SILWERS

SENIORS ARTIFICIAL INTELLIGENCE LEARNING – WELL EDUCATED AND RISK SECURE

Co-funded by the European Union

Expert fora report

Erasmus+ KA220-ADU – Cooperation partnerships in adult education, Project No: ***2024-1-IS01-KA220-ADU-000256952***

Co-funded by the
European Union

Cíle panelu expertů

1. Diskuse o obtížích a obavách, kterým skupina senioru čelí v souvislosti s novými technologiemi, spolu s identifikací oblastí použití umělé inteligence a souvisejících rizik.
2. Identifikace současných a budoucích online hrozeb pro osoby starší 55 let.
3. Prezentace reálných příkladů incidentů a naopak výhod plynoucích z používání umělé inteligence.
4. Definice kritických digitálních kompetencí pro osoby starší 55 let.

Co-funded by the European Union

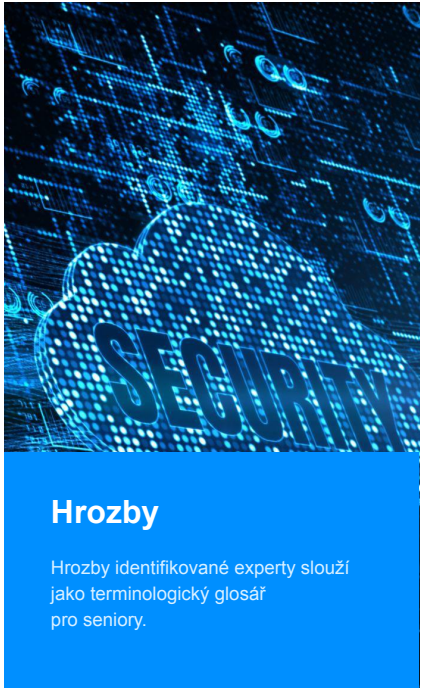
Výsledky - Polsko

Co-funded by the
European Union

Nejčastěji uváděné online hrozby pro osoby starší 55 let

Lidé ve věku 55 let a starší čelí v digitálním světě unikátním výzvám, které je činí zranitelnými vůči řadě online hrozeb.

Pochopení nejběžnějších a nejzávažnějších nebezpečí je nezbytné pro lepší povědomí o kybernetické bezpečnosti a ochraně.



Co-funded by the
European Union

Online hrozby pro osoby starší 55 let

- Phishing podvodných e-mailů, SMS, odkazů, hlasových hovorů
- Deepfake útoky pomocí falešného audio/video záznamu, vydávání se za člena rodiny
- Falešné internetové obchody a podvodné webové stránky
- Emoční manipulace a taktiky zastrašování využívající sociální inženýrství
- Krádež identity s využitím odcizených osobních údajů

Co-funded by the
European Union

Online hrozby pro osoby starší 55 let

- Zneužití vydávání se za vnouče, které je v nouzi.
- Falešné žádosti o pomoc přes WhatsApp nebo Messenger
- Romantické podvody a podvody založené na vztazích budovaných online
- Investiční podvody, falešné reklamy využívající obličej celebrit
- Soubory a přílohy infikované malwarem a ransomwarem

Co-funded by the
European Union

Online hrozby pro osoby starší 55 let

- Neověřené aplikace a stahování nebezpečného softwaru
- Sdílení citlivých dat, fotografií a informací s cizími lidmi
- Používání zastaralých zařízení nebo softwaru
- Masové personalizované útoky s využitím umělé inteligence, zaměřené na uživatelské profily
- Dezinformace o zdraví nebo nebezpečné lékařské rady z nástrojů umělé inteligence

Co-funded by the
European Union

Online hrozby pro osoby starší 55 let

- Podvody zneužívající digitální vyloučení v občanských a bankovních službách
- Nedostatek vícefaktorového ověřování, zjednodušená hesla a jejich opakované použití
- Ztráta přístupu ke kritickým službám v důsledku technologických změn, kdy je přístup pouze přes aplikaci, omezené alternativy
- Automatizovaná manipulace s feedy sociálních médií, produkující dezinformace a stres
- Heslo, identifikace, biometrie, 2FA

Co-funded by the
European Union

10 největších obav podle odborníků

Experty zdůrazněné klíčové obavy, které nejvíce postihují lidi ve věku 55 let a starší při interakci s digitálními technologiemi.

Řešení těchto obav je klíčové pro posílení jejich sebevědomí a bezpečnosti při každodenních online aktivitách.

Motivace

Rozvoj cílených podpůrných a vzdělávacích programů.

Co-funded by the
European Union

10 největších obav podle odborníků

- **Technologické změny** a jejich složitost: Rychlé tempo vývoje technologií ztěžuje seniorům adaptaci, zejména s ohledem na aktualizace a nová zařízení.
- Strach a **emoční manipulace:** Podvody často zneužívají emoce, jako je strach nebo naléhavost, čímž seniory činí zranitelnějšími.
- **Sociální vyloučení** a osamělost: Omezený kontakt s rodinou a přáteli, často zhoršený nahrazováním přímých interakcí digitální komunikací.
- **Váhání požádat o pomoc:** Senioři se často stydí, když žádají mladší lidi o pomoc s technologiemi.
- **Finanční omezení:** Neochota nebo neschopnost utratit peníze za nová zařízení nebo software, což má za následek zastaralou a nezabezpečenou technologii.

Co-funded by the
European Union

10 největších obav podle odborníků

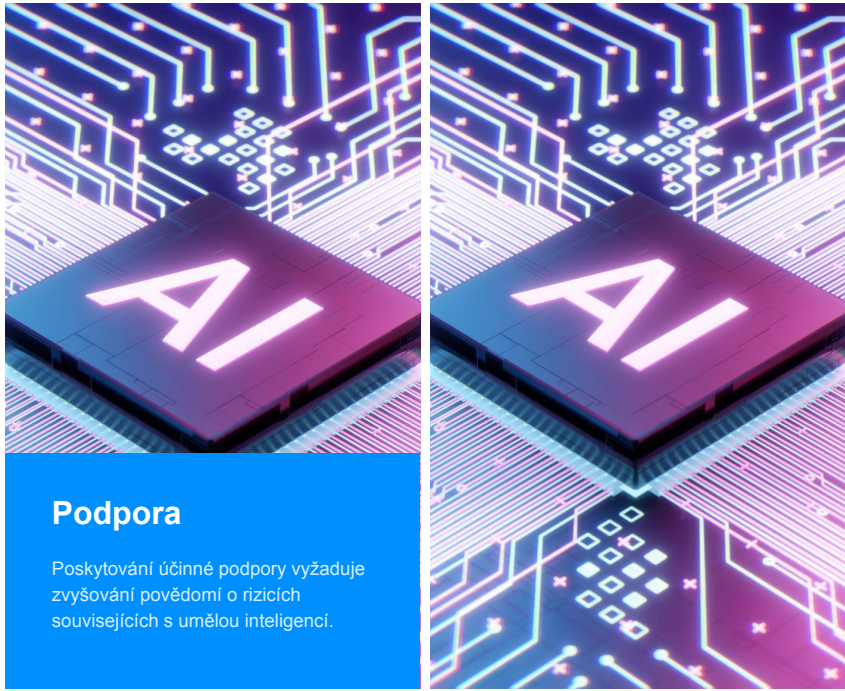
- **Digitální vyloučení** ve službách: Každodenní úkony (jako je nákup jízdenek, bankovnictví, lékařské schůzky) se stále častěji přesouvají do online prostředí, seniorům nezbývají alternativy.
- Nízké **digitální kompetence:** Nedostatek základních dovedností a zkušeností, někdy zhoršený nedostatkem počítačového vzdělání v raném věku.
- Impulzivnost a **riskantní rozhodnutí:** Tendence jednat rychle, když se setkáte s technologickými problémy – někdy to vede k chybám nebo náchylnosti k podvodům.
- **Důvěřivost** k dezinformacím: Problém s rozlišením pravdivých informací od digitální manipulace, zejména online.
- Zařízení a **problémy s údržbou softwaru:** Problémy s aktualizací zařízení, správou hesel a nízkým porozuměním osvědčeným postupům digitální bezpečnosti zvyšují riziko.

Co-funded by the European Union

Klíčové oblasti využití umělé inteligence a kybernetická rizika

Umělá inteligence se stále více integruje do mnoha aspektů každodenního života a nabízí významné výhody, ale také přináší nová kybernetická bezpečnostní rizika.

Pochopení hlavních oblastí použití umělé inteligence a s nimi spojených hrozeb je nezbytné pro ochranu zranitelných skupin, jako jsou osoby ve věku 55 let a starší.



