use and exposure to online risks. Online fraud and cybercrime represent an increasingly significant concern in the Spanish context. Common threats include phishing emails, fraudulent SMS messages, identity theft, fake online services, and financial scams. Adults aged 45+ are particularly vulnerable, as they often combine regular use of digital services (such as online banking, messaging applications, and e-commerce) with lower awareness of cybersecurity risks and preventive practices. In addition, the growing sophistication of social engineering techniques, including the use of AI-supported fraud mechanisms, is further intensifying these vulnerabilities and making detection more difficult for less experienced users.

At the institutional level, Spain has developed a range of national strategies addressing digital transformation, cybersecurity, and digital inclusion. These policy frameworks aim to strengthen citizens' digital competences, improve data protection mechanisms, and promote safer and more responsible engagement with digital technologies. Alongside these national strategies, public institutions, regional governments, and civil society organisations have implemented various training programmes and awareness-raising initiatives targeting adult digital literacy and online safety.

Nevertheless, existing initiatives remain fragmented and unevenly distributed across regions. Moreover, many programmes tend to prioritise basic digital skills acquisition,

while giving less attention to digital safety, fraud prevention, and critical awareness of online risks. This gap highlights the need for more structured, accessible, and targeted educational interventions specifically designed to enhance digital resilience among adults aged 45 and above.

In this context, the digiSAFE project responds directly to these challenges by combining research, non-formal education, and practical tools aimed at strengthening online safety competences and supporting safer participation in the digital society.

National Regulations and Policies

Spain's response to digital safety and fraud prevention is framed within a multi-level governance system that combines national legislation with broader strategic policy frameworks aimed at fostering digital transformation and inclusion. In recent years, the Spanish government has increasingly complemented regulatory approaches with comprehensive national strategies designed to reduce digital inequalities and strengthen citizens' digital capabilities, particularly among vulnerable groups such as adults aged 45 and over.

A key pillar of this approach is the national strategy Digital Spain 2026, which acts as the main roadmap for the country's digital transformation. This strategy promotes economic growth, social cohesion, and territorial inclusion through digitalisation, while explicitly addressing existing digital divides related to age, gender, and geography. Among its priorities are the expansion of digital infrastructure, the promotion of emerging technologies, and the strengthening of citizens' digital skills as a means to ensure that no group is left behind in the digital transition.

Within this framework, the National Digital Skills Plan (Plan Nacional de Competencias Digitales) plays a central role in promoting digital inclusion. It aims to equip citizens, workers, and public administrations with the necessary skills to operate in an increasingly digital society. The plan specifically targets structural gaps in digital literacy, which still affect a significant share of the population, particularly older adults and other vulnerable groups. Its measures include large-scale training programmes, reskilling initiatives, and actions to reduce gender and territorial inequalities in access to digital competencies.

In addition, programmes such as the UNICO Broadband initiative aim to expand high-speed internet access in rural and underserved areas, reducing territorial disparities and ensuring more equitable access to digital services across the country. These initiatives highlight the importance of addressing not only individual skills but also structural conditions of access, such as connectivity.

These strategic initiatives are embedded within the broader Recovery, Transformation and Resilience Plan, which integrates digitalisation as a core pillar for economic and social development. Through coordinated investments and reforms, Spain seeks not only to

modernise its economy but also to ensure inclusive access to digital technologies and services across the entire population.

Alongside these strategic frameworks, Spain has developed a solid legal structure addressing digital safety. The core legal framework is established by Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDgdd), which implements the General Data Protection Regulation (GDPR) into the Spanish legal system. These instruments regulate the processing and protection of personal data while recognising digital rights as fundamental rights. However, awareness and effective understanding of these rights remain uneven, particularly among older users who increasingly rely on digital services.

In the field of cybersecurity, Royal Decree-Law 12/2018 and Royal Decree 43/2021 transpose European cybersecurity requirements into national law, strengthening Spain's institutional capacity in managing digital risks. Similarly, online fraud is addressed through the Spanish Penal Code (Organic Law 10/1995), which criminalises a wide range of cyber offences, including phishing and identity theft. Nevertheless, the growing sophistication of digital fraud highlights the need for complementary measures focused on prevention and user awareness.

Consumer protection and platform regulation further reinforce this framework through instruments such as Royal Legislative Decree 1/2007 and Law 34/2002 (LSSI), aligned with European developments such as the Digital Services Act. These regulations enhance transparency, accountability, and user protection in digital environments.

Finally, the rapid expansion of digital public services has been accompanied by initiatives such as the Digitalisation Plan for Public Administrations, which aims to improve accessibility, efficiency, and user experience in interactions with public institutions. However, while these developments represent significant progress, they may also unintentionally reinforce existing inequalities if not accompanied by adequate digital literacy measures. In particular, older adults with limited digital skills may face additional barriers when accessing essential services that are increasingly available primarily online.

Overall, Spain combines a comprehensive legal framework with an increasingly robust set of national strategies aimed at digital transformation and inclusion. However, a significant gap remains between the existence of these policies and their effective impact on citizens' everyday digital practices. In particular, adults aged 45 and over often lack the necessary knowledge and skills to fully benefit from these measures. This gap highlights the importance of educational and awareness-raising initiatives such as digiSAFE, which translate regulatory and strategic frameworks into practical knowledge and everyday competencies.

Existing Programmes and Initiatives

In Spain, several initiatives address digital inclusion among older adults, particularly within the framework of national programmes aimed at improving digital competences across the population. Public initiatives promoted by the Spanish Government, as well as local programmes implemented by municipalities, NGOs, and adult education centres, provide basic digital literacy training for older citizens, focusing on the use of smartphones, internet navigation, and access to digital public services. For example, programmes such as digital training workshops offered in public libraries and community centres provide hands-on support to older adults in learning how to use mobile applications and access e-government platforms. In addition, initiatives promoted within the framework of the National Digital Skills Plan include basic courses aimed at improving digital autonomy among older citizens. Similarly, non-governmental organisations often organise introductory sessions focused on everyday digital tasks, such as online banking or booking medical appointments, reinforcing practical engagement with digital tools.

However, these initiatives tend to prioritise general digital inclusion rather than digital safety. Training activities often focus on how to use digital tools, with limited attention to the risks associated with online environments, such as fraud, phishing, or emerging AI-based scams. In Spain, a key role is played by the Instituto Nacional de Ciberseguridad (INCIBE), which acts as a national reference point for cybersecurity. This public institution provides awareness campaigns, educational resources, and support services aimed at preventing cyber threats and assisting citizens in responding to digital risks. However, despite the important role played by INCIBE, these initiatives are generally designed for the broader population and do not specifically target adults aged 45+ through structured and continuous learning pathways.

Overall, although Spain has developed a comprehensive national framework for digital inclusion and cybersecurity, as outlined in section 1.2, its practical implementation remains uneven. Differences in access to training, levels of digital literacy, and the lack of targeted programmes for specific age groups limit the effectiveness of these policies. This gap between regulatory frameworks and practical outcomes highlights the need for more inclusive and tailored approaches. As a result, a significant gap persists between digital inclusion efforts and the development of practical skills for fraud prevention among older adults. This highlights the need for targeted educational approaches that combine digital literacy with hands-on training in recognising and responding to online threats. In this context, digiSAFE directly addresses this gap by offering a tailored, scenario-based learning model specifically designed for adults aged 45 and over.

3.3 Slovakia

Digital Literacy and Main Challenges

The Slovak Republic faces a distinctive challenge: while digital infrastructure and connectivity have improved considerably, the human capital required to navigate digital environments securely remains significantly underdeveloped, particularly among the older population. According to the European Commission's 2024 Digital Decade Country Report, Slovakia has achieved a basic digital skills coverage of 51.3% – a slight decline from previous measurements and below the EU average of 55.6%.

The disparities are particularly severe among older demographic cohorts. Among Slovak seniors aged 65–74, only 11% possess basic or above-basic digital skills – less than half the EU average of 24% for the same age group. Furthermore, 27% of seniors in this age group have never used the internet, and only 39% have used a computer within the previous twelve months. For adults aged 45–64, digital skills are frequently limited to routine operations, lacking the critical depth and analytical frameworks required to navigate evolving cybersecurity threats.

Slovakia faces specific and severe fraud typologies. A highly prevalent tactic involves fraudsters impersonating police officers, bank security employees, or representatives of the National Bank of Slovakia, exploiting number spoofing technology to manipulate caller ID displays and employing fear-based tactics to extract banking credentials or coerce victims into transferring funds to fraudulent accounts. In addition, the Slovak digital space is heavily exposed to misinformation and disinformation campaigns linked to geopolitical positioning and domestic political polarisation.

National Regulations and Policies

To protect citizens' digital rights and counter cyber threats, the Slovak Republic has developed a regulatory framework strictly aligned with European Union directives. The foundation of data protection in Slovakia is the General Data Protection Regulation (GDPR), integrated into national law through Act No. 18/2018 Coll. on the Protection of Personal Data. Effective since May 2018, this legislation establishes clear guidelines for the lawful processing of personal data, mandating transparency, data minimization, and purpose limitation. It guarantees citizens the right to access, rectify, and erase their data, alongside protection against unauthorized automated decision-making.

The Office for Personal Data Protection of the Slovak Republic (ÚOOÚ) oversees these regulations. As an independent supervisory authority, the ÚOOÚ ensures compliance across public and private sectors. It also provides binding guidance on complex data protection issues, such as conducting Data Protection Impact Assessments. Notably, Slovak law strictly regulates the use of the national birth number (rodné číslo). Public disclosure of this identifier is prohibited unless explicitly authorized by the individual or mandated by specific legislation, which serves as a critical measure to prevent identity theft.

Regarding cybersecurity, the primary legislative tool is Act No. 69/2018 Coll. on Cybersecurity, which originally transposed the European NIS Directive. This act established the baseline for national cybersecurity governance, defining the legal obligations of essential service operators, incident reporting requirements, and audit procedures. To address evolving threats, Slovakia updated this framework to meet the advanced requirements of the NIS2 Directive (Directive (EU) 2022/2555). Through Act No. 366/2024 Coll., effective January 1, 2025, Slovakia significantly expanded the scope of its cybersecurity regulations. The amendment introduces a precise mechanism for identifying obliged entities, capturing a broader range of critical sectors, and enforces stricter security measures.

The National Security Authority (NBÚ) coordinates these legislative efforts through the National Cybersecurity Strategy 2021–2025. The strategy outlines priorities including ensuring state readiness, detecting cybercrime, building a resilient private sector, integrating cybersecurity into public administration, and advancing the digital skills of both professionals and the general public. This emphasis on public education highlights that technical defenses must be directly supported by citizen awareness and individual digital resilience.

Existing Programmes and Initiatives

The implementation of Slovakia's digital strategy relies on collaboration between public institutions, NGOs, law enforcement, and the private sector to bridge the digital divide and enhance online safety for adults.

The Ministry of Investments, Regional Development and Informatization (MIRRI) leads these efforts, managing key components of the national Recovery and Resilience Plan. Its flagship initiative, "Digitálni seniori" (Digital Seniors), aims to provide digital skills training to over 100,000 seniors (aged 65+) and disadvantaged individuals by 2026. The program delivers localized training sessions and provides graduates with a configured tablet and a mobile data package, directly addressing both educational and hardware barriers.

