

KA210-ADU Malé partnerstvo vo vzdelávaní dospelých

**Posilnenie postavenia dospelých:
Digitálna bezpečnosť a prevencia
podvodov v ére technológií | digiSAFE**



Číslo projektu:

2025-1-IT02-KA210-ADU-000359787

Nadnárodná správa



Oznámenie o otvorenej licencii

Tento dokument je licencovaný podľa licencie Creative Commons Attribution 4.0 International (CC BY 4.0).

Akronym projektu	digiSAFE
Názov projektu	Posilnenie postavenia dospelých: Digitálna bezpečnosť a prevencia podvodov v ére technológií
Číslo projektu	2025-1-IT02-KA210-ADU-000359787
Trvanie	Dátum začatia: 01-09-2025 Dátum ukončenia: 31-08-2027
Podprogram	Malé partnerstvo vo vzdelávaní dospelých
Webová stránka projektu	www.digisafeproject.eu
Dátum dodania	
Stav	Verzia 1.0
Autor	UNO
Zodpovedný autor	

Obsah

1. Úvod	4
2. Metodológia	5
3. Národný kontext	7
4. Osvedčené postupy	16
6. Nadnárodná analýza	55
7. Kľúčové zistenia	59
8. Identifikované medzery a vzdelávacie potreby	60
9. Odporúčania pre tvorbu kurikula	62
10. Záver	66
Bibliografia / Zdroje	67

1. Úvod

Projekt digiSAFE – "Posilnenie postavenia dospelých: Digitálna bezpečnosť a prevencia podvodov v ére technológií" – je malé partnerstvo programu Erasmus+ vo vzdelávaní dospelých (KA210-ADU, grantová dohoda č. 2025-1-IT02-KA210-ADU-000359787), ktoré realizuje medzinárodné konzorcium troch partnerských organizácií: Associazione Italiana Socio-Educatori per la Cooperazione – AISEC APS (Taliansko, koordinátor projektu), Asociación UNO (Španielsko) a IKREON (Slovensko). Projekt prebieha od 1. septembra 2025 do 31. augusta 2027.

Digitálna transformácia mení takmer každý aspekt každodenného života v celej Európe – od spôsobu, akým občania pristupujú k verejným službám a spravujú svoje osobné financie, až po to, ako komunikujú a prijímajú informácie. Hoci digitalizácia prináša nepopierateľné príležitosti, vytvára aj nové a rýchlo sa vyvíjajúce riziká, najmä online podvody, kybernetickú kriminalitu, dezinformácie a úniky údajov. Dospelí vo veku 45 a viac rokov sú týmito rizikami postihnutí neúmerne, keďže často kombinujú vysokú mieru digitálnej aktivity s obmedzeným povedomím o kybernetickej bezpečnosti a nedostatočným prístupom k cieľnému vzdelávaniu v oblasti digitálnej bezpečnosti.

Projekt digiSAFE vznikol s cieľom priamo riešiť túto medzeru. Jeho hlavnými výstupmi sú kurikulum neformálneho vzdelávania (NFE) zamerané na digitálnu bezpečnosť a prevenciu podvodov a praktická sada nástrojov na prevenciu digitálnych podvodov, pričom oba sú špecificky navrhnuté pre dospelých vo veku 45+. Aby boli tieto výstupy podložené dôkazmi, prvá fáza projektu zahŕňala komplexný národný výskum vo všetkých troch partnerských krajinách. Táto nadnárodná správa syntetizuje a porovnáva zistenia z týchto národných výskumných aktivít a predstavuje hlavný výstup aktivity A1 (fáza hodnotenia potrieb), ktorá poskytuje dôkazovú základňu pre tvorbu kurikula a sady nástrojov.

Cieľom tohto dokumentu je konsolidovať a analyzovať výsledky národného výskumu z Talianska, Španielska a Slovenska a porovnať zistenia naprieč tromi krajinami s cieľom identifikovať spoločné trendy, významné rozdiely a transnacionálne vzorce. Ďalej sa snaží identifikovať konkrétne medzery vo vzdelávaní a vzdelávacie potreby dospelých vo veku 45+ v súvislosti s digitálnou bezpečnosťou, prevenciou online podvodov a povedomím o kybernetickej bezpečnosti, pričom zároveň poskytuje odporúčania založené na dôkazoch pre návrh kurikula NFE a sady nástrojov na prevenciu digitálnych podvodov projektu digiSAFE.

Primárnou cieľovou skupinou, ktorej sa táto správa venuje, sú dospelí vo veku 45 a viac rokov, s osobitným zameraním na jednotlivcov s nízkou až strednou úrovňou digitálnych zručností, ktorí sú zraniteľnejší voči online rizikám. Táto skupina je v digitálnom prostredí

čoraz aktívnejšia, často jej však chýbajú potrebné kompetencie, sebadôvera a povedomie, aby sa v ňom pohybovala bezpečne a samostatne.

V tomto kontexte je správa v súlade s kľúčovými prioritami programu Erasmus+ a širšími prioritami Európskej únie, najmä s tými, ktoré sa týkajú digitálnej transformácie, sociálnej inklúzie a celoživotného vzdelávania, a to podporou rozvoja inkluzívnych a prístupných vzdelávacích prístupov pre dospelých.

2. Metodológia

Výskum, z ktorého vychádza táto nadnárodná správa, prebiehal súčasne vo všetkých troch partnerských krajinách počas prvej fázy projektu digiSAFE (koniec roka 2025 – začiatok roka 2026). Bola prijatá spoločná, harmonizovaná metodológia s cieľom zabezpečiť porovnateľnosť údajov a zistení naprieč národnými kontextami. Táto metodológia vychádzala zo spoločného výskumného rámca vypracovaného na úrovni projektu, pričom vedúci partner aktivity A1 (Asociación UNO) bol zodpovedný za prípravu výskumných usmernení, ktoré všetci partneri jednotne uplatňovali vo všetkých troch krajinách. Výskum kombinoval dva komplementárne prístupy: sekundárny výskum a kvantitatívny dotazník sebahodnotenia.

2.1 Sekundárny výskum

Každý národný partner vykonal rozsiahlu analýzu sekundárnych zdrojov vrátane oficiálnych štatistických údajov, národných politických dokumentov, legislatívnych nástrojov, správ Európskej komisie a akademickej a šedej literatúry, vybraných na základe ich relevantnosti a spoľahlivosti v súlade s výskumnými usmerneniami. Okrem mapovania národného kontextu na makroúrovni partneri tiež identifikovali súbor národných osvedčených postupov, ktoré majú slúžiť ako podklad pre tvorbu výstupov projektu. Cieľom sekundárneho výskumu bolo poskytnúť komplexný prehľad o každej krajine vrátane súčasného stavu digitálnej gramotnosti medzi dospelými vo veku 45+, existujúcich regulačných rámcov upravujúcich ochranu údajov a kybernetickú bezpečnosť a aktívnych programov alebo iniciatív podporujúcich digitálne vzdelávanie dospelých a online bezpečnosť. Použité zdroje sú zdokumentované v národných správach a konsolidované v bibliografickej časti tohto dokumentu.

2.2 Dotazník sebahodnotenia

V každej partnerskej krajine bol dospelým vo veku 45 a viac rokov predložený štandardizovaný kvantitatívny dotazník sebahodnotenia. Vo všetkých krajinách sa použil rovnaký dotazník s cieľom zabezpečiť porovnateľnosť výsledkov. Nástroj využíval kombináciu 5-bodových škál a otázok s viacerými možnosťami na posúdenie každodenných digitálnych návykov účastníkov, ich vnímanej sebadôvery v online

prostredí, špecifických zručností v oblasti digitálnej bezpečnosti, povedomia o rôznych typoch online hrozieb, priamej skúsenosti s digitálnymi podvodmi a vnímaných vzdelávacích potrieb. Hlavným účelom prieskumu bolo identifikovať digitálne kompetencie, úroveň povedomia o rizikách a vzdelávacie potreby medzi dospelými vo veku 45+.

Prieskum bol distribuovaný online prostredníctvom sietí jednotlivých partnerov s využitím komunikačných kanálov prispôsobených tak, aby oslovili cieľovú demografickú skupinu. Zber údajov prebiehal na dobrovoľnom a plne anonymnom základe v súlade so všeobecným nariadením o ochrane údajov (GDPR). Minimálny cieľ aspoň 50 platných odpovedí na krajinu, ako bolo stanovené v projektovom návrhu, bol stanovený s cieľom zabezpečiť spoľahlivosť údajov a porovnateľnosť výsledkov naprieč tromi národnými kontextami.

2.3 Účastníci

Údaje z prieskumu boli zozbierané vo všetkých troch partnerských krajinách, pričom každá krajina prispela porovnateľnou veľkosťou vzorky, čím sa zabezpečil vyvážený základ pre medzinárodnú analýzu. Vo všetkých troch vzorkách tvorili väčšinu respondentov ženy. Vekové rozloženie sa sústreďovalo v kategóriách 45–54 a 55–64 rokov, s menším zastúpením respondentov vo veku 65 a viac rokov. Účastníci pochádzali z rôznorodého mestského, prímestského a vidieckeho prostredia a vyznačovali sa rozmanitým vzdelaním a zamestnaním vrátane zamestnaných dospelých, samostatne zárobkovo činných osôb a dôchodcov. Celkovo vzorka odráža rozmanitú skupinu dospelých vo veku 45+, čím sa zvyšuje relevantnosť a reprezentatívnosť zistení.

2.4 Analýza údajov

Národné súbory údajov analyzoval každý partner nezávisle pomocou deskriptívnych štatistických metód. Analýza sa zameriavala na frekvencie, rozloženie odpovedí a identifikáciu opakujúcich sa vzorcov v rámci každej národnej vzorky. Partneri skúmali najmä kľúčové premenné, ako sú miera digitálneho používania, vnímaná sebadôvera, povedomie o online rizikách, skúsenosti s digitálnymi podvodmi a vyjadrené vzdelávacie potreby.

S cieľom zabezpečiť konzistentnosť sa vo všetkých krajinách uplatňoval spoločný analytický prístup, ktorý umožnil štruktúrované porovnanie výsledkov. Zistenia sa následne skúmali prostredníctvom medzikrajinových porovnaní, pričom sa zdôraznili podobnosti aj rozdiely v správaní, vnímaní a zraniteľnostiach účastníkov. Osobitná pozornosť sa venovala identifikácii vzorcov, ktoré sú relevantné pre návrh vzdelávacích

intervencií, vrátane oblastí spoločnej potreby, ako aj výziev špecifických pre jednotlivé krajiny.

Táto správa syntetizuje tieto analýzy a vyvodzuje nadnárodné závery na základe kombinovaných dôkazov, čím poskytuje súdržný základ pre tvorbu kurikula a sady nástrojov projektu digiSAFE.

3. Národný kontext

Táto časť poskytuje porovnávací prehľad digitálneho prostredia pre dospelých vo veku 45+ v každej partnerskej krajine. Pre každú krajinu analýza zahŕňa súčasný stav digitálnej gramotnosti, hlavné výzvy, ktorým čelí cieľová skupina, relevantné národné predpisy a politiky a existujúce programy a iniciatívy.

3.1 Taliansko

Digitálna gramotnosť a hlavné výzvy

Taliansko predstavuje pozoruhodný paradox: hoci sa dosiahol významný pokrok v oblasti digitálnej infraštruktúry a zavádzania digitálnych verejných služieb, štrukturálne medzery v digitálnych kompetenciách občanov pretrvávajú, najmä medzi staršími dospelými. Podľa správy Európskej komisie Digital Decade Country Report 2025 Taliansko dosiahlo pokrok v oblasti pripojiteľnosti a e-governmentu; pretrvávajú však kritické výzvy v schopnosti občanov efektívne a bezpečne používať digitálne technológie.

Údaje úradu ISTAT potvrdzujú tento dvojaký trend. V roku 2024 malo 86,2 % talianskych domácností prístup na internet, no toto číslo klesá na 60,6 % v domácnostiach zložených výlučne zo starších osôb. Používanie internetu sa výrazne líši podľa veku: zatiaľ čo internet v predchádzajúcich troch mesiacoch používalo 81,9 % celkovej populácie vo veku 6 a viac rokov, vo vekovej skupine 65–74 rokov to bolo len 68,1 %. Tento obraz ešte zhoršujú regionálne rozdiely, pričom južné regióny zaostávajú za centrálnym a severným Talianskom v prístupe aj používaní.

Úroveň digitálnych zručností medzi staršími dospelými zostáva kritickým problémom. V roku 2023 malo len 45,9 % jednotlivcov vo veku 16–74 rokov, ktorí používali internet, aspoň základné digitálne zručnosti. Tento podiel klesá od 48,7 % v skupine 45–54 rokov, na 38,5 % v skupine 55–64 rokov a iba 19,3 % v skupine 65–74 rokov. V dôsledku toho mnohí dospelí v skupine 45+ narážajú na ťažkosti pri samostatnom prístupe k digitálnym službám, hodnotení online informácií a ochrane pred online rizikami.

Online podvody a kybernetická kriminalita predstavujú rastúci a konkrétny problém. ISTAT odhaduje, že približne 1,7 milióna jednotlivcov – čo zodpovedá 3,3 % používateľov internetu – sa stalo obeťou online podvodov alebo podvodných praktík v 12 mesiacoch predchádzajúcich prieskumu v rokoch 2022–2023. Prípady finančných podvodov

prostredníctvom online bankovníctva vzrástli o 74 % v porovnaní s obdobím 2015–2016. V roku 2024 platforma Commissariato di PS Online zaznamenala približne 3 milióny návštev, vyše 82 000 hlásení a približne 23 000 žiadostí o pomoc súvisiacich s phishingom a online podvodmi.

Tieto údaje naznačujú, že pre dospelých vo veku 45+ už problémom nie je samotný prístup, ale kvalita a samostatnosť digitálneho používania.

Národné predpisy a politiky

Taliansko vyvinulo komplexný regulačný a politický rámec pre digitálnu bezpečnosť. Ochrana údajov sa riadi nariadením GDPR (EÚ 2016/679), ktoré sa na národnej úrovni vykonáva prostredníctvom legislatívneho dekrétu č. 196/2003 v znení neskorších predpisov, pričom dohľad zabezpečuje taliansky úrad na ochranu údajov (Garante per la protezione dei dati personali). Kódex digitálnej administratívy stanovuje digitálne práva občanov v interakciách s verejnou správou, zatiaľ čo Agentúra pre digitálne Taliansko (AgID) podporuje digitálne občianstvo a nahlásovanie porušení. Kybernetická bezpečnosť sa koordinuje prostredníctvom Národnej stratégie kybernetickej bezpečnosti 2022–2026, ktorú spravuje Národná agentúra pre kybernetickú bezpečnosť (ACN). Taliansko tiež transponovalo smernicu NIS2 prostredníctvom legislatívneho dekrétu č. 138/2024 a vo finančnom sektore implementovalo nariadenie o digitálnej prevádzkovej odolnosti (DORA).

Existujúce programy a iniciatívy

Popri regulačných opatreniach Taliansko vyvinulo širokú škálu programov a iniciatív na podporu digitálnej inklúzie a vzdelávania dospelých. Ústrednú úlohu zohráva Repubblica Digitale, národná iniciatíva vedená Oddelením pre digitálnu transformáciu, ktorá koordinuje Národnú stratégiu pre digitálne zručnosti a podporuje spoluprácu medzi verejnými inštitúciami, aktérmi súkromného sektora a organizáciami občianskej spoločnosti. V rámci tohto rámca má sieť digitálnej facilitácie (Digital Facilitation Network) za cieľ osloviť do roku 2026 dva milióny občanov prostredníctvom 4 000 fyzických prístupových bodov (Punti Digitale Facile), ktoré poskytujú podporu pri prístupe k digitálnym službám a zlepšovaní online bezpečnosti.

Medzi ďalšie iniciatívy patrí Servizio Civile Digitale a ciele programy financovania ako Dritti al Punto, ktoré podporujú vzdelávacie aktivity zamerané na povedomie o kybernetickej bezpečnosti, kritické používanie informácií a bezpečný prístup k verejným digitálnym službám. Paralelné politiky trhu práce, ako program GOL (Garanzia di Occupabilità dei Lavoratori), majú za cieľ zapojiť tri milióny prijímateľov so silným dôrazom na rozvoj digitálnych zručností.

Vzdelávanie dospelých ďalej podporujú Centrá vzdelávania dospelých (CPIA), ktoré slúžia ako kľúčové územné centrá celoživotného vzdelávania. Tieto centrá poskytujú príležitosti

na formálne aj neformálne vzdelávanie a zohrávajú kľúčovú úlohu pri oslovovaní zraniteľných skupín vrátane starších dospelých s nízkou úrovňou vzdelania alebo digitálnych zručností. Ich funkcia je súčasťou širších politík podporujúcich celoživotné vzdelávanie a rozvoj zručností v celej populácii.

Napokon k zvyšovaniu povedomia a podpore bezpečného online správania prispieva široká škála inštitucionálnych a sektorových aktérov. Agentúra pre digitálne Taliansko (AgID) a Národná agentúra pre kybernetickú bezpečnosť (ACN) podporujú šírenie digitálnych a kyberbezpečnostných zručností, zatiaľ čo Poštová polícia poskytuje preventívne a asistenčné služby. Úrad na ochranu údajov podporuje povedomie o právach na súkromie a finančné inštitúcie ako Talianska národná banka spolu s iniciatívami ako I Navigati prispievajú k vzdelávaniu občanov o online podvodoch a finančných kyberbezpečnostných rizikách.

Celkovo taliansky kontext poukazuje na významnú medzeru medzi rýchlou digitalizáciou služieb a skutočnou schopnosťou dospelých (najmä vo veku 45 a viac rokov) používať tieto nástroje bezpečne a efektívne. Hoci je regulačný a inštitucionálny rámec dobre rozvinutý, kľúčovou výzvou zostáva zabezpečiť, aby všetci občania, najmä starší dospelí, získali potrebné zručnosti na plnohodnotnú a bezpečnú účasť v digitálnej spoločnosti.

3.2 Španielsko

Digitálna gramotnosť a hlavné výzvy

Španielsko zaznamenalo za posledné desaťročie rýchlu digitálnu transformáciu, ktorá zmenila spôsoby, akými občania komunikujú s verejnými službami, finančnými inštitúciami, zdravotníckymi systémami a komunikačnými platformami. Rozšírené prijatie online bankovníctva, platforiem e-governmentu, digitálnych zdravotníckych služieb a sociálnych médií výrazne zvýšilo digitálnu prepojenosť populácie, čím sa zlepšila dostupnosť aj administratívna efektívnosť.

Napriek tomuto celkovému pokroku však v Španielsku pretrváva digitálna priepasť. Táto priepasť je silne spojená s vekom, vzdelaním a sociálno-ekonomickými podmienkami. Dospelí vo veku 45 a viac rokov, a najmä tí nad 55 rokov, majú tendenciu uvádzať nižšiu úroveň digitálnej sebadôvery a obmedzenejšiu oboznámenosť s postupmi digitálnej bezpečnosti. Mnohí jednotlivci v tejto vekovej skupine nezískali digitálne zručnosti počas svojho formálneho vzdelávania alebo profesijnej kariéry, čo robí prispôbenie sa rýchlo sa vyvíjajúcim digitálnym prostrediam zložitejším a často pomalším.