Co-funded by the
European Union

Klíčové oblasti využití umělé inteligence a kybernetická rizika

- **Osobní asistenti** v telefonech a zařízeních (např. hlasových asistentech jako Alexa), které podporují seniory v každodenních úkonech, ale vyžadují pochopení ochrany soukromí a zabezpečení.
- Umělá inteligence v **monitorování zdravotní péče** (nositelná elektronika, detekce anomálií v srdeční frekvenci), která poskytuje včasná varování, ale k ovládání vyžaduje důvěru a základní digitální dovednosti.
- AI schopnosti při odhalování**odhalování podvodů**(identifikace phishingu, rozpoznávání deepfake) na ochranu seniorů před cílenými útoky, ale vyžadující znalost rozpoznávání podezřelého obsahu.
- AI generované **personalizované útoky,** které se přizpůsobují chování a emocím jednotlivých seniorů, což ztěžuje odhalování online hrozeb.
- **Generování obsahu** a dezinformací prostřednictvím umělé inteligence (deepfakes, falešné reklamy, falešné zprávy), které ovlivňují rozhodnutí a způsobují zmatek mezi seniory, kteří postrádají dovednosti kritického hodnocení.

Co-funded by the
European Union

Klíčové oblasti využití umělé inteligence a kybernetická rizika

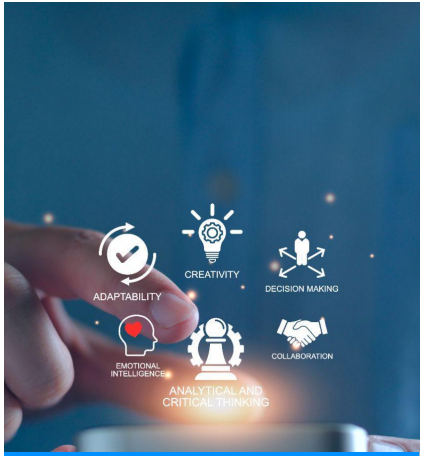
- Umělá inteligence v **chytré domácnosti a** zařízení IoT, která pomáhají v každodenním životě, ale představují rizika, pokud nejsou zabezpečená nebo špatně spravovaná.
- Cestování s podporou umělé inteligence a **plánování volného času** pomáhá s organizací výletů a aktivit, zvyšuje pohodlí, ale vyžaduje určitou digitální gramotnost pro bezpečné používání.
- Automatizované **sociální interakce:** boti simulující lidskou konverzaci, často používané v podvodech nebo ke snížení izolace, vyžadující povědomí, aby se zabránilo podvodu.
- Umělá inteligence v digitálním světě **finančních služeb** a automatizace transakcí a bankovnictví, která může zlepšit dostupnost, ale vyžaduje znalost bezpečnostních postupů a prevence podvodů.
- Nástroje umělé inteligence v komunikaci s rodinou a pečovateli (monitorování v reálném čase, systémy nouzového varování) zvyšující bezpečnost, ale vyžadující kompetenci v nastavení a interpretaci.

Co-funded by the
European Union

Klíčové kompetence pro seniory

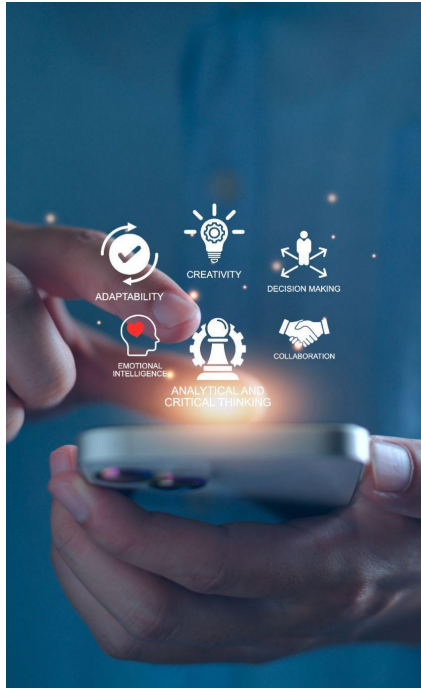
Rozvoj základních digitálních kompetencí je zásadní pro to, aby se senioři mohli bezpečně a sebejistě orientovat v online světě.

Tyto dovednosti jim pomáhají efektivně využívat technologie ke zlepšení jejich každodenního života a zvyšují odolnosti vůči kybernetickým hrozbám.



Kompetence

Umožnit seniorům lépe se chránit a sebevědomě využívat moderní technologie.



Co-funded by the
European Union

Klíčové kompetence pro seniory

- **Porozumění z**ákladům ovládání digitálních zařízení a nastavení zabezpečení.
- **Rozpoznání** manipulace založené na umělé inteligenci a podvodném obsahu.
- **Digitální gramotnost v oblasti** bezpečné komunikace s asistenty s umělou inteligencí a chytrými zařízeními.
- **Povědomí o** opatřeních na ochranu soukromí a ochrany dat v aplikacích umělé inteligence.
- **Schopnost** vyhledávat důvěryhodné informace a ověřovat obsah generovaný umělou inteligencí.

Co-funded by the
European Union

Klíčové kompetence pro seniory

- Emocionální **odolnost,** aby se vyhnuli manipulaci nebo podvodům řízeným umělou inteligencí.
- **Pohodlí** při řešení základních problémů a údržbou digitálních nástrojů.
- **Znalost** bezpečných postupů správy hesel a ověřování.
- Kompetence k **použití n**ástrojů umělé inteligence pro zdraví, bezpečnost a komunikaci.
- **Otevřenost** k neustálému učení kvůli rychlému rozvoji technologií umělé inteligence.

Co-funded by the European Union

Hrozby z reálného života identifikované experty

Odborníci sdíleli příklady z reálného života, které ilustrují rizika i přínosy digitálních technologií pro lidi ve věku 55 let a starší.
Tyto případy poskytují cenné poznatky o běžných kybernetických hrozbách umělé inteligence v každodenním životě seniorů.

Hrozby

Příklady z reálného života zdůrazňují důležitost rozpoznávání a zmírňování kybernetických hrozeb.

Co-funded by the
European Union

Hrozby z reálného života identifikované experty

- Použití **deepfake t**echnologie pro vydávání se za člena rodiny: Senior přijme telefonní hovor, ve kterém volající přesvědčivě simulovaným hlasem vnoučete nebo dítěte tvrdí, že potřebuje okamžitě peníze (např. na nehodu). Senior, přesvědčen emocionální manipulací a známostí hlasu, převede peníze, často pomocí karty nebo bankovního převodu.
- Romantické **podvody** zahrnující umělou inteligenci: Senioři jsou online cílem jednotlivců (někdy chatbotů nebo automatizovaných profilů), kteří navazují emocionální „vztahy“ a poté pod falešnými záminkami žádají o peníze, zneužívajíc osamělost a důvěru.
- Falešné **loterie**nebo výhry: Senior je informován, často telefonicky nebo e-mailem, s použitím obsahu generovaného umělou inteligencí, že vyhrál velkou částku peněz. Aby si ji mohl nárokovat, je požádán o zálohu nebo osobní údaje, což má za následek finanční ztrátu a někdy i krádež identity.

Co-funded by the
European Union

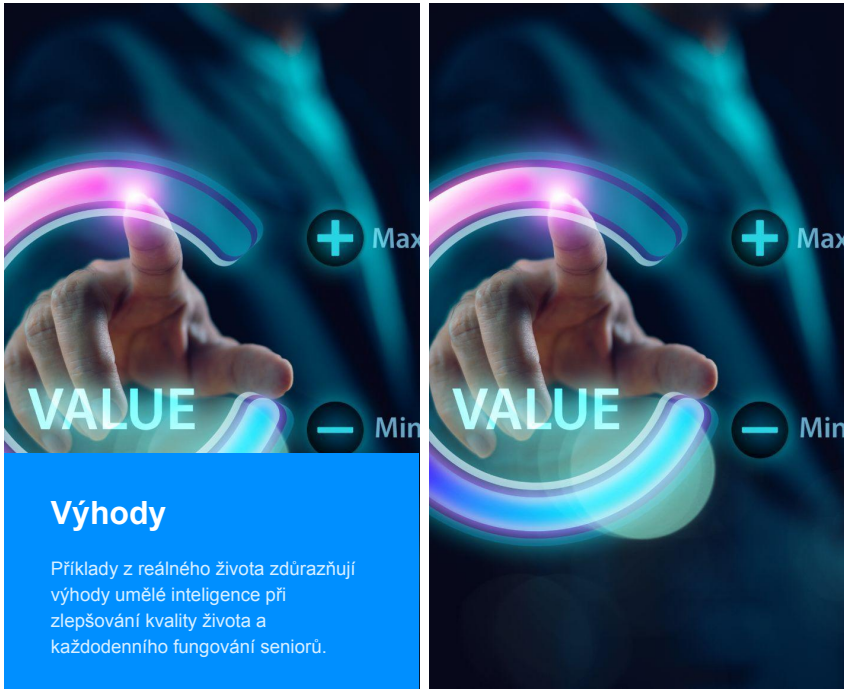
Hrozby z reálného života identifikované experty

- **Manipulace** prostřednictvím falešných internetových obchodů: Senioři nevědomky nakupují zboží z webových stránek, které jsou téměř identické s legitimními obchody (s drobnou změnou pravopisu v adrese nebo názvu). Platí za zboží, které nikdy nedorazí, a stávají se tak obětí sofistikovaných phishingových stránek založených na umělé inteligenci.
- Lékařství s využitím umělé inteligence **dezinformace** Senioři se obracejí na chatboty s umělou inteligencí nebo online nástroje, aby získali rady ohledně zdraví. Někdy jsou rady zavádějící, což vede k tomu, že se vyhnou konzultaci s lékařem nebo dokonce užívají nesprávné léky, což může být pro jejich zdraví nebezpečné.