In the realm of security, the National Security Authority (NBÚ) and the National Cyber Security Centre (SK-CERT) manage technical cybersecurity and national incident response while also contributing to public awareness campaigns. Additionally, the Police Force of the Slovak Republic actively combats digital fraud and disinformation. Through its dedicated public communication channel, "Hoaxy a podvody – Polícia SR" (Hoaxes and Scams), the police monitor the digital space, debunk viral hoaxes, alert citizens to emerging financial scams, and educate the public on identifying fraudulent communications.

Cross-sector collaboration is formalized through the Digital Coalition (Digitálna koalícia), a partnership uniting government, the IT industry, academia, and civil society. This platform conducts national assessments, such as the IT Fitness Test, to evaluate the population's digital competencies and identify demographic groups requiring educational intervention. The coalition also partners with MIRRI to design tailored training for seniors and older public administration employees.

NGOs and the private sector provide essential specialized support. Independent initiatives like Konšpirátori.sk offer the public transparent databases of websites known for spreading disinformation or fraudulent content, serving as practical tools for source verification. In the

financial sector, the Slovak Banking Association and individual banks regularly run targeted awareness campaigns to prevent online banking fraud. These campaigns teach customers how to recognize phishing attempts, use multi-factor authentication, and safely navigate electronic banking.

While Slovakia has established a solid institutional foundation, achieving widespread digital resilience among adults aged 45 and older requires sustained effort. Success depends on the continuous expansion of accessible, non-formal education programs and the effective dissemination of practical cybersecurity tools.

4. Best Practices

The national desk research identified a total of fifteen best practices across the three partner countries – five per country – representing a diverse range of actors, methodologies, and target approaches. These initiatives demonstrate how digital safety challenges are addressed through prevention, education, and empowerment at different levels of governance and civil society. The practices are presented below by country, using a consistent format.

4.1 Italy

Five relevant national best practices were identified during the desk research, reflecting a diverse ecosystem of initiatives aimed at strengthening digital literacy, online safety, and fraud prevention among adults. These include institutional programmes, awareness campaigns, regional initiatives, European projects, and actions led by the third sector. At the national level, Repubblica Digitale represents a strategic framework promoting digital skills development and inclusion through coordinated actions such as the Digital Facilitation Network, supporting citizens, especially adults, in the safe use of digital services. Similarly, the campaign I Navigati, promoted by financial and public institutions, focuses specifically on raising awareness about online fraud and cybersecurity risks, particularly in the context of digital financial services. At the regional level, the programme Pane e Internet developed by the Emilia-Romagna Region provides structured training opportunities for adults, with a strong emphasis on practical skills, including online safety and responsible use of digital tools. From the European perspective, the Erasmus+ project DIGITOL offers a relevant example of non-formal education targeting older adults, aiming to improve digital competences and promote safe engagement with digital technologies. Finally, the Fondazione Mondo Digitale plays a key role in the Italian context by implementing inclusive educational programmes that support vulnerable groups, including adults, in developing digital awareness and cybersecurity skills. Together, these initiatives demonstrate a multi-level and multi-actor approach to digital safety education, combining policy, training, awareness, and innovation.

Here are the best practices identified:

1. **Repubblica Digitale (Digital Republic)**

<i>Title of the Best Practice</i>	Repubblica Digitale (Digital Republic)
<i>Type of Best Practice</i>	National initiative
<i>Implementing Organisation</i>	Steering Technical Committee, coordinated by the Department for Digital Transformation of the Prime Minister's Office, Italy. https://innovazione.gov.it/
<i>Main Objectives</i>	● To bridge the digital divide, tackle all forms of digital illiteracy and promote education in future technologies, thus supporting the country's development. ● To ensure a gradual and inclusive transition to a fully digital society.
<i>Target Group(s)</i>	Primarily focusing on: ● citizens at risk of digital exclusion (such as the elderly or those in remote areas); ● workers needing to upgrade their tech skills; ● students pursuing digital literacy; ● public Administration to modernise government services; ● third-sector organisations to create a widespread network of digital facilitators.
<i>Educational Outcomes & Impact</i>	● In 2024, 272,270 public employees have enrolled in personalized learning paths to improve their digital skills via the Syllabus platform. Furthermore, a new directive has been introduced that, starting in 2025, mandates at least 40 hours of annual training for every public employee with a specific focus on digitalization, signaling a significant shift in trend compared to the past. ● Repubblica Digitale's fund has funded 73 projects that, in 2024, trained over 13,000 people (including NEETs, the unemployed, and at-risk workers) helping to bridge the gap of ICT professionals in the Italian labor market.

	● Digital Education Hubs were Funded with €60 million from the PNRR (National Recovery and Resilience Plan), representing an effort to strengthen the university system in the fields of technology transfer and advanced training, supporting the preparation of highly qualified specialists. ● "Punti Digitale Facile" (Easy Digital Points). These hubs engaged over 1.8 million citizens by October 2025, helping to reduce the digital divide and promoting access to digital services for the general public. ● Training and digitalization efforts actively involve public entities, businesses, and the third sector. This strategy guides interventions in both the public and private spheres, fostering long-term continuity beyond extraordinary investments.
<i>Description of the Activity and Methodological Approach</i>	A key pillar of this activity is the Servizio Civile Digitale (Digital Civil Service), a program where young volunteers aged 18–28 work for 12 months as mentors, guiding citizens through the "learning by doing" process. This peer-to-peer and intergenerational learning is further grounded in the Punti Digitale Facile (Easy Digital Points): with over 4000 physical hubs established across the country, these centres serve as accessible community spaces where citizens can go to activate their digital identity, such as SPID or CIE (Electronic Identity Card). Beyond simple activation, facilitators provide the training necessary to navigate these tools, teaching users how to access healthcare records, pay taxes online, or sign digital documents. Furthermore, Repubblica Digitale launched the "Italian Coalition for Digital Skills and Employment", an open alliance that aims to identify and engage as many stakeholders as possible (e.g. businesses, public bodies, NGOs, etc.) to create a digital and human network of people willing to cooperate and develop a national scientific-technological culture. To date, more than 180 organisations have joined the Italian Coalition and launched over 220 projects. To join the coalition, an organisation must formally adhere to the "Repubblica Digitale's Manifesto", ensuring that all members are committed to the same values of inclusion, ethics, and

	digital sovereignty.
<i>Innovative Features</i>	The initiative utilizes both formal and non-formal education integrated across its various activities and projects and strongly values a multi-sectoral cooperation, from the public and private sectors as well as civil society. A distinctive feature of its approach model is the use of a peer-to-peer approach and intergenerational learning. These elements, combined with a commitment to broad inclusion and a focus on vulnerable groups, establish it as a strategic and integrated foundation for national digital literacy and training.
<i>Link / Reference</i>	https://repubblicadigitale.gov.it/portale/
<i>Visual Materials</i>	 https://repubblicadigitale.gov.it/portale/-/l-italia-delle-competenze-digitali-si-fa-rete-i-risultati-raggiunti-e-le-sfide-del-futuro-martedì%2031-marzo-a-roma 

Adaptability Assessment of the Repubblica Digitale (Digital Republic)

Criteria	Completely	To a certain extent	Not at all	Comments (optional)
a) Different target groups (e.g., youth, seniors, professionals)	☒	☐	☐	

b) Different organisations (e.g., NGOs, schools, public authorities)	☒	☐	☐	
c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)	☐	☒	☐	

2. *I Navigati*

<i>Title of the Best Practice</i>	<i>I Navigati</i>
<i>Type of Best Practice</i>	Campaign, Online Tool
<i>Implementing Organisation</i>	CERTFin (Computer Emergency Response Team of the Italian finances sector) https://www.certfin.it/en/
<i>Main Objectives</i>	To promote digital literacy and raise awareness and educate people on the informed and secure use of digital tools and platforms, so as to avoid falling into the traps set by cybercriminals
<i>Target Group(s)</i>	The target audience is broad: from young people to adults, the main target consists of people who regularly use digital channels (online banking, payment apps, online trading) to manage their finances and people with limited digital skills that faces difficulties in distinguishing a scam from a legitimate process.
<i>Educational Outcomes & Impact</i>	● Users learn to pause and verify requests through official channels before acting. ● Participants gain the skills to identify sophisticated scams that bypass traditional filters ● By targeting the "human factor" the campaign significantly reduces participant vulnerability. Users learn to identify sophisticated AI-generated voice or video deepfakes, preventing them from falling victim to emotional scams that impersonate family

	members
<i>Description of the Activity and Methodological Approach</i>	● The campaign typically runs in annual "waves," often peaking in October to coincide with <i>European Cybersecurity Month</i>. The campaign is sponsored via the main TV channels, radio, official website, and social media. The campaign uses storytelling to grant an easier understanding of difficult themes: ● A web series of short videos where Navigati's family members tackle different risks inherent in the digital world; ● "Al Sicuro" Podcast hosted by tech expert. Fjona Cakalli talks about different online frauds, making these audio lessons a way to offer practical advice on how to spot scammers' psychological tricks.
<i>Innovative Features</i>	What truly sets I Navigati apart is its innovative use of storytelling and a multi-channel media strategy designed to turn complex cybersecurity topics into relatable daily life scenarios. The campaign centres on the "Navigati family", experts in digital security, whose domestic adventures serve as educational templates for the public. Through a series of short video episodes (roughly 3 minutes each), the family demonstrates how to defend oneself and recognize the early warning signs of a scam. This familiar, light-hearted tone makes the technical advice accessible and less intimidating for non-experts. To ensure the message reaches citizens on the go, the campaign also features a short podcast series, offering flexible audio lessons on digital safety.
<i>Link / Reference</i>	https://inavigati.certfin.it/index.html
<i>Visual Materials</i>	Media coverage: https://www.bancaditalia.it/media/notizia/i-navigati-al-via-la-nuova-campagna-sulla-sicurezza-informatica/?dotcache=refresh

Adaptability Assessment of the I Navigati

Criteria	Completely	To a certain extent	Not at all	Comments (optional)
a) Different target groups (e.g., youth, seniors, professionals)	☒	☐	☐	
b) Different organisations (e.g., NGOs, schools, public authorities)	☒	☐	☐	
c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)	☒	☐	☐	

3. **Pane e Internet**

<i>Title of the Best Practice</i>	<i>Pane e Internet</i>
<i>Type of Best Practice</i>	Project/Training
<i>Implementing Organisation</i>	Emilia-Romagna region, Italy, pei@paneeinternet.it
<i>Main Objectives</i>	To promote the development of digital skills and strengthen the regional network at both the local and regional levels and enhance citizens' digital awareness of global issues
<i>Target Group(s)</i>	Citizens of any age who use technology to access information, use online services, and take advantage of the digital opportunities available in their community.
<i>Educational Outcomes & Impact</i>	Pane e Internet's training programs have been designed and implemented in accordance with the European DigComp model, the reference framework for citizens' digital competencies and its trainings were recognised as one of the best European practices in the field of digital literacy education by the European Commission. Participants can be gradually introduced to the digital

	world with webinars and courses adapted to their needs and knowledge. Participants not only improve their own digital awareness, but become active contributors to Emilia-Romagna's transformation into a more advanced and technologically inclusive region, driving a collective shift toward a more connected and future-ready community.
<i>Description of the Activity and Methodological Approach</i>	The initiative operates by offering many online workshops and courses. Throughout the year, it offers dozens of free courses and webinars that have different duration depending on the topic. A permanent action is the maintenance of over Pel Points (Punti Pane e Internet) across the region thanks to the collaboration with City Halls and municipalities, ensuring that digital support is always physically reachable within the community. Pane e Internet offers tailored digital literacy courses, ranging from foundational computer skills and hardware usage to advanced cybersecurity awareness. This leveled approach ensures users can progress from basic technical operations to identifying and defending against complex online risks. When creating the courses, a special focus is put on vulnerable groups as well, ensuring the maximum outreach and accessibility.
<i>Innovative Features</i>	The European Commission has recognized Pei's educational program as one of Europe's best practices in the field of digital literacy education. Training events and webinars are held online for maximum accessibility, reaching also remote areas of the region. At the same time, the project maintains a strong territorial presence through physical hubs strategically located throughout the region. These local centres are essential for fostering community cooperation and ensuring the widespread dissemination of digital tools.
<i>Link / Reference</i>	https://www.paneeinternet.it/
<i>Visual Materials</i>	https://www.paneeinternet.it/public/elenco-news