Táto generačná priepasť sa ďalej odráža vo vzorcoch digitálneho používania a vystavenia online rizikám. Online podvody a kybernetická kriminalita predstavujú v španielskom kontexte čoraz významnejší problém. Medzi bežné hrozby patria phishingové e-maily,

podvodné SMS správy, krádeže identity, falošné online služby a finančné podvody. Dospelí vo veku 45+ sú obzvlášť zraniteľní, keďže často kombinujú pravidelné používanie digitálnych služieb (ako online bankovníctvo, aplikácie na zasielanie správ a elektronický obchod) s nižším povedomím o kyberbezpečnostných rizikách a preventívnych postupoch. Okrem toho rastúca sofistikovanosť techník sociálneho inžinierstva, vrátane využívania podvodných mechanizmov podporovaných umelou inteligenciou, tieto zraniteľnosti ďalej zintenzívňuje a sťažuje odhalenie menej skúseným používateľom.

Na inštitucionálnej úrovni Španielsko vypracovalo súbor národných stratégií zameraných na digitálnu transformáciu, kybernetickú bezpečnosť a digitálnu inklúziu. Tieto politické rámce majú za cieľ posilniť digitálne kompetencie občanov, zlepšiť mechanizmy ochrany údajov a podporiť bezpečnejšie a zodpovednejšie zaobchádzanie s digitálnymi technológiami. Popri týchto národných stratégiách verejné inštitúcie, regionálne vlády a organizácie občianskej spoločnosti zaviedli rôzne vzdelávacie programy a osvetové iniciatívy zamerané na digitálnu gramotnosť dospelých a online bezpečnosť.

Existujúce iniciatívy však zostávajú fragmentované a nerovnomerne rozložené medzi regiónmi. Mnohé programy navyše majú tendenciu uprednostňovať získavanie základných digitálnych zručností, pričom menej pozornosti venujú digitálnej bezpečnosti, prevencii podvodov a kritickému povedomiu o online rizikách. Táto medzera zdôrazňuje potrebu štruktúrovanejších, prístupnejších a cielenejších vzdelávacích intervencií osobitne navrhnutých na posilnenie digitálnej odolnosti dospelých vo veku 45 a viac rokov.

V tomto kontexte projekt digiSAFE priamo reaguje na tieto výzvy kombináciou výskumu, neformálneho vzdelávania a praktických nástrojov zameraných na posilnenie kompetencií v oblasti online bezpečnosti a podporu bezpečnejšej účasti v digitálnej spoločnosti.

Národné predpisy a politiky

Reakcia Španielska na digitálnu bezpečnosť a prevenciu podvodov je zasadená do viacúrovňového systému správy, ktorý kombinuje národnú legislatívu so širšími strategickými politickými rámcami zameranými na podporu digitálnej transformácie a inklúzie. V posledných rokoch španielska vláda čoraz viac dopĺňa regulačné prístupy komplexnými národnými stratégiami navrhnutými na zníženie digitálnych nerovností a posilnenie digitálnych schopností občanov, najmä medzi zraniteľnými skupinami, ako sú dospelí vo veku 45 a viac rokov.

Kľúčovým pilierom tohto prístupu je národná stratégia Digital Spain 2026, ktorá slúži ako hlavná mapa digitálnej transformácie krajiny. Táto stratégia podporuje hospodársky rast, sociálnu súdržnosť a územnú inklúziu prostredníctvom digitalizácie, pričom výslovne rieši existujúce digitálne priepasti súvisiace s vekom, pohlavím a geografiou. Medzi jej priority

patrí rozšírenie digitálnej infraštruktúry, podpora nových technológií a posilnenie digitálnych zručností občanov ako prostriedku na zabezpečenie toho, aby žiadna skupina nezostala v digitálnom prechode pozadu.

V rámci tohto rámca zohráva ústrednú úlohu pri podpore digitálnej inklúzie Národný plán digitálnych zručností (Plan Nacional de Competencias Digitales). Jeho cieľom je vybaviť občanov, pracovníkov a verejnú správu potrebnými zručnosťami na fungovanie v čoraz digitálnejšej spoločnosti. Plán sa osobitne zameriava na štrukturálne medzery v digitálnej gramotnosti, ktoré stále zasahujú významnú časť populácie, najmä starších dospelých a iné zraniteľné skupiny. Medzi jeho opatrenia patria rozsiahle vzdelávacie programy, rekvalifikačné iniciatívy a opatrenia na zníženie rodových a územných nerovností v prístupe k digitálnym kompetenciám.

Okrem toho programy ako iniciatíva UNICO Broadband majú za cieľ rozšíriť prístup k vysokorýchlostnému internetu vo vidieckych a nedostatočne obsluhovaných oblastiach, čím sa znižujú územné rozdiely a zabezpečuje sa spravodlivejší prístup k digitálnym službám v celej krajine. Tieto iniciatívy zdôrazňujú dôležitosť riešenia nielen individuálnych zručností, ale aj štrukturálnych podmienok prístupu, ako je pripojiteľnosť.

Tieto strategické iniciatívy sú zasadené do širšieho Plánu obnovy, transformácie a odolnosti, ktorý integruje digitalizáciu ako základný pilier hospodárskeho a sociálneho rozvoja. Prostredníctvom koordinovaných investícií a reforiem sa Španielsko snaží nielen modernizovať svoju ekonomiku, ale aj zabezpečiť inkluzívny prístup k digitálnym technológiám a službám pre celú populáciu.

Popri týchto strategických rámcoch Španielsko vyvinulo pevnú právnu štruktúru zameranú na digitálnu bezpečnosť. Základný právny rámec stanovuje Organický zákon 3/2018 o ochrane osobných údajov a záruke digitálnych práv (LOPDgdd), ktorý implementuje všeobecné nariadenie o ochrane údajov (GDPR) do španielskeho právneho systému. Tieto nástroje regulujú spracúvanie a ochranu osobných údajov, pričom uznávajú digitálne práva ako základné práva. Povedomie a efektívne porozumenie týchto práv však zostáva nerovnomerné, najmä medzi staršími používateľmi, ktorí sa čoraz viac spoliehajú na digitálne služby.

V oblasti kybernetickej bezpečnosti kráľovský zákonný dekrét 12/2018 a kráľovský dekrét 43/2021 transponujú európske požiadavky kybernetickej bezpečnosti do národného práva, čím posilňujú inštitucionálnu kapacitu Španielska pri riadení digitálnych rizík. Podobne online podvody rieši španielsky trestný zákonník (Organický zákon 10/1995), ktorý kriminalizuje širokú škálu kybernetických trestných činov vrátane phishingu a krádeže identity. Rastúca sofistikovanosť digitálnych podvodov však zdôrazňuje potrebu doplnkových opatrení zameraných na prevenciu a povedomie používateľov.

Ochrana spotrebiteľa a regulácia platforiem ďalej posilňujú tento rámec prostredníctvom nástrojov ako kráľovský legislatívny dekrét 1/2007 a zákon 34/2002 (LSSI), zosúladených s

európskym vývojom, ako je nariadenie o digitálnych službách (Digital Services Act). Tieto predpisy zvyšujú transparentnosť, zodpovednosť a ochranu používateľov v digitálnom prostredí.

Napokon, rýchle rozširovanie digitálnych verejných služieb sprevádzali iniciatívy ako Plán digitalizácie verejnej správy, ktorého cieľom je zlepšiť dostupnosť, efektívnosť a používateľskú skúsenosť v interakciách s verejnými inštitúciami. Hoci však tento vývoj predstavuje významný pokrok, môže tiež neúmyselne posilniť existujúce nerovnosti, ak nie je sprevádzaný primeranými opatreniami v oblasti digitálnej gramotnosti. Najmä starší dospelí s obmedzenými digitálnymi zručnosťami môžu čeliť ďalším bariéram pri prístupe k základným službám, ktoré sú čoraz častejšie dostupné predovšetkým online.

Celkovo Španielsko kombinuje komplexný právny rámec s čoraz robustnejším súborom národných stratégií zameraných na digitálnu transformáciu a inklúziu. Medzi existenciou týchto politík a ich účinným vplyvom na každodenné digitálne praktiky občanov však zostáva významná medzera. Najmä dospelým vo veku 45 a viac rokov často chýbajú potrebné znalosti a zručnosti, aby mohli z týchto opatrení plne ťažiť. Táto medzera zdôrazňuje dôležitosť vzdelávacích a osvetových iniciatív, ako je digiSAFE, ktoré pretvárajú regulačné a strategické rámce do praktických znalostí a každodenných kompetencií.

Existujúce programy a iniciatívy

V Španielsku sa digitálnej inklúzii starších dospelých venuje niekoľko iniciatív, najmä v rámci národných programov zameraných na zlepšovanie digitálnych kompetencií v celej populácii. Verejné iniciatívy podporované španielskou vládou, ako aj miestne programy realizované obcami, mimovládny organizáciami a centrami vzdelávania dospelých poskytujú starším občanom základné školenie digitálnej gramotnosti so zameraním na používanie smartfónov, navigáciu na internete a prístup k digitálnym verejným službám. Napríklad programy ako workshopy digitálneho vzdelávania ponúkané vo verejných knižniciach a komunitných centrách poskytujú starším dospelým praktickú podporu pri učení sa používať mobilné aplikácie a pristupovať k platformám e-governmentu. Okrem toho iniciatívy podporované v rámci Národného plánu digitálnych zručností zahŕňajú základné kurzy zamerané na zlepšenie digitálnej samostatnosti starších občanov. Podobne mimovládne organizácie často organizujú úvodné stretnutia zamerané na každodenné digitálne úlohy, ako je online bankovníctvo alebo objednávanie sa k lekárovi, čím posilňujú praktické používanie digitálnych nástrojov.

Tieto iniciatívy však majú tendenciu uprednostňovať všeobecnú digitálnu inklúziu pred digitálnou bezpečnosťou. Vzdelávacie aktivity sa často zameriavajú na to, ako používať digitálne nástroje, s obmedzenou pozornosťou venovanou rizikám spojeným s online prostredím, ako sú podvody, phishing alebo nové podvody založené na umelej

inteligencii. V Španielsku zohráva kľúčovú úlohu Instituto Nacional de Ciberseguridad (INCIBE), ktorý pôsobí ako národné referenčné miesto pre kybernetickú bezpečnosť. Táto verejná inštitúcia poskytuje osvetové kampane, vzdelávacie zdroje a podporné služby zamerané na predchádzanie kybernetickým hrozbám a pomoc občanom pri reagovaní na digitálne riziká. Napriek dôležitej úlohe, ktorú INCIBE zohráva, sú však tieto iniciatívy vo všeobecnosti navrhnuté pre širšiu populáciu a nezameriavajú sa konkrétne na dospelých vo veku 45+ prostredníctvom štruktúrovaných a kontinuálnych vzdelávacích dráh.

Celkovo, hoci Španielsko vyvinulo komplexný národný rámec pre digitálnu inklúziu a kybernetickú bezpečnosť, ako sa uvádza v časti 1.2, jeho praktická implementácia zostáva nerovnomerná. Rozdiely v prístupe k vzdelávaniu, úrovne digitálnej gramotnosti a nedostatok cielených programov pre konkrétne vekové skupiny obmedzujú účinnosť týchto politík. Táto medzera medzi regulačnými rámcami a praktickými výsledkami zdôrazňuje potrebu inkluzívnejších a prispôbených prístupov. V dôsledku toho pretrváva významná medzera medzi snahami o digitálnu inklúziu a rozvojom praktických zručností na prevenciu podvodov medzi staršími dospelými. To zdôrazňuje potrebu cielených vzdelávacích prístupov, ktoré kombinujú digitálnu gramotnosť s praktickým nácvikom rozpoznávania online hrozieb a reagovania na ne. V tomto kontexte digiSAFE priamo rieši túto medzeru tým, že ponúka prispôbený model učenia založený na scenároch, špecificky navrhnutý pre dospelých vo veku 45 a viac rokov.

3.3 Slovensko

Digitálna gramotnosť a hlavné výzvy

Slovenská republika čelí špecifickej výzve: hoci sa digitálna infraštruktúra a pripojiteľnosť výrazne zlepšili, ľudský kapitál potrebný na bezpečný pohyb v digitálnom prostredí zostáva výrazne nedostatočne rozvinutý, najmä medzi staršou populáciou. Podľa správy Európskej komisie Digital Decade Country Report 2024 Slovensko dosiahlo pokrytie základnými digitálnymi zručnosťami na úrovni 51,3 % – mierny pokles oproti predchádzajúcim meraniam a pod priemerom EÚ vo výške 55,6 %.

Rozdiely sú obzvlášť výrazné medzi staršími demografickými skupinami. Medzi slovenskými seniormi vo veku 65–74 rokov má len 11 % základné alebo mierne pokročilé digitálne zručnosti – menej ako polovica priemeru EÚ vo výške 24 % pre rovnakú vekovú skupinu. Okrem toho 27 % seniorov v tejto vekovej skupine nikdy nepoužilo internet a iba 39 % použilo počítač v predchádzajúcich dvanástich mesiacoch. Pre dospelých vo veku 45–64 rokov sú digitálne zručnosti často obmedzené na rutinné operácie a chýba im

kritická hĺbka a analytické rámce potrebné na zvládanie vyvíjajúcich sa kyberbezpečnostných hrozieb.

Slovensko čelí špecifickým a závažným typológiám podvodov. Veľmi rozšírená taktika spočíva v tom, že podvodníci sa vydávajú za policajtov, bezpečnostných zamestnancov bánk alebo zástupcov Národnej banky Slovenska, pričom zneužívajú technológiu falšovania telefónnych čísel (spoofing) na manipuláciu zobrazenia volajúceho a využívajú taktiky založené na strachu na získanie bankových prihlasovacích údajov alebo na donútenie obetí, aby previedli prostriedky na podvodné účty. Slovenský digitálny priestor je navyše silne vystavený kampaniam šíriacim mylné informácie a dezinformácie spojeným s geopolitickým postavením a domácou politickou polarizáciou.

Národné predpisy a politiky

Na ochranu digitálnych práv občanov a boj proti kybernetickým hrozbám Slovenská republika vypracovala regulačný rámec prísne zosúladený so smernicami Európskej únie. Základom ochrany údajov na Slovensku je všeobecné nariadenie o ochrane údajov (GDPR), integrované do národného práva prostredníctvom zákona č. 18/2018 Z. z. o ochrane osobných údajov. Táto legislatíva, účinná od mája 2018, stanovuje jasné usmernenia pre zákonné spracúvanie osobných údajov a vyžaduje transparentnosť, minimalizáciu údajov a obmedzenie účelu. Občanom zaručuje právo na prístup k svojim údajom, ich opravu a vymazanie, ako aj ochranu pred neoprávneným automatizovaným rozhodovaním.

Na dodržiavanie týchto predpisov dohliada Úrad na ochranu osobných údajov Slovenskej republiky (ÚOOÚ). Ako nezávislý dozorný orgán ÚOOÚ zabezpečuje súlad vo verejnom aj súkromnom sektore. Poskytuje tiež záväzné usmernenia ku komplexným otázkam ochrany údajov, ako je vykonávanie posúdení vplyvu na ochranu údajov. Slovenské právo prísne reguluje používanie národného rodného čísla. Verejné zverejnenie tohto identifikátora je zakázané, pokiaľ ho výslovne nepovolí daná osoba alebo ho nevyžaduje osobitná legislatíva, čo slúži ako kľúčové opatrenie na predchádzanie krádeži identity.

Pokiaľ ide o kybernetickú bezpečnosť, primárnym legislatívnym nástrojom je zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorý pôvodne transponoval európsku smernicu NIS. Tento zákon stanovil základ národnej správy kybernetickej bezpečnosti, pričom definoval právne povinnosti prevádzkovateľov základných služieb, požiadavky na hlásenie incidentov a audítorské postupy. S cieľom riešiť vyvíjajúce sa hrozby Slovensko aktualizovalo tento rámec tak, aby spĺňal pokročilé požiadavky smernice NIS2 (smernica (EÚ) 2022/2555). Prostredníctvom zákona č. 366/2024 Z. z. s účinnosťou od 1. januára 2025 Slovensko výrazne rozšírilo rozsah svojich predpisov o kybernetickej bezpečnosti. Novela zavádza presný mechanizmus na identifikáciu povinných subjektov, zachytáva širší okruh kritických sektorov a presadzuje prísnejšie bezpečnostné opatrenia.

Národný bezpečnostný úrad (NBÚ) koordinuje tieto legislatívne úsilia prostredníctvom Národnej stratégie kybernetickej bezpečnosti 2021–2025. Stratégia načrtáva priority vrátane

zabezpečenia pripravenosti štátu, odhaľovania kybernetickej kriminality, budovania odolného súkromného sektora, integrácie kybernetickej bezpečnosti do verejnej správy a rozvoja digitálnych zručností odborníkov aj širokej verejnosti. Tento dôraz na verejné vzdelávanie zdôrazňuje, že technická obrana musí byť priamo podporená povedomím občanov a individuálnou digitálnou odolnosťou.

Existujúce programy a iniciatívy

Implementácia digitálnej stratégie Slovenska sa opiera o spoluprácu medzi verejnými inštitúciami, mimovládnyimi organizáciami, orgánmi činnými v trestnom konaní a súkromným sektorom s cieľom preklenúť digitálnu priepasť a zvýšiť online bezpečnosť dospelých.

Tieto úsilie vedie Ministerstvo investícií, regionálneho rozvoja a informatizácie (MIRRI), ktoré spravuje kľúčové súčasti národného Plánu obnovy a odolnosti. Jeho vlajková iniciatíva "Digitálni seniori" má za cieľ poskytnúť do roku 2026 školenie digitálnych zručností viac ako 100 000 seniorom (vo veku 65+) a znevýhodneným jednotlivcom. Program poskytuje lokalizované školenia a absolventom dáva nakonfigurovaný tablet a balík mobilných dát, čím priamo rieši vzdelávacie aj hardvérové bariéry.

V oblasti bezpečnosti Národný bezpečnostný úrad (NBÚ) a Národné centrum kybernetickej bezpečnosti (SK-CERT) riadia technickú kybernetickú bezpečnosť a národnú reakciu na incidenty, pričom zároveň prispievajú k osvetovým kampaniam pre verejnosť. Okrem toho Policajný zbor Slovenskej republiky aktívne bojuje proti digitálnym podvodom a dezinformáciám. Prostredníctvom svojho dedikovaného verejného komunikačného kanála "Hoaxy a podvody – Polícia SR" polícia monitoruje digitálny priestor, vyvracia virálne hoaxy, upozorňuje občanov na nové finančné podvody a vzdeláva verejnosť v rozpoznávaní podvodných komunikácií.

Medzisektorová spolupráca je formalizovaná prostredníctvom Digitálnej koalície, partnerstva spájajúceho vládu, IT priemysel, akademickú obec a občiansku spoločnosť. Táto platforma vykonáva národné hodnotenia, ako je IT Fitness Test, na vyhodnotenie digitálnych kompetencií populácie a identifikáciu demografických skupín vyžadujúcich vzdelávaciu intervenciu. Koalícia tiež spolupracuje s MIRRI na navrhovaní prispôsobených školení pre seniorov a starších zamestnancov verejnej správy.

Mimovládne organizácie a súkromný sektor poskytujú nevyhnutnú špecializovanú podporu. Nezávislé iniciatívy ako Konšpiratori.sk ponúkajú verejnosti transparentné databázy webových stránok známych šírením dezinformácií alebo podvodného obsahu, ktoré slúžia ako praktické nástroje na overovanie zdrojov. Vo finančnom sektore Slovenská banková asociácia a jednotlivé banky pravidelne realizujú ciele osvetové kampane na prevenciu podvodov v online bankovníctve. Tieto kampane učia zákazníkov, ako rozpoznať pokusy o phishing, používať viacfaktorovú autentifikáciu a bezpečne sa pohybovať v elektronickom bankovníctve.