Co-funded by the
European Union

Výhody v reálném životě identifikované odborníky

Odborníci sdíleli příklady z reálného života, které ilustrují rizika i přínosy digitálních technologií pro lidi ve věku 55 let a starší.
Tyto případy poskytují cenné poznatky o výhodách vlivu umělé inteligence na každodenní život seniorů.



Co-funded by the
European Union

Výhody v reálném životě identifikované odborníky

- Seniory využívaný nástroj umělé inteligence k plánování výletů, s upřesněním dat a osobních preferencí (jako jsou muzea nebo outdoorové aktivity) a následné obdržení podrobného, na míru šitého itineráře – což výlet usnadní a zpříjemní.
- Nástroje umělé inteligence v lékařství, které jsou využívány k včasné diagnostice zdravotních problémů (jako jsou nepravidelné srdeční rytmy u pacientů s kardiostimulátorem a diabetem), což vede k včasnému lékařskému zásahu a zlepšení celkové pohody.
- Seniory využívaní asitenti umělé inteligence (jako Alexa) pro denní připomenutí (např. časy užívání léků a schůzky), správu domácnosti a udržování sociálního kontaktu, snižování osamělosti a zvyšování nezávislosti.

Co-funded by the
European Union

Výhody v reálném životě identifikované odborníky

- Příklad zahrnoval chytré **nositelné** zařízení (náramky s umělou inteligencí), které nepřetržitě monitorovalo klíčové zdravotní ukazatele seniorů žijících osaměle a v případě anomálií nebo nouzových situací automaticky upozorňovalo pečovatele nebo záchranné složky.
- Rozpoznávání obrázků pomocí umělé inteligence. Vyhledávání pomohlo seniorovi identifikovat neznámou rostlinu v jeho zahradě, poskytlo mu okamžité rady ohledně péče o ni, a tím zlepšilo jeho zahradnické dovednosti a sebevědomí.

Co-funded by the
European Union

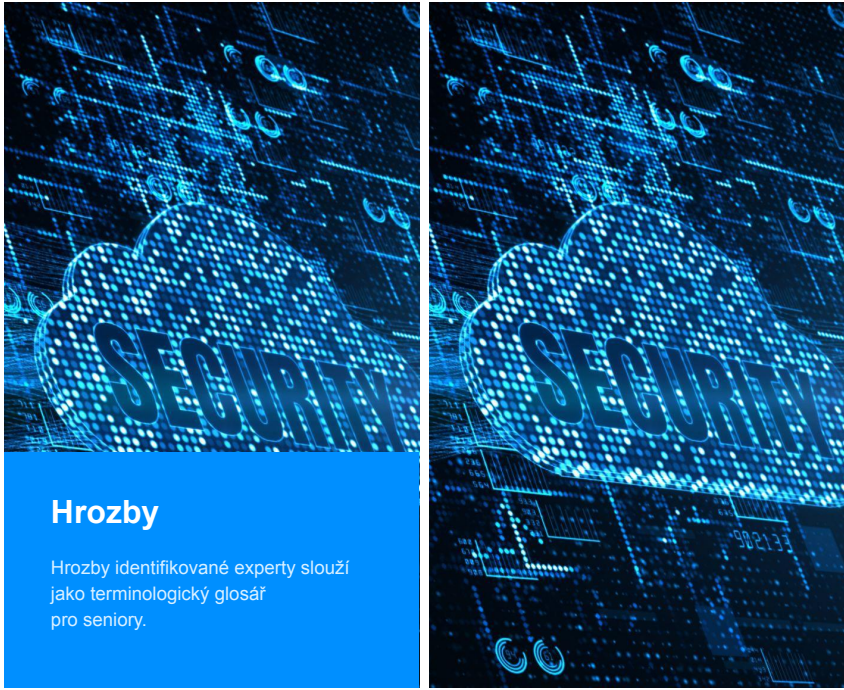
Výsledky - Česká republika

Co-funded by the
European Union

Nejčastěji citované online hrozby pro osoby starší 55 let

Lidé ve věku 55 let a starší čelí v digitálním světě jedinečným výzvám, které je činí zranitelnými vůči řadě online hrozeb.

Pochopení nejběžnějších a nejzávažnějších nebezpečí je nezbytné pro zlepšení jejich povědomí o kybernetické bezpečnosti a ochrany.



Co-funded by the
European Union

Online hrozby pro osoby starší 55 let

- Phishingové útoky, včetně e-mailů, SMS a telefonních hovorů, kdy se útočníci vydávají za banky nebo důvěryhodné instituce, aby ukradli citlivá data.
- Falešné internetové obchody a podvody zaměřené na seniory, s podvodnými nabídkami a webovými stránkami.
- Krádež identity, kdy jsou osobní údaje zneužity k získání peněz nebo k vydávání se za oběť.
- Manipulace prostřednictvím krátkých videí a dezinformací, včetně vymyšlených zpráv a podprahových sdělení.

Co-funded by the
European Union

Online hrozby pro osoby starší 55 let

- Nedostatečná údržba IT, jako je zastaralý firmware a ignorované bezpečnostní aktualizace, což má za následek zranitelnost systémů.
- Podvod zneužívající osamělost – podvodníci navazující falešná přátelství nebo romantické vztahy.
- Nebezpečná synchronizace mezi zařízeními a nezabezpečené ukládání hesel v prohlížečích.
- Rostoucí hrozba podvodů založených na umělé inteligenci, včetně klonovaných hlasů vydávajících se za příbuzné a žádajících o naléhavou finanční pomoc.
- Rostoucí rizika v důsledku umělé inteligence v antivirových programech, která činí konfiguraci a bezpečné používání pro seniory klíčovými.

Co-funded by the
European Union

10 největších obav podle odborníků

Odborníci zdůraznili klíčové obavy, které nejvíce postihují lidi ve věku 55 let a starší při interakci s digitálními technologiemi.

Řešení těchto obav je klíčové pro posílení jejich sebevědomí a bezpečnosti při každodenních online aktivitách.

Motivace

Rozvoj cílených podpůrných a vzdělávacích programů.

Co-funded by the
European Union

10 největších obav podle odborníků

- **Obtížnost udržet krok** se složitostí a rychlým vývojem technologií.
- **Strach ze ztráty přístupu** k osobním údajům nebo financím a z toho, že se stanu obětí podvodů.
- **Rozpaky** nebo ztráta sebevědomí, kdy se obávají používat technologie před rodinou.
- **Závislost** na ostatních (příbuzných nebo odbornících), což brání budování samostatnosti.
- Bezpečnost veřejných Wi-Fi sítí, které často používají senioři bez **bezpečnostního povědomí.**