Adaptability Assessment of Pane e Internet

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☒	☐	☐	
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☒	☐	☐	
<i>c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)</i>	☒	☐	☐	

4. **Erasmus+ project DIGITOL**

<i>Title of the Best Practice</i>	Erasmus+ project DIGITOL
<i>Type of Best Practice</i>	Project
<i>Implementing Organisation</i>	Partnership composed of six organizations from six different European countries: Consorzio Comunità Brianza (Italy), Pro Arbeit (Germany), 50PLUS Hellas (Greece), Znanie (Bulgaria), Tree Agency (Estonia), AGE Platform , Europe (Belgium).
<i>Main Objectives</i>	DIGITOL promotes EU values like solidarity and diversity through innovative digital literacy programs. The project aims to create a more respectful Internet while combating discrimination and xenophobia by uniting generations to identify and contain fake news and online hate speech.
<i>Target Group(s)</i>	Older European adults (+55)
<i>Educational Outcomes & Impact</i>	● 10 young people(aged 18-30) from the partners' countries were formed in a training for trainers 30 hours worth focused on combatting fake news and polarisation. ● 25 seniors (aged over 55) participated to the DIGITOL 60-hours capacity building programme

	led by young people and external experts aimed to equip participants with theoretical and practical tools to better understand the evolution of contemporary society in alignment with our European values.
<i>Description of the Activity and Methodological Approach</i>	● Training of Trainers (ToT): "Young Ambassadors" (ages 18-30) learnt how to be intergenerational mentors. They learnt not only digital skills but also pedagogical techniques to teach seniors. ● Capacity Building Program (CBP): The core educational phase where the Young Ambassadors lead workshops for seniors (aged 55+) on media literacy, identifying fake news, and combating online hate speech. ● Pilot Actions & follow-up activities: Participants move from the classroom to the real world by organizing "Human Libraries" and "Digitol Festivals" to promote social cohesion and European values within their local communities.
<i>Link / Reference</i>	https://digitol.eu/it/
<i>Visual Materials</i>	https://digitol.eu/wp-content/uploads/2020/07/DIGITOL-Project-Brochure-English.pdf Toolkit: https://digitol.eu/wp-content/uploads/2022/01/toolkit-ITA-DEF.pdf

Adaptability Assessment of Erasmus+ project DIGITOL

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☒	☐	☐	
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☒	☐	☐	
<i>c) Different topics or</i>	☒	☐	☐	

challenges (e.g., privacy, misinformation, cybersecurity)				
---	--	--	--	--

5. **Fondazione Mondo Digitale**

<i>Title of the Best Practice</i>	Fondazione Mondo Digitale
<i>Type of Best Practice</i>	Training
<i>Implementing Organisation</i>	Fondazione Mondo Digitale ETS, Italy, info@mondodigitale.org https://www.mondodigitale.org/
<i>Main Objectives</i>	● To promote a culture of innovation and foster a new knowledge-based economy as a driver of the country's development. ● Use of digital technologies for social progress, to fuel growth, well-being, productivity, and competitiveness.
<i>Target Group(s)</i>	People of all ages and working-background: the website allows users to select the term that best represents them (e.g: <i>women, unemployed, executives, artists...</i>)
<i>Educational Outcomes & Impact</i>	The people that take part in the <i>Fondazione Mondo Digitale's</i> projects and events gain expertise in STEAM field while creating at the same time a network of connections in their frame work. Thanks to the way the projects are structured, digital skills are complemented by social skills and active citizenship. This is achieved by encouraging participation in events, local competitions and webinars.
<i>Description of the Activity and Methodological Approach</i>	<i>Fondazione Mondo Digitale</i> focuses on providing participants with STEAM laboratories in different areas. In addition, workshops and seminars are directly integrated with local and national contests, providing participants with immediate opportunities to apply theoretical concepts through hands-on competition (e.g.: RomeCup , Digital Made). Projects can range from short, intensive 3-hour workshops to year-long

	curricular pathways integrated into the school calendar. The use of the tactic <i>learning by doing</i> is used in every project and the main representation of that are the " Innovation Gyms ", hybrid physical and virtual spaces spread all around Italy where people of all ages can go and learn both technical mastery and soft skills.
<i>Innovative Features</i>	What truly sets this project apart is its tailored webpage, which categorizes opportunities into specific target groups (ranging from women and youth to the elderly, migrants, artists...) allowing users to instantly identify the courses and initiatives best suited for their personal or professional growth. This accessibility is paired with a "learning by doing" philosophy, where practical educational activities are directly intertwined with national and local contests. By participating in these competitions, learners can immediately apply their theoretical knowledge to real-world challenges.
<i>Link / Reference</i>	https://www.mondodigitale.org/
<i>Visual Materials</i>	https://youtu.be/m-Jd6NR31uk?si=DBQRTWNVSPVP4Ycx https://www.repubblica.it/tecnologia/sicurezza/2020/02/04/news/google_premia_4_progetti_italiani_su_sicurezza_online-247591358/

Adaptability Assessment of Fondazione Mondo Digitale

Criteria	Completely	To a certain extent	Not at all	Comments (optional)
a) Different target groups (e.g., youth, seniors, professionals)	☒	☐	☐	
b) Different organisations (e.g., NGOs, schools, public authorities)	☒	☐	☐	
c) Different topics or challenges (e.g., privacy, misinformation,	☒	☐	☐	

cybersecurity)				
----------------	--	--	--	--

4.2 Spain

As part of the digiSAFE research phase, a mapping of national best practices was conducted to identify effective initiatives in Spain that promote digital safety, fraud prevention, and digital literacy among adults, with particular relevance for individuals aged 45 and over. The objective of this analysis was to highlight existing approaches that can inform the development of the digiSAFE Non-Formal Education Curriculum and the Digital Fraud Prevention Toolkit. The selected best practices represent a diverse range of actors and methodologies, including public institutions, law enforcement bodies, non-governmental organisations, national awareness campaigns, and community-based training initiatives. Together, they demonstrate how digital safety challenges are addressed in Spain through prevention, education, and empowerment, rather than relying exclusively on technical or regulatory measures.

Special attention was given to initiatives adopting non-formal and accessible learning approaches, recognising that adults aged 45+ often benefit most from practical, experience-based, and user-friendly educational methods. The identified practices focus on strengthening digital confidence, raising awareness of online risks, improving the ability to recognise fraud and scams, and encouraging responsible use of digital technologies in everyday life.

Furthermore, the selected best practices show a high degree of adaptability and transferability to other national and European contexts. Many of them are scalable, inclusive, and designed to be implemented by different types of organisations, making them particularly suitable for replication within the digiSAFE project framework. Here are the 5 best practices identified in Spain:

1. **Fundación Cibervoluntarios – Digital Inclusion and Digital Skills for Adults**

<i>Title of the Best Practice</i>	Fundación Cibervoluntarios – Digital Inclusion and Digital Skills for Adults
<i>Type of Best Practice</i>	Project / Training / Workshops
<i>Implementing Organisation</i>	Fundación Cibervoluntarios, Spain https://www.cibervoluntarios.org
<i>Main Objectives</i>	Summarise goals (e.g., raise To reduce the digital divide by empowering adults and seniors with digital skills, confidence, and awareness to participate safely in the digital society.

<i>Target Group(s)</i>	Adults, seniors, vulnerable groups, adults aged 45+.
<i>Educational Outcomes & Impact</i>	Participants improve basic and intermediate digital skills, increase confidence in using digital tools, and develop greater awareness of online risks, fraud, and misinformation.
<i>Description of the Activity and Methodological Approach</i>	Free digital training activities delivered online and face-to-face through community centres, associations, and public institutions. The methodology is based on non-formal education, practical exercises, peer learning, and real-life digital scenarios.
<i>Innovative Features</i>	Volunteer-led digital mentoring, community-based approach, and tailored learning pathways for adults and seniors.
<i>Link / Reference</i>	https://www.cibervoluntarios.org
<i>Visual Materials</i>	Training materials, videos, infographics, project reports, and online resources available on the organisation's website.

Adaptability Assessment of the Fundación Cibervoluntarios – Digital Inclusion and Digital Skills for Adults

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☒	☐	☐	
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☒	☐	☐	
<i>c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)</i>	☒	☐	☐	

2. Aula Mentor – Adult Education and Digital Skills Programme

<i>Title of the Best Practice</i>	Aula Mentor – Adult Education and Digital Skills Programme
-----------------------------------	--

<i>Type of Best Practice</i>	Training / Online Learning Programme
<i>Implementing Organisation</i>	Ministry of Education and Vocational Training, Spain https://www.aulamentor.es
<i>Main Objectives</i>	To promote lifelong learning by providing adults with flexible access to digital skills and ICT training.
<i>Target Group(s)</i>	Adults (18+), including adults aged 45+.
<i>Educational Outcomes & Impact</i>	Learners acquire basic digital competences, improve autonomy in using online tools, and increase confidence in digital environments.
<i>Description of the Activity and Methodological Approach</i>	Online courses supported by trained mentors, allowing adults to learn at their own pace through a flexible non-formal learning model adapted to adult learners' needs.
<i>Innovative Features</i>	Nationwide coverage, mentor-supported learning, and flexible access for adult learners.
<i>Link / Reference</i>	https://www.aulamentor.es
<i>Visual Materials</i>	Online course catalogues, platform screenshots, and informational materials available on the official website.

Adaptability Assessment of Aula Mentor – Adult Education and Digital Skills Programme

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☒	☐	☐	
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☐	☒	☐	
<i>c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)</i>	☒	☐	☐	

3. *Policía Nacional – Plan Mayor Seguridad*

<i>Title of the Best Practice</i>	Policía Nacional – Plan Mayor Seguridad
<i>Type of Best Practice</i>	Campaign / Awareness Initiative
<i>Implementing Organisation</i>	Policía Nacional, Spain https://www.policia.es
<i>Main Objectives</i>	To prevent crime and fraud affecting older adults by raising awareness of digital and offline risks and promoting safe behaviours.
<i>Target Group(s)</i>	Older adults, seniors, associations for older people.
<i>Educational Outcomes & Impact</i>	Increased awareness of fraud schemes, improved ability to recognise scams, and strengthened trust between older citizens and public institutions.
<i>Description of the Activity and Methodological Approach</i>	Informative talks and workshops delivered by police officers in community centres and associations, using practical examples and prevention-oriented guidance.
<i>Innovative Features</i>	Direct involvement of law enforcement professionals and strong community engagement.
<i>Link / Reference</i>	https://www.policia.es/_es/colabora_plan_mayor_seguridad.php
<i>Visual Materials</i>	Posters, leaflets, presentation materials, and campaign visuals available through Policía Nacional channels.