Hoci Slovensko vybudovalo pevný inštitucionálny základ, dosiahnutie širokej digitálnej odolnosti medzi dospelými vo veku 45 a viac rokov si vyžaduje trvalé úsilie. Úspech závisí od nepretržitého rozširovania prístupných programov neformálneho vzdelávania a účinného šírenia praktických kyberbezpečnostných nástrojov.

4. Osvedčené postupy

Národný sekundárny výskum identifikoval celkovo pätnásť osvedčených postupov naprieč tromi partnerskými krajinami – päť na krajinu – ktoré predstavujú rozmanitú škálu aktérov, metodológií a cielených prístupov. Tieto iniciatívy ukazujú, ako sa výzvy digitálnej bezpečnosti riešia prostredníctvom prevencie, vzdelávania a posilňovania na rôznych úrovniach správy a občianskej spoločnosti. Postupy sú nižšie prezentované podľa krajín, s použitím jednotného formátu.

4.1 Taliansko

Počas sekundárneho výskumu bolo identifikovaných päť relevantných národných osvedčených postupov, ktoré odrážajú rozmanitý ekosystém iniciatív zameraných na posilňovanie digitálnej gramotnosti, online bezpečnosti a prevencie podvodov medzi dospelými. Patria medzi ne inštitucionálne programy, osvetové kampane, regionálne iniciatívy, európske projekty a aktivity vedené tretím sektorom. Na národnej úrovni predstavuje Repubblica Digitale strategický rámec podporujúci rozvoj digitálnych zručností a inklúziu prostredníctvom koordinovaných aktivít, ako je sieť digitálnej facilitácie, ktorá podporuje občanov, najmä dospelých, pri bezpečnom používaní digitálnych služieb. Podobne kampaň I Navigati, podporovaná finančnými a verejnými inštitúciami, sa zameriava konkrétne na zvyšovanie povedomia o online podvodoch a kyberbezpečnostných rizikách, najmä v kontexte digitálnych finančných služieb. Na regionálnej úrovni program Pane e Internet vyvinutý regiónom Emilia-Romagna poskytuje štruktúrované vzdelávacie príležitosti pre dospelých so silným dôrazom na praktické zručnosti vrátane online bezpečnosti a zodpovedného používania digitálnych nástrojov. Z európskej perspektívy projekt Erasmus+ DIGITOL ponúka relevantný príklad neformálneho vzdelávania zameraného na starších dospelých s cieľom zlepšiť digitálne kompetencie a podporiť bezpečné zaobchádzanie s digitálnymi technológiami. Napokon Fondazione Mondo Digitale zohráva kľúčovú úlohu v talianskom kontexte realizáciou inkluzívnych vzdelávacích programov, ktoré podporujú zraniteľné skupiny vrátane dospelých pri rozvoji digitálneho povedomia a kyberbezpečnostných zručností. Spoločne tieto iniciatívy demonštrujú viacúrovňový a viacaktérsky prístup k vzdelávaniu o digitálnej bezpečnosti, ktorý kombinuje politiku, školenia, osvetu a inováciu.

Tu sú identifikované osvedčené postupy:

1. *Repubblica Digitale (Digitálna republika)*

Názov osvedčeného postupu	Repubblica Digitale (Digitálna republika)
Typ osvedčeného postupu	Národná iniciatíva

<i>Realizujúca organizácia</i>	Riadiaci technický výbor, koordinovaný Oddelením pre digitálnu transformáciu Úradu predsedu vlády, Taliansko. https://innovazione.gov.it/
<i>Hlavné ciele</i>	● Preklenúť digitálnu priepasť, riešiť všetky formy digitálnej negramotnosti a podporovať vzdelávanie v oblasti budúcich technológií, čím sa podporí rozvoj krajiny. ● Zabezpečiť postupný a inkluzívny prechod na plne digitálnu spoločnosť.
<i>Cieľová skupina/skupiny</i>	Zameriava sa predovšetkým na: ● občanov ohrozených digitálnym vylúčením (ako sú starší ľudia alebo osoby v odľahlých oblastiach); ● pracovníkov, ktorí potrebujú zlepšiť svoje technické zručnosti; ● študentov, ktorí si osvojujú digitálnu gramotnosť; ● verejnú správu na modernizáciu vládnych služieb; ● organizácie tretieho sektora na vytvorenie rozšírenej siete digitálnych facilitátorov.
<i>Vzdelávacie výsledky a vplyv</i>	● V roku 2024 sa 272 270 verejných zamestnancov zapojilo do personalizovaných vzdelávacích dráh na zlepšenie svojich digitálnych zručností prostredníctvom platformy Syllabus . Okrem toho bola zavedená nová smernica, ktorá od roku 2025 nariaďuje aspoň 40 hodín ročného školenia pre každého verejného zamestnanca s osobitným zameraním na digitalizáciu, čo signalizuje významný posun v trende v porovnaní s minulosťou. ● Fond Repubblica Digitale financoval 73 projektov, ktoré v roku 2024 vyškolili viac ako 13 000 ľudí (vrátane NEET, nezamestnaných a ohrozených pracovníkov), čím pomohli preklenúť nedostatok IKT odborníkov na talianskom trhu práce. ● Centrá digitálneho vzdelávania (Digital Education Hubs) boli financované sumou 60 miliónov € z PNRR (Národný plán obnovy a odolnosti), čo predstavuje

	snahu posilniť univerzitný systém v oblastiach transferu technológií a pokročilého vzdelávania a podporiť prípravu vysokokvalifikovaných špecialistov. ● "Punti Digitale Facile" (Body jednoduchého digitálneho prístupu). Tieto centrá do októbra 2025 zapojili viac ako 1,8 milióna občanov, čím pomohli znížiť digitálnu priepasť a podporiť prístup verejnosti k digitálnym službám. ● Vzdelávacie a digitalizačné úsilie aktívne zapájajú verejné subjekty, podniky a tretí sektor. Táto stratégia usmerňuje intervencie vo verejnej aj súkromnej sfére a podporuje dlhodobú kontinuitu nad rámec mimoriadnych investícií.
Opis aktivity a metodologického prístupu	Kľúčovým pilierom tejto aktivity je Servizio Civile Digitale (Digitálna občianska služba), program, v ktorom mladí dobrovoľníci vo veku 18–28 rokov pracujú 12 mesiacov ako mentori a sprevádzajú občanov procesom "učenia sa praxou". Toto rovesnícke a medzigeneračné učenie sa ďalej opiera o Punti Digitale Facile (Body jednoduchého digitálneho prístupu): s viac ako 4000 fyzickými centrami zriadenými po celej krajine slúžia tieto centrá ako prístupné komunitné priestory, kde si občania môžu aktivovať svoju digitálnu identitu, ako je SPID alebo CIE (elektronický preukaz totožnosti). Okrem jednoduchej aktivácie facilitátori poskytujú školenie potrebné na používanie týchto nástrojov a učia používateľov, ako pristupovať k zdravotnej dokumentácii, platiť dane online alebo podpisovať digitálne dokumenty. Okrem toho Repubblica Digitale spustila "Taliansku koalíciu pre digitálne zručnosti a zamestnanosť", otvorenú alianciu, ktorá má za cieľ identifikovať a zapojiť čo najviac zainteresovaných strán (napr. podniky, verejné orgány, MVO atď.) s cieľom vytvoriť digitálnu a ľudskú sieť ľudí ochotných spolupracovať a rozvíjať národnú vedecko-technologickú kultúru. K dnešnému dňu sa k Talianskej koalícii pripojilo viac ako 180 organizácií a spustilo vyše 220 projektov. Aby sa organizácia mohla pripojiť ku koalícii, musí formálne pristúpiť k "Manifestu Repubblica Digitale", čím sa zabezpečí, že všetci členovia sa hlásia k rovnakým hodnotám inklúzie, etiky a digitálnej suverenity.

<i>Inovatívne prvky</i>	Iniciatíva využíva formálne aj neformálne vzdelávanie integrované naprieč jej rôznymi aktivitami a projektmi a vysoko si cení viacsektorovú spoluprácu z verejného aj súkromného sektora, ako aj z občianskej spoločnosti. Charakteristickou črtou jej modelu prístupu je využívanie rovesníckeho prístupu a medzigeneračného učenia. Tieto prvky v kombinácii so záväzkom k širokej inklúzii a zameraním na zraniteľné skupiny z neho robia strategický a integrovaný základ národnej digitálnej gramotnosti a vzdelávania.
<i>Odkaz / Zdroj</i>	https://repubblicadigitale.gov.it/portale/
<i>Vizuálne materiály</i>	 https://repubblicadigitale.gov.it/portale/-/l-italia-delle-competenze-digitali-si-fa-rete-i-risultati-raggiunti-e-le-sfide-del-futuro-martedì-31-marzo-a-roma 

Hodnotenie adaptability iniciatívy Repubblica Digitale (Digitálna republika)

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	
b) Rôzne organizácie (napr. ...)	☒	☐	☐	

MVO, školy, orgány verejnej moci)				
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☐	☒	☐	

2. I Navigati

Názov osvedčeného postupu	I Navigati
Typ osvedčeného postupu	Kampaň, Online nástroj
Realizujúca organizácia	CERTFin (Computer Emergency Response Team talianskeho finančného sektora) https://www.certfin.it/en/
Hlavné ciele	Podporovať digitálnu gramotnosť, zvyšovať povedomie a vzdelávať ľudí o informovanom a bezpečnom používaní digitálnych nástrojov a platforiem, aby sa nestali obeťami pascí nastražených kyberzločincami
Cieľová skupina/skupiny	Cieľové publikum je široké: od mladých ľudí po dospelých, pričom hlavnú cieľovú skupinu tvoria ľudia, ktorí pravidelne používajú digitálne kanály (online bankovníctvo, platobné aplikácie, online obchodovanie) na správu svojich financií, a ľudia s obmedzenými digitálnymi zručnosťami, ktorí majú problém odlíšiť podvod od legitímneho procesu.
Vzdelávacie výsledky a vplyv	● Používatelia sa učia zastaviť sa a overiť si požiadavky prostredníctvom oficiálnych kanálov predtým, ako konajú. ● Účastníci získavajú zručnosti na identifikáciu sofistikovaných podvodov, ktoré obchádzajú tradičné filtre ● Zameraním sa na "ľudský faktor" kampaň výrazne znižuje zraniteľnosť účastníkov. Používatelia sa učia identifikovať sofistikované hlasové alebo video deepfaky generované umelou inteligenciou, čím sa zabráni tomu,

	aby sa stali obeťami emocionálnych podvodov, ktoré sa vydávajú za členov rodiny
Opis aktivít a metodologického prístupu	● Kampaň zvyčajne prebieha v ročných "vlnách", ktoré často vrcholia v októbri, aby sa zhodovali s Európskym mesiacom kybernetickej bezpečnosti. Kampaň je propagovaná prostredníctvom hlavných televíznych kanálov, rádia, oficiálnej webovej stránky a sociálnych médií. Kampaň využíva rozprávanie príbehov na ľahšie pochopenie náročných tém: ● Webová séria krátkych videí, v ktorých členovia rodiny Navigati riešia rôzne riziká spojené s digitálnym svetom; ● Podcast "Al Sicuro" moderovaný technologickou expertkou. Fjona Cakalli hovorí o rôznych online podvodoch, čím sa tieto audio lekcie stávajú spôsobom, ako ponúknuť praktické rady, ako odhaliť psychologické triky podvodníkov.
Inovatívne prvky	Čo skutočne odlišuje I Navigati, je jeho inovatívne využitie rozprávania príbehov a multikanálovej mediálnej stratégie navrhnuté tak, aby premenila zložité kyberbezpečnostné témy na zrozumiteľné scenáre z bežného života. Kampaň sa sústreďuje na "rodinu Navigati", expertov na digitálnu bezpečnosť, ktorých domáce dobrodružstvá slúžia ako vzdelávacie šablóny pre verejnosť. Prostredníctvom série krátkych video epizód (každá približne 3 minúty) rodina ukazuje, ako sa brániť a rozpoznať prvé varovné signály podvodu. Tento dôverný, odľahčený tón robí technické rady prístupnými a menej zastrašujúcimi pre laikov. Aby správa zasiahla občanov aj na cestách, kampaň zahŕňa aj krátku sériu podcastov, ktorá ponúka flexibilné audio lekcie o digitálnej bezpečnosti.
Odkaz / Zdroj	https://inavigati.certfin.it/index.html
Vizuálne materiály	Mediálne pokrytie:

	https://www.bancaditalia.it/media/notizia/i-navigati-al-via-la-nuova-campagna-sulla-sicurezza-informatica/?dotcache=refresh
--	---

Hodnotenie adaptability kampane I Navigati

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	
b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☒	☐	☐	
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	

3. Pane e Internet

Názov osvedčeného postupu	Pane e Internet
Typ osvedčeného postupu	Projekt/Školenie
Realizujúca organizácia	Región Emilia-Romagna, Taliansko, pei@paneeinternet.it
Hlavné ciele	Podporovať rozvoj digitálnych zručností a posilňovať regionálnu sieť na miestnej aj regionálnej úrovni a zvyšovať digitálne povedomie občanov o globálnych otázkach
Cieľová skupina/skupiny	Občania akéhokoľvek veku, ktorí využívajú technológie na prístup k informáciám, používanie online služieb a využívanie digitálnych príležitostí dostupných v ich komunite.
Vzdelávacie výsledky a vplyv	Vzdelávacie programy Pane e Internet boli navrhnuté a realizované v súlade s európskym modelom DigComp, referenčným rámcom pre digitálne kompetencie

	občanov, a jeho školenia boli Európskou komisiou uznané za jeden z najlepších európskych postupov v oblasti vzdelávania digitálnej gramotnosti. Účastníci môžu byť postupne uvádzaní do digitálneho sveta prostredníctvom webinárov a kurzov prispôsobených ich potrebám a znalostiam. Účastníci nielen zlepšujú svoje vlastné digitálne povedomie, ale stávajú sa aktívnymi prispievateľmi k premene regiónu Emilia-Romagna na vyspelejší a technologicky inkluzívnejší región, čím poháňajú kolektívny posun smerom k prepojenejšej a na budúcnosť pripravej komunite.
<i>Opis aktivity a metodologického prístupu</i>	Iniciatíva funguje tak, že ponúka množstvo online workshopov a kurzov. Počas roka ponúka desiatky bezplatných kurzov a webinárov s rôznou dĺžkou trvania v závislosti od témy. Trvalou aktivitou je udržiavanie viacerých bodov Pei (Punti Pane e Internet) v celom regióne vďaka spolupráci s mestskými úradmi a obcami, čím sa zabezpečuje, že digitálna podpora je v rámci komunity vždy fyzicky dostupná. Pane e Internet ponúka prispôsobené kurzy digitálnej gramotnosti, od základných počítačových zručností a používania hardvéru až po pokročilé povedomie o kybernetickej bezpečnosti. Tento odstupňovaný prístup zabezpečuje, že používatelia môžu postupovať od základných technických operácií až po identifikáciu zložitých online rizík a obranu pred nimi. Pri tvorbe kurzov sa osobitná pozornosť venuje aj zraniteľným skupinám, čím sa zabezpečuje maximálny dosah a dostupnosť.
<i>Inovatívne prvky</i>	Európska komisia uznala vzdelávací program Pei za jeden z najlepších európskych postupov v oblasti vzdelávania digitálnej gramotnosti. Vzdelávacie podujatia a webináre sa konajú online pre maximálnu dostupnosť a oslovujú aj odľahlé oblasti regiónu. Projekt si zároveň udržiava silnú územnú prítomnosť prostredníctvom fyzických centier strategicky umiestnených po celom regióne. Tieto miestne centrá

	sú nevyhnutné na podporu komunitnej spolupráce a zabezpečenie širokého šírenia digitálnych nástrojov.
Odkaz / Zdroj	https://www.paneeinternet.it/
Vizuálne materiály	https://www.paneeinternet.it/public/elenco-news

Hodnotenie adaptability iniciatívy Pane e Internet

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	
b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☒	☐	☐	
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	

4. Projekt Erasmus+ DIGITOL

Názov osvedčeného postupu	Erasmus+ projekt DIGITOL
Typ osvedčeného postupu	Projekt
Realizujúca organizácia	Partnerstvo zložené zo šiestich organizácií zo šiestich rôznych európskych krajín: Consorzio Comunità Brianza (Taliansko), Pro Arbeit (Nemecko), 50PLUS Hellas (Grécko), Znanie (Bulharsko), Tree Agency (Estónsko), AGE Platform Europe (Belgicko).
Hlavné ciele	DIGITOL podporuje hodnoty EÚ ako solidarita a rozmanitosť prostredníctvom inovatívnych programov digitálnej gramotnosti. Cieľom projektu je vytvoriť ohľaduplnejší internet a zároveň bojovať proti diskriminácii a xenofóbii spájaním generácií s cieľom identifikovať a obmedziť falošné správy a online nenávistné prejavy.
Cieľová skupina/skupiny	Starší európski dospelí (55+)

Vzdelávacie výsledky a vplyv	● 10 mladých ľudí (vo veku 18–30 rokov) z partnerských krajín bolo zaškolených v 30-hodinovom školení pre školiteľov zameranom na boj proti falošným správam a polarizácii. ● 25 seniorov (vo veku nad 55 rokov) sa zúčastnilo 60-hodinového programu budovania kapacít DIGITOL vedeného mladými ľuďmi a externými expertmi, ktorého cieľom bolo vybaviť účastníkov teoretickými a praktickými nástrojmi na lepšie pochopenie vývoja súčasnej spoločnosti v súlade s našimi európskymi hodnotami.
Opis aktivity a metodologického prístupu	● Školenie školiteľov (ToT): "Mladí ambasádori" (vo veku 18–30 rokov) sa naučili, ako byť medzigeneračnými mentormi. Naučili sa nielen digitálne zručnosti, ale aj pedagogické techniky na vzdelávanie seniorov. ● Program budovania kapacít (CBP): Hlavná vzdelávacia fáza, v ktorej Mladí ambasádori vedú workshopy pre seniorov (vo veku 55+) o mediálnej gramotnosti, identifikácii falošných správ a boji proti online nenávisťným prejavom. ● Pilotné aktivity a následné aktivity: Účastníci sa presúvajú z učebne do reálneho sveta organizovaním "Živých knižníc" a "Festivalov Digitol" na podporu sociálnej súdržnosti a európskych hodnôt v rámci svojich miestnych komunít.
Odkaz / Zdroj	https://digitol.eu/it/
Vizuálne materiály	https://digitol.eu/wp-content/uploads/2020/07/DIGITOL-Project-Brochure-English.pdf Sada nástrojov: https://digitol.eu/wp-content/uploads/2022/01/toolkit-ITA-DEF.pdf

Hodnotenie adaptability projektu Erasmus+ DIGITOL

Kritériá	Úplne	Do určitej	Vôbec	Poznámky
----------	-------	------------	-------	----------

Tento projekt bol financovaný z programu Erasmus+ Európskej únie na základe grantovej zmluvy č. 2025-1-IT02-KA210-ADU-000359787. Táto publikácia / komunikácia vyjadruje výlučne názory autora. Európska komisia nenesie zodpovednosť za akékoľvek použitie informácií, ktoré sú v nej uvedené.

		miery	nie	(voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	
b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☒	☐	☐	
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	