Co-funded by the
European Union

10 největších obav podle odborníků

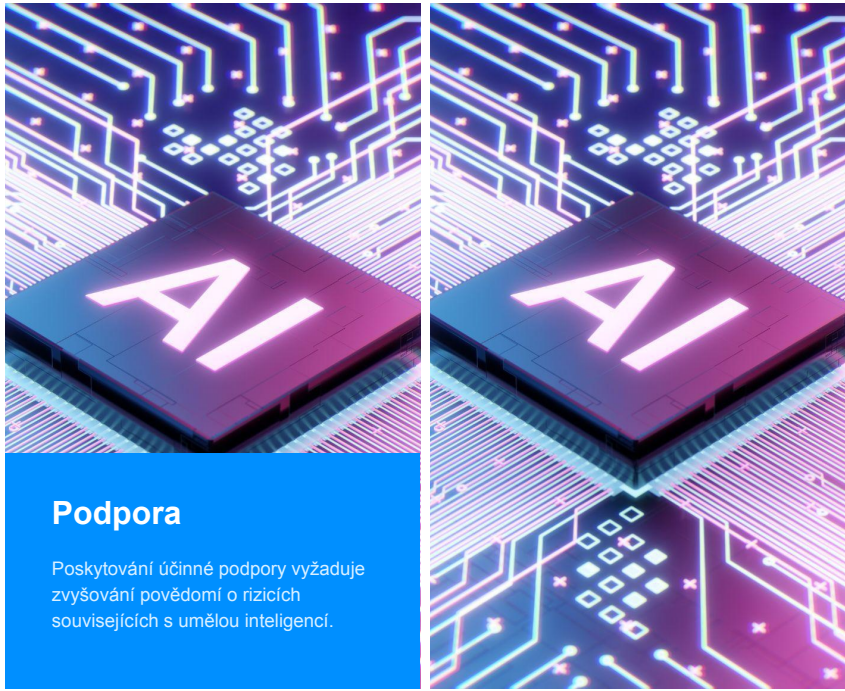
- **Nebezpečné uchovávání hesel**, například používání prohlížečů místo správců hesel.
- **Digitální komunikace** nahrazuje cenný osobní kontakt, což vede k sociální izolaci.
- Zakázání aktualizací nebo bezpečnostních funkcí z důvodu **nedostatečného porozumění**, čímž je zařízení zranitelnější.
- **Boj s měnícím se systémem r**ozvržení plochy, ikony nebo neočekávané nové funkce.
- Neschopnost rozpoznat **podezřelý nebo manipulovaný obsah**, což činí seniory náchylnějšími k podvodům.

Co-funded by the European Union

Klíčové oblasti využití umělé inteligence a kybernetická rizika

Umělá inteligence se stále více integruje do mnoha aspektů každodenního života a nabízí významné výhody, ale také přináší nová kybernetická bezpečnostní rizika.

Pochopení hlavních oblastí použití umělé inteligence a s nimi spojených hrozeb je nezbytné pro ochranu zranitelných skupin, jako jsou osoby ve věku 55 let a starší.



Co-funded by the
European Union

Klíčové oblasti využití umělé inteligence a kybernetická rizika

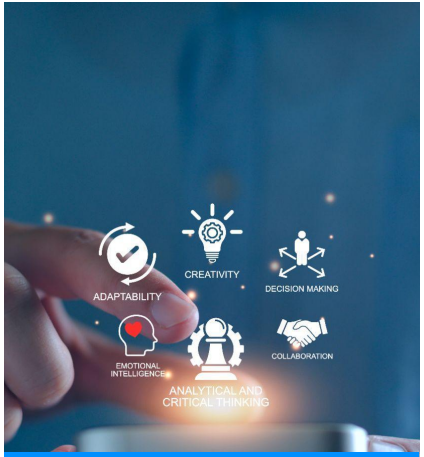
- **Umělá inteligence ve zdravotnictví:** telemedicína, monitorování zdravotního stavu a tlumočení pro komunikaci s rodinou.
- **Denní podpora:** Hlasoví asistenti s umělou inteligencí, zařízení pro chytrou domácnost, antivirové nástroje.
- Riziko **manipulace s daty**, deepfake útoky a šíření dezinformací.
- **Klonování hlasu s** podporou umělé inteligence, vydávání se za příbuzné, což vede k finančním podvodům.
- **Přílišná závislost na nástrojích umělé inteligence** bez pochopení jejich omezení – umělá inteligence by měla být vnímána jako nástroj, nikoli jako neomylná autorita.

Co-funded by the
European Union

Klíčové kompetence pro seniory

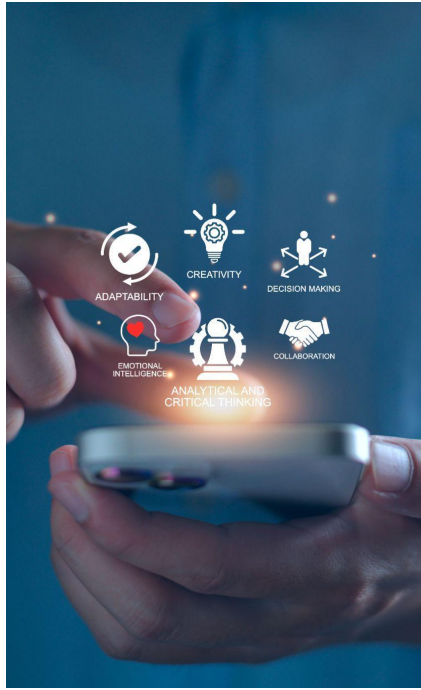
Rozvoj základních digitálních kompetencí je zásadní pro to, aby se senioři mohli bezpečně a sebejistě orientovat v online světě.

Tyto dovednosti jim pomáhají efektivně využívat technologie ke zlepšení jejich každodenního života a odolnosti vůči kybernetickým hrozbám.



Kompetence

Umožnit seniorům lépe se chránit a sebevědomě využívat moderní technologie.



Co-funded by the
European Union

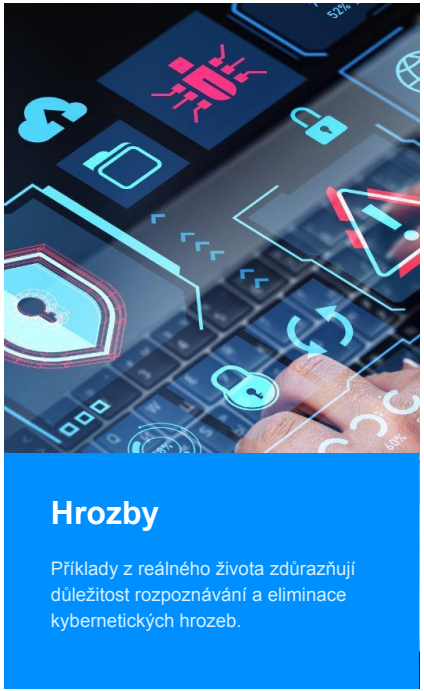
Klíčové kompetence pro seniory

- Stanovení silných a jedinečných hesel a **řízení bezpečnosti** (vyhněte se úložišti v prohlížeči, použijte správce hesel).
- Povolení **dvoufaktorového ověřování** pro zabezpečení účtů.
- Porozumění a **konfigurace antivirových programů**, zejména nástroje založené na umělé inteligenci.
- **Rozpoznání** podezřelého, manipulovaného nebo **podvodného online obsahu**.
- **Používání asistentů s umělou inteligencí** prakticky, ale zůstávat kritický k výsledkům.
- Základní **digitální gramotnost**: aktualizace zařízení, bezpečné prohlížení, bezpečné používání Wi-Fi.
- **Budování sebevědomí:** snížit závislost na ostatních a podpořit průběžné digitální vzdělávání.

Co-funded by the European Union

Hrozby z reálného života identifikované experty

Odborníci sdíleli příklady z reálného života, které ilustrují rizika i přínosy digitálních technologií pro osoby ve věku 55 let a starší.
Tyto případy poskytují cenné poznatky o běžných kybernetických hrozbách spojených s umělou inteligencí v každodenním životě seniorů.



Co-funded by the
European Union

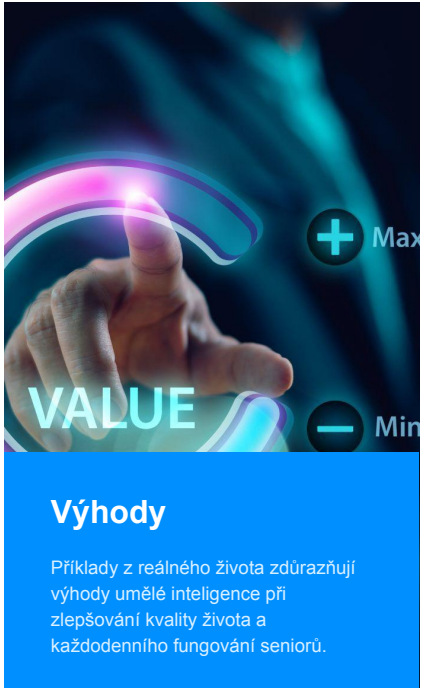
Hrozby z reálného života identifikované experty

- Příklad: Starší žena byla podvedena, když volající použil technologii deepfake k naklonování hlasu jejího vnuka a naléhavě požadoval hotovost, kterou doručila kurýrovi.
- Podvody v oblasti romantiky nebo přátelství zneužívají emocionální vazby, často prostřednictvím zpráv nebo hovorů.
- Dezinformace šířící se prostřednictvím videí nebo krátkých zpráv, což seniorům ztěžuje ověření jejich pravosti.
- Špatná údržba IT nebo používání nezabezpečených sítí vedoucí ke skutečným narušením bezpečnosti.