Adaptability Assessment of Policía Nacional – Plan Mayor Seguridad

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☐	☒	☐	
<i>b) Different organisations (e.g.,</i>		☒	☐	

NGOs, schools, public authorities)	☐			
c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)	☒	☐	☐	

4. **INCIBE – 017 Cybersecurity Helpline and Awareness Programme**

<i>Title of the Best Practice</i>	INCIBE – 017 Cybersecurity Helpline and Awareness Programme
<i>Type of Best Practice</i>	Public Service / Awareness Campaign / Online Tool
<i>Implementing Organisation</i>	Instituto Nacional de Ciberseguridad (INCIBE), Spain https://www.incibe.es
<i>Main Objectives</i>	To improve citizens' awareness of cybersecurity risks and provide guidance on fraud prevention and safe digital behaviour.
<i>Target Group(s)</i>	General population, adults, seniors, vulnerable users.
<i>Educational Outcomes & Impact</i>	Users improve awareness of digital threats, increase ability to recognise fraud and scams, and adopt safer online practices.
<i>Description of the Activity and Methodological Approach</i>	Free public helpline offering personalised support via phone, chat, and messaging apps, combined with awareness campaigns and educational online resources.
<i>Innovative Features</i>	Multi-channel access, real-time personalised support,

	and integration of education with incident response.
Link / Reference	https://www.incibe.es/linea-017

Adaptability Assessment of INCIBE – 017 Cybersecurity Helpline and Awareness Programme

Criteria	Completely	To a certain extent	Not at all	Comments (optional)
a) Different target groups (e.g., youth, seniors, professionals)	☒	☐	☐	
b) Different organisations (e.g., NGOs, schools, public authorities)	☐	☒	☐	
c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)	☒	☐	☐	

5. Regional Digital Skills Programmes for Seniors (Spain)

Title of the Best Practice	Regional Digital Skills Programmes for Seniors (Spain)
Type of Best Practice	Training / Workshops / Public Initiative
Implementing Organisation	Regional and local public authorities, Spain
Main Objectives	To promote digital inclusion and safe use of digital technologies among older adults at local level.
Target Group(s)	Older adults, seniors, adults with low digital skills.
Educational Outcomes & Impact	Participants improve basic digital competences, increase confidence in using online services, and gain awareness of online risks and fraud prevention strategies.
Description of the Activity and Methodological Approach	Hands-on training activities delivered in community centres, libraries, or adult education centres through small-group, practice-oriented sessions.
Innovative Features	Localised approach, direct community engagement, and

	adaptation to learners' specific needs.
--	---

Adaptability Assessment of Regional Digital Skills Programmes for Seniors (Spain)

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☒	☐	☐	
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☒	☐	☐	
<i>c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)</i>	☒	☐	☐	

4.3 Slovakia

The desk research phase identified five distinct national best practices in Slovakia led by private sectors, non-profit organizations, and community networks. These initiatives offer highly adaptable approaches to combating digital exclusion and preventing online fraud among older adults.

Bezpečne na nete (Safely on the Net) Created by the Slovak cybersecurity company ESET, this comprehensive educational portal provides free, accessible resources on digital safety. While available to the general public, its straightforward articles, podcasts, and video guides are highly effective for adults and seniors. The platform translates complex cybersecurity threats—such as malware, phishing, and data privacy—into simple, everyday language. Its primary innovation is leveraging private-sector cybersecurity expertise to provide the public with high-quality, constantly updated educational content that individuals can consume at their own pace.

Zrelí na dobu digitálnu (Mature for the Digital Age) Managed by the Slovak Telekom Endowment Fund, this grant and educational program specifically targets the digital inclusion of seniors. The initiative funds and supports local organizations, care homes, and community centers to run tailored digital literacy courses. The methodology focuses on small-group, hands-on learning environments where older adults can safely practice using smartphones, managing online accounts, and identifying common scams. This decentralized approach ensures that education reaches seniors in their local communities, making learning highly accessible and socially engaging.

Zodpovedne.sk (Responsibly.sk) Operated by the civic association eSlovensko, this national awareness center focuses on safe internet usage across all generations. For the

45+ demographic, it provides targeted printed handbooks, instructional videos, and advisory services regarding cyber threats. The initiative acts as a preventative educational tool, teaching adults how to secure their devices, protect their personal data, and recognize psychological manipulation online. Its strong point is its longevity and extensive library of localized, easy-to-understand materials that can be widely distributed by educators and NGOs.

Senior bezpečne online (Senior Safely Online) Seminars Organized through local branches of the Union of Pensioners in Slovakia (JDS) in collaboration with regional IT experts, these grassroots seminars offer direct, peer-supported education. The workshops take place in familiar community spaces and focus heavily on immediate threats, such as local financial scams, fraudulent e-shops, and secure communication with family. The methodological strength lies in its peer-to-peer trust model; learning within a network of peers significantly reduces the anxiety older adults often feel when adopting new digital habits.

Smart Senior Academies at Regional Libraries Public libraries across Slovakia, such as the regional libraries in Žilina and Bratislava, have transformed into vital hubs for adult digital education. These institutions regularly host structured "Smart Senior" courses. Librarians and volunteer IT trainers guide participants through basic digital navigation, evaluating online information, and recognizing fraudulent emails. This practice utilizes existing, trusted community infrastructure to provide continuous, free, and highly patient educational support, making it an easily adaptable model for any municipality. Here are the 5 best practices identified:

1. **Bezpečne na nete (Safely on the Net)**

<i>Title of the Best Practice</i>	Bezpečne na nete (Safely on the Net)
<i>Type of Best Practice</i>	Online Tool / Campaign
<i>Implementing Organisation</i>	ESET, Slovakia. https://bezpecnenanete.eset.com/sk/
<i>Main Objectives</i>	To increase awareness of cybersecurity threats and provide free, practical education on how to navigate the internet safely, tailored for all user groups including seniors.
<i>Target Group(s)</i>	General public, adults, seniors, educators, and parents.
<i>Educational Outcomes & Impact</i>	Users gain access to a continuously updated library of articles, videos, and podcasts. Participants learn to recognize modern cyber threats, secure their digital privacy, and operate safely online without fear of digital exclusion.

<i>Description of the Activity and Methodological Approach</i>	The portal operates as a centralized educational hub offering step-by-step learning materials. The methodology relies on translating complex IT security concepts (like malware, phishing, and data breaches) into simple, everyday language. Content is categorized to suit different skill levels and life situations, making it easy for older adults to consume at their own pace.
<i>Innovative Features</i>	It leverages the profound, global cybersecurity expertise of a leading private-sector tech company (ESET) to provide completely free, high-quality, and non-commercial educational content for the public good.
<i>Link / Reference</i>	https://bezpecnenanete.eset.com/sk/
<i>Visual Materials</i>	Screenshots of the portal and podcast library available at: https://bezpecnenanete.eset.com/sk/

Adaptability Assessment of Bezpečne na nete (Safely on the Net):

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☒	☐	☐	Content is already segmented for different age groups and technical proficiencies.
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☒	☐	☐	Private sector companies across Europe could replicate this CSR model.
<i>c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)</i>	☒	☐	☐	The platform format easily allows for the addition of new topics, like AI threats.

2. Zrelí na dobu digitálnu (Mature for the Digital Age)

<i>Title of the Best Practice</i>	Zrelí na dobu digitálnu (Mature for the Digital Age)
<i>Type of Best Practice</i>	Project / Funding / Training
<i>Implementing Organisation</i>	Slovak Telekom Endowment Fund (Nadačný fond Telekom pri Nadácii Pontis), Slovakia. https://nadacnyfondtelekom.sk/
<i>Main Objectives</i>	To promote digital literacy and raise awareness and educate people on the informed and secure use of digital tools and platforms, so as to avoid falling into the traps set by cybercriminals
<i>Target Group(s)</i>	Seniors aged 65 and older, local NGOs, care homes, and community centers.
<i>Educational Outcomes & Impact</i>	The grant program has funded dozens of local organizations with over €200,000, training thousands of seniors. Participants improve their critical thinking, verify information sources, and develop resilience against emotional manipulation used by fraudsters.
<i>Description of the Activity and Methodological Approach</i>	Rather than a single central course, this is a grant mechanism that empowers local entities to deliver training. Supported projects utilize small-group, hands-on learning methodologies. Seniors are taught in familiar environments to safely practice using smartphones, identifying scams, and communicating with family, ensuring patient and tailored instruction. to offer practical advice on how to spot scammers' psychological tricks.
<i>Innovative Features</i>	The decentralized funding model relies heavily on grassroots community networks, ensuring that digital education reaches isolated seniors in rural areas who might not attend large, state-run courses.
<i>Link / Reference</i>	https://nadacnyfondtelekom.sk/
<i>Visual Materials</i>	Campaign details available at https://nadacnyfondtelekom.sk/aktual-ne-vyzvy/

Adaptability Assessment of Zrelí na dobu digitálnu (Mature for the Digital Age)

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☐	☒	☐	The grant model is specifically, tailored to the needs and pacing of older adults.
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☒	☐	☐	Any corporate foundation or state body can adopt this decentralized grant methodology.
<i>c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)</i>	☒	☐	☐	The grants can be themed annually to focus on specific issues like phishing or AI.

3. **Zodpovedne.sk (Responsibly.sk)**

<i>Title of the Best Practice</i>	Zodpovedne.sk (Responsibly.sk)
<i>Type of Best Practice</i>	Campaign / Online Tool
<i>Implementing Organisation</i>	Civic Association eSlovensko, Slovakia. https://www.zodpovedne.sk/
<i>Main Objectives</i>	To raise national awareness about internet safety, prevent cybercrime, and provide educational resources and advisory services regarding cyber threats across generations.
<i>Target Group(s)</i>	General public, adults, seniors, parents, and educators.
<i>Educational Outcomes & Impact</i>	Seniors learn to independently search for information, operate email accounts, and recognize fraudulent communications. It fosters a sense of independence and integration into the modern digital society.
<i>Description of the Activity and Methodological Approach</i>	Libraries host structured, multi-week "Smart Senior" courses or IT drop-in sessions. Librarians and volunteer IT trainers guide small groups through practical exercises. The methodology is highly patient, allowing seniors to practice on library computers or their own devices, covering everything from turning the device on to advanced internet safety.
<i>Innovative Features</i>	It ingeniously utilizes the existing, highly trusted, and accessible infrastructure of public libraries to deliver continuous, free, and non-intimidating adult education.
<i>Link / Reference</i>	https://www.krajskakniznicazilina.sk/
<i>Visual Materials</i>	Course descriptions at https://www.krajskakniznicazilina.sk/index.php/2023/10/19/digitalne-zrucni-seniori/

Adaptability Assessment of Zodpovedne.sk (Responsibly.sk)

Criteria	Completely	To a certain extent	Not at all	Comments (optional)
a) Different target groups (e.g., youth, seniors, professionals)	☒	☐	☐	Libraries serve the entire community and can adjust classes for any demographic.
b) Different organisations (e.g., NGOs, schools, public authorities)	☒	☐	☐	Can be utilized by schools, adult education centers, and public authorities.
c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)	☒	☐	☐	Constantly updated to address new phenomenon s like gambling, AI, and data misuse.