5. **Fondazione Mondo Digitale**

Názov osvedčeného postupu	Fondazione Mondo Digitale
Typ osvedčeného postupu	Školenie
Realizujúca organizácia	Fondazione Mondo Digitale ETS, Taliansko, info@mondodigitale.org https://www.mondodigitale.org/
Hlavné ciele	● Podporovať kultúru inovácie a rozvíjať novú ekonomiku založenú na znalostiach ako hnaciu silu rozvoja krajiny. ● Využívanie digitálnych technológií na sociálny pokrok, na podporu rastu, blahobytu, produktivity a konkurencieschopnosti.
Cieľová skupina/skupiny	Ľudia všetkých vekových kategórií a pracovného zázemia: webová stránka umožňuje používateľom vybrať si pojem, ktorý ich najlepšie vystihuje (napr.: ženy, nezamestnaní, manažéri, umelci...)
Vzdelávacie výsledky a vplyv	Ľudia, ktorí sa zúčastňujú na <i>projektoch a podujatiach Fondazione Mondo Digitale</i> získavajú odbornosť v oblasti STEAM a zároveň si vytvárajú sieť kontaktov v rámci nej. Vďaka spôsobu štruktúrovania projektov sú digitálne zručnosti doplnené o sociálne zručnosti a aktívne občianstvo. To sa dosahuje podporou účasti na podujatiach, miestnych súťažiach a webinároch.
Opis aktivity a	<i>Fondazione Mondo Digitale</i> sa zameriava na

<i>metodologického prístupu</i>	poskytovanie laboratórií STEAM účastníkom v rôznych oblastiach. Okrem toho sú workshopy a semináre priamo integrované s miestnymi a národnými súťažami, čo účastníkom poskytuje okamžité príležitosti aplikovať teoretické koncepty prostredníctvom praktickej súťaže (napr.: RomeCup , Digital Made). Projekty môžu siahať od krátkych, intenzívnych 3-hodinových workshopov až po celoročné kurikulárne dráhy integrované do školského kalendára. Taktika <i>učenia sa praxou</i> sa používa v každom projekte a jej hlavným predstaviteľom sú " Innovation Gyms ", hybridné fyzické a virtuálne priestory rozšírené po celom Taliansku, kam môžu ľudia všetkých vekových kategórií prísť a naučiť sa technické zručnosti aj mäkké zručnosti.
<i>Inovatívne prvky</i>	Čo skutočne odlišuje tento projekt, je jeho prispôsobená webová stránka, ktorá kategorizuje príležitosti do konkrétnych cieľových skupín (od žien a mládeže až po starších ľudí, migrantov, umelcov...), čo používateľom umožňuje okamžite identifikovať kurzy a iniciatívy najvhodnejšie pre ich osobný alebo profesijný rast. Táto dostupnosť je spojená s filozofiou "učenia sa praxou", kde sú praktické vzdelávacie aktivity priamo prepojené s národnými a miestnymi súťažami. Účastou na týchto súťažiach môžu študujúci okamžite aplikovať svoje teoretické znalosti na výzvy reálneho sveta.
<i>Odkaz / Zdroj</i>	https://www.mondodigitale.org/
<i>Vizuálne materiály</i>	https://youtu.be/m-si=DBQRTWNVSPVP4Ycx https://www.repubblica.it/tecnologia/sicurezza/2020/02/04/news/google_premia_4_progetti_italiani_su_sicurezza_online-247591358/

Hodnotenie adaptability iniciatívy Fondazione Mondo Digitale

<i>Kritériá</i>	<i>Úplne</i>	<i>Do určitej miery</i>	<i>Vôbec nie</i>	<i>Poznámky (voliteľné)</i>
<i>a) Rôzne cieľové skupiny (napr.</i>	☒	☐	☐	

<i>mládež, seniori, profesionáli)</i>				
<i>b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)</i>	☒	☐	☐	
<i>c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)</i>	☒	☐	☐	

4.2 Španielsko

V rámci výskumnej fázy projektu digiSAFE bolo vykonané zmapovanie národných osvedčených postupov s cieľom identifikovať účinné iniciatívy v Španielsku, ktoré podporujú digitálnu bezpečnosť, prevenciu podvodov a digitálnu gramotnosť medzi dospelými, s osobitnou relevantnosťou pre jednotlivcov vo veku 45 a viac rokov. Cieľom tejto analýzy bolo zvýrazniť existujúce prístupy, ktoré môžu slúžiť ako podklad pre tvorbu kurikula neformálneho vzdelávania a sady nástrojov na prevenciu digitálnych podvodov projektu digiSAFE. Vybrané osvedčené postupy predstavujú rozmanitú škálu aktérov a metodológií vrátane verejných inštitúcií, orgánov činných v trestnom konaní, mimovládnych organizácií, národných osvetových kampaní a komunitných vzdelávacích iniciatív. Spoločne ukazujú, ako sa výzvy digitálnej bezpečnosti v Španielsku riešia prostredníctvom prevencie, vzdelávania a posilňovania, namiesto výlučného spoliehania sa na technické alebo regulačné opatrenia.

Osobitná pozornosť sa venovala iniciatívam využívajúcim neformálne a prístupné vzdelávacie prístupy, pričom sa uznáva, že dospelí vo veku 45+ často najviac profitujú z praktických, na skúsenostiach založených a používateľsky prívetivých vzdelávacích metód. Identifikované postupy sa zameriavajú na posilňovanie digitálnej sebadôvery, zvyšovanie povedomia o online rizikách, zlepšovanie schopnosti rozpoznať podvody a nekalé praktiky a podporu zodpovedného používania digitálnych technológií v každodennom živote.

Vybrané osvedčené postupy navyše vykazujú vysoký stupeň adaptability a prenositeľnosti do iných národných a európskych kontextov. Mnohé z nich sú škálovateľné, inkluzívne a navrhnuté tak, aby ich mohli realizovať rôzne typy organizácií, čo ich robí obzvlášť vhodnými na replikáciu v rámci projektu digiSAFE. Tu je 5 osvedčených postupov identifikovaných v Španielsku:

1. *Fundación Cibervoluntarios – Digitálna inklúzia a digitálne zručnosti pre dospelých*

<i>Názov osvedčeného postupu</i>	Fundación Cibervoluntarios – Digitálna inklúzia a digitálne zručnosti pre dospelých
<i>Typ osvedčeného postupu</i>	Projekt / Školenie / Workshopy
<i>Realizujúca organizácia</i>	Fundación Cibervoluntarios, Španielsko https://www.cibervoluntarios.org
<i>Hlavné ciele</i>	Zhrnúť ciele (napr. zvýšiť Znížiť digitálnu priepasť posilnením dospelých a seniorov digitálnymi zručnosťami, sebadôverou a povedomím, aby sa mohli bezpečne zapájať do digitálnej spoločnosti.
<i>Cieľová skupina/skupiny</i>	Dospelí, seniori, zraniteľné skupiny, dospelí vo veku 45+.
<i>Vzdelávacie výsledky a vplyv</i>	Účastníci si zlepšujú základné a stredne pokročilé digitálne zručnosti, zvyšujú sebadôveru pri používaní digitálnych nástrojov a rozvíjajú väčšie povedomie o online rizikách, podvodoch a mylných informáciách.
<i>Opis aktivity a metodologického prístupu</i>	Bezplatné aktivity digitálneho vzdelávania realizované online a prezenčne prostredníctvom komunitných centier, združení a verejných inštitúcií. Metodológia je založená na neformálnom vzdelávaní, praktických cvičeniach, rovesníckom učení a digitálnych scenároch z reálneho života.
<i>Inovatívne prvky</i>	Digitálne mentorstvo vedené dobrovoľníkmi, komunitný prístup a prispôbené vzdelávacie dráhy pre dospelých a seniorov.
<i>Odkaz / Zdroj</i>	https://www.cibervoluntarios.org
<i>Vizuálne materiály</i>	Vzdelávacie materiály, videá, infografiky, projektové správy a online zdroje dostupné na webovej stránke organizácie.

Hodnotenie adaptability iniciatívy Fundación Cibervoluntarios – Digitálna inklúzia a digitálne zručnosti pre dospelých

<i>Kritériá</i>	<i>Úplne</i>	<i>Do určitej miery</i>	<i>Vôbec nie</i>	<i>Poznámky (voliteľné)</i>
<i>a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)</i>	☒	☐	☐	

b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☒	☐	☐	
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	

2. Aula Mentor – Program vzdelávania dospelých a digitálnych zručností

Názov osvedčeného postupu	Aula Mentor – Vzdelávanie dospelých a digitálne zručnosti Program
Typ osvedčeného postupu	Školenie / Online vzdelávanie Program
Realizujúca organizácia	Ministerstvo školstva a odborného vzdelávania, Španielsko https://www.aulamentor.es
Hlavné ciele	Podporovať celoživotné vzdelávanie poskytovaním flexibilného prístupu dospelých k digitálnym zručnostiam a školeniam v oblasti IKT.
Cieľová skupina/skupiny	Dospelí (18+), vrátane dospelých vo veku 45+.
Vzdelávacie výsledky a vplyv	Študenti získavajú základné digitálne kompetencie, zlepšujú samostatnosť pri používaní online nástrojov a zvyšujú sebadôveru v digitálnom prostredí.
Opis aktivity a metodologického prístupu	Online kurzy podporované vyškolenými mentormi, ktoré umožňujú dospelým učiť sa vlastným tempom prostredníctvom flexibilného modelu neformálneho vzdelávania prispôbeného potrebám dospelých študentov.
Inovatívne prvky	Celoštátne pokrytie, vzdelávanie podporované mentormi a flexibilný prístup pre dospelých študentov.
Odkaz / Zdroj	https://www.aulamentor.es
Vizuálne materiály	Katalógy online kurzov, snímky obrazovky platformy

	a informačné materiály dostupné na oficiálnej webovej stránke.
--	--

Hodnotenie adaptability iniciatívy Aula Mentor – Program vzdelávania dospelých a digitálnych zručností

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	
b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☐	☒	☐	
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	

3. **Policía Nacional – Plan Mayor Seguridad**

Názov osvedčeného postupu	Policía Nacional – Plan Mayor Seguridad
Typ osvedčeného postupu	Kampaň / Osvetová iniciatíva
Realizujúca organizácia	Policía Nacional, Španielsko https://www.policia.es
Hlavné ciele	Predchádzať trestnej činnosti a podvodom postihujúcim starších dospelých zvyšovaním povedomia o digitálnych a offline rizikách a podporou bezpečného správania.
Cieľová skupina/skupiny	Starší dospelí, seniori, združenia pre starších ľudí.
Vzdelávacie výsledky a vplyv	Zvýšené povedomie o podvodných schémach, zlepšená schopnosť rozpoznať podvody a posilnená dôvera medzi staršími občanmi a verejnými inštitúciami.
Opis aktivity a metodologického prístupu	Informačné prednášky a workshopy vedené policajtmi v komunitných centrách a združeniach s

	využitím praktických príkladov a preventívne orientovaných usmernení.
<i>Inovatívne prvky</i>	Priame zapojenie profesionálov z orgánov činných v trestnom konaní a silné zapojenie komunity.
<i>Odkaz / Zdroj</i>	https://www.policia.es/_es/colabora_plan_mayor_seguridad.php
<i>Vizuálne materiály</i>	Plagáty, letáky, prezentačné materiály a vizuály kampane dostupné prostredníctvom kanálov Policia Nacional.

Hodnotenie adaptability iniciatívy Policía Nacional – Plan Mayor Seguridad

<i>Kritériá</i>	<i>Úplne</i>	<i>Do určitej miery</i>	<i>Vôbec nie</i>	<i>Poznámky (voliteľné)</i>
<i>a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)</i>	☐	☒	☐	
<i>b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)</i>	☐	☒	☐	
<i>c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)</i>	☒	☐	☐	

4. INCIBE – 017 Linka pomoci a osvetový program v oblasti kybernetickej bezpečnosti

Názov osvedčeného postupu	INCIBE – 017 Linka pomoci a osvetový program v oblasti kybernetickej bezpečnosti
Typ osvedčeného postupu	Verejná služba / Osveta Kampaň / Online nástroj
Realizujúca organizácia	Instituto Nacional de Ciberseguridad (INCIBE), Španielsko https://www.incibe.es
Hlavné ciele	Zlepšiť povedomie občanov o kyberbezpečnostných rizikách a poskytnúť usmernenia o prevencii podvodov a bezpečnom digitálnom správaní.
Cieľová skupina/skupiny	Široká verejnosť, dospelí, seniori, zraniteľní používatelia.
Vzdelávacie výsledky a vplyv	Používatelia si zlepšujú povedomie o digitálnych hrozbách, zvyšujú schopnosť rozpoznať podvody a nekalé praktiky a osvojujú si bezpečnejšie online postupy.
Opis aktivity a metodologického prístupu	Bezplatná verejná linka pomoci ponúkajúca personalizovanú podporu prostredníctvom telefónu, chatu a aplikácií na zasielanie správ, v kombinácii s osvetovými kampaňami a vzdelávacími online zdrojmi.
Inovatívne prvky	Viackanálový prístup, personalizovaná podpora v reálnom čase a integrácia vzdelávania s reakciou na incidenty.
Odkaz / Zdroj	https://www.incibe.es/linea-017

Hodnotenie adaptability iniciatívy INCIBE – 017 Linka pomoci a osvetový program v oblasti kybernetickej bezpečnosti

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	
b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☐	☒	☐	

c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	
---	-------------------------------------	--------------------------	--------------------------	--

5. Regionálne programy digitálnych zručností pre seniorov (Španielsko)

Názov osvedčeného postupu	Regionálne programy digitálnych zručností pre seniorov (Španielsko)
Typ osvedčeného postupu	Školenie / Workshopy / Verejná iniciatíva
Realizujúca organizácia	Regionálne a miestne orgány verejnej moci, Španielsko
Hlavné ciele	Podporovať digitálnu inklúziu a bezpečné používanie digitálnych technológií medzi staršími dospelými na miestnej úrovni.
Cieľová skupina/skupiny	Starší dospelí, seniori, dospelí s nízkymi digitálnymi zručnosťami.
Vzdelávacie výsledky a vplyv	Účastníci si zlepšujú základné digitálne kompetencie, zvyšujú sebadôveru pri používaní online služieb a získavajú povedomie o online rizikách a stratégiách prevencie podvodov.
Opis aktivity a metodologického prístupu	Praktické vzdelávacie aktivity realizované v komunitných centrách, knižniciach alebo centrách vzdelávania dospelých prostredníctvom maloskupinových, prakticky orientovaných stretnutí.
Inovatívne prvky	Lokalizovaný prístup, priame zapojenie komunity a prispôsobenie konkrétnym potrebám študujúcich.

Hodnotenie adaptability regionálnych programov digitálnych zručností pre seniorov (Španielsko)

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	

b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☒	☐	☐	
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	

4.3 Slovensko

Fáza sekundárneho výskumu identifikovala päť odlišných národných osvedčených postupov na Slovensku vedených súkromným sektorom, neziskovými organizáciami a komunitnými sieťami. Tieto iniciatívy ponúkajú vysoko adaptabilné prístupy k boju proti digitálnemu vylúčeniu a prevencii online podvodov medzi staršími dospelými.

Bezpečne na nete – Tento komplexný vzdelávací portál, ktorý vytvorila slovenská kyberbezpečnostná spoločnosť ESET, poskytuje bezplatné, prístupné zdroje o digitálnej bezpečnosti. Hoci je dostupný širokej verejnosti, jeho zrozumiteľné články, podcasty a videonávody sú veľmi účinné pre dospelých a seniorov. Platforma prekladá zložité kyberbezpečnostné hrozby – ako malvér, phishing a ochranu údajov – do jednoduchého, každodenného jazyka. Jej hlavnou inováciou je využívanie kyberbezpečnostnej odbornosti súkromného sektora na poskytovanie kvalitného, neustále aktualizovaného vzdelávacieho obsahu verejnosti, ktorý si jednotlivci môžu osvojiť vlastným tempom.

Zrelí na dobu digitálnu – Tento grantový a vzdelávací program spravovaný Nadačným fondom Telekom sa osobitne zameriava na digitálnu inklúziu seniorov. Iniciatíva financuje a podporuje miestne organizácie, domovy sociálnych služieb a komunitné centrá pri realizácii prispôbených kurzov digitálnej gramotnosti. Metodológia sa zameriava na maloskupinové, praktické vzdelávacie prostredia, kde si starší dospelí môžu bezpečne precvičovať používanie smartfónov, správu online účtov a rozpoznávanie bežných podvodov. Tento decentralizovaný prístup zabezpečuje, že vzdelávanie sa dostane k seniorom v ich miestnych komunitách, čím sa učenie stáva vysoko prístupným a sociálne pútavým.

Zodpovedne.sk – Toto národné osvetové centrum prevádzkované občianskym združením eSlovensko sa zameriava na bezpečné používanie internetu naprieč všetkými generáciami. Pre demografickú skupinu 45+ poskytuje cielené tlačené príručky, inštruktážne videá a poradenské služby týkajúce sa kybernetických hrozieb. Iniciatíva pôsobí ako preventívny vzdelávací nástroj, ktorý učí dospelých, ako zabezpečiť svoje zariadenia, chrániť svoje osobné údaje a rozpoznávať psychologickú manipuláciu online. Jej silnou stránkou je dlhodobé pôsobenie a rozsiahla knižnica lokalizovaných, ľahko zrozumiteľných materiálov, ktoré môžu pedagógovia a mimovládne organizácie široko šíriť.

Senior bezpečne online – Tieto semináre, organizované prostredníctvom miestnych pobočiek Jednoty dôchodcov na Slovensku (JDS) v spolupráci s regionálnymi IT expertmi, ponúkajú priame, rovesnícky podporované vzdelávanie. Workshopy sa konajú v známych komunitných

priestoroch a silno sa zameriavajú na bezprostredné hrozby, ako sú miestne finančné podvody, podvodné e-shopy a bezpečná komunikácia s rodinou. Metodologická sila spočíva v jeho modeli rovesníckej dôvery; učenie v rámci siete rovesníkov výrazne znižuje úzkosť, ktorú starší dospelí často pociťujú pri osvojovaní si nových digitálnych návykov.

Akadémie Smart Senior v regionálnych knižniciach – Verejné knižnice na celom Slovensku, ako napríklad regionálne knižnice v Žiline a Bratislave, sa premenili na dôležité centrá digitálneho vzdelávania dospelých. Tieto inštitúcie pravidelne organizujú štruktúrované kurzy "Smart Senior". Knižovníci a dobrovoľní IT škoolitelia sprevádzajú účastníkov základnou digitálnou navigáciou, hodnotením online informácií a rozpoznávaním podvodných e-mailov. Tento postup využíva existujúcu, dôveryhodnú komunitnú infraštruktúru na poskytovanie nepretržitej, bezplatnej a veľmi trpezlivej vzdelávacej podpory, čo z neho robí ľahko adaptabilný model pre akúkoľvek obec. Tu je 5 identifikovaných osvedčených postupov:

1. **Bezpečne na nete**

Názov osvedčeného postupu	Bezpečne na nete
Typ osvedčeného postupu	Online nástroj / Kampaň
Realizujúca organizácia	ESET, Slovensko. https://bezpecnenanete.eset.com/sk/
Hlavné ciele	Zvýšiť povedomie o kyberbezpečnostných hrozbách a poskytnúť bezplatné, praktické vzdelávanie o tom, ako sa bezpečne pohybovať na internete, prispôbené všetkým skupinám používateľov vrátane seniorov.
Cieľová skupina/skupiny	Široká verejnosť, dospelí, seniori, pedagógovia a rodičia.
Vzdelávacie výsledky a vplyv	Používatelia získavajú prístup k neustále aktualizovanej knižnici článkov, videí a podcastov. Účastníci sa učia rozpoznávať moderné kybernetické hrozby, zabezpečiť svoje digitálne súkromie a bezpečne fungovať online bez obavy z digitálneho vylúčenia.
Opis aktivity a metodologického prístupu	Portál funguje ako centralizované vzdelávacie centrum ponúkajúce vzdelávacie materiály krok za krokom. Metodológia sa opiera o preklad zložitých konceptov IT bezpečnosti (ako malvér, phishing a úniky údajov) do jednoduchého, každodenného jazyka. Obsah

	je kategorizovaný tak, aby vyhovoval rôznym úrovniam zručností a životným situáciám, čo starším dospelým uľahčuje jeho osvojenie vlastným tempom.
<i>Inovatívne prvky</i>	Využíva hlbokú, globálnu kyberbezpečnostnú odbornosť poprednej technologickej spoločnosti súkromného sektora (ESET) na poskytovanie úplne bezplatného, kvalitného a nekomerčného vzdelávacieho obsahu pre verejné blaho.
<i>Odkaz / Zdroj</i>	https://bezpecnenanete.eset.com/sk/
<i>Vizuálne materiály</i>	Snímky obrazovky portálu a knižnica podcastov dostupné na: https://bezpecnenanete.eset.com/sk/

Hodnotenie adaptability iniciatívy Bezpečne na nete:

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	Obsah je už segmentovaný pre rôzne vekové skupiny a technické úrovne.
b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☒	☐	☐	Spoločnosti súkromného sektora v celej Európe by mohli tento model spoločenskej zodpovednosti (CSR) replikovať.
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	Formát platformy ľahko umožňuje pridávanie nových tém, ako sú hrozby súvisiace s umelou inteligenciou.