Co-funded by the
European Union

Výhody v reálném životě identifikované odborníky

Odborníci sdíleli příklady z reálného života, které ilustrují rizika i přínosy digitálních technologií pro osoby ve věku 55 let a starší.
Tyto případy poskytují cenné poznatky o výhodách umělé inteligence na každodenní život seniorů.



Co-funded by the
European Union

Výhody v reálném životě identifikované odborníky

- Dvaasedmdesátiletá žena použila k překladu hlasového asistenta s umělou inteligencí, který jí umožnil zapojit se do rodinných videohovorů, rozumět jim a cítit se součástí mezinárodních konverzací.
- Senioři používají umělou inteligenci k plánování (např. tipy pro Windows, DYI – udělej si sám) nebo chatboti v centrech péče o Alzheimerovu chorobu.
- Umělá inteligence nabízí personalizované poradenství a podporuje každodenní samostatnost, ale funguje nejlépe v kombinaci se silnými základními dovednostmi.

Co-funded by the
European Union

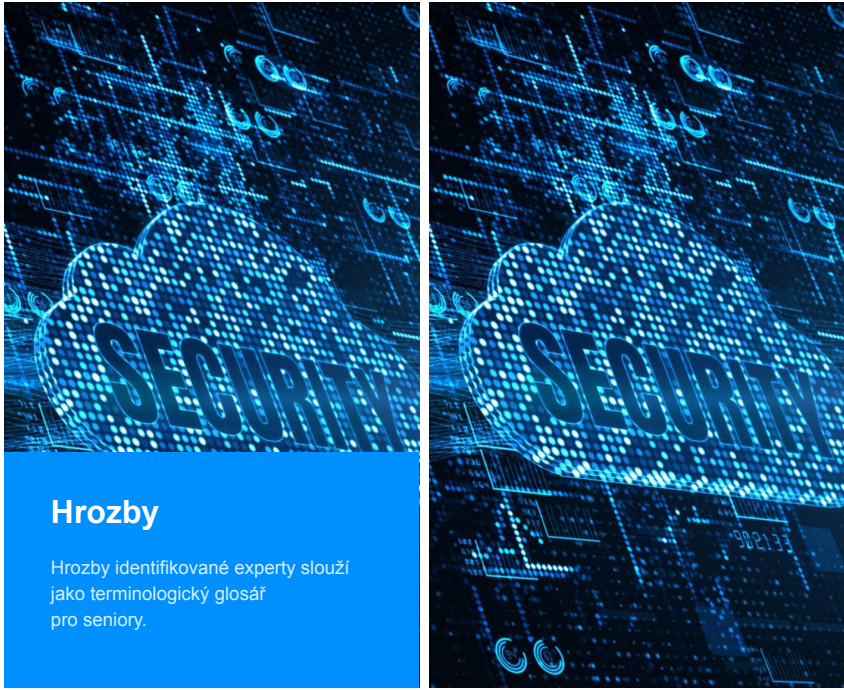
Výsledky - Island

Co-funded by the
European Union

Nejčastěji citované online hrozby pro osoby starší 55 let

Lidé ve věku 55 let a starší čelí v digitálním světě jedinečným výzvám, které je činí zranitelnými vůči řadě online hrozeb.

Pochopení nejběžnějších a nejzávažnějších nebezpečí je nezbytné pro zlepšení jejich povědomí o kybernetické bezpečnosti a ochrany.



Co-funded by the
European Union

Online hrozby pro osoby starší 55 let

- **Podvody s deepfake**s falešnými obrázky a videi, zejména na WhatsAppu, kde se zločinci vydávají za členy rodiny a stěžují si na naléhavou potřebu peněz.
- Sofistikovaný **phishing** využívající sociální inženýrství, prostřednictvím aplikací pro zasílání zpráv s přesvědčivými falešnými telefonními hovory a zprávami.
- **Milostné podvody,** na seznamovacích platformách, zaměřené na osamělé seniory po celém světě, včetně Islandu, což vede k finanční a emocionální újmě.
- Zločinci se vydávají za jiné osoby, např. zástupce technické podpory nebo banky a navštěvují domovy seniorů..

Co-funded by the
European Union

10 největších obav podle odborníků

Odborníci zdůraznili klíčové obavy, které nejvíce postihují osoby ve věku 55 let a starší při interakci s digitálními technologiemi.

Řešení těchto obav je klíčové pro posílení jejich sebevědomí a bezpečnosti při každodenních online aktivitách.

Motivace

Rozvoj cílených podpůrných a vzdělávacích programů.

Co-funded by the
European Union

10 největších obav podle odborníků

- Potíže se složitostí **přihlašovacích procesů** včetně požadavků na heslo a časté resetování.
- Zmatek a **odpor k dvoufaktorovému ověřování** mezi staršími uživateli.
- **Špatná znalost e-mailů** brání obnovení hesla.
- **Malá velikost textu** a starší telefony omezující použitelnost a bezpečnostní funkcí.
- **Nedostatek jasných pokynů** u služeb vyžadujících elektronický průkaz totožnosti nebo podobné ověřování.

Co-funded by the
European Union

10 největších obav podle odborníků

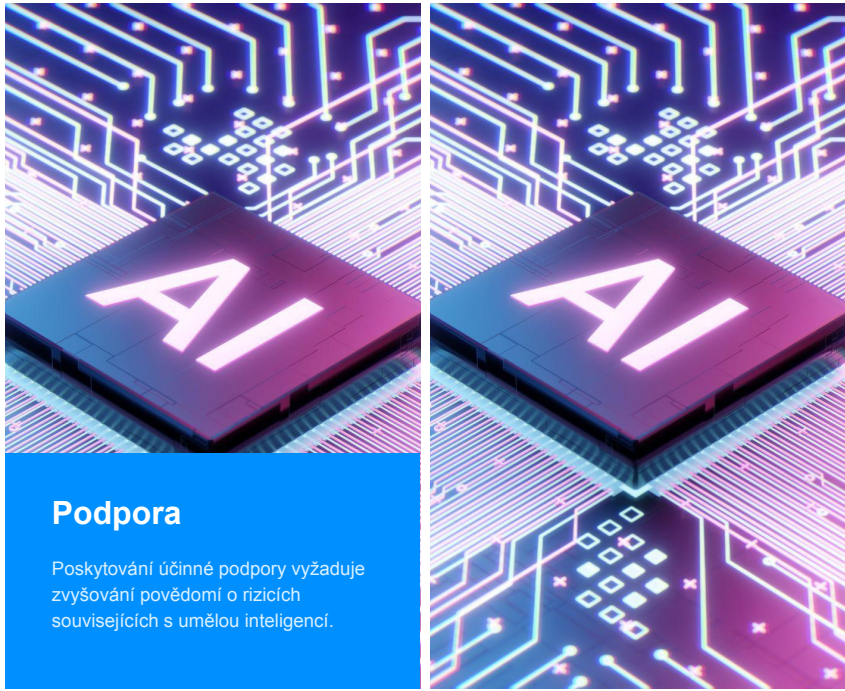
- Senioři **opakovaně používají stejná hesla** napříč kritickými weby, čímž riskují napadení více účtů.
- **Zosobnění domény a** vytváření přesvědčivých falešných webových stránek za účelem krádeže citlivých dat.
- Neustálé nepozorované narušení přihlašovacích údajů z monitorování dark webu.
- **Obecná nedůvěra** nebo nepochopení kybernetických hrozeb ovlivňujících reakce seniorů.
- Bariéry vytvořené **technologickou složitostí a** snížení sebevědomí a nezávislosti.

Co-funded by the European Union

Klíčové oblasti využití umělé inteligence a kybernetická rizika

Umělá inteligence se stále více integruje do mnoha aspektů každodenního života a nabízí významné výhody, ale také přináší nová kybernetická bezpečnostní rizika.

Pochopení hlavních oblastí použití umělé inteligence a s nimi spojených hrozeb je nezbytné pro ochranu zranitelných skupin, jako jsou osoby ve věku 55 let a starší.