4. Erasmus+ project DIGITOL

Title of the Best Practice	Erasmus+ project DIGITOL
Type of Best Practice	Project
Implementing Organisation	Union of Pensioners in Slovakia (JDS) in collaboration with regional IT experts and universities.

	https://www.jednotadochodcov.sk
<i>Main Objectives</i>	To provide localized, peer-supported education that helps seniors safely navigate the internet, recognize local financial scams, and reduce anxiety around digital tools.
<i>Target Group(s)</i>	Seniors and retired adults.
<i>Educational Outcomes & Impact</i>	Participants successfully transition from avoiding digital tools to actively and safely using smartphones, chatting applications, and online banking, significantly reducing their isolation and vulnerability to basic fraud.
<i>Description of the Activity and Methodological Approach</i>	These are grassroots seminars organized directly by the pensioners' union in local community spaces. The methodology emphasizes peer-to-peer learning and practical, immediate application. Topics are highly relevant to daily life: spotting fraudulent e-shops, recognizing fake news, and learning how to ignore or block unsolicited communication.
<i>Innovative Features</i>	The peer-to-peer trust model is highly effective. Learning within a network of peers (other seniors) drastically lowers the psychological barrier and anxiety that older adults frequently experience in formal, fast-paced IT classes.
<i>Link / Reference</i>	https://www.jednotadochodcov.sk/
<i>Visual Materials</i>	N/A

Adaptability Assessment of Erasmus+ project DIGITOL

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☐	☒	☐	The peer-support model works best when participants share similar age/life

				experiences.
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☒	☐	☐	Highly adaptable for community centers, local NGOs, and senior clubs.
<i>c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)</i>	☒	☐	☐	Seminars can easily incorporate new threat landscapes into the discussion.

5. **Smart Senior Academies at Regional Libraries**

<i>Title of the Best Practice</i>	<i>Smart Senior Academies at Regional Libraries</i>
<i>Type of Best Practice</i>	Training / Project
<i>Implementing Organisation</i>	Regional public libraries (e.g., Krajská knižnica Žilina), Slovakia. https://www.krajskakniznicazilina.sk/
<i>Main Objectives</i>	To transform public libraries into vital hubs for adult digital education, teaching seniors basic device navigation and how to safely evaluate online information.
<i>Target Group(s)</i>	Seniors, disadvantaged adults, and local community members.
<i>Educational Outcomes & Impact</i>	Seniors learn to independently search for information, operate email accounts, and recognize fraudulent communications. It fosters a sense of independence and integration into the modern digital society.

<i>Description of the Activity and Methodological Approach</i>	Libraries host structured, multi-week "Smart Senior" courses or IT drop-in sessions. Librarians and volunteer IT trainers guide small groups through practical exercises. The methodology is highly patient, allowing seniors to practice on library computers or their own devices, covering everything from turning the device on to advanced internet safety.
<i>Innovative Features</i>	It ingeniously utilizes the existing, highly trusted, and accessible infrastructure of public libraries to deliver continuous, free, and non-intimidating adult education.
<i>Link / Reference</i>	https://www.krajskakniznicazilina.sk/
<i>Visual Materials</i>	Course descriptions at https://www.krajskakniznicazilina.sk/index.php/2023/10/19/digitalne-zrucni-seniori/

Adaptability Assessment Smart Senior Academies at Regional Libraries

<i>Criteria</i>	<i>Completely</i>	<i>To a certain extent</i>	<i>Not at all</i>	<i>Comments (optional)</i>
<i>a) Different target groups (e.g., youth, seniors, professionals)</i>	☒	☐	☐	Libraries serve the entire community and can adjust classes for any demographic.
<i>b) Different organisations (e.g., NGOs, schools, public authorities)</i>	☒	☐	☐	This model can be replicated by any public institution with space and computers.
<i>c) Different topics or challenges (e.g., privacy, misinformation, cybersecurity)</i>	☒	☐	☐	The curriculum can pivot from basic hardware use to advanced anti-phishing training.

5. Analysis of Survey Results

5.1 Italy

Purpose and Method

The Italian survey was conducted as part of the national needs assessment to collect quantitative data on digital literacy, online safety awareness, and exposure to online fraud among adults aged 45+ in Italy. The questionnaire was administered online via Google Forms and disseminated through multiple channels to ensure broad outreach.

It was initially shared within the network of Associazione Italiana Socio-Educatori per la Cooperazione (AISEC APS) through internal communication tools, including email exchanges and presentations during the association's annual assemblies. In addition, the survey was distributed through the official communication channels of Confcooperative Lazio Nord, with which AISEC is affiliated, using newsletters, circulars, and direct emails targeting its network across the provinces of Rieti, Viterbo, and Rome.

For the purposes of the national analysis, only responses from participants residing in Italy were considered. The final sample consisted of 63 respondents aged 45 and over, including 39 women and 24 men. The largest age group was 45–54 (28 respondents), followed by 65–74 (19), 55–64 (14), and 75+ (2).

From a territorial perspective, respondents were drawn from a broad area of the Lazio region, including both Northern Lazio and the metropolitan area of Rome. The sample was heterogeneous in terms of living context, encompassing urban, rural, and semi-urban areas, as well as diverse employment statuses and educational backgrounds. This diversity provides a comprehensive overview of the experiences, practices, and perceived needs of adults aged 45+ in the Italian context.

Key Results

The Italian dataset indicates that adults aged 45+ are generally active users of digital technologies, although their level of confidence varies depending on the type of skill involved.

Daily use of digital devices is widespread: 77.8% of respondents rated their use of smartphones or computers at the highest levels (4 or 5), with a mean score of 4.19/5. General confidence in using the Internet is also relatively high (mean 3.79/5), suggesting that most participants feel comfortable engaging in routine online activities.

This confidence becomes less consistent when more specific digital safety competences are considered. The strongest self-reported behaviours relate to basic precautionary practices in everyday navigation. A large majority of respondents reported avoiding clicking on unknown or suspicious links (73.0%) and double-checking information before

sharing it online (71.4%), while 60.3% stated that they block or report suspicious messages, profiles, or websites. These findings indicate the presence of basic defensive habits developed through experience.

At the same time, more technical or specialised skills reveal clear gaps. Less than half of respondents (47.6%) reported being able to identify whether a website is secure, for example by checking for HTTPS or security indicators. Similarly, only 50.8% felt confident adjusting privacy or security settings on their devices, and the same proportion reported using strong and unique passwords. Even weaker results emerge in relation to device and software maintenance: only 36.5% stated that they regularly update their devices, applications, and antivirus software, while a significant share expressed uncertainty in this area.

The most critical weakness concerns the recognition of AI-generated or manipulated content. Only 38.1% of respondents rated themselves highly in their ability to identify altered images, videos, or messages, and less than half reported regularly verifying whether digital content may have been manipulated. This confirms a significant competence gap in relation to emerging digital risks.

Awareness of online fraud is present but uneven across different types of threats. Traditional risks such as phishing and social media misinformation are relatively well known, with around two thirds of respondents reporting moderate or strong awareness. Awareness is slightly lower for scams related to fake online stores, payment fraud, or identity theft, and drops further when it comes to AI-based threats. Only 54.0% of respondents reported moderate or strong awareness of AI-generated scams, while a substantial proportion indicated limited or no awareness.

Direct experience with fraud is also significant. More than one third of respondents (38.1%) reported having been victims of some form of digital fraud, most commonly bank or financial fraud and fake purchase scams, followed by phishing and identity theft. This indicates that exposure to digital risks is not only perceived but also experienced in concrete terms.

Concern about future victimisation is particularly high: 84.1% of respondents expressed clear levels of concern about becoming victims of online fraud or misinformation. Overall, the results highlight a mismatch between routine digital use and more advanced safety competences.

Interpretation

The Italian findings confirm that frequent digital engagement does not necessarily translate into effective digital safety competences among adults aged 45+.

A first key issue can be described as an “illusion of competence.” Many participants rely on routine use and experiential learning, developing basic precautionary habits such as avoiding suspicious links or informally verifying information. However, this familiarity is not supported by structured knowledge, resulting in weaknesses in areas such as recognising secure websites, managing privacy settings, maintaining software updates, and identifying manipulated or AI-generated content. As a result, users may overestimate their ability to navigate safely in digital environments.

A second critical vulnerability relates to the evolving nature of online threats. The difficulty in recognising AI-generated content signals a shift in digital risk, where traditional detection strategies are increasingly insufficient. This exposes a generational gap, as emerging forms of fraud require new forms of critical and technical awareness.

The data also point to a tendency towards informal and reactive coping strategies. Many respondents rely on intuition, avoidance behaviours, or external support—such as asking family members for help, rather than on structured prevention strategies. While these approaches may offer partial protection, they are not sufficient in more complex scenarios and may contribute to insecurity or limited engagement with digital services.

At the same time, the high level of concern about potential victimisation, combined with the significant proportion of respondents who have already experienced fraud, indicates a strong perceived need for support. Participants appear aware of the risks but lack the tools to manage them effectively.

From a learning perspective, these findings underline the need for targeted, practical, and accessible educational interventions. Training should go beyond general awareness and focus on developing concrete competences, including recognising fraudulent patterns, verifying digital information, managing personal data securely, and responding appropriately to suspicious situations. Particular attention should be given to emerging risks, especially those linked to artificial intelligence and manipulated content.

Educational approaches should be user-friendly and grounded in real-life scenarios, in order to bridge the gap between everyday digital practices and more advanced safety competences. Strengthening digital confidence in a structured and informed way will be essential to support adults aged 45+ in transitioning towards safe, autonomous, and resilient use of digital technologies.

5.2 Spain

Purpose and Method

The Spanish survey was conducted as part of the digiSAFE needs assessment to collect quantitative data on digital habits, awareness of online risks, experiences with online fraud, and training needs among adults aged 45 and over. The objective was to provide comparable evidence across partner countries.

The questionnaire was administered online and distributed through Asociación UNO's networks, including local associations and informal adult learning channels. Participation was voluntary and anonymous, in full compliance with the General Data Protection Regulation (GDPR).

A minimum of 50 valid responses were collected from Spanish participants aged 45+, meeting the project's comparability requirements and ensuring the reliability of the dataset. The sample included a slight majority of women (58.8%). Respondents were concentrated in the 45–54 and 65–74 age groups, with all participants aged over 45.

The sample was relatively well-educated, with most participants holding at least secondary or tertiary qualifications. A significant proportion was retired (47.1%), while the remaining respondents were either employed or self-employed. From a territorial perspective, most participants lived in urban areas, with a smaller share residing in rural or semi-urban contexts. Overall, the sample provides a representative overview of digitally engaged adults aged 45+ in Spain, while also reflecting differences in life situations and levels of digital autonomy.

Key Results

The Spanish dataset shows that adults aged 45+ are actively engaged in the digital environment, particularly in relation to everyday activities. Most respondents reported using digital tools on a daily basis, especially for communication (messaging applications and email), online banking, social media, and access to public services.

At the same time, the results reveal important vulnerabilities. Overall daily device use reaches a moderate level (mean 3.29/5), while general confidence in using the Internet is slightly lower (mean 3.00/5), with a considerable share of respondents reporting limited confidence. Qualitative responses suggest that many individuals rely on external support—particularly younger family members—when facing difficulties online, indicating a degree of digital dependency rather than full autonomy.

Self-assessed digital skills are generally limited across several key areas. Basic competences such as recognising secure websites show relatively low levels of confidence (mean 2.76/5), while more technical skills, such as adjusting privacy settings,

managing secure passwords, or identifying AI-generated content, represent the weakest areas. In addition, many respondents reported uncertainty in distinguishing legitimate messages from phishing attempts and in knowing how to respond appropriately in case of suspected fraud.

Awareness of online risks varies depending on the type of threat. Traditional forms of fraud, such as phishing and fake investment offers, are relatively well recognised, and several respondents reported direct experience with these risks. In contrast, awareness of more recent threats—particularly those related to artificial intelligence, such as deepfakes or AI-generated misinformation—is significantly lower, with a notable proportion of participants unfamiliar with these forms of deception.