2. Zrelí na dobu digitálnu

Názov osvedčeného postupu	Zrelí na dobu digitálnu
Typ osvedčeného postupu	Projekt / Financovanie / Školenie
Realizujúca organizácia	Nadačný fond Telekom pri Nadácii Pontis, Slovensko. https://nadačnýfondtelekom.sk/
Hlavné ciele	Podporovať digitálnu gramotnosť, zvyšovať povedomie a vzdelávať ľudí o informovanom a bezpečnom používaní digitálnych nástrojov a platforiem, aby sa nestali obeťami pascí nastrožených kyberzločincami
Cieľová skupina/skupiny	Seniori vo veku 65 a viac rokov, miestne mimovládne organizácie, domovy sociálnych služieb a komunitné centrá.
Vzdelávacie výsledky a vplyv	Grantový program financoval desiatky miestnych organizácií sumou viac ako 200 000 €, čím vyškoliť tisíce seniorov. Účastníci si zlepšujú kritické myslenie, overujú zdroje informácií a rozvíjajú odolnosť voči emocionálnej manipulácii, ktorú používajú podvodníci.
Opis aktivity a metodologického prístupu	Namiesto jediného centrálného kurzu ide o grantový mechanizmus, ktorý umožňuje miestnym subjektom poskytovať školenia. Podporované projekty využívajú maloskupinové, praktické vzdelávacie metodológie. Seniori sa v známom prostredí učia bezpečne precvičovať používanie smartfónov, rozpoznávanie podvodov a komunikáciu s rodinou, čím sa zabezpečuje trpezlivá a prispôsobená výučba, ktorá ponúka praktické rady, ako odhaliť psychologické triky podvodníkov.
Inovatívne prvky	Decentralizovaný model financovania sa vo veľkej miere opiera o komunitné siete na lokálnej úrovni, čím zabezpečuje, že digitálne vzdelávanie sa dostane k izolovaným seniorom vo vidieckych oblastiach, ktorí by sa nemuseli zúčastniť veľkých, štátom riadených kurzov.
Odkaz / Zdroj	https://nadačnýfondtelekom.sk/
Vizuálne materiály	Podrobnosti o kampani dostupné na https://nadačnýfondtelekom.sk/aktual ne-vyzvy/

Hodnotenie adaptability iniciatívy Zrelí na dobu digitálnu

<i>Kritériá</i>	<i>Úplne</i>	<i>Do určitej miery</i>	<i>Vôbec nie</i>	<i>Poznámky (voliteľné)</i>
<i>a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)</i>	☐	☒	☐	Grantový model je špecificky prispôsobený potrebám a tempu starších dospelých.
<i>b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)</i>	☒	☐	☐	Akákoľvek podniková nadácia alebo štátny orgán môže prevziať túto decentralizovanú grantovú metodológiu.
<i>c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)</i>	☒	☐	☐	Granty môžu byť tematicky ročne zamerané na zameranie na konkrétne otázky ako phishing alebo umelá inteligencia.

3. **Zodpovedne.sk**

Názov osvedčeného postupu	Zodpovedne.sk
Typ osvedčeného postupu	Kampaň / Online nástroj
Realizujúca organizácia	Občianske združenie eSlovensko, Slovensko. https://www.zodpovedne.sk/
Hlavné ciele	Zvyšovať národné povedomie o bezpečnosti na internete, predchádzať kybernetickej kriminalite a poskytovať vzdelávacie zdroje a poradenské služby týkajúce sa kybernetických hrozieb naprieč generáciami.
Cieľová skupina/skupiny	Široká verejnosť, dospelí, seniori, rodičia a pedagógovia.
Vzdelávacie výsledky a vplyv	Seniori sa učia samostatne vyhľadávať informácie, ovládať e-mailové účty a rozpoznávať podvodné komunikácie. Podporuje to pocit samostatnosti a integrácie do modernej digitálnej spoločnosti.
Opis aktivity a metodologického prístupu	Knižnice organizujú štruktúrované, viactýždňové kurzy "Smart Senior" alebo IT konzultačné stretnutia. Knižovníci a dobrovoľní IT školitelia sprevádzajú malé skupiny praktickými cvičeniami. Metodológia je veľmi trpezlivá a umožňuje seniorom precvičovať si na knižničných počítačoch alebo vlastných zariadeniach, pričom pokrýva všetko od zapnutia zariadenia až po pokročilú bezpečnosť na internete.
Inovatívne prvky	Dômyselne využíva existujúcu, vysoko dôveryhodnú a prístupnú infraštruktúru verejných knižníc na poskytovanie nepretržitého, bezplatného a nezastrašujúceho vzdelávania dospelých.
Odkaz / Zdroj	https://www.krajskakniznicazilina.sk/

Vizuálne materiály	Opisy kurzov na https://www.krajskajniznicazilina.sk/index.php/2023/10/19/digitalne-zrucni-seniori/
--------------------	---

Hodnotenie adaptability iniciatívy Zodpovedne.sk

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	Knižnice slúžia celej komunite a môžu prispôbiť kurzy akejkoľvek demografickej skupine.
b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☒	☐	☐	Môžu ho využívať školy, centrá vzdelávania dospelých a orgány verejnej moci.
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	Neustále aktualizované s cieľom riešiť nové javy ako hazardné hry, umelú inteligenciu a zneužívanie údajov.

4. Projekt Erasmus+ DIGITOL

Názov osvedčeného postupu	Erasmus+ projekt DIGITOL
Typ osvedčeného postupu	Projekt
Realizujúca organizácia	Jednota dôchodcov na Slovensku (JDS) v spolupráci s regionálnymi IT expertmi a univerzitami. https://www.jednotadochodcov.sk
Hlavné ciele	Poskytovať lokalizované, rovesnícky podporované vzdelávanie, ktoré pomáha seniorom bezpečne sa pohybovať na internete, rozpoznávať miestne finančné podvody a znižovať úzkosť z digitálnych nástrojov.
Cieľová skupina/skupiny	Seniori a dospelí v dôchodku.
Vzdelávacie výsledky a vplyv	Účastníci úspešne prechádzajú od vyhýbania sa digitálnym nástrojom k aktívnemu a bezpečnému používaniu smartfónov, chatovacích aplikácií a online bankovníctva, čím sa výrazne znižuje ich izolácia a zraniteľnosť voči základným podvodom.
Opis aktivity a metodologickéh o prístupu	Ide o semináre na lokálnej úrovni organizované priamo jednotou dôchodcov v miestnych komunitných priestoroch. Metodológia kladie dôraz na rovesnícke učenie a praktické, okamžité uplatnenie. Témy sú veľmi relevantné pre každodenný život: odhaľovanie podvodných e-shopov, rozpoznávanie falošných správ a učenie sa, ako ignorovať alebo blokovat' nevyžiadajú komunikáciu.
Inovatívne prvky	Model rovesníckej dôvery je veľmi účinný. Učenie v rámci siete rovesníkov (iných seniorov) drasticky znižuje psychologickú bariéru a úzkosť, ktorú starší dospelí často zažívajú vo formálnych, rýchlo tempovaných IT kurzoch.
Odkaz / Zdroj	https://www.jednotadochodcov.sk/
Vizuálne materiály	N/A

Hodnotenie adaptability projektu Erasmus+ DIGITOL

Kritériá	Úplne	Do určitej	Vôbec nie	Poznámky
----------	-------	------------	-----------	----------

		<i>miery</i>		<i>(voliteľné)</i>
a) <i>Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)</i>	☐	☒	☐	Model rovesníckej podpory funguje najlepšie, keď účastníci zdieľajú podobný age/life skúsenosti.
b) <i>Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)</i>	☒	☐	☐	Vysoko adaptabilný pre komunitné centrá, miestne mimovládne organizácie a seniorské kluby.
c) <i>Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)</i>	☒	☐	☐	Semináre môžu ľahko začleniť nové hrozby do prostredia do diskusie.

5. Akadémia Smart Senior v regionálnych knižniciach

Názov osvedčeného postupu	Akadémie Smart Senior v regionálnych knižniciach
Typ osvedčeného postupu	Školenie / Projekt
Realizujúca organizácia	Regionálne verejné knižnice (napr. Krajská knižnica Žilina), Slovensko. https://www.krajskakniznicazilina.sk/
Hlavné ciele	Premenit' verejné knižnice na dôležité centrá digitálneho vzdelávania dospelých, učiť seniorov základnú navigáciu v zariadeniach a ako bezpečne hodnotiť online informácie.
Cieľová skupina/skupiny	Seniori, znevýhodnení dospelí a členovia miestnej komunity.
Vzdelávacie výsledky a vplyv	Seniori sa učia samostatne vyhľadávať informácie, ovládať e-mailové účty a rozpoznávať podvodné komunikácie. Podporuje to pocit samostatnosti a integrácie do modernej digitálnej spoločnosti.
Opis aktivity a metodologického prístupu	Knižnice organizujú štruktúrované, viactýždňové kurzy "Smart Senior" alebo IT konzultačné stretnutia. Knižovníci a dobrovoľní IT škoolitelia sprevádzajú malé skupiny praktickými cvičeniami. Metodológia je veľmi trpezlivá a umožňuje seniorom precvičovať si na knižničných počítačoch alebo vlastných zariadeniach, pričom pokrýva všetko od zapnutia zariadenia až po pokročilú bezpečnosť na internete.
Inovatívne prvky	Dômyselne využíva existujúcu, vysoko dôveryhodnú a prístupnú infraštruktúru verejných knižníc na poskytovanie nepretržitého, bezplatného a nezastrašujúceho vzdelávania dospelých.
Odkaz / Zdroj	https://www.krajskakniznicazilina.sk/
Vizuálne materiály	Opisy kurzov na https://www.krajskakniznicazilina.sk/index.php/2023/10/19/digitalne-zrucni-seniori/

Hodnotenie adaptability Akadémie Smart Senior v regionálnych knižniciach

Kritériá	Úplne	Do určitej miery	Vôbec nie	Poznámky (voliteľné)
----------	-------	------------------	-----------	----------------------

a) Rôzne cieľové skupiny (napr. mládež, seniori, profesionáli)	☒	☐	☐	Knižnice slúžia celej komunite a môžu prispôbiť kurzy akejkoľvek demografickej skupine.
b) Rôzne organizácie (napr. MVO, školy, orgány verejnej moci)	☒	☐	☐	Tento model môže replikovať akákoľvek verejná inštitúcia s priestorom a počítačmi.
c) Rôzne témy alebo výzvy (napr. súkromie, mylné informácie, kybernetická bezpečnosť)	☒	☐	☐	Kurikulum sa môže preorientovať od základného používania hardvéru na pokročilé školenie proti phishingu.

5. Analýza výsledkov prieskumu

5.1 Taliansko

Účel a metóda

Taliansky prieskum sa uskutočnil ako súčasť národného hodnotenia potrieb s cieľom zozbierať kvantitatívne údaje o digitálnej gramotnosti, povedomí o online bezpečnosti a vystavení online podvodom medzi dospelými vo veku 45+ v Taliansku. Dotazník bol administrovaný online prostredníctvom Google Forms a šírený viacerými kanálmi s cieľom zabezpečiť široký dosah.

Pôvodne bol zdieľaný v rámci siete Associazione Italiana Socio-Educatori per la Cooperazione (AISEC APS) prostredníctvom interných komunikačných nástrojov vrátane e-mailovej korešpondencie a prezentácií počas výročných zhromaždení združenia. Okrem toho bol prieskum distribuovaný prostredníctvom oficiálnych komunikačných kanálov Confcooperative Lazio Nord, s ktorou je AISEC pridružená, s využitím newsletterov, obežníkov a priamych e-mailov zameraných na jej sieť v provinciách Rieti, Viterbo a Rím.

Na účely národnej analýzy sa zohľadňovali iba odpovede účastníkov s pobytom v Taliansku. Konečnú vzorku tvorilo 63 respondentov vo veku 45 a viac rokov, vrátane 39

žien a 24 mužov. Najpočetnejšou vekovou skupinou bola 45–54 rokov (28 respondentov), nasledovaná skupinou 65–74 rokov (19), 55–64 rokov (14) a 75+ (2).

Z územného hľadiska respondenti pochádzali zo širokej oblasti regiónu Lazio vrátane severného Lazia aj metropolitnej oblasti Ríma. Vzorka bola heterogénna z hľadiska životného prostredia a zahŕňala mestské, vidiecke a prímestské oblasti, ako aj rozmanité pracovné statusy a vzdelanostné zázemie. Táto rozmanitosť poskytuje komplexný prehľad o skúsenostiach, postupoch a vnímaných potrebách dospelých vo veku 45+ v talianskom kontexte.

Kľúčové výsledky

Taliansky súbor údajov naznačuje, že dospelí vo veku 45+ sú vo všeobecnosti aktívnymi používateľmi digitálnych technológií, hoci ich úroveň sebadôvery sa líši v závislosti od typu danej zručnosti.

Každodenné používanie digitálnych zariadení je rozšírené: 77,8 % respondentov hodnotilo svoje používanie smartfónov alebo počítačov na najvyšších úrovniach (4 alebo 5), s priemerným skóre 4,19/5. Všeobecná sebadôvera pri používaní internetu je tiež pomerne vysoká (priemer 3,79/5), čo naznačuje, že väčšina účastníkov sa cíti komfortne pri vykonávaní bežných online aktivít.

Táto sebadôvera sa stáva menej konzistentnou pri zvažovaní špecifickejších kompetencií digitálnej bezpečnosti. Najsilnejšie samohodnotené správanie sa týka základných preventívnych postupov pri každodennej navigácii. Veľká väčšina respondentov uviedla, že sa vyhýba klikaniu na neznáme alebo podozrivé odkazy (73,0 %) a overuje si informácie pred ich zdieľaním online (71,4 %), zatiaľ čo 60,3 % uviedlo, že blokuje alebo nahlasuje podozrivé správy, profily alebo webové stránky. Tieto zistenia naznačujú prítomnosť základných obranných návykov vyvinutých prostredníctvom skúseností.

Technickejšie alebo špecializovanejšie zručnosti zároveň odhaľujú jasné medzery. Menej ako polovica respondentov (47,6 %) uviedla, že dokáže identifikovať, či je webová stránka bezpečná, napríklad kontrolou HTTPS alebo bezpečnostných indikátorov. Podobne sa len 50,8 % cítilo isto pri úprave nastavení súkromia alebo bezpečnosti na svojich zariadeniach a rovnaký podiel uviedol používanie silných a jedinečných hesiel. Ešte slabšie výsledky sa objavujú v súvislosti s údržbou zariadení a softvéru: iba 36,5 % uviedlo, že pravidelne aktualizuje svoje zariadenia, aplikácie a antivírusový softvér, zatiaľ čo významný podiel vyjadril neistotu v tejto oblasti.

Najkritickejšia slabina sa týka rozpoznávania obsahu generovaného alebo manipulovaného umelou inteligenciou. Iba 38,1 % respondentov sa vysoko ohodnotilo v schopnosti identifikovať pozmenené obrázky, videá alebo správy a menej ako polovica

uviedla, že pravidelne overuje, či digitálny obsah nebol manipulovaný. Potvrďuje to významnú medzeru v kompetenciách vo vzťahu k novovznikajúcim digitálnym rizikám.

Povedomie o online podvodoch je prítomné, ale nerovnomerné naprieč rôznymi typmi hrozieb. Tradičné riziká ako phishing a mylné informácie na sociálnych sieťach sú pomerne dobre známe, pričom približne dve tretiny respondentov uvádzajú mierne alebo silné povedomie. Povedomie je o niečo nižšie pri podvodoch súvisiacich s falošnými online obchodmi, platobnými podvodmi alebo krádežou identity a ďalej klesá pri hrozbách založených na umelej inteligencii. Iba 54,0 % respondentov uviedlo mierne alebo silné povedomie o podvodoch generovaných umelou inteligenciou, zatiaľ čo podstatný podiel uviedol obmedzené alebo žiadne povedomie.

Priama skúsenosť s podvodmi je tiež významná. Viac ako tretina respondentov (38,1 %) uviedla, že sa stali obeťami nejakej formy digitálneho podvodu, najčastejšie bankového alebo finančného podvodu a podvodov s falošnými nákupmi, nasledovaných phishingom a krádežou identity. To naznačuje, že vystavenie digitálnym rizikám nie je len vnímané, ale aj konkrétne zažité.

Obavy z budúcej viktimizácie sú obzvlášť vysoké: 84,1 % respondentov vyjadrilo jasné úrovne obáv zo stania sa obeťami online podvodov alebo mylných informácií. Celkovo výsledky poukazujú na nesúlad medzi bežným digitálnym používaním a pokročilejšími bezpečnostnými kompetenciami.

Interpretácia

Talianske zistenia potvrdzujú, že časté digitálne zapojenie sa nemusí nevyhnutne premietnuť do účinných kompetencií v oblasti digitálnej bezpečnosti medzi dospelými vo veku 45+.

Prvý kľúčový problém možno opísať ako "ilúziu kompetencie." Mnohí účastníci sa spoliehajú na bežné používanie a učenie prostredníctvom skúseností a rozvíjajú základné preventívne návyky, ako je vyhýbanie sa podozrivým odkazom alebo neformálne overovanie informácií. Táto oboznámenosť však nie je podložená štruktúrovanými znalosťami, čo vedie k slabinám v oblastiach ako rozpoznávanie bezpečných webových stránok, správa nastavení súkromia, udržiavanie softvérových aktualizácií a identifikácia manipulovaného alebo umelou inteligenciou generovaného obsahu. V dôsledku toho môžu používatelia preceňovať svoju schopnosť bezpečne sa pohybovať v digitálnom prostredí.

Druhá kritická zraniteľnosť súvisí s vyvíjajúcou sa povahou online hrozieb. Ťažkosti pri rozpoznávaní obsahu generovaného umelou inteligenciou signalizujú posun v digitálnom riziku, kde sú tradičné stratégie odhaľovania čoraz nedostatočnejšie. Odhaľuje to generačnú priepasť, keďže novovznikajúce formy podvodov si vyžadujú nové formy kritického a technického povedomia.

Údaje tiež poukazujú na tendenciu k neformálnym a reaktívnym stratégiám zvládania. Mnohí respondenti sa spoliehajú na intuíciu, vyhýbavé správanie alebo externú podporu – napríklad žiadanie o pomoc členov rodiny – namiesto štruktúrovaných preventívnych stratégií. Hoci tieto prístupy môžu ponúkať čiastočnú ochranu, v zložitejších scenároch nie sú dostatočné a môžu prispievať k neistote alebo obmedzenému využívaniu digitálnych služieb.