Co-funded by the
European Union

Klíčové oblasti využití umělé inteligence a kybernetická rizika

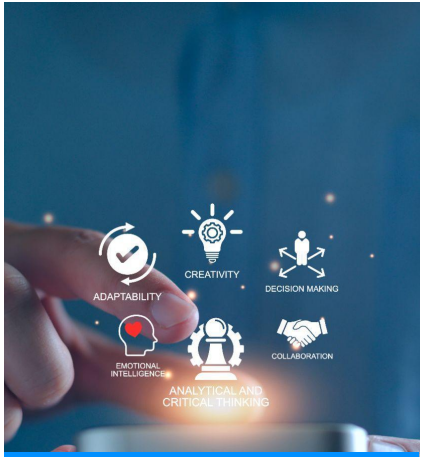
- **Vzdělávání ohledně rizik** falešného internetového obsahu generovaného umělou inteligencí, zejména videí s tvrzeními o rodinných nouzových situacích.
- **Školení** seniorů, aby si ověřovali naléhavé telefonické zprávy přímo od rodiny. Zdůrazněno bylo, že skutečné nouzové situace obvykle zahrnují telefonáty, nikoli textové zprávy.
- **Povědomí,** že umělá inteligence dokáže napodobit jakákoli data včetně videí a obrázků, což vyžaduje kritické myšlení a alternativní ověření.
- Rizika z **nadměrného sdílení osobních údajů** v chatbotech s umělou inteligencí a nástrojích, jako je ChatGPT, kde jsou uložena data.
- Důraz na**udržování kritického myšlení** a ověřování informací prostřednictvím jiných komunikačních kanálů.

Co-funded by the
European Union

Klíčové kompetence pro seniory

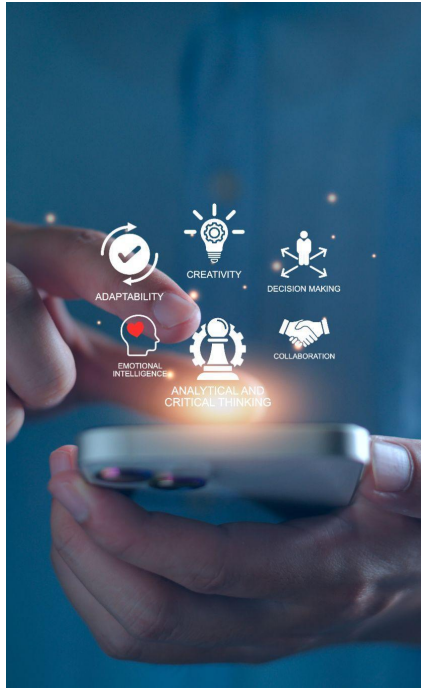
Rozvoj základních digitálních kompetencí je zásadní pro to, aby senioři mohli bezpečně a sebejistě orientovat v online světě.

Tyto dovednosti jim pomáhají efektivně využívat technologie ke zlepšení jejich každodenního života a odolnosti vůči kybernetickým hrozbám.



Kompetence

Umožnit seniorům lépe se chránit a sebevědomě využívat moderní technologie.



Co-funded by the
European Union

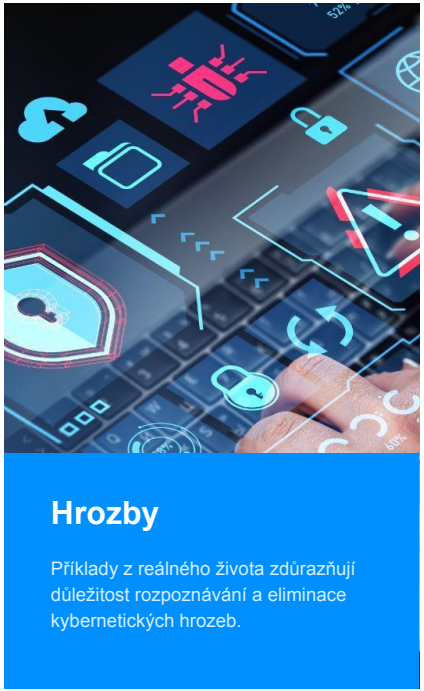
Klíčové kompetence pro seniory

- Pochopení **důležitosti ověřování** předtím, než budou reagovat na naléhavé požadavky prostřednictvím digitálních médií.
- Základní **digitální dovednosti** včetně bezpečné správy hesel a povědomí o rizicích umělé inteligence.
- **Schopnost klást otázky** a ověřovat neočekávané nebo emotivní zprávy, zejména ty, které se zdají být naléhavé nebo znepokojivé.
- **Skepticismus** směrem k autenticitě online obsahu, zejména obsahu generovaném umělou inteligencí.
- Posílení budování důvěry s členy rodiny pro **přímou komunikaci** a pomoc.

Co-funded by the European Union

Hrozby z reálného života identifikované experty

Odborníci sdíleli příklady z reálného života, které ilustrují rizika i přínosy digitálních technologií pro osoby ve věku 55 let a starší.
Tyto případy poskytují cenné poznatky o běžných kybernetických hrozbách umělé inteligence v každédenním životě seniorů.



Co-funded by the
European Union

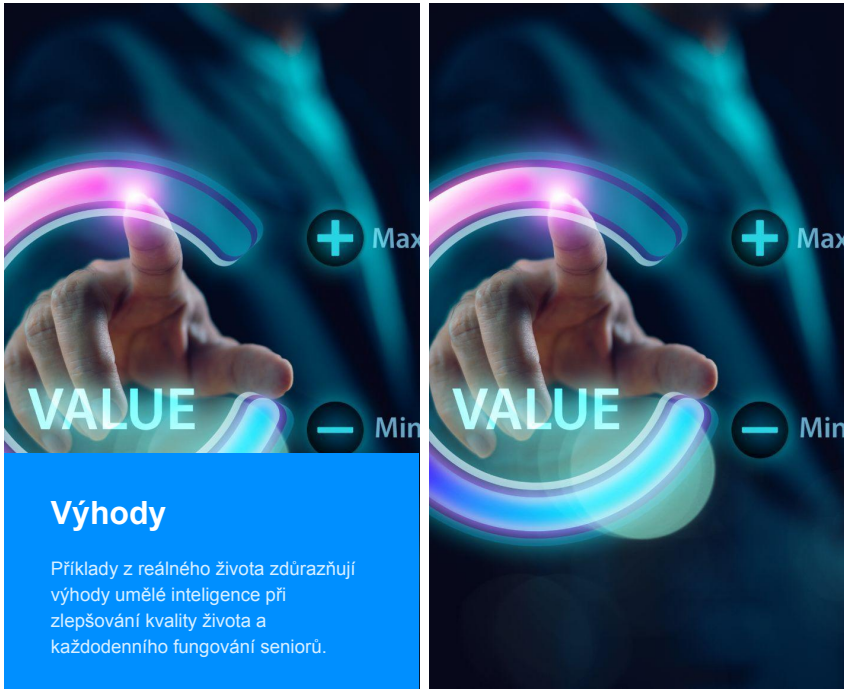
Hrozby z reálného života identifikované experty

- Příklady obětí, které přišly o úspory kvůli podvodům s deepfake romantikou využívajícími podobizny celebrit generované umělou inteligencí.
- Podvody přes WhatsApp zahrnující falešné zprávy o nemocných příbuzných, kteří potřebují vklady peněz, někdy zastavené zásahem rodiny.
- Podvody na sociálních sítích a seznamovacích aplikacích vedou seniory k placení falešné zdravotní péče nebo cestování do zahraničí za neexistujícími partnery.
- Podvody s prací, které kradou informace o kreditních kartách prostřednictvím podvodných nabídek zaměstnání s nápodobou hlasu.
- Případy zranitelných osob, které neúmyslně zveřejňují kompromitující obsah online, aniž by chápaly následky.

Co-funded by the
European Union

Výhody v reálném životě identifikované odborníky

Odborníci sdíleli příklady z reálného života, které ilustrují rizika i přínosy digitálních technologií pro osoby ve věku 55 let a starší.
Tyto případy poskytují cenné poznatky o výhodách vlivu umělé inteligence na každodenní život seniorů.



Co-funded by the
European Union

Výhody v reálném životě identifikované odborníky

- Umělá inteligence pomáhá seniorům s praktickými radami každodenního života, jako je úklid, opravy domácnosti a rychlé řešení problémů.
- Chatboti s umělou inteligencí poskytující emocionální podporu a společnost, nabízející nepřetržitou dostupnost pro úlevu od úzkosti a obecnou konverzaci.
- Využití nástrojů umělé inteligence, jako je ChatGPT, k ověřování podezřelých e-mailů nebo zpráv souvisejících s kybernetickou bezpečností.
- Úspěšnost zavádění umělé inteligence se značně liší v závislosti na individuálních technických dovednostech seniorů a jejich důvěře v technologie.

Co-funded by the European Union

Online hrozby pro osoby starší 55 let – glosář

Co-funded by the
European Union

Phishing (podvodné e-maily, SMS, odkazy, hlasové hovory).