Self-reported safety behaviours reveal a mixed pattern. More intuitive practices, such as avoiding suspicious links or verifying information before sharing, are relatively common. However, more technical and preventive behaviours, such as regularly updating software, managing privacy settings, or verifying manipulated content, are less consistently adopted. This suggests that basic awareness does not always translate into effective protective practices.

Experiences with digital fraud are relatively frequent. Over one third of respondents (35.3%) reported having been victims of online scams, most commonly phishing, fraudulent purchases, and financial fraud. Even in cases where no financial loss occurred, these experiences contributed to reduced trust in digital environments and increased uncertainty in online interactions.

Concern about future victimisation is notably high, with more than 80% of respondents expressing moderate to strong levels of concern. At the same time, participants showed a strong interest in further training, particularly in areas such as recognising and preventing online fraud, protecting personal data, ensuring safe online banking practices, identifying misinformation, and developing practical strategies to improve digital security in everyday life.

Overall, the findings highlight a gap between widespread digital engagement and more advanced digital safety competences.

Interpretation

The Spanish findings point to a structural gap between digital participation and the ability to manage online risks independently among adults aged 45+.

While basic digital use is widespread, specific knowledge related to fraud prevention, cybersecurity practices, and risk recognition remains limited. This creates a situation in

which individuals are actively engaged in digital environments but not fully equipped to navigate them safely, increasing their exposure to both traditional and emerging threats.

Importantly, this vulnerability does not stem from a lack of motivation or resistance to technology. On the contrary, respondents expressed a clear willingness to learn and improve their skills. The main issue lies in the limited availability of accessible, targeted, and practice-oriented training specifically focused on digital safety.

The data also reveal a reliance on informal and reactive learning strategies. Many participants depend on family members, trial-and-error approaches, or online searches to solve problems, rather than drawing on structured knowledge or formal training. While these strategies may provide temporary solutions, they do not ensure consistent or effective protection, particularly in more complex or evolving risk scenarios.

In addition, the limited awareness of AI-related threats highlights a growing challenge. As digital risks become more sophisticated, traditional forms of detection based on intuition or prior experience are increasingly insufficient. This reinforces the need to update digital safety competences in line with technological developments.

The high level of concern about future victimisation, combined with the frequency of past experiences of fraud, indicates a strong perceived need for support. Respondents are aware of the risks but lack the confidence and tools required to address them effectively.

From a learning perspective, these findings underline the importance of developing targeted educational interventions that are practical, accessible, and tailored to adult learners. Training should focus on strengthening concrete competences, including recognising fraudulent patterns, managing personal data securely, verifying digital content, and responding appropriately to suspicious situations.

Non-formal educational approaches are particularly relevant in this context. Programmes should use clear language, real-life scenarios, and hands-on exercises to bridge the gap between everyday digital practices and more advanced safety skills. Strengthening digital autonomy and resilience will be essential to support adults aged 45+ in engaging safely and confidently in the digital society.

5.3 Slovakia

Purpose and Method

The Slovak survey was conducted as part of the digiSAFE needs assessment to evaluate the digital habits, technical confidence, awareness of online risks, and experiences with digital fraud among adults aged 45 and over. The data collected are intended to directly inform the development of the project's educational curriculum and digital safety toolkit.

The research adopted a quantitative approach, using a standardized online questionnaire designed to ensure accessibility and comparability across partner countries. The survey included a combination of Likert-scale and multiple-choice questions aimed at assessing key areas such as daily internet use, self-perceived digital competences, awareness of both traditional and emerging cyber threats, and direct experiences with online fraud.

At transnational level, a total of 131 responses were collected. For the purposes of the national analysis, the dataset was carefully filtered to include only respondents residing in Slovakia or in another European country, in line with project criteria. This process resulted in a final sample of 51 valid responses, meeting the minimum threshold required for comparability.

The sample is primarily composed of individuals in active professional and early-retirement stages: 43% of respondents are aged 45–54, 35% are 55–64, and 22% are 65+. Women represent 65% of the sample. Participants are relatively well educated, with most holding upper secondary or post-secondary qualifications, and are fairly evenly distributed between urban (55%) and rural (45%) areas. Overall, the sample reflects a digitally engaged population with diverse socio-demographic characteristics.

Key Results

The Slovak dataset reveals a high level of digital engagement among adults aged 45+, accompanied by significant gaps in cybersecurity competence.

Connectivity is particularly strong: 92% of respondents report daily use of a smartphone or computer. General confidence in performing basic online activities, such as emailing or online shopping, is also relatively high (68%). However, this frequent use does not translate into effective technical security.

Important weaknesses emerge in core digital safety competences. Only 35% of respondents feel fully confident in recognising whether a website is secure, for example by identifying HTTPS protocols or security indicators. Similarly, less than half (41%) report being able to adjust privacy and security settings on their devices. These findings suggest that while users are operationally active online, they lack the technical skills required to manage risks independently.

A clear divide is observed in the awareness of different types of cyber threats. Traditional risks are widely recognised: 85% of respondents report moderate or strong awareness of phishing emails, fraudulent SMS messages, and fake online stores. In contrast, awareness of emerging threats is significantly lower. A striking 78% of participants report being only slightly aware or not aware at all of AI-generated scams, such as deepfakes or voice

cloning. Similarly, 72% indicate low confidence in their ability to identify AI-manipulated media or news content.

Direct experience with digital fraud is also notable. One quarter of respondents (25%) report having been victims of online scams. The response patterns among victims highlight a critical issue: most rely on informal reactions, with 62% reporting that they either deleted the malicious message or sought help from family and friends. Only a small minority (15%) formally reported the incident to banks, online platforms, or law enforcement authorities.

Overall, the findings point to a strong imbalance between high levels of digital activity and limited capacity to manage both traditional and emerging online risks.

Interpretation

The Slovak findings highlight a pronounced gap between digital engagement and effective cybersecurity competence among adults aged 45+.

While respondents are frequent and confident users of digital technologies for everyday purposes, their ability to manage risks remains limited. This creates a “confidence gap,” in which individuals possess the operational skills needed to navigate digital environments but lack the technical knowledge required to ensure their own security. Digital adoption appears to be driven primarily by convenience and necessity, rather than by a comprehensive understanding of the digital ecosystem.

A key vulnerability concerns the rapid evolution of digital threats. While respondents demonstrate solid awareness of traditional forms of cybercrime, such as phishing or fake online stores, they are significantly less prepared to deal with more advanced forms of fraud. The very low awareness of AI-generated scams and limited ability to identify manipulated content indicate a critical generational gap. These emerging threats often rely on psychological manipulation and emotional triggers, making them more difficult to detect using conventional strategies.

Another important issue relates to behavioural responses to cyber incidents. The data reveal a strong reliance on informal coping mechanisms, such as ignoring suspicious messages or seeking help from personal networks. The extremely low rate of formal reporting suggests both a lack of knowledge about official procedures and the presence of psychological barriers, including embarrassment, fear, or a sense of inevitability. This limits the effectiveness of institutional protection mechanisms and increases the long-term impact of fraud.

From a learning perspective, these findings point to the need for a shift from basic digital participation towards more structured and proactive digital safety competences. Educational interventions should prioritise practical and scenario-based approaches, enabling learners to recognise and respond to real-life situations, particularly those involving sophisticated or AI-driven scams.

In addition, training should include clear and accessible guidance on configuring privacy and security settings, as well as step-by-step instructions on how to report incidents and seek institutional support. Addressing the psychological dimension of cybercrime, by normalising victimisation and reducing stigma, will also be essential to encourage more proactive and confident behaviours.

Strengthening both technical competence and user confidence will be key to supporting adults aged 45+ in Slovakia in moving from passive or reactive strategies towards more autonomous, informed, and resilient engagement in the digital environment.

6. Transnational Analysis

Comparing the national findings from Italy, Spain, and Slovakia reveals a set of striking convergences that point to a shared European challenge, alongside some meaningful national differences that have implications for the design of tailored educational interventions.

6.1 Common Challenges Across Countries

All three countries demonstrate a consistent and structurally significant gap between digital engagement and digital safety competence. Adults aged 45+ in Italy, Spain, and Slovakia are, to varying degrees, regular and active internet users – engaging with digital services for communication, banking, information retrieval, and e-commerce. Yet across all three contexts, self-assessed confidence and actual competency sharply decline when more specific digital safety skills are assessed: recognising secure websites, managing privacy settings, maintaining software updates, and handling data securely.

A second convergent pattern is the near-universal weakness in recognising AI-generated or AI-manipulated content. In all three countries, this is consistently identified as the most vulnerable area among respondents, far below awareness of traditional threats such as phishing or fake online stores. This finding is particularly urgent: AI-based fraud – deepfakes, voice cloning, AI-generated scam messages – is the fastest-growing category of digital threat, yet it is the one for which the 45+ population across Europe is least prepared.

A third shared challenge is reliance on informal, reactive coping strategies. In Italy, Spain, and Slovakia alike, many respondents rely on intuition, caution, or external support from family members rather than structured knowledge and skills. This "informal defence" approach may reduce some risks but is wholly inadequate in the face of sophisticated, AI-assisted deception. It also tends to reinforce digital avoidance behaviour rather than building genuine resilience.

Finally, all three countries report significant levels of concern about future victimisation (84.1% in Italy, over 80% in Spain, high in Slovakia as well) and notable rates of past victimisation – 38.1% in Italy, 35.3% in Spain, and 25% in Slovakia. The gap between concern and competence is a consistent feature across the transnational dataset.

6.2 Main Differences

Despite these convergences, meaningful differences exist between the three national contexts. Italy and Slovakia both show very high levels of daily digital engagement (77.8% and 92% respectively rating daily device use at the highest levels), while Spain's respondents show somewhat more moderate engagement patterns (mean daily device use 3.29/5). This suggests that Spanish respondents, while digitally active, may be somewhat less embedded in intensive digital routines than their Italian and Slovak counterparts.

The nature of predominant fraud threats varies across contexts. In Slovakia, a particularly severe and specific threat pattern has been documented: sophisticated vishing attacks in which fraudsters impersonate police officers or bank officials to manipulate victims into transferring funds. This form of social engineering exploits institutional trust in ways that are less documented in the Italian and Spanish contexts. Slovakia also faces a distinctive challenge related to the volume and impact of disinformation campaigns, amplified by the country's geopolitical situation.

Formal incident reporting rates differ starkly. Slovak respondents showed an alarmingly low formal reporting rate (only 15% of victims formally reported incidents), significantly lower than what emerged in the Italian and Spanish contexts. This points to a stronger culture of shame around victimisation in Slovakia and/or a weaker awareness of institutional reporting channels – a specific area requiring targeted intervention.

Italy presents a stronger institutional and programmatic infrastructure for digital inclusion (Repubblica Digitale, CPIA, GOL Programme) compared to Slovakia, where nationally led programmes are more recent and have reached fewer people. Spain occupies an intermediate position, with strong national frameworks (INCIBE, Digital Spain 2026) but uneven implementation across regions.

6.3 Behaviour Patterns

Across all three countries, respondents display a consistent behavioural pattern: confidence in high-frequency routine tasks (checking email, online banking, using messaging apps) coexists with insecurity and low competence in lower-frequency but high-stakes tasks (verifying website security, configuring privacy settings, identifying manipulated content). This pattern suggests that digital habitude creates a false sense of overall competence that does not extend to safety-critical behaviours.