Vysoká úroveň obáv z potenciálnej viktimizácie v kombinácii s významným podielom respondentov, ktorí už zažili podvod, zároveň naznačuje silnú vnímanú potrebu podpory. Zdá sa, že účastníci si uvedomujú riziká, ale chýbajú im nástroje na ich účinné zvládanie.

Z hľadiska vzdelávania tieto zistenia zdôrazňujú potrebu cielených, praktických a prístupných vzdelávacích intervencií. Školenie by malo presahovať všeobecné povedomie a zameriavať sa na rozvoj konkrétnych kompetencií vrátane rozpoznávania podvodných vzorcov, overovania digitálnych informácií, bezpečnej správy osobných údajov a primeranej reakcie na podozrivé situácie. Osobitná pozornosť by sa mala venovať novovznikajúcim rizikám, najmä tým, ktoré súvisia s umelou inteligenciou a manipulovaným obsahom.

Vzdelávacie prístupy by mali byť používateľsky prívetivé a založené na scenároch z reálneho života, aby sa preklenula medzera medzi každodennými digitálnymi praktikami a pokročilejšími bezpečnostnými kompetenciami. Posilňovanie digitálnej sebadôvery štruktúrovaným a informovaným spôsobom bude nevyhnutné na podporu dospelých vo veku 45+ pri prechode k bezpečnému, samostatnému a odolnému používaniu digitálnych technológií.

5.2 Španielsko

Účel a metóda

Španielsky prieskum sa uskutočnil ako súčasť hodnotenia potrieb projektu digiSAFE s cieľom zozbierať kvantitatívne údaje o digitálnych návykoch, povedomí o online rizikách, skúsenostiach s online podvodmi a vzdelávacích potrebách medzi dospelými vo veku 45 a viac rokov. Cieľom bolo poskytnúť porovnateľné dôkazy naprieč partnerskými krajinami.

Dotazník bol administrovaný online a distribuovaný prostredníctvom sietí Asociación UNO vrátane miestnych združení a neformálnych kanálov vzdelávania dospelých. Účasť bola dobrovoľná a anonymná, v plnom súlade so všeobecným nariadením o ochrane údajov (GDPR).

Od španielskych účastníkov vo veku 45+ bolo zozbieraných minimálne 50 platných odpovedí, čím sa splnili požiadavky projektu na porovnateľnosť a zabezpečila sa spoľahlivosť súboru údajov. Vzorka zahŕňala miernu väčšinu žien (58,8 %). Respondenti boli sústredení vo vekových skupinách 45–54 a 65–74 rokov, pričom všetci účastníci boli starší ako 45 rokov.

Vzorka bola pomerne dobre vzdelaná, pričom väčšina účastníkov mala aspoň stredoškolskú alebo vysokoškolskú kvalifikáciu. Významný podiel tvorili dôchodcovia (47,1 %), zatiaľ čo zvyšní respondenti boli buď zamestnaní, alebo samostatne zárobkovo činní. Z územného hľadiska väčšina účastníkov žila v mestských oblastiach, s menším podielom v vidieckych alebo prímestských kontextoch. Celkovo vzorka poskytuje reprezentatívny prehľad o digitálne aktívnych dospelých vo veku 45+ v Španielsku, pričom zároveň odráža rozdiely v životných situáciách a úrovniach digitálnej samostatnosti.

Kľúčové výsledky

Španielsky súbor údajov ukazuje, že dospelí vo veku 45+ sú aktívne zapojení do digitálneho prostredia, najmä v súvislosti s každodennými aktivitami. Väčšina respondentov uviedla, že používa digitálne nástroje každodenne, najmä na komunikáciu (aplikácie na zasielanie správ a e-mail), online bankovníctvo, sociálne médiá a prístup k verejným službám.

Výsledky zároveň odhaľujú dôležité zraniteľnosti. Celkové každodenné používanie zariadení dosahuje miernu úroveň (priemer 3,29/5), zatiaľ čo všeobecná sebadôvera pri používaní internetu je o niečo nižšia (priemer 3,00/5), pričom značný podiel respondentov uvádza obmedzenú sebadôveru. Kvalitatívne odpovede naznačujú, že mnohí jednotlivci sa pri ťažkostiach online spoliehajú na externú podporu – najmä mladších členov rodiny – čo naznačuje určitý stupeň digitálnej závislosti, a nie plnú samostatnosť.

Samohodnotené digitálne zručnosti sú vo všeobecnosti obmedzené v niekoľkých kľúčových oblastiach. Základné kompetencie ako rozpoznávanie bezpečných webových stránok vykazujú pomerne nízku úroveň sebadôvery (priemer 2,76/5), zatiaľ čo technickejšie zručnosti, ako úprava nastavení súkromia, správa bezpečných hesiel alebo identifikácia obsahu generovaného umelou inteligenciou, predstavujú najslabšie oblasti. Okrem toho mnohí respondenti uviedli neistotu pri rozlišovaní legitímnych správ od pokusov o phishing a pri tom, ako primerane reagovať v prípade podozrenia z podvodu.

Povedomie o online rizikách sa líši v závislosti od typu hrozby. Tradičné formy podvodov, ako phishing a falošné investičné ponuky, sú pomerne dobre rozpoznané a viacerí respondenti uviedli priamu skúsenosť s týmito rizikami. Naproti tomu povedomie o novších hrozbách – najmä tých, ktoré súvisia s umelou inteligenciou, ako deepfaky alebo mylné informácie generované umelou inteligenciou – je výrazne nižšie, pričom značný podiel účastníkov nie je oboznámený s týmito formami klamania.

Samohodnotené bezpečnostné správanie odhaľuje zmiešaný vzorec. Intuitívnejšie postupy, ako vyhýbanie sa podozrivým odkazom alebo overovanie informácií pred zdieľaním, sú pomerne bežné. Technickejšie a preventívne správanie, ako pravidelná aktualizácia softvéru, správa nastavení súkromia alebo overovanie manipulovaného obsahu, sa však prijíma menej konzistentne. To naznačuje, že základné povedomie sa nie vždy premieňa do účinných ochranných postupov.

Skúsenosti s digitálnymi podvodmi sú pomerne časté. Viac ako tretina respondentov (35,3 %) uviedla, že sa stali obeťami online podvodov, najčastejšie phishingu, podvodných nákupov a finančných podvodov. Aj v prípadoch, keď nedošlo k finančnej strate, tieto skúsenosti prispeli k zníženej dôvere v digitálne prostredie a zvýšenej neistote v online interakciách.

Obavy z budúcej viktimizácie sú pozoruhodne vysoké, pričom viac ako 80 % respondentov vyjadrilo mierne až silné úrovne obáv. Účastníci zároveň prejavili silný záujem o ďalšie vzdelávanie, najmä v oblastiach ako rozpoznávanie a prevencia online podvodov, ochrana osobných údajov, zabezpečenie bezpečných postupov online bankovníctva, identifikácia mylných informácií a rozvoj praktických stratégií na zlepšenie digitálnej bezpečnosti v každodennom živote.

Celkovo zistenia poukazujú na medzeru medzi rozšíreným digitálnym zapojením a pokročilejšími kompetenciami v oblasti digitálnej bezpečnosti.

Interpretácia

Španielske zistenia poukazujú na štrukturálnu medzeru medzi digitálnou účasťou a schopnosťou samostatne zvládať online riziká medzi dospelými vo veku 45+.

Hoci je základné digitálne používanie rozšírené, špecifické znalosti týkajúce sa prevencie podvodov, kyberbezpečnostných postupov a rozpoznávania rizík zostávajú obmedzené. To vytvára situáciu, v ktorej sú jednotlivci aktívne zapojení do digitálneho prostredia, ale nie sú plne vybavení na to, aby sa v ňom pohybovali bezpečne, čím sa zvyšuje ich vystavenie tradičným aj novovznikajúcim hrozbám.

Dôležité je, že táto zraniteľnosť nevyplýva z nedostatku motivácie alebo odporu voči technológiám. Naopak, respondenti vyjadrili jasnú ochotu učiť sa a zlepšovať svoje zručnosti. Hlavný problém spočíva v obmedzenej dostupnosti prístupného, cieleného a prakticky orientovaného školenia osobitne zameraného na digitálnu bezpečnosť.

Údaje tiež odhaľujú spoliehanie sa na neformálne a reaktívne stratégie učenia. Mnohí účastníci sa pri riešení problémov spoliehajú na členov rodiny, prístupy pokus-omyl alebo online vyhľadávanie, namiesto toho, aby čerpali zo štruktúrovaných znalostí alebo formálneho školenia. Hoci tieto stratégie môžu poskytovať dočasné riešenia, nezabezpečujú konzistentnú ani účinnú ochranu, najmä v zložitejších alebo vyvíjajúcich sa rizikových scenároch.

Okrem toho obmedzené povedomie o hrozbách súvisiacich s umelou inteligenciou poukazuje na rastúcu výzvu. Keďže digitálne riziká sú čoraz sofistikovanejšie, tradičné formy odhaľovania založené na intuícii alebo predchádzajúcej skúsenosti sú čoraz nedostatočnejšie. Posilňuje to potrebu aktualizovať kompetencie v oblasti digitálnej bezpečnosti v súlade s technologickým vývojom.

Vysoká úroveň obáv z budúcej viktimizácie v kombinácii s frekvenciou minulých skúseností s podvodmi naznačuje silnú vnímanú potrebu podpory. Respondenti si uvedomujú riziká, ale chýba im sebadôvera a nástroje potrebné na ich účinné riešenie.

Z hľadiska vzdelávania tieto zistenia zdôrazňujú dôležitosť rozvoja cielených vzdelávacích intervencií, ktoré sú praktické, prístupné a prispôsobené dospelým študujúcim. Školenie by sa malo zameriavať na posilňovanie konkrétnych kompetencií vrátane rozpoznávania podvodných vzorcov, bezpečnej správy osobných údajov, overovania digitálneho obsahu a primeranej reakcie na podozrivé situácie.

Neformálne vzdelávacie prístupy sú v tomto kontexte obzvlášť relevantné. Programy by mali používať jasný jazyk, scenáre z reálneho života a praktické cvičenia na preklenutie medzery medzi každodennými digitálnymi praktikami a pokročilejšími bezpečnostnými zručnosťami. Posilňovanie digitálnej samostatnosti a odolnosti bude nevyhnutné na podporu dospelých vo veku 45+ pri bezpečnom a sebadomom zapájaní sa do digitálnej spoločnosti.

5.3 Slovensko

Účel a metóda

Slovenský prieskum sa uskutočnil ako súčasť hodnotenia potrieb projektu digiSAFE s cieľom vyhodnotiť digitálne návyky, technickú sebadôveru, povedomie o online rizikách a skúsenosti s digitálnymi podvodmi medzi dospelými vo veku 45 a viac rokov. Zozbierané

údaje sú určené na to, aby priamo informovali tvorbu vzdelávacieho kurikula a sady nástrojov digitálnej bezpečnosti projektu.

Výskum prijal kvantitatívny prístup s použitím štandardizovaného online dotazníka navrhnutého tak, aby zabezpečil prístupnosť a porovnateľnosť naprieč partnerskými krajinami. Prieskum zahŕňal kombináciu otázok na Likertovej škále a otázok s viacerými možnosťami zameraných na posúdenie kľúčových oblastí, ako je každodenné používanie internetu, vnímané digitálne kompetencie, povedomie o tradičných aj novovznikajúcich kybernetických hrozbách a priame skúsenosti s online podvodmi.

Na medzinárodnej úrovni bolo zozbieraných celkovo 131 odpovedí. Na účely národnej analýzy bol súbor údajov starostlivo filtrovaný tak, aby zahŕňal iba respondentov s pobytom na Slovensku alebo v inej európskej krajine, v súlade s kritériami projektu. Tento proces viedol ku konečnej vzorke 51 platných odpovedí, ktorá spĺňa minimálny prah požadovaný na porovnateľnosť.

Vzorka sa skladá predovšetkým z jednotlivcov v aktívnej profesijnej fáze a fáze skorého dôchodku: 43 % respondentov je vo veku 45–54 rokov, 35 % má 55–64 rokov a 22 % je 65+. Ženy predstavujú 65 % vzorky. Účastníci sú pomerne dobre vzdelaní, pričom väčšina má vyššie stredoškolské alebo pomaturitné vzdelanie, a sú pomerne rovnomerne rozdelení medzi mestské (55 %) a vidiecke (45 %) oblasti. Celkovo vzorka odráža digitálne aktívnu populáciu s rozmanitými sociálno-demografickými charakteristikami.

Kľúčové výsledky

Slovenský súbor údajov odhaľuje vysokú úroveň digitálneho zapojenia medzi dospelými vo veku 45+, sprevádzanú významnými medzerami v kyberbezpečnostných kompetenciách.

Pripojiteľnosť je obzvlášť silná: 92 % respondentov uvádza každodenné používanie smartfónu alebo počítača. Všeobecná sebadôvera pri vykonávaní základných online aktivít, ako je e-mailovanie alebo online nakupovanie, je tiež pomerne vysoká (68 %). Toto časté používanie sa však nepremiata do účinnej technickej bezpečnosti.

Dôležité slabiny sa objavujú v kľúčových kompetenciách digitálnej bezpečnosti. Iba 35 % respondentov sa cíti úplne isto pri rozpoznávaní, či je webová stránka bezpečná, napríklad identifikáciou protokolov HTTPS alebo bezpečnostných indikátorov. Podobne menej ako polovica (41 %) uvádza, že dokáže upraviť nastavenia súkromia a bezpečnosti na svojich zariadeniach. Tieto zistenia naznačujú, že hoci sú používatelia operačne aktívni online, chýbajú im technické zručnosti potrebné na samostatné zvládanie rizík.

V povedomí o rôznych typoch kybernetických hrozieb je pozorovaná jasná priepasť. Tradičné riziká sú široko rozpoznávané: 85 % respondentov uvádza mierne alebo silné povedomie o phishingových e-mailoch, podvodných SMS správach a falošných online obchodoch. Naproti tomu povedomie o novovznikajúcich hrozbách je výrazne nižšie. Pozoruhodných 78 % účastníkov uvádza len mierne povedomie alebo žiadne povedomie o podvodoch generovaných umelou inteligenciou, ako sú deepfaky alebo klonovanie hlasu. Podobne 72 % naznačuje nízku sebadôveru v schopnosť identifikovať médiá alebo spravodajský obsah manipulovaný umelou inteligenciou.

Pozoruhodná je aj priama skúsenosť s digitálnymi podvodmi. Štvrtina respondentov (25 %) uvádza, že sa stali obeťami online podvodov. Vzorce reakcií medzi obeťami poukazujú na kritický problém: väčšina sa spolieha na neformálne reakcie, pričom 62 % uvádza, že buď vymazali škodlivú správu, alebo vyhľadali pomoc u rodiny a priateľov. Iba malá menšina (15 %) formálne nahlásila incident bankám, online platformám alebo orgánom činným v trestnom konaní.

Celkovo zistenia poukazujú na silnú nerovnováhu medzi vysokou úrovňou digitálnej aktivity a obmedzenou kapacitou zvládať tradičné aj novovznikajúce online riziká.

Interpretácia

Slovenské zistenia poukazujú na výraznú medzeru medzi digitálnym zapojením a účinnou kyberbezpečnostnou kompetenciou medzi dospelými vo veku 45+.

Hoci sú respondenti častými a sebedomými používateľmi digitálnych technológií na každodenné účely, ich schopnosť zvládať riziká zostáva obmedzená. Vytvára to "priepasť v sebadôvere," v ktorej jednotlivci disponujú operačnými zručnosťami potrebnými na pohyb v digitálnom prostredí, ale chýbajú im technické znalosti potrebné na zabezpečenie vlastnej bezpečnosti. Zdá sa, že prijímanie digitálnych technológií je poháňané predovšetkým pohodlnosťou a nevyhnutnosťou, a nie komplexným porozumením digitálneho ekosystému.

Kľúčová zraniteľnosť sa týka rýchleho vývoja digitálnych hrozieb. Hoci respondenti preukazujú solídne povedomie o tradičných formách kybernetickej kriminality, ako je phishing alebo falošné online obchody, sú výrazne menej pripravení vyrovnať sa s pokročilejšími formami podvodov. Veľmi nízke povedomie o podvodoch generovaných umelou inteligenciou a obmedzená schopnosť identifikovať manipulovaný obsah naznačujú kritickú generačnú priepasť. Tieto novovznikajúce hrozby sa často spoliehajú na psychologickú manipuláciu a emocionálne spúšťače, čo ich robí ťažšie odhaliteľnými pomocou konvenčných stratégií.

Ďalší dôležitý problém sa týka behaviorálnych reakcií na kybernetické incidenty. Údaje odhaľujú silné spoliehanie sa na neformálne mechanizmy zvládania, ako je ignorovanie podozrivých správ alebo vyhľadávanie pomoci v osobných sieťach. Mimoriadne nízka miera formálneho nahlasovania naznačuje tak nedostatok znalostí o oficiálnych postupoch, ako aj prítomnosť psychologických bariér vrátane rozpakov, strachu alebo pocitu nevyhnutnosti. To obmedzuje účinnosť inštitucionálnych ochranných mechanizmov a zvyšuje dlhodobý vplyv podvodov.

Z hľadiska vzdelávania tieto zistenia poukazujú na potrebu posunu od základnej digitálnej účasti smerom k štruktúrovanejším a proaktívnejším kompetenciám v oblasti digitálnej bezpečnosti. Vzdelávacie intervencie by mali uprednostňovať praktické a na scenároch založené prístupy, ktoré študujúcim umožňujú rozpoznávať situácie z reálneho života a reagovať na ne, najmä na tie, ktoré zahŕňajú sofistikované podvody alebo podvody poháňané umelou inteligenciou.

Okrem toho by školenie malo zahŕňať jasné a prístupné usmernenia o konfigurácii nastavení súkromia a bezpečnosti, ako aj pokyny krok za krokom o tom, ako nahlasovať incidenty a vyhľadať inštitucionálnu podporu. Riešenie psychologického rozmeru kybernetickej kriminality prostredníctvom normalizácie viktimizácie a znižovania stigmy bude tiež nevyhnutné na podporu proaktívnejšieho a sebavedomejšieho správania.

Posilňovanie technickej kompetencie aj sebadôvery používateľov bude kľúčové pre podporu dospelých vo veku 45+ na Slovensku pri prechode od pasívnych alebo reaktívnych stratégií smerom k samostatnejšiemu, informovanejšiemu a odolnejšiemu zapojeniu do digitálneho prostredia.

6. Nadnárodná analýza

Porovnanie národných zistení z Talianska, Španielska a Slovenska odhaľuje súbor výrazných zhôd, ktoré poukazujú na spoločnú európsku výzvu, popri niektorých významných národných rozdieloch, ktoré majú dôsledky pre návrh prispôbených vzdelávacích intervencií.

6.1 Spoločné výzvy naprieč krajinami

Všetky tri krajiny vykazujú konzistentnú a štrukturálne významnú medzeru medzi digitálnym zapojením a kompetenciou v oblasti digitálnej bezpečnosti. Dospelí vo veku 45+ v Taliansku, Španielsku a na Slovensku sú v rôznej miere pravidelnými a aktívnymi používateľmi internetu – využívajú digitálne služby na komunikáciu, bankovníctvo, vyhľadávanie informácií a elektronický obchod. No vo všetkých troch kontextoch samohodnotená sebadôvera a skutočná kompetencia prudko klesajú, keď sa posudzujú

špecifickéjšie zručnosti digitálnej bezpečnosti: rozpoznávanie bezpečných webových stránok, správa nastavení súkromia, udržiavanie softvérových aktualizácií a bezpečné zaobchádzanie s údajmi.