Phishing je typ kybernetického útoku, při kterém zločinci rozesílají falešné e-maily, textové zprávy, telefonní hovory nebo odkazy a vydávají se za někoho, komu důvěřujete, například za banku nebo přítele. Jejich cílem je oklamat vás a přimět vás, abyste poskytli důležité osobní údaje, jako jsou hesla, čísla kreditních karet nebo údaje o bankovním účtu. Tyto falešné zprávy často vypadají velmi reálně a snaží se vás přimět k rychlé akci tím, že ve vás vyvolají pocit naléhavosti nebo strachu. Útočníci vám chtějí ukrást peníze nebo identitu tím, že vás oklamou a přimějí vás kliknout na nebezpečné odkazy nebo sdílet citlivá data. Abyste zůstali v bezpečí, vždy si dvakrát ověřte, kdo zprávu odeslal, neklikejte na podezřelé odkazy a nikdy nesdílejte osobní údaje, pokud si nejste naprosto jisti, že jsou bezpečné.

Co-funded by the
European Union

Deepfake útoky (falešný zvuk/video, vydávání se za rodinu)

Útoky typu deepfake zahrnují vytváření falešných zvukových nebo obrazových nahrávek pomocí umělé inteligence, které vypadají a zní velmi realisticky. Při těchto útocích zločinci napodobují hlas nebo obličej někoho známého, často člena rodiny, aby lidi oklamali a přiměli je věřit, že mluví s milovanou osobou. Podvodník může například použít technologii deepfake k uskutečnění telefonního hovoru, který zní přesně jako hovor vnoučete, které naléhavě žádá o peníze. Tyto falešné nahrávky jsou velmi přesvědčivé a dokáží oklamat i opatrné lidi. Útoky typu deepfake jsou nebezpečné, protože zneužívají důvěru a emoce, takže je těžké si podvod uvědomit, dokud není příliš pozdě. Abyste se ochránili, vždy si před provedením jakýchkoli kroků ověřte neobvyklé požadavky tím, že danou osobu kontaktujete přímo prostřednictvím různých komunikačních kanálů.

Co-funded by the
European Union

Falešné internetové obchody a podvody (padělané webové stránky)

Falešné internetové obchody a podvody jsou podvodné webové stránky, které vypadají jako legitimní obchody, ale ve skutečnosti jsou vytvořeny tak, aby lidi oklamaly a přiměly k nákupu produktů, které neexistují nebo jsou nekvalitní. Tyto falešné obchody často kopírují loga, popisy produktů a fotografie skutečných společností, aby vypadaly přesvědčivě. Podvodníci tyto stránky používají k tomu, aby ukradli peníze a osobní údaje nic netušícím zákazníkům. Lákají kupující sliby velmi nízkých cen nebo speciálních nabídek, které se zdají být příliš dobré na to, aby byly pravdivé.

Tyto webové stránky mohou mít podivné webové adresy, obsahovat pravopisné chyby nebo postrádat správné kontaktní údaje. Poté, co zákazníci zaplatí, často svou objednávku nikdy neobdrží nebo dostanou padělané zboží. Abyste se chránili, nakupujte vždy v důvěryhodných obchodech, prostudujte si recenze na webových stránkách, vyhněte se nabídkám, které se zdají nerealisticky levné, a nikdy nesdílejte platební informace na podezřelých stránkách. Pokud se vám něco zdá divné, je lepší si to před nákupem dvakrát ověřit.

Co-funded by the
European Union

Emoční manipulace a sociální inženýrství (zastrašovací taktiky).

Emoční manipulace a sociální inženýrství zahrnují podvádění lidí hraním na jejich city, aby se chovali způsobem, jakým by se normálně nechovali. Kyberzločinci používají taktiky, jako jsou strašidelné historky, naléhavost, falešná autorita nebo laskavost, k vytvoření pocitu strachu, důvěry nebo povinnosti. Mohou se například vydávat za bankovního úředníka, který vás varuje před problémem s vaším účtem a naléhá na vás, abyste jednali rychle, abyste bez přemýšlení poskytli citlivé informace. Tyto taktiky zneužívají přirozené lidské reakce – strach, důvěru, zvědavost nebo ochotu pomoci – a je tak těžké jim odolat. Nejlepší obranou je uvědomění si: rozpoznání těchto emocionálních triků a zastavení se, abyste si ověřili, kdo se o informace skutečně ptá, než odpovíte.

Co-funded by the
European Union

Krádež identity (s využitím ukradených osobních údajů)

Krádež identity znamená, že někdo bez vašeho svolení ukradne vaše osobní údaje a použije je k tomu, aby se za vás vydával. Může použít vaše jméno, číslo sociálního zabezpečení, údaje o bankovním účtu nebo jiné údaje k otevření účtů, sjednání půjček nebo k nákupům vaším jménem. To může způsobit velké finanční problémy a poškodit vaši pověst.

Co-funded by the
European Union

Podvod „na vnoučeti“ (podvodníci předstírající, že jsou členy rodiny v nouzi)

Podvod „na vnoučeti“, známý také jako „podvod s prarodiči“, je běžná metoda používaná zločinci, kteří se vydávají za člena rodiny – obvykle vnouče nebo dítě – v nouzi. Obvykle se to děje telefonicky, kdy podvodník zavolá starší osobě a tvrdí, že je ve vážných potížích, například že měla nehodu, byla zatčena nebo potřebuje naléhavou finanční pomoc. Volající často požádá o rychlé zaslání peněz a trvá na tom, aby oběť to udržela v tajnosti, například slovy: „Neříkej to mámě, bude se bát.“

Tento podvod hraje na emoce, jako je láska a zájem o členy rodiny, a v dané osobě vyvolává touhu okamžitě pomoci, aniž by se musela zastavit. Podvodníci stále častěji využívají technologie, jako je umělá inteligence, k napodobení hlasu skutečného vnoučete, díky čemuž hovor zní velmi přesvědčivě.

Co-funded by the
European Union

Falešné žádosti o „pomoc“ přes WhatsApp nebo Messenger

Falešné žádosti o „pomoc“ přes WhatsApp nebo Messenger jsou podvody, kdy se někdo vydává za přítele nebo člena rodiny v naléhavých nouzích a žádá o peníze nebo osobní údaje. Tyto zprávy často přicházejí nečekaně od neznámých nebo maskovaných kontaktů. Podvodník může tvrdit, že ztratil telefon, že se mu zablokoval účet nebo že potřebuje naléhavou finanční pomoc. Snaží se vytvořit pocit naléhavosti a důvěry, aby oběti přiměl k rychlé reakci, aniž by si ověřoval, zda je to pravda.

Co-funded by the
European Union

Romantické podvody a podvody založené na vztazích budovaných online

Romantické podvody jsou typem podvodu, kdy zločinci vytvářejí falešné online profily a předstírají romantický zájem o někoho. Postupem času si budují důvěru a emocionální pouto, čímž oběť přesvědčí, že je ve skutečném vztahu. Jakmile si podvodníci získají důvěru, vymýšlejí si nouzové situace nebo naléhavé finanční potřeby – jako jsou lékařské výdaje nebo cestovní náklady – a po oběti žádají o peníze nebo dárky.

Tito podvodníci jsou velmi zruční v předstírání starostlivosti a důvěryhodnosti a často se vyhýbají osobním schůzkám nebo videohovorům podáním výmluv. Zneužívají osamělosti a emocionální zranitelnosti, což zvyšuje pravděpodobnost, že jim oběti dají peníze.

Co-funded by the
European Union

Investiční podvod (falešné reklamy s celebritami).

Investiční podvod zahrnující falešné reklamy celebrit je typ podvodu, kdy zločinci používají obrázky, videa nebo jména slavných osobností, aby investiční příležitost vypadala legitimně a důvěryhodně. Někdy tyto reklamy obsahují falešná videa, na kterých celebrity podporují investici, nebo se vydávají za novinové články spojující celebrity s finančním úspěchem na určitých platformách.

Podvodníci klamou lidi, aby věřili, že mohou dosáhnout rychlých a velkých zisků, často v kryptoměnách nebo obchodování s devizami. Lákají oběti k vytvoření účtů, vložení peněz a poté požadují další prostředky na zaplacení falešných poplatků nebo daní. Důvěru lze získat předčasným výběrem, ale když se oběti pokusí vybrat své peníze, jsou zablokovány a požadovány vysoké dodatečné platby.

Co-funded by the
European Union

Malware a ransomware (infikované soubory, přílohy)

Malware je škodlivý software, který může infikovat váš počítač nebo telefon a způsobit škodu, například krádež osobních údajů, poškození souborů nebo převzetí kontroly nad vaším zařízením. Ransomware je speciální typ malwaru, který uzamyká nebo šifruje vaše soubory a znepřístupňuje je, dokud útočníkovi nezaplatíte výkupné – obvykle v kryptoměně. Ransomware se do vašeho zařízení může dostat prostřednictvím infikovaných e-mailových příloh, škodlivých webových stránek nebo nebezpečných stahovaných souborů.