Trust in digital tools is generally moderate to high for familiar, well-known platforms and services, but drops significantly when confronted with unknown sources, unfamiliar requests, or ambiguous situations. Respondents across all three countries tend to deal with such ambiguity by avoidance (not clicking, not engaging) rather than active verification – a risk-reducing but not risk-managing approach.

Exposure to risk is highest in Italy (38.1% victimisation rate), followed by Spain (35.3%), then Slovakia (25%). However, these differences may partly reflect differences in sample composition and survey dissemination channels. In all three countries, the most common forms of experienced fraud are financial (bank fraud, fake purchases, phishing), confirming that the financial domain is the primary arena of harm.

6.4 Transnational Insights from Best Practices

Across Italy, Spain, and Slovakia, the analysis of best practices reveals a number of common patterns that go beyond the specific national contexts and highlight shared approaches to digital safety education for adults aged 45+.

A strong emphasis on non-formal and practice-oriented learning emerges consistently across all three countries. Initiatives are rarely based on theoretical instruction alone; they prioritise hands-on activities, real-life scenarios, and step-by-step guidance. This reflects the need to translate abstract digital risks into concrete and understandable situations for adult learners. In Slovakia, this orientation is particularly evident in the Smart Senior Academies hosted by regional public libraries, where librarians and volunteer trainers guide small groups through practical exercises at their own pace, and in the grassroots seminars organised by the Union of Pensioners (JDS), which focus on immediate, locally relevant threats such as fraudulent e-shops and fake phone calls.

Many best practices also adopt a community-based and inclusive approach, implemented through local centres, associations, or public institutions that are already familiar and trusted by the target group. In all three countries, learning environments are designed to be accessible and low-threshold, reducing barriers to participation and fostering confidence among learners. Slovakia's decentralised model - most notably through the Slovak Telekom Endowment Fund's Zrelí na dobu digitálnu programme, which channels

funding directly to care homes and community centres - offers a particularly replicable example of how grassroots delivery can reach isolated seniors in rural areas who might not attend large, centrally organised courses.

The use of peer learning and intergenerational or peer-supported models represents another shared feature. In Italy, this is most visible in initiatives such as the Digital Civil Service, while in Spain volunteer-based mentoring and community engagement play a similar role. In Slovakia, the peer-to-peer trust model adopted by the JDS seminars, where learning takes place within networks of fellow seniors, demonstrates that reducing psychological anxiety around digital tools is as important as delivering content. Adults aged 45+ consistently benefit from collaborative and socially embedded learning processes rather than individual, self-directed models.

A pattern more visible in Slovakia than in the other two countries is the active involvement of the private sector in public digital education. The Bezpečne na nete portal, created by the cybersecurity company ESET, exemplifies how private-sector expertise can be channelled into free, continuously updated, and publicly accessible educational content, a model that other European contexts could replicate through corporate social responsibility frameworks.

Alongside these convergences, meaningful differences can be observed. Italy shows a stronger integration between national strategies and multi-level initiatives, with coordinated actions linking policy frameworks, training programmes, and awareness campaigns. Spain presents a more decentralised and varied landscape, where a wide range of actors operate at national, regional, and local levels, sometimes without strong coordination between them. Slovakia sits in an intermediate position: while its institutional framework is robust (coordinated by entities such as the NBÚ and MIRRI) the reach of formal programmes among the 45–64 age group remains limited, and the most effective initiatives tend to be non-formal and community-driven.

The overall evidence across all three partner countries points to the same conclusion: effective digital safety education for adults aged 45+ relies on a combination of accessibility, practical relevance, social learning, and trust. These elements represent key transferable components that should directly inform the development of the digiSAFE curriculum and toolkit.

7. Key Findings

The following key findings emerge from the transnational analysis of national research results:

1. Digital engagement does not equal digital safety. Across Italy, Spain, and Slovakia, adults aged 45+ are active and frequent internet users, yet consistently demonstrate low competence in digital safety-specific skills such as recognising secure websites, configuring privacy settings, and managing account security.
2. AI-based threats represent the most critical and universal gap. Awareness and recognition of AI-generated scams, deepfakes, and manipulated media are the weakest competency areas in all three countries. This is simultaneously the fastest-growing category of online threat, making it the most urgent priority for educational intervention.
3. Informal coping strategies predominate and are insufficient. The primary behavioural response to perceived risk across all three national samples is informal, intuitive, and reactive (avoidance, family support, general caution) rather than structured and proactive. This approach provides inadequate protection against sophisticated social engineering and AI-assisted fraud.
4. Past victimisation rates are high and underestimated. Between one quarter and nearly two fifths of survey respondents across the three countries reported direct experience with digital fraud, confirming that these risks are not theoretical but real and immediate for the target group.
5. Concern is high but is not matched by skills. Across all three countries, the vast majority of respondents (over 80%) express clear concern about future victimisation. This high level of concern, combined with acknowledged skill deficits, indicates a strong and unmet demand for targeted training.
6. Formal incident reporting is critically underused. A consistent pattern across all three countries – most pronounced in Slovakia – is the tendency to deal with fraud incidents informally, without reporting to banks, platforms, or law enforcement. This underreporting limits systemic responses and leaves victims without institutional support.
7. The "confidence gap" is a systemic vulnerability. In all three countries, respondents tend to overestimate their overall digital safety based on high proficiency in routine tasks, while underestimating their specific vulnerability in high-stakes, less familiar situations. This illusion of competence requires educational approaches that challenge assumptions and build genuinely critical digital awareness.
8. National policy frameworks exist but their implementation is uneven. All three countries have developed relevant regulatory frameworks and digital skills

programmes, but their reach among the 45+ demographic remains limited, particularly in Slovakia and in rural areas across all three countries.

8. Identified Gaps and Training Needs

Based on the desk research, survey analysis, and transnational comparison, the following specific gaps and training needs have been identified for adults aged 45+ across Italy, Spain, and Slovakia. While several of these gaps are common to all three contexts, their intensity and manifestation differ in ways that are directly relevant to curriculum design.

8.1 Skills Gaps

Across all three countries, a significant gap emerges between the frequency with which adults aged 45+ use digital technologies and their actual ability to manage online risks. In Slovakia, 92% of respondents reported daily use of a smartphone or computer - a figure consistent with the high connectivity rates observed in Italy and Spain - yet this frequency does not translate into structured knowledge of digital safety practices. In Slovakia, only 35% of respondents felt confident in recognising a secure website, and fewer than half (41%) reported knowing how to adjust privacy and security settings on their own devices. This pattern, which the Slovak report aptly describes as a "confidence gap", is structurally present across all three national samples, though it appears most acute in Spain, where heavy reliance on family members as a primary source of digital support suggests a form of dependency rather than genuine digital autonomy.

More specifically, the ability to technically verify the safety and authenticity of digital environments remains weak across all three countries: identifying secure websites (HTTPS indicators, padlock icons), recognising phishing email markers, or distinguishing legitimate from fraudulent SMS messages are competencies that a significant share of respondents have not developed. Device and account security management - including configuring privacy settings, using strong and unique passwords, enabling two-factor authentication, and performing regular software and antivirus updates - is practised by a minority and understood by fewer still. Italian respondents appear slightly more confident in some routine protective behaviours, while Spanish and Slovak participants show greater uncertainty in applying these practices consistently.

8.2 Knowledge Gaps

The most critical and universal knowledge gap across all three countries concerns the recognition of AI-generated or manipulated content. In Italy, this is already identified as one of the weakest competency areas, with consistently low self-assessment scores in identifying AI-based risks. The Slovak data reinforce this finding with particular clarity:

78% of respondents indicated they were only slightly aware or entirely unaware of AI-generated scams such as deepfakes and voice cloning, and 72% admitted little or no confidence in identifying AI-manipulated media or news. In Spain, awareness of such threats is even less developed, with a significant share of respondents reporting little or no familiarity with AI-related scams. Across all three contexts, this represents the most urgent educational gap - one that requires dedicated, scenario-based training rather than generic awareness-raising.

Beyond AI-related threats, significant knowledge deficits persist regarding the mechanisms of social engineering and the psychological manipulation tactics used by cybercriminals. In Slovakia, this is compounded by a specific and particularly damaging threat landscape: fraudsters frequently impersonate police officers or bank employees using number-spoofing technology, exploiting precisely the kind of institutional trust that older adults are most likely to extend - a pattern that formal training has not yet adequately addressed. Knowledge of data protection rights and of the formal procedures to follow after a fraud incident (who to report to, what recovery options exist) is also critically insufficient across all three national samples.

8.3 Awareness Gaps and Incident Response

A further gap, consistently present but varying in intensity across the three countries, concerns incident response and reporting behaviour. Among the 25% of Slovak respondents who had experienced digital fraud, only 15% chose to formally report the incident to a bank, platform, or law enforcement authority. The majority (62%) simply deleted the malicious message or sought informal help from family or friends. This pattern is mirrored in the Italian and Spanish findings and reflects a shared set of psychological barriers: shame, embarrassment, and a perceived sense of fatalism about cybercrime actively deter victims from engaging with institutional support systems. Addressing this barrier requires not only procedural guidance on reporting channels but a deliberate effort to destigmatise victimisation within educational programmes.

At the level of general awareness, the most significant gap concerns emerging threats. AI-based scams, deepfakes, voice cloning, and AI-generated disinformation are categories of risk that the majority of respondents in all three countries have limited or no familiarity with. There is also a broader lack of awareness regarding the concrete consequences of victimization (financial, social, and psychological) which may contribute to underestimating risk among those who have not yet been directly targeted.

Taken together, the comparative picture across Italy, Spain, and Slovakia highlights the importance of designing training approaches that are both transnationally coherent and adaptable to specific national needs. Slovakia presents a particularly pronounced vulnerability regarding AI-driven threats and the exploitation of institutional trust, while Spain shows stronger dependency on informal support networks, and Italy reflects a

slightly higher but still fragile baseline of technical confidence. These differences point to the value of a modular curriculum framework that can address shared competency gaps while allowing for country-level contextualisation.

9. Recommendations for Curriculum Development

The evidence gathered across the three national research phases provides a clear and evidence-based foundation for the digiSAFE Non-Formal Education (NFE) Curriculum. The following recommendations reflect the gaps and training needs identified in Section 8 and are structured around the core domains that should be addressed by the curriculum.

9.1 Thematic Modules

The curriculum is organised into a structured sequence of learning components, consisting of six core modules, supported by an initial orientation phase and a final closing and action-planning step.

The overall design allows flexibility in delivery. The full curriculum can be implemented as a 2-day intensive workshop, as a series of shorter sessions, or in a blended format combining in-person and online elements. At the same time, each module is designed to function as a standalone session of approximately 90 minutes, making the curriculum adaptable to different learning environments and time constraints.

This modular structure ensures that the curriculum can be both comprehensive and flexible, supporting full programme delivery as well as targeted interventions based on specific local needs.

1. **Module 0: Orientation & pre-assessment.** This introductory module responds to the diverse starting levels of digital confidence identified across all partner countries. The research shows that while many adults aged 45+ are active digital users, their awareness of risks and self-perceived competences vary significantly. This module is essential to build trust, reduce initial anxiety, and help participants reflect on their own digital habits, risk exposure, and learning needs before engaging with more technical content.
2. **Module 1: Safe everyday digital use.** This module directly addresses the gap identified between frequent digital use and limited understanding of basic safety principles. Across all countries, respondents reported high levels of daily digital engagement but showed inconsistencies in recognising safe environments and applying routine protective behaviours. The module supports learners in identifying safe-use practices, recognising trust signals, and developing more conscious and secure everyday digital habits.