Druhým zhodným vzorcom je takmer univerzálna slabina v rozpoznávaní obsahu generovaného alebo manipulovaného umelou inteligenciou. Vo všetkých troch krajinách je to konzistentne identifikované ako najzraniteľnejšia oblasť medzi respondentmi, ďaleko pod povedomím o tradičných hrozbách, ako je phishing alebo falošné online obchody. Toto zistenie je obzvlášť naliehavé: podvody založené na umelej inteligencii – deepfaky, klonovanie hlasu, podvodné správy generované umelou inteligenciou – sú najrýchlejšie rastúcou kategóriou digitálnej hrozby, no zároveň tou, na ktorú je populácia 45+ v celej Európe najmenej pripravená.

Tretou spoločnou výzvou je spoliehanie sa na neformálne, reaktívne stratégie zvládania. V Taliansku, Španielsku aj na Slovensku sa mnohí respondenti spoliehajú na intuíciu, opatrnosť alebo externú podporu od členov rodiny namiesto štruktúrovaných znalostí a zručností. Tento prístup "neformálnej obrany" môže znížiť niektoré riziká, ale je úplne nedostatočný tvárou v tvár sofistikovanému klamaniu s podporou umelej inteligencie. Tiež má tendenciu posilňovať digitálne vyhýbavé správanie namiesto budovania skutočnej odolnosti.

Napokon všetky tri krajiny uvádzajú významné úrovne obáv z budúcej viktimizácie (84,1 % v Taliansku, viac ako 80 % v Španielsku, vysoké aj na Slovensku) a pozoruhodné miery minulej viktimizácie – 38,1 % v Taliansku, 35,3 % v Španielsku a 25 % na Slovensku. Medzera medzi obavami a kompetenciou je konzistentnou črtou naprieč celým súborom údajov.

6.2 Hlavné rozdiely

Napriek týmto zhodám existujú medzi tromi národnými kontextami významné rozdiely. Taliansko aj Slovensko vykazujú veľmi vysoké úrovne každodenného digitálneho zapojenia (77,8 % a 92 % hodnotí každodenné používanie zariadení na najvyšších úrovniach), zatiaľ čo španielski respondenti vykazujú o niečo umiernennejšie vzorce zapojenia (priemerné každodenné používanie zariadení 3,29/5). To naznačuje, že španielski respondenti, hoci sú digitálne aktívni, môžu byť o niečo menej zakorenení v intenzívnych digitálnych rutinách ako ich talianski a slovenskí protívkovia.

Povaha prevažujúcich podvodných hrozieb sa líši naprieč kontextami. Na Slovensku bol zdokumentovaný obzvlášť závažný a špecifický vzorec hrozieb: sofistikované vishingové útoky, pri ktorých sa podvodníci vydávajú za policajtov alebo bankových úradníkov, aby manipulovali obeť k prevodu finančných prostriedkov. Táto forma sociálneho inžinierstva zneužíva inštitucionálnu dôveru spôsobmi, ktoré sú v talianskom a španielskom kontexte menej zdokumentované. Slovensko tiež čelí špecifickej výzve

súvisiacej s objemom a vplyvom dezinformačných kampaní, zosilnených geopolitickou situáciou krajiny.

Miery formálneho nahlasovania incidentov sa výrazne líšia. Slovenskí respondenti vykázali alarmujúco nízku mieru formálneho nahlasovania (iba 15 % obetí formálne nahlásilo incidenty), výrazne nižšiu, než aká sa objavila v talianskom a španielskom kontexte. Poukazuje to na silnejšiu kultúru hanby okolo viktimizácie na Slovensku a/alebo slabšie povedomie o inštitucionálnych kanáloch nahlasovania – konkrétna oblasť vyžadujúca cieleňú intervenciu.

Taliansko predstavuje silnejšiu inštitucionálnu a programovú infraštruktúru pre digitálnu inklúziu (Repubblica Digitale, CPIA, program GOL) v porovnaní so Slovenskom, kde sú národne vedené programy novšie a oslovili menej ľudí. Španielsko zaujíma medzipozíciu so silnými národnými rámcami (INCIBE, Digital Spain 2026), ale nerovnomernou implementáciou naprieč regiónmi.

6.3 Vzorce správania

Naprieč všetkými tromi krajinami respondenti vykazujú konzistentný vzorec správania: sebadôvera pri vysokofrekvenčných rutinných úlohách (kontrola e-mailu, online bankovníctvo, používanie aplikácií na zasielanie správ) koexistuje s neistotou a nízkou kompetenciou pri menej frekventovaných, ale rizikovejších úlohách (overovanie bezpečnosti webových stránok, konfigurácia nastavení súkromia, identifikácia manipulovaného obsahu). Tento vzorec naznačuje, že digitálna navyknutosť vytvára falošný pocit celkovej kompetencie, ktorý sa nevztahuje na bezpečnostne kritické správanie.

Dôvera v digitálne nástroje je vo všeobecnosti stredná až vysoká pri známych, dobre známych platformách a službách, ale výrazne klesá pri konfrontácii s neznámymi zdrojmi, neznámymi požiadavkami alebo nejednoznačnými situáciami. Respondenti vo všetkých troch krajinách majú tendenciu riešiť takúto nejednoznačnosť vyhýbaním sa (neklíkaním, nezapájaním sa) namiesto aktívneho overovania – prístup, ktorý znižuje riziko, ale neriadi ho.

Vystavenie riziku je najvyššie v Taliansku (38,1 % miera viktimizácie), nasledované Španielskom (35,3 %) a potom Slovenskom (25 %). Tieto rozdiely však môžu čiastočne odrážať rozdiely v zložení vzorky a kanáloch šírenia prieskumu. Vo všetkých troch krajinách sú najbežnejšími formami zažitých podvodov finančné (bankové podvody, falošné nákupy, phishing), čo potvrdzuje, že finančná oblasť je primárnym priestorom škôd.

6.4 Medzinárodné poznatky z osvedčených postupov

Naprieč Talianskom, Španielskom a Slovenskom analýza osvedčených postupov odhaľuje množstvo spoločných vzorcov, ktoré presahujú konkrétne národné kontexty a poukazujú na spoločné prístupy k vzdelávaniu o digitálnej bezpečnosti pre dospelých vo veku 45+.

Silný dôraz na neformálne a prakticky orientované učenie sa konzistentne objavuje vo všetkých troch krajinách. Iniciatívy sa zriedka zakladajú iba na teoretickej výučbe; uprednostňujú praktické aktivity, scenáre z reálneho života a usmernenia krok za krokom. Odráža to potrebu pretaviť abstraktné digitálne riziká do konkrétnych a zrozumiteľných situácií pre dospelých študujúcich. Na Slovensku je táto orientácia obzvlášť zjavná v Akadémiách Smart Senior organizovaných regionálnymi verejnými knižnicami, kde knihovníci a dobrovoľní škoolitelia sprevádzajú malé skupiny praktickými cvičeniami ich vlastným tempom, a v seminároch na lokálnej úrovni organizovaných Jednotou dôchodcov (JDS), ktoré sa zameriavajú na bezprostredné, lokálne relevantné hrozby, ako sú podvodné e-shopy a falošné telefonáty.

Mnohé osvedčené postupy tiež prijímajú komunitný a inkluzívny prístup realizovaný prostredníctvom miestnych centier, združení alebo verejných inštitúcií, ktoré sú cieľovej skupine už známe a dôveryhodné. Vo všetkých troch krajinách sú vzdelávacie prostredia navrhnuté tak, aby boli prístupné a s nízkym prahom, čím sa znižujú bariéry účasti a podporuje sa sebadôvera medzi študujúcimi. Slovenský decentralizovaný model – najvýraznejšie prostredníctvom programu Zrelí na dobu digitálnu Nadačného fondu Telekom, ktorý smeruje financovanie priamo do domovov sociálnych služieb a komunitných centier – ponúka obzvlášť replikovateľný príklad toho, ako môže poskytovanie na lokálnej úrovni osloviť izolovaných seniorov vo vidieckych oblastiach, ktorí by sa nemuseli zúčastniť veľkých, centrálne organizovaných kurzov.

Využívanie rovesníckeho učenia a medzigeneračných alebo rovesnícky podporovaných modelov predstavuje ďalšiu spoločnú črtu. V Taliansku je to najviditeľnejšie v iniciatívach ako Digitálna občianska služba, zatiaľ čo v Španielsku zohráva podobnú úlohu mentorstvo založené na dobrovoľníkoch a zapojenie komunity. Na Slovensku model rovesníckej dôvery prijatý seminármi JDS, kde sa učenie odohráva v rámci sietí spoluseniorov, ukazuje, že znižovanie psychologickéj úzkosti okolo digitálnych nástrojov je rovnako dôležité ako poskytovanie obsahu. Dospelí vo veku 45+ konzistentne profitujú z kolaboratívnych a sociálne zakorenených vzdelávacích procesov, a nie z individuálnych, samostatne riadených modelov.

Vzorcom viditeľnejším na Slovensku než v ostatných dvoch krajinách je aktívne zapojenie súkromného sektora do verejného digitálneho vzdelávania. Portál Bezpečne na nete, ktorý vytvorila kyberbezpečnostná spoločnosť ESET, je príkladom toho, ako možno odbornosť súkromného sektora smerovať do bezplatného, neustále aktualizovaného a verejne prístupného vzdelávacieho obsahu, model, ktorý by ostatné európske kontexty mohli replikovať prostredníctvom rámcov spoločenskej zodpovednosti podnikov.

Popri týchto zhodách možno pozorovať významné rozdiely. Taliansko vykazuje silnejšiu integráciu medzi národnými stratégiami a viacúrovňovými iniciatívami, s koordinovanými aktivitami prepájajúcimi politické rámce, vzdelávacie programy a osvetové kampane. Španielsko predstavuje decentralizovanejšiu a rozmanitejšiu krajinu, kde široká škála aktérov pôsobí na národnej, regionálnej a miestnej úrovni, niekedy bez silnej koordinácie medzi nimi. Slovensko zaujíma medzipozíciu: hoci je jeho inštitucionálny rámec robustný (koordinovaný subjektmi ako NBÚ a MIRRI), dosah formálnych programov medzi vekovou skupinou 45–64 rokov zostáva obmedzený a najúčinnnejšie iniciatívy bývajú neformálne a komunitne riadené.

Celkové dôkazy naprieč všetkými tromi partnerskými krajinami poukazujú na rovnaký záver: účinné vzdelávanie o digitálnej bezpečnosti pre dospelých vo veku 45+ sa opiera o kombináciu prístupnosti, praktickej relevantnosti, sociálneho učenia a dôvery. Tieto prvky predstavujú kľúčové prenositeľné komponenty, ktoré by mali priamo informovať tvorbu kurikula a sady nástrojov projektu digiSAFE.

7. Kľúčové zistenia

Z nadnárodnej analýzy výsledkov národného výskumu vyplývajú nasledujúce kľúčové zistenia:

1. Digitálne zapojenie sa nerovná digitálnej bezpečnosti. Naprieč Talianskom, Španielskom a Slovenskom sú dospelí vo veku 45+ aktívnymi a častými používateľmi internetu, no konzistentne preukazujú nízku kompetenciu v zručnostiach špecifických pre digitálnu bezpečnosť, ako je rozpoznávanie bezpečných webových stránok, konfigurácia nastavení súkromia a správa bezpečnosti účtov.
2. Hrozby založené na umelej inteligencii predstavujú najkritickejšiu a univerzálnu medzeru. Povedomie a rozpoznávanie podvodov generovaných umelou inteligenciou, deepfakov a manipulovaných médií sú najslabšími oblasťami kompetencií vo všetkých troch krajinách. Zároveň ide o najrýchlejšie rastúcu kategóriu online hrozby, čo z nej robí najnaliehavejšiu prioritu pre vzdelávaciu intervenciu.
3. Neformálne stratégie zvládania prevažujú a sú nedostatočné. Primárna behaviorálna reakcia na vnímané riziko naprieč všetkými tromi národnými vzorkami je neformálna, intuitívna a reaktívna (vyhýbanie sa, rodinná podpora, všeobecná opatrnosť), a nie štruktúrovaná a proaktívna. Tento prístup poskytuje

nedostatočnú ochranu pred sofistikovaným sociálnym inžinierstvom a podvodmi s podporou umelej inteligencie.

4. Miery minulej viktimizácie sú vysoké a podceňované. Medzi štvrtinou a takmer dvomi pätinami respondentov prieskumu naprieč tromi krajinami uviedlo priamu skúsenosť s digitálnym podvodom, čo potvrdzuje, že tieto riziká nie sú teoretické, ale reálne a bezprostredné pre cieľovú skupinu.
5. Obavy sú vysoké, ale nezodpovedajú zručnostiam. Naprieč všetkými tromi krajinami veľká väčšina respondentov (viac ako 80 %) vyjadruje jasné obavy z budúcej viktimizácie. Táto vysoká úroveň obáv v kombinácii s priznanými deficitmi zručností naznačuje silný a neuspokojený dopyt po cieleňom školení.
6. Formálne nahlasovanie incidentov je kriticky nedostatočne využívané. Konzistentným vzorcom naprieč všetkými tromi krajinami – najvýraznejším na Slovensku – je tendencia riešiť podvodné incidenty neformálne, bez nahlásenia bankám, platformám alebo orgánom činným v trestnom konaní. Toto nedostatočné nahlasovanie obmedzuje systémové reakcie a ponecháva obeť bez inštitucionálnej podpory.
7. "Priepasť v sebadôvere" je systémovou zraniteľnosťou. Vo všetkých troch krajinách majú respondenti tendenciu preceňovať svoju celkovú digitálnu bezpečnosť na základe vysokej zdatnosti v rutinných úlohách, pričom podceňujú svoju špecifickú zraniteľnosť v rizikových, menej známych situáciách. Táto ilúzia kompetencie si vyžaduje vzdelávacie prístupy, ktoré spochybňujú predpoklady a budujú skutočne kritické digitálne povedomie.
8. Národné politické rámce existujú, ale ich implementácia je nerovnomerná. Všetky tri krajiny vyvinuli relevantné regulačné rámce a programy digitálnych zručností, ale ich dosah medzi demografickou skupinou 45+ zostáva obmedzený, najmä na Slovensku a vo vidieckych oblastiach naprieč všetkými tromi krajinami.

8. Identifikované medzery a vzdelávacie potreby

Na základe sekundárneho výskumu, analýzy prieskumu a medzinárodného porovnania boli identifikované nasledujúce konkrétne medzery a vzdelávacie potreby pre dospelých vo veku 45+ naprieč Talianskom, Španielskom a Slovenskom. Hoci sú viaceré z týchto medzier spoločné všetkým trom kontextom, ich intenzita a prejav sa líšia spôsobmi, ktoré sú priamo relevantné pre návrh kurikula.

8.1 Medzery v zručnostiach

Naprieč všetkými tromi krajinami sa objavuje významná medzera medzi frekvenciou, s akou dospelí vo veku 45+ používajú digitálne technológie, a ich skutočnou schopnosťou zvládať online riziká. Na Slovensku 92 % respondentov uviedlo každodenné používanie

smartfónu alebo počítača – číslo konzistentné s vysokými mierami pripojiteľnosti pozorovanými v Taliansku a Španielsku – no táto frekvencia sa nepremiata do štruktúrovaných znalostí postupov digitálnej bezpečnosti. Na Slovensku sa iba 35 % respondentov cítilo isto pri rozpoznávaní bezpečnej webovej stránky a menej ako polovica (41 %) uviedla, že vie, ako upraviť nastavenia súkromia a bezpečnosti na svojich vlastných zariadeniach. Tento vzorec, ktorý slovenská správa výstižne opisuje ako "priepasť v sebadôvere", je štrukturálne prítomný naprieč všetkými tromi národnými vzorkami, hoci sa javí najakútnejší v Španielsku, kde silné spoliehanie sa na členov rodiny ako primárny zdroj digitálnej podpory naznačuje formu závislosti, a nie skutočnú digitálnu samostatnosť.

Konkrétnejšie, schopnosť technicky overiť bezpečnosť a autentickosť digitálnych prostredí zostáva slabá naprieč všetkými tromi krajinami: identifikácia bezpečných webových stránok (indikátory HTTPS, ikony zámku), rozpoznávanie znakov phishingových e-mailov alebo rozlišovanie legitímnych od podvodných SMS správ sú kompetencie, ktoré si významný podiel respondentov nevyvinul. Správu bezpečnosti zariadení a účtov – vrátane konfigurácie nastavení súkromia, používania silných a jedinečných hesiel, zapnutia dvojfaktorovej autentifikácie a vykonávania pravidelných aktualizácií softvéru a antivírusu – praktizuje menšina a rozumie jej ešte menej ľudí. Talianski respondenti sa zdajú o niečo sebedomejši v niektorých rutinných ochranných správaniach, zatiaľ čo španielski a slovenskí účastníci vykazujú väčšiu neistotu pri konzistentnom uplatňovaní týchto postupov.

8.2 Medzery v znalostiach

Najkritickejšia a univerzálna medzera v znalostiach naprieč všetkými tromi krajinami sa týka rozpoznávania obsahu generovaného alebo manipulovaného umelou inteligenciou. V Taliansku je to už identifikované ako jedna z najslabších oblastí kompetencií, s konzistentne nízkym samohodnotiacim skóre v identifikácii rizík založených na umelej inteligencii. Slovenské údaje toto zistenie potvrdzujú s osobitnou jasnosťou: 78 % respondentov uviedlo, že majú len mierne povedomie alebo úplne žiadne povedomie o podvodoch generovaných umelou inteligenciou, ako sú deepfaky a klonovanie hlasu, a 72 % priznalo malú alebo žiadnu sebadôveru v identifikácii médií alebo správ manipulovaných umelou inteligenciou. V Španielsku je povedomie o takýchto hrozbách ešte menej rozvinuté, pričom významný podiel respondentov uvádza malú alebo žiadnu oboznámenosť s podvodmi súvisiacimi s umelou inteligenciou. Naprieč všetkými tromi kontextami to predstavuje najnaliehavejšiu vzdelávaciu medzeru – takú, ktorá si vyžaduje špecializované, na scenároch založené školenie, a nie všeobecné zvyšovanie povedomia.

Okrem hrozieb súvisiacich s umelou inteligenciou pretrvávajú významné deficity znalostí týkajúce sa mechanizmov sociálneho inžinierstva a psychologických manipulačných taktík používaných kyberzločincami. Na Slovensku je to umocnené špecifickým a obzvlášť

škodlivým prostredím hrozieb: podvodníci sa často vydávajú za policajtov alebo bankových zamestnancov pomocou technológie falšovania telefónnych čísel, pričom zneužívajú práve ten druh inštitucionálnej dôvery, ktorý starší dospelí s najväčšou pravdepodobnosťou prejavia – vzorec, ktorý formálne školenie zatiaľ adekvátne nerieši. Znalosť práv na ochranu údajov a formálnych postupov, ktoré treba dodržať po podvodnom incidente (komu nahlásiť, aké možnosti nápravy existujú), je tiež kriticky nedostatočná naprieč všetkými tromi národnými vzorkami.