Jakmile je ransomware infikován, znemožní vám používat důležité soubory a někdy požaduje peníze za obnovení přístupu. Zaplacení výkupného nezaručuje, že vaše data budou uvolněna, a povzbuzuje zločince k pokračování v těchto útocích.

Co-funded by the
European Union

Neověřené aplikace a stahování nebezpečného softwaru

Neověřené aplikace a nebezpečné stahování softwaru jsou kybernetické hrozby, kdy si lidé stahují a instalují aplikace nebo soubory z neznámých nebo nespolehlivých zdrojů. Tyto aplikace nebo stahování mohou obsahovat skrytý malware, viry nebo spyware, které mohou poškodit vaše zařízení, ukrást osobní údaje nebo poskytnout hackerům neoprávněný přístup.

Protože tyto aplikace nejsou kontrolovány ani schvalovány důvěryhodnými platformami, mohou narušovat zabezpečení vašeho zařízení, způsobovat pády nebo vás vystavovat podvodům. Falešné aplikace mohou vypadat jako skutečné, ale po instalaci mohou shromažďovat vaše data nebo šířit škodlivý software.

Co-funded by the
European Union

Sdílení citlivých údajů s cizími lidmi (fotografie, informace).

Sdílení citlivých dat s cizími lidmi, jako jsou fotografie nebo osobní údaje, je kybernetická hrozba, kdy lidé online sdělují soukromé údaje neznámým nebo nedůvěryhodným lidem. Může se to zdát neškodné, jako sdílení fotografie, ale tyto údaje mohou být zneužity k odcizení vaší identity, spáchání podvodu nebo poškození vaší pověsti.

Fotografie mohou odhalit váš domov, polohu nebo osobní zvyky, aniž byste si to uvědomovali. Cizí lidé mohou tyto informace použít k tomu, aby vás oklamali nebo se na vás zaměřili v podvodných akcích. Abyste zůstali v bezpečí, sdílejte osobní údaje a fotografie pouze s lidmi, kterým důvěřujete, pečlivě si rozmyslete, než je zveřejníte online, a upravte nastavení soukromí tak, abyste omezili, kdo může vaše informace vidět.

Co-funded by the
European Union

Úniky dat z používání zastaralých zařízení nebo softwaru

Používání zastaralých zařízení nebo softwaru představuje kybernetickou hrozbu, protože staré verze často neobsahují nejnovější bezpečnostní aktualizace. Tyto chybějící aktualizace vytvářejí slabiny, které mohou hackeři snadno zneužít k přístupu k vašim osobním údajům nebo k ovládání vašeho zařízení. To může vést k úniku dat, krádeži nebo napadení malwarem.

Zastaralý software také zpomaluje vaše zařízení a může přestat fungovat s novějšími programy, což vám ztěžuje každodenní činnosti. Abyste se chránili, je důležité pravidelně aktualizovat zařízení a důležitý software nejnovějšími záplatami a bezpečnostními opravami. Tím se odstraní bezpečnostní mezery, zajistí se bezpečnější data a zajistí se bezproblémový chod zařízení.

Co-funded by the
European Union

Masové personalizované útoky s využitím umělé inteligence, zaměřené na uživatelské profily

Masově personalizované útoky s využitím umělé inteligence jsou kybernetické hrozby, kdy útočníci využívají umělou inteligenci k vytváření vysoce personalizovaných a přesvědčivých zpráv zaměřených na jednotlivce, na základě jejich osobních údajů. Umělá inteligence analyzuje informace ze sociálních médií, e-mailů a veřejných zdrojů a vytváří zprávy, které cíli působí velmi povědomě a důvěryhodně.

Tyto útoky mohou zahrnovat personalizované phishingové e-maily nebo zprávy, které zmiňují jméno oběti, její zaměstnání, nedávné aktivity či zájmy. Cílem je oklamat lidi, aby klikli na škodlivé odkazy, odhalili hesla nebo převedli peníze. Protože se umělá inteligence neustále učí a přizpůsobuje, stávají se tyto útoky efektivnějšími a hůře odhalitelnými.

Co-funded by the
European Union

Zdravotní dezinformace nebo nebezpečné lékařské rady z nástrojů umělé inteligence

Zdravotní dezinformace nebo nebezpečné lékařské rady z nástrojů umělé inteligence představují kybernetickou hrozbu, kdy umělá inteligence generuje nesprávné, zavádějící nebo škodlivé zdravotní informace. Lidé mohou důvěřovat chatbotům s umělou inteligencí nebo online nástrojům, pokud jde o lékařské rady, ale tyto systémy někdy vytvářejí nesprávné diagnózy, navrhují nebezpečnou léčbu nebo šíří nepravdivá tvrzení o nemocech.

Tato dezinformace může vést k tomu, že lidé odkládají poskytnutí řádné lékařské péče, používají neúčinné léky nebo se dopouštějí škodlivých činů. Obsah generovaný umělou inteligencí může znít velmi profesionálně a přesvědčivě, takže je obtížné určit, zda je rada spolehlivá.

Co-funded by the
European Union

Podvody zneužívající digitální vyloučení v občanských a bankovních službách

Podvody zneužívající digitální vyloučení v občanských a bankovních službách jsou hrozby zaměřené na osoby, které mají omezený přístup k digitálním technologiím nebo o nich mají malou znalost. Tyto podvody zneužívají lidi, kteří mají potíže s používáním online vládních nebo bankovních služeb, někdy proto, že jim chybí zařízení, přístup k internetu, digitální dovednosti nebo sebevědomí.

Zločinci tyto osoby podvádějí tím, že nabízejí falešnou pomoc s online procesy nebo zasílají podvodné zprávy napodobující oficiální instituce v naději, že oběti sdílejí citlivé údaje nebo pošlou peníze. Protože tito lidé mají méně zdrojů nebo podpory k rozpoznání podvodů, jsou zranitelnější.

Co-funded by the
European Union

Nedostatek postupů vícefaktorového ověřování (zjednodušená hesla, opakované použití)

Absence vícefaktorového ověřování (MFA) znamená používání pouze hesla – často jednoduchého nebo opakovaného na mnoha webech – k ochraně online účtů. To je riskantní, protože pokud někdo vaše heslo ukradne nebo uhádne, může se snadno dostat k vašim účtům.

Vícefaktorové ověřování přidává další vrstvu zabezpečení tím, že vyžaduje dvě nebo více forem ověření. Například po zadání hesla můžete zadat kód odeslaný na váš telefon nebo použít skenování otisků prstů. To hackerům výrazně ztěžuje přístup k vašemu účtu, i když znají vaše heslo.

Co-funded by the
European Union

Ztráta přístupu ke klíčovým službám v důsledku technologických změn (přístup pouze přes aplikaci, omezené alternativy)

Ke ztrátě přístupu ke klíčovým službám v důsledku technologických změn dochází, když důležité veřejné nebo bankovní služby přecházejí do čistě digitálních formátů, jako jsou aplikace nebo online portály, bez snadných alternativ pro lidi, kteří se k jejich používání necítí dobře nebo nejsou vybaveni. To znamená, že lidé, kteří nemají chytré telefony, počítače nebo digitální dovednosti, mohou mít potíže s přístupem k základním službám, jako jsou návštěvy zdravotní péče, důchodové dávky nebo bankovní transakce, nebo jim tento přístup vůbec nemohou umožnit.

Tento digitální posun může vyloučit mnoho lidí, zejména starší dospělé nebo osoby s omezenými zdroji, a učinit je tak závislými na ostatních nebo neschopnými plnit důležité úkoly.

Co-funded by the
European Union

Automatizovaná manipulace sociálních médií, produkující dezinformace a stres

Automatizovaná manipulace se sociálními sítěmi je kybernetická hrozba, kdy počítačové programy, nazývané boti, a umělá inteligence ovládají obsah, který vidíte na svých stránkách sociálních sítí. Tyto systémy analyzují, co se vám líbí, co sdílíte nebo co komentujete, a poté vám zobrazují podobné příspěvky, abyste si udrželi zájem.

Tohoto přístupu bohužel lze využít k šíření dezinformací, falešných zpráv nebo extrémního obsahu, který vyvolává stres, strach nebo hněv. Boti mohou uměle zvyšovat popularitu takových příspěvků lajkováním, sdílením nebo komentováním, čímž vytvářejí dojem, že s nimi mnoho lidí souhlasí.