3. **Module 2: Phishing, smishing & scam patterns.** This module responds to the high levels of exposure to online fraud identified in the research. In all three countries, phishing, fraudulent messages, and financial scams were among the most common threats experienced by respondents. The findings highlight the need for participants to recognise scam patterns, identify warning signs, and develop the ability to pause and critically assess suspicious communications before acting.
4. **Module 3: Safe payments, shopping & financial protection.** This module is justified by the widespread experience of financial fraud and fake online offers reported across the datasets. Many respondents indicated difficulties in distinguishing legitimate transactions from fraudulent ones, particularly in online shopping and digital payments. The module focuses on strengthening safer financial behaviours, helping learners recognise unreliable platforms and apply more secure decision-making strategies.
5. **Module 4: Privacy, passwords & device protection.** This module addresses consistent weaknesses in technical safety practices identified in all countries. The research highlights limited knowledge and inconsistent use of privacy settings, secure passwords, and software updates. These gaps significantly increase vulnerability to cyber threats. The module therefore focuses on strengthening account protection and promoting practical, everyday security routines.
6. **Module 5: AI, misinformation & manipulated content.** This module responds to one of the most critical and transversal gaps identified in the research: the limited ability to recognise AI-generated content and emerging forms of digital manipulation. Across all partner countries, awareness of AI-based threats—such as deepfakes, voice cloning, and synthetic media—was significantly lower than awareness of traditional risks. This module aims to develop critical thinking and verification skills needed to navigate increasingly complex digital information environments.
7. **Module 6: What to do when something goes wrong.** This module addresses a major gap in response knowledge and behaviour identified across the datasets. Many respondents reported uncertainty about how to react in case of fraud and relied primarily on informal strategies, such as ignoring incidents or seeking help from family members. Formal reporting rates were low. The module therefore focuses on providing clear response pathways, improving confidence in handling incidents, and increasing awareness of available support mechanisms.
8. **Closing: Personal digital safety plan.** The closing component responds to the need to translate learning into concrete behavioural change. The research findings show high levels of concern about digital risks but limited structured strategies to address them. This final step supports learners in consolidating their knowledge, defining personal safety actions, and increasing confidence in their ability to navigate digital environments safely and autonomously.

9.2 Methodological Principles

The research findings point clearly to a set of methodological principles that should guide the curriculum's design:

1. **Non-formal and experiential learning:** the curriculum must be grounded in real-life scenarios, case studies, and practical exercises rather than theoretical instruction. Adults aged 45+ respond best to learning that is immediately applicable to their daily digital experience.
2. **Scenario-based practice:** particular attention should be given to simulated scenarios in which learners can safely practise recognising and responding to fraud attempts (phishing emails, suspicious calls, AI-generated messages) without real-world risk.
3. **Accessible language and format:** technical cybersecurity concepts must be translated into clear, jargon-free language. Visual materials, step-by-step guides, and multimedia content should be used to support learners at different literacy levels.
4. **Graduated complexity:** the curriculum should be structured to build confidence progressively, beginning with immediately recognisable risks and advancing towards more complex and emerging threats. This graduated approach avoids overwhelming learners and reduces digital avoidance behaviour.
5. **Destigmatisation of victimisation:** given the documented reluctance to formally report fraud incidents, the curriculum should explicitly address the psychological aspects of cybercrime victimisation, normalising the experience and empowering learners to seek institutional support without shame.
6. **Adaptability to national and local contexts:** while the curriculum framework should be transnational, modules should allow for adaptation to reflect the specific fraud typologies, legal frameworks, and reporting channels relevant in each partner country.

10. Conclusion

The Transnational Report of the digiSAFE project synthesises the findings of national research conducted in Italy, Spain, and Slovakia, providing a comprehensive, evidence-based picture of the digital safety challenges and learning needs of adults aged 45+ across three European countries.

The evidence is clear and consistent: while adults in the target group are increasingly active in digital environments – using the internet for banking, communication, public services, and information – they are not adequately equipped to navigate the online risks these activities entail. The gap between digital engagement and digital safety competence is a structural feature of all three national contexts, not an individual failing. It reflects the pace of digital transformation, the insufficiency of existing educational provision targeted at this age group, and the rapidly evolving nature of threats – most notably the emergence of AI-driven fraud that outpaces existing awareness and defence strategies.

The research has identified concrete, actionable gaps: in skills (technical verification, device security, AI content recognition), in knowledge (fraud mechanisms, data protection rights, reporting procedures), and in awareness (emerging AI threats, institutional support channels). These gaps are the direct input for the digiSAFE NFE Curriculum and Digital Fraud Prevention Toolkit, which will be developed in the next phase of the project.

The best practices identified across all three countries demonstrate that effective, accessible, and community-based educational interventions for the 45+ demographic are entirely feasible. Initiatives ranging from the Italian digital facilitation network to Slovak peer-learning seminars and Spanish volunteer-led digital mentoring programmes show what works and provide replicable models for the digiSAFE educational outputs.

By building directly on the findings of the national research presented in this report, the digiSAFE project establishes a clear link between evidence and action. The identified gaps, needs, and behavioural patterns will directly inform the design and structure of the Non-Formal Education Curriculum and the Digital Fraud Prevention Toolkit, ensuring that both outputs are grounded in real user needs. In this way, the project is positioned to deliver a meaningful and measurable contribution to the digital resilience of older adults in Italy, Spain, Slovakia, and beyond, supporting safer, more informed, and more autonomous participation in the European digital society.

Bibliography / References

1. Agency for Digital Italy (AgID) (n.d.). Digital Skills Initiatives. <https://www.agid.gov.it/it/agenzia/competenze-digitali>
2. Bank of Italy (n.d.). Financial Education and Cybersecurity Awareness. <https://economieapertutti.bancaditalia.it>
3. CERTFin (n.d.). I Navigati Campaign. <https://inavigati.certfin.it/index.html>
4. Civic Association eSlovensko (n.d.). Zodpovedne.sk. <https://www.zodpovedne.sk/>
5. Department for Digital Transformation, Italy (n.d.). Repubblica Digitale Strategy. <https://repubblicadigitale.gov.it/portale/strategia>
6. Digitálna koalícia (n.d.). Improving the Digital Skills of Seniors. <https://digitalnakoalicia.sk>
7. Digital Skills and Jobs Platform – European Commission (2024). Spain: A Snapshot of Digital Skills. <https://digital-skills-jobs.europa.eu/en/latest/briefs/spain-snapshot-digital-skills>
8. Digital Skills and Jobs Platform – European Commission (2024). Slovakia: A Snapshot of Digital Skills. <https://digital-skills-jobs.europa.eu/en/latest/briefs/slovakia-snapshot-digital-skills>
9. ESET (n.d.). Bezpečne na nete. <https://bezpecnenanete.eset.com/sk/>
10. EU DisinfoLab (2023). Disinformation Landscape in Slovakia. <https://www.disinfo.eu>
11. European Commission (2024). Slovakia 2025 Digital Decade Country Report. <https://digital-strategy.ec.europa.eu/en/factpages/slovakia-2025-digital-decade-country-report>
12. European Commission (2025). Italy Digital Decade Country Report 2025. <https://digital-strategy.ec.europa.eu/en/factpages/italy-2025-digital-decade-country-report>
13. European Commission – Joint Research Centre (2025). How to Reach the EU Target of 80% of Adults with Basic Digital Skills by 2030. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/how-reach-eu-target-80-adults-basic-digital-skills-2030-2025-03-05_en
14. European Parliament and Council of the EU (2016). Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR). OJ L 119, 4.5.2016.
15. European Parliament and Council of the EU (2022). Directive (EU) 2022/2555 – NIS2 Directive.
16. Eurostat (2024). Digitalisation in Europe – 2024 Edition. <https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024>
17. Fundación Cibervoluntarios (n.d.). Digital Inclusion Programmes. <https://www.cibervoluntarios.org>

18. Gobierno de España (2018). Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (LOPDgdd). BOE.
19. Gobierno de España (2021). Plan Nacional de Competencias Digitales. <https://portal.mineco.gob.es>
20. Gobierno de España (2022). España Digital 2026 – Agenda Nacional de Transformación Digital. <https://espanadigital.gob.es/espana-digital>
21. INCIBE (2024). Los incidentes de ciberseguridad de 2023 gestionados por INCIBE. <https://www.incibe.es>
22. INCIBE (n.d.). Línea de Ayuda en Ciberseguridad 017. <https://www.incibe.es/linea-017>
23. ISTAT (2024). Citizens and ICT Report. https://www.istat.it/wp-content/uploads/2025/04/REPORT_CITTADINI-E-ICT_2024.pdf
24. ISTAT (2024). Digital Skills Statistics. <https://www.istat.it/wp-content/uploads/2024/04/2.pdf>
25. ISTAT (2025). Crimes Against Persons and Property Report. Italian National Institute of Statistics.
26. Italian Data Protection Authority – Garante (n.d.). Personal Data Protection Code. <https://www.garanteprivacy.it>
27. Krajská knižnica Žilina (n.d.). Smart Senior Academies. <https://www.krajskakniznicazilina.sk/>
28. Ministerio de Educación y Formación Profesional, Spain (n.d.). Aula Mentor. <https://www.aulamentor.es>
29. Ministry of Investments, Regional Development and Informatization of the Slovak Republic – MIRRI (n.d.). Digitálni seniori Programme. <https://www.digitalniseniori.gov.sk>
30. Ministry of Labour and Social Policies, Italy (n.d.). GOL Programme. <https://www.lavoro.gov.it/temi-e-priorita/occupazione/focus/pagine/programma-gol>
31. National Cybersecurity Agency – ACN, Italy (n.d.). National Cybersecurity Strategy 2022–2026. <https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza>
32. National Security Authority – NBÚ, Slovak Republic (2021). National Cybersecurity Strategy 2021–2025. <https://www.nbu.gov.sk/national-cybersecurity-strategy-of-the-slovak-republic-for-years-2021-2025/>
33. OECD (2024). Enhancing the Digital Skills of Seniors in the Slovak Republic. <https://www.oecd.org/en/about/programmes/dg-reform/enhancing-the-digital-skills-of-seniors-in-the-slovak-republic.html>
34. Policía Nacional, Spain (n.d.). Plan Mayor Seguridad. https://www.policia.es/_es/colabora_plan_mayor_seguridad.php

35. Polizia Postale, Italy (n.d.). Annual Cybersecurity Reports and Data.
<https://www.commissariatodips.it>
36. Repubblica Digitale (2025). Quarto rapporto di monitoraggio – Ottobre 2025.
 Department for Digital Transformation, Italy.
37. SafeHorizon Project (2026). Spain's Situation in the Cyberspace Domain.
<https://www.project-safehorizon.eu>
38. Slovak Republic (2018). Act No. 18/2018 Coll. on the Protection of Personal Data.
 National Council of the Slovak Republic.
39. Slovak Republic (2018). Act No. 69/2018 Coll. on Cybersecurity. <https://www.sk-cert.sk>
40. Slovak Republic (2024). Act No. 366/2024 Coll. – Transposition of the NIS2 Directive. National Council of the Slovak Republic.
41. Slovak Telekom Endowment Fund (n.d.). Zrelí na dobu digitálnu.
<https://nadcnyfondtelekom.sk/>
42. Union of Pensioners in Slovakia – JDS (n.d.). <https://www.jednotadochodcov.sk/>