8.3 Medzery v povedomí a reakcia na incidenty

Ďalšia medzera, konzistentne prítomná, ale s rôznou intenzitou naprieč tromi krajinami, sa týka reakcie na incidenty a správania pri nahlasovaní. Spomedzi 25 % slovenských respondentov, ktorí zažili digitálny podvod, sa iba 15 % rozhodlo formálne nahlásiť incident banke, platforme alebo orgánu činnému v trestnom konaní. Väčšina (62 %) jednoducho vymazala škodlivú správu alebo vyhľadala neformálnu pomoc u rodiny alebo priateľov. Tento vzorec sa odzrkadľuje v talianskych a španielskych zisteniach a odráža spoločný súbor psychologických bariér: hanba, rozpaky a vnímaný pocit fatalizmu ohľadom kybernetickej kriminality aktívne odrádzajú obeť od zapojenia sa do inštitucionálnych podporných systémov. Riešenie tejto bariéry si vyžaduje nielen procedurálne usmernenie o kanáloch nahlasovania, ale aj zámerné úsilie o destigmatizáciu viktimizácie v rámci vzdelávacích programov.

Na úrovni všeobecného povedomia sa najvýznamnejšia medzera týka novovznikajúcich hrozieb. Podvody založené na umelej inteligencii, deepfaky, klonovanie hlasu a dezinformácie generované umelou inteligenciou sú kategórie rizika, s ktorými má väčšina respondentov vo všetkých troch krajinách obmedzenú alebo žiadnu oboznámenosť. Existuje tiež širší nedostatok povedomia o konkrétnych dôsledkoch viktimizácie (finančných, sociálnych a psychologických), čo môže prispievať k podceňovaniu rizika medzi tými, ktorí ešte neboli priamo zacielení.

Spoločne komparatívny obraz naprieč Talianskom, Španielskom a Slovenskom zdôrazňuje dôležitosť navrhovania vzdelávacích prístupov, ktoré sú koherentné aj adaptabilné na konkrétne národné potreby. Slovensko predstavuje obzvlášť výraznú zraniteľnosť ohľadom hrozieb poháňaných umelou inteligenciou a zneužívania inštitucionálnej dôvery, zatiaľ čo Španielsko vykazuje silnejšiu závislosť od neformálnych podporných sietí a Taliansko odráža o niečo vyššiu, ale stále krehkú základnú úroveň technickej sebadôvery. Tieto rozdiely poukazujú na hodnotu modulárneho rámca kurikula, ktorý dokáže riešiť spoločné medzery v kompetenciách a zároveň umožňuje kontextualizáciu na úrovni krajín.

9. Odporúčania pre tvorbu kurikula

Dôkazy zozbierané naprieč tromi fázami národného výskumu poskytujú jasný a na dôkazoch založený základ pre kurikulum neformálneho vzdelávania (NFE) projektu digiSAFE. Nasledujúce odporúčania odrážajú medzery a vzdelávacie potreby identifikované v časti 8 a sú štruktúrované okolo kľúčových oblastí, ktoré by malo kurikulum riešiť.

9.1 Tematické moduly

Kurikulum je usporiadané do štruktúrovanej postupnosti vzdelávacích komponentov, ktorá pozostáva zo šiestich základných modulov, podporených úvodnou orientačnou fázou a záverečným krokom uzavretia a plánovania aktivít.

Celkový návrh umožňuje flexibilitu pri poskytovaní. Celé kurikulum možno realizovať ako 2-dňový intenzívny workshop, ako sériu kratších stretnutí alebo v zmiešanom formáte kombinujúcom prezenčné a online prvky. Zároveň je každý modul navrhnutý tak, aby fungoval ako samostatné stretnutie v dĺžke približne 90 minút, čím sa kurikulum stáva prispôsobiteľným rôznym vzdelávacím prostrediam a časovým obmedzeniam.

Táto modulárna štruktúra zabezpečuje, že kurikulum môže byť komplexné aj flexibilné, podporujúce realizáciu celého programu, ako aj ciele intervencie založené na konkrétnych miestnych potrebách.

1. Modul 0: Orientácia a predbežné hodnotenie. Tento úvodný modul reaguje na rozmanité počiatočné úrovne digitálnej sebadôvery identifikované naprieč všetkými partnerskými krajinami. Výskum ukazuje, že hoci sú mnohí dospelí vo veku 45+ aktívnymi digitálnymi používateľmi, ich povedomie o rizikách a vnímané kompetencie sa výrazne líšia. Tento modul je nevyhnutný na budovanie dôvery, znižovanie počiatočnej úzkosti a pomoc účastníkom zamyslieť sa nad vlastnými digitálnymi návykmi, vystavením riziku a vzdelávacími potrebami pred tým, než sa zapoja do technickejšieho obsahu.
2. Modul 1: Bezpečné každodenné používanie digitálnych technológií. Tento modul priamo rieši medzeru identifikovanú medzi častým digitálnym používaním a obmedzeným porozumením základných bezpečnostných princípov. Naprieč všetkými krajinami respondenti uvádzali vysokú úroveň každodenného digitálneho zapojenia, ale vykazovali nekonzistentnosti v rozpoznávaní bezpečných prostredí a uplatňovaní rutinných ochranných správ. Modul podporuje študujúcich pri identifikácii postupov bezpečného používania, rozpoznávaní signálov dôvery a rozvíjaní uvedomejších a bezpečnejších každodenných digitálnych návykov.
3. Modul 2: Phishing, smishing a vzorce podvodov. Tento modul reaguje na vysoké úrovne vystavenia online podvodom identifikované vo výskume. Vo všetkých troch

krajinách patrili phishing, podvodné správy a finančné podvody medzi najbežnejšie hrozby, ktoré respondenti zažili. Zistenia zdôrazňujú potrebu, aby účastníci rozpoznávali vzorce podvodov, identifikovali varovné signály a rozvíjali schopnosť zastaviť sa a kriticky posúdiť podozrivé komunikácie pred tým, než budú konať.

4. Modul 3: Bezpečné platby, nakupovanie a finančná ochrana. Tento modul je opodstatnený rozšírenou skúsenosťou s finančnými podvodmi a falošnými online ponukami uvádzanými naprieč súbormi údajov. Mnohí respondenti naznačili ťažkosti pri rozlišovaní legitímnych transakcií od podvodných, najmä pri online nakupovaní a digitálnych platbách. Modul sa zameriava na posilňovanie bezpečnejšieho finančného správania, pomáhajúc študujúcim rozpoznávať nespoľahlivé platformy a uplatňovať bezpečnejšie stratégie rozhodovania.
5. Modul 4: Súkromie, heslá a ochrana zariadení. Tento modul rieši konzistentné slabiny v technických bezpečnostných postupoch identifikované vo všetkých krajinách. Výskum zdôrazňuje obmedzené znalosti a nekonzistentné používanie nastavení súkromia, bezpečných hesiel a softvérových aktualizácií. Tieto medzery výrazne zvyšujú zraniteľnosť voči kybernetickým hrozbám. Modul sa preto zameriava na posilňovanie ochrany účtov a podporu praktických, každodenných bezpečnostných rutín.
6. Modul 5: Umelá inteligencia, mylné informácie a manipulovaný obsah. Tento modul reaguje na jednu z najkritickejších a prierezových medzier identifikovaných vo výskume: obmedzenú schopnosť rozpoznať obsah generovaný umelou inteligenciou a novovznikajúce formy digitálnej manipulácie. Naprieč všetkými partnerskými krajinami bolo povedomie o hrozbách založených na umelej inteligencii – ako deepfaky, klonovanie hlasu a syntetické médiá – výrazne nižšie ako povedomie o tradičných rizikách. Cieľom tohto modulu je rozvíjať kritické myslenie a overovacie zručnosti potrebné na pohyb v čoraz zložitejších digitálnych informačných prostrediach.
7. Modul 6: Čo robiť, keď sa niečo pokazí. Tento modul rieši významnú medzeru v znalostiach a správaní pri reakcii identifikovanú naprieč súbormi údajov. Mnohí respondenti uvádzali neistotu ohľadom toho, ako reagovať v prípade podvodu, a spoliehali sa predovšetkým na neformálne stratégie, ako je ignorovanie incidentov alebo vyhľadávanie pomoci u členov rodiny. Miery formálneho nahlasovania boli nízke. Modul sa preto zameriava na poskytovanie jasných postupov reakcie, zlepšovanie sebadôvery pri riešení incidentov a zvyšovanie povedomia o dostupných podporných mechanizmoch.
8. Záver: Osobný plán digitálnej bezpečnosti. Záverečný komponent reaguje na potrebu pretaviť učenie do konkrétnej zmeny správania. Zistenia výskumu ukazujú vysoké úrovne obáv z digitálnych rizík, ale obmedzené štruktúrované stratégie na ich riešenie. Tento posledný krok podporuje študujúcich pri konsolidácii ich

znalostí, definovaní osobných bezpečnostných aktivít a zvyšovaní sebadôvery v ich schopnosť pohybovať sa v digitálnom prostredí bezpečne a samostatne.

9.2 Metodologické princípy

Zistenia výskumu jasne poukazujú na súbor metodologických princípov, ktoré by mali usmerňovať návrh kurikula:

1. Neformálne a zážitkové učenie: kurikulum musí byť založené na scenároch z reálneho života, prípadových štúdiách a praktických cvičeniach, a nie na teoretickej výučbe. Dospelí vo veku 45+ najlepšie reagujú na učenie, ktoré je okamžite použiteľné v ich každodennej digitálnej skúsenosti.
2. Nácvik založený na scenároch: osobitná pozornosť by sa mala venovať simulovaným scenárom, v ktorých si študujúci môžu bezpečne precvičiť rozpoznávanie pokusov o podvod a reagovanie na ne (phishingové e-maily, podozrivé hovory, správy generované umelou inteligenciou) bez rizika v reálnom svete.
3. Prístupný jazyk a formát: technické kyberbezpečnostné koncepty musia byť pretavené do jasného jazyka bez žargónu. Vizuálne materiály, návody krok za krokom a multimediálny obsah by sa mali používať na podporu študujúcich na rôznych úrovniach gramotnosti.
4. Odstupňovaná zložitosť: kurikulum by malo byť štruktúrované tak, aby budovalo sebadôveru postupne, počnúc okamžite rozpoznateľnými rizikami a postupujúc k zložitejším a novovznikajúcim hrozbám. Tento odstupňovaný prístup zabraňuje preťaženiu študujúcich a znižuje digitálne vyhýbavé správanie.
5. Destigmatizácia viktimizácie: vzhľadom na zdokumentovanú neochotu formálne nahlasovať podvodné incidenty by sa kurikulum malo výslovne zaoberať psychologickými aspektmi viktimizácie kybernetickou kriminalitou, normalizovať túto skúsenosť a posilniť študujúcich, aby vyhľadali inštitucionálnu podporu bez hanby.
6. Adaptabilita na národné a miestne kontexty: hoci by mal byť rámec kurikula nadnárodný, moduly by mali umožňovať prispôsobenie tak, aby odrážali konkrétne typológie podvodov, právne rámce a kanály nahlasovania relevantné v každej partnerskej krajine.

10. Záver

Nadnárodná správa projektu digiSAFE syntetizuje zistenia národného výskumu vykonaného v Taliansku, Španielsku a na Slovensku a poskytuje komplexný, na dôkazoch založený obraz výziev digitálnej bezpečnosti a vzdelávacích potrieb dospelých vo veku 45+ naprieč tromi európskymi krajinami.

Dôkazy sú jasné a konzistentné: hoci sú dospelí v cieľovej skupine čoraz aktívnejší v digitálnom prostredí – používajú internet na bankovníctvo, komunikáciu, verejné služby a informácie – nie sú adekvátne vybavení na zvládanie online rizík, ktoré tieto aktivity prinášajú. Medzera medzi digitálnym zapojením a kompetenciou v oblasti digitálnej bezpečnosti je štrukturálnou črtou všetkých troch národných kontextov, nie individuálnym zlyhaním. Odráža tempo digitálnej transformácie, nedostatočnosť existujúcej vzdelávacej ponuky zameranej na túto vekovú skupinu a rýchlo sa vyvíjajúcu povahu hrozieb – najvýraznejšie vznik podvodov poháňaných umelou inteligenciou, ktoré predbiehajú existujúce povedomie a obranné stratégie.

Výskum identifikoval konkrétne, realizovateľné medzery: v zručnostiach (technické overovanie, bezpečnosť zariadení, rozpoznávanie obsahu umelej inteligencie), v znalostiach (mechanizmy podvodov, práva na ochranu údajov, postupy nahlasovania) a v povedomí (novovznikajúce hrozby umelej inteligencie, inštitucionálne kanály podpory). Tieto medzery sú priamym vstupom pre kurikulum NFE a sadu nástrojov na prevenciu digitálnych podvodov projektu digiSAFE, ktoré budú vyvinuté v ďalšej fáze projektu.

Osvedčené postupy identifikované naprieč všetkými tromi krajinami ukazujú, že účinné, prístupné a komunitné vzdelávacie intervencie pre demografickú skupinu 45+ sú úplne realizovateľné. Iniciatívy siahajúce od talianskej siete digitálnej facilitácie cez slovenské semináre rovesníckeho učenia až po španielske programy digitálneho mentorstva vedené dobrovoľníkmi ukazujú, čo funguje, a poskytujú replikovateľné modely pre vzdelávacie výstupy projektu digiSAFE.

Tým, že priamo stavia na zisteniach národného výskumu prezentovaného v tejto správe, projekt digiSAFE vytvára jasné prepojenie medzi dôkazmi a konaním. Identifikované medzery, potreby a vzorce správania budú priamo informovať návrh a štruktúru kurikula neformálneho vzdelávania a sady nástrojov na prevenciu digitálnych podvodov, čím sa zabezpečí, že oba výstupy budú založené na skutočných potrebách používateľov. Týmto spôsobom je projekt pripravený poskytnúť zmysluplný a merateľný príspevok k digitálnej odolnosti starších dospelých v Taliansku, Španielsku, na Slovensku a aj mimo nich, podporujúc bezpečnejšiu, informovanejšiu a samostatnejšiu účasť v európskej digitálnej spoločnosti.

Bibliografia / Zdroje

1. Agentúra pre digitálne Taliansko (AgID) (b.d.). Iniciatívy v oblasti digitálnych zručností. <https://www.agid.gov.it/it/agenzia/competenze-digitali>
2. Talianska národná banka (b.d.). Finančné vzdelávanie a povedomie o kybernetickej bezpečnosti. <https://economieapertutti.bancaditalia.it>
3. CERTFin (b.d.). Kampaň I Navigati. <https://inavigati.certfin.it/index.html>
4. Občianske združenie eSlovensko (b.d.). Zodpovedne.sk. <https://www.zodpovedne.sk/>
5. Oddelenie pre digitálnu transformáciu, Taliansko (b.d.). Stratégia Repubblica Digitale. <https://repubblicadigitale.gov.it/portale/strategia>
6. Digitálna koalícia (b.d.). Zlepšovanie digitálnych zručností seniorov. <https://digitalnakoalicia.sk>
7. Platforma digitálnych zručností a pracovných miest – Európska komisia (2024). Španielsko: Prehľad digitálnych zručností. <https://digital-skills-jobs.europa.eu/en/latest/briefs/spain-snapshot-digital-skills>
8. Platforma digitálnych zručností a pracovných miest – Európska komisia (2024). Slovensko: Prehľad digitálnych zručností. <https://digital-skills-jobs.europa.eu/en/latest/briefs/slovakia-snapshot-digital-skills>
9. ESET (b.d.). Bezpečne na nete. <https://bezpecnenanete.eset.com/sk/>
10. EU DisinfoLab (2023). Prostredie dezinformácií na Slovensku. <https://www.disinfo.eu>
11. Európska komisia (2024). Správa o digitálnom desaťročí pre Slovensko 2025. <https://digital-strategy.ec.europa.eu/en/factpages/slovakia-2025-digital-decade-country-report>
12. Európska komisia (2025). Správa o digitálnom desaťročí pre Taliansko 2025. <https://digital-strategy.ec.europa.eu/en/factpages/italy-2025-digital-decade-country-report>
13. Európska komisia – Spoločné výskumné centrum (2025). Ako dosiahnuť cieľ EÚ 80 % dospelých so základnými digitálnymi zručnosťami do roku 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. Európsky parlament a Rada EÚ (2016). Nariadenie (EÚ) 2016/679 – Všeobecné nariadenie o ochrane údajov (GDPR). Ú. v. EÚ L 119, 4.5.2016.
15. Európsky parlament a Rada EÚ (2022). Smernica (EÚ) 2022/2555 – Smernica NIS2.

16. Eurostat (2024). Digitalizácia v Európe – vydanie 2024.
<https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2024>
17. Fundación Cibervoluntarios (b.d.). Programy digitálnej inklúzie.
<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 (b.d.). Línea de Ayuda en Ciberseguridad 017. <https://www.incibe.es/linea-017>
23. ISTAT (2024). Správa o občanoch a IKT.
https://www.istat.it/wp-content/uploads/2025/04/REPORT_CITTADINI-E-ICT_2024.pdf
24. ISTAT (2024). Štatistiky digitálnych zručností.
<https://www.istat.it/wp-content/uploads/2024/04/2.pdf>
25. ISTAT (2025). Správa o trestných činoch proti osobám a majetku. Taliansky národný štatistický inštitút.
26. Taliansky úrad na ochranu údajov – Garante (b.d.). Kódex ochrany osobných údajov. <https://www.garanteprivacy.it>
27. Krajská knižnica Žilina (b.d.). Akadémie Smart Senior.
<https://www.krajskakniznicazilina.sk/>
28. Ministerio de Educación y Formación Profesional, Španielsko (b.d.). Aula Mentor.
<https://www.aulamentor.es>
29. Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky – MIRRI (b.d.). Program Digitálni seniori. <https://www.digitalniseniori.gov.sk>
30. Ministerstvo práce a sociálnych politík, Taliansko (b.d.). Program GOL.
<https://www.lavoro.gov.it/temi-e-priorita/occupazione/focus/pagine/programma-gol>
31. Národná agentúra pre kybernetickú bezpečnosť – ACN, Taliansko (b.d.). Národná stratégia kybernetickej bezpečnosti 2022–2026.
<https://www.acn.gov.it/portale/strategia-nazionale-di-cybersicurezza>
32. Národný bezpečnostný úrad – NBÚ, Slovenská republika (2021). Národná stratégia kybernetickej bezpečnosti 2021–2025. <https://www.nbu.gov.sk/national-cybersecurity-strategy-of-the-slovak-republic-for-years-2021-2025/>

33. OECD (2024). Posilňovanie digitálnych zručností seniorov v Slovenskej republike.
<https://www.oecd.org/en/about/programmes/dg-reform/enhancing-the-digital-skills-of-seniors-in-the-slovak-republic.html>
34. Policía Nacional, Španielsko (b.d.). Plan Mayor Seguridad.
https://www.policia.es/_es/colabora_plan_mayor_seguridad.php
35. Polizia Postale, Taliansko (b.d.). Výročné správy a údaje o kybernetickej bezpečnosti. <https://www.commissariatodips.it>
36. Repubblica Digitale (2025). Quarto rapporto di monitoraggio – Ottobre 2025. Oddelenie pre digitálnu transformáciu, Taliansko.
37. Projekt SafeHorizon (2026). Situácia Španielska v oblasti kybernetického priestoru.
<https://www.project-safehorizon.eu>
38. Slovenská republika (2018). Zákon č. 18/2018 Z. z. o ochrane osobných údajov. Národná rada Slovenskej republiky.
39. Slovenská republika (2018). Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti.
<https://www.sk-cert.sk>
40. Slovenská republika (2024). Zákon č. 366/2024 Z. z. – Transpozícia smernice NIS2. Národná rada Slovenskej republiky.
41. Nadačný fond Telekom (b.d.). Zrelí na dobu digitálnu.
<https://nadcnyfondtelekom.sk/>
42. Jednota dôchodcov na Slovensku – JDS (b.d.). <https://www.jednotadochodcov.sk/>