Budování digitální odolnosti
Manuál a metodika

Budování digitální odolnosti zpřístupněním digitální pohody a bezpečnosti pro všechny

2022-2-SK01-KA220-ADU-000096888

Co-funded by the European Union

Erasmus+ projekt KA220 Kooperativní partnerství ve vzdělávání dospělých

Budování digitální odolnosti zpřístupněním digitální pohody a bezpečnosti pro všechny

2022-2-SK01-KA220-ADU-000096888

DigiWELL

Budování digitální odolnosti manuál a metodika

Září 2023

Tato publikace byla připravena jako výsledek projektu "Budování digitální odolnosti zpřístupněním digitální pohody a bezpečnosti pro všechny" (Projeckt č: 2022-2-SK01-KA220-ADU-000096888), který je implementován v rámci Erasmus+ KA220 Kooperativní partnerství ve vzdělávání dospělých.

DigiWELL konsorcium

Slovak University of Agriculture in Nitra, Slovakia

Muğla Sıtkı Koçman University, Turkey

Czech technical university in Prague, Czech

Innovation, Training, and Employment Association for Sustainable Development (AIFED), Spain

European Institute for Innovation – Technology (EIfI-Tech), Germany

Foundation Maker's Place Private Company (Found.ation), Greece

Syzigia Skopje Foundation (SYZYGY), Macedonia

Faculty of Economics and Management
Slovak University of Agriculture in Nitra |
Tr. Andreja Hlinku 2 | 949 76 Nitra | Slovakia | email: digiwell@uniag.sk

Webová stránka: www.digiwell.sk

Zřeknutí se odpovědnosti:

" Spolufinancováno programem Erasmus+ Evropské unie. Tato publikace odráží pouze názory přispěvatelů a Evropská komise a Slovenská akademická asociace pro mezinárodní spolupráci nenesou odpovědnost za jakékoli použití informací v ní obsažených."

Pracovní balíček 2: **Budování digitální odolnosti manuál a metodika**

Seznam přispěvatelů:

Murat Sümer, Czech Technical University,

David Vaneček, Czech Technical University,

Martina Hanová, Slovak University of Agriculture in Nitra, Slovakia

Marcela Hallová, Slovak University of Agriculture in Nitra, Slovakia

Eva Oláhová, Slovak University of Agriculture in Nitra, Slovakia

Eyüp Şen, Muğla Sıtkı Koçman University, Turkey

İlker Yorulmaz, Muğla Sıtkı Koçman University, Turkey

Maria Martinez, AIFED, Spain

Jesus de Haro Martinez, AIFED, Spain

Chris Ashe, Elfl-Tech, Germany

Mattia Ferrari, Elfl-Tech, Germany

Maria Kandilioti, Found.ation, Greece

Roula Mourmouri, Found.ation, Greece

Suzana Trajkovska, SYZYGY, Macedonia

Aleksandar Kochankovski, SYZYGY, Macedonia

Contents

Souhrn

Po pandemii COVID-19 se některé potřeby staly životně důležitými díky používání digitálních technologií a internetu, které jsou v našem životě velmi rozšířené. Nejdůležitější z nich je možnost bezpečně provádět transakce v digitálním světě, aniž by došlo k jejich poškození. Zejména dospělí potřebují digitální bezpečnostní opatření a určité kompetence, aby se mohli chránit před kybernetickými hrozbami. Také internet a digitální technologie nejen usnadňují život, ale také vytvářejí některé negativní psychické problémy. Například kyberšikana se stala obtížně řešitelným problémem. V souladu s tím se zajištění pohody v digitálním světě stalo v současných podmínkách nutností. I v souvislosti s touto problematikou platí, že rostoucí využívání digitálních technologií a bod, kterého digitální transformace dosáhla, přinesly lidem některé problémy, jako je digitální únava.

V tomto ohledu je cílem projektu DigiWELL začlenit zásady digitální pohody do vzdělávání dospělých. Jeho iniciativy směřují k přispění k celkové praxi organizací, sítí a iniciativ v oblasti vzdělávání dospělých. Projekt si uvědomuje, jak zásadní je zabývat se tím, jak technologie ovlivňují duševní zdraví, produktivitu a celkovou pohodu dospělých v digitálním věku. Hlavním cílem projektu DigiWELL je poskytnout dospělým účastníkům vzdělávání informace, schopnosti a zdroje potřebné k etické a svědomité orientaci v digitálním světě. Projekt DigiWELL zahrnuje také vytvoření a realizaci dalších iniciativ pro posílení postavení dospělých studentů. Cílem těchto aktivit je poskytnout podpůrné prostředí, ve kterém mohou dospělí sdílet své zkušenosti, potíže a úspěchy při podpoře digitální pohody. S ohledem na to projekt DigiWELL představuje mnoho příležitostí pro jednotlivce a organizace dospělých, aby si uvědomili a poučili se o významu digitální pohody a o tom, jak podporovat digitální pohodu dospělých jednotlivců a vzdělavatelů a školitelů dospělých. Umožnění digitální pohody s holistickým přístupem je mnohem více možné, pokud všechny příslušné strany přijmou opatření na podporu potřeb digitální pohody jednotlivců. Informace, tipy a osvědčené postupy uvedené v této příručce proto vybízejí lidi a zainteresované organizace, aby se chopili iniciativy, díky níž bude mít více z nás lepší digitální pohodu a také silnější digitální život.

1. Úvod

1.1 Cíl metody a Manuel

- Přispět k umožnění digitální pohody a digitální bezpečnosti přístupné všem tím, že dospělí budou povzbuzováni a informováni o digitální pohodě a digitální bezpečnosti a o kompetencích, které jsou pro ně nezbytné.
- Představit digitální odolnost, digitální pohodu a digitální bezpečnost, terminologický rámec a osvědčené postupy digitální pohody a digitální bezpečnosti mezi všemi lidmi.
- Zajistit multikulturnost a přizpůsobit vytvořené výstupy příslušným organizacím v partnerských zemích.

1.2 Rámec EU DigComp

V rámci DigComp digitální kompetence zahrnují "sebevědomé, kritické a zodpovědné využívání digitálních technologií a zapojení se do nich při učení, v práci a při zapojení do společnosti. Je definována jako kombinace znalostí, dovedností a postojů". (Doporučení Rady o klíčových kompetencích pro celoživotní učení, 2018).

Rámec DigComp identifikuje klíčové složky digitálních kompetencí v pěti oblastech. Tyto oblasti jsou shrnuty níže:

Informační a datová gramotnost: Vyjádřit informační potřeby, vyhledávat a získávat digitální data, informace a obsah. Posoudit relevanci zdroje a jeho obsahu. Ukládat, spravovat a organizovat digitální data, informace a obsah.

Komunikace a spolupráce: Umění komunikovat, komunikovat a spolupracovat prostřednictvím digitálních technologií s ohledem na kulturní a generační rozmanitost. Zapojit se do společnosti prostřednictvím veřejných a soukromých digitálních služeb a participativního občanství. Spravovat svou digitální přítomnost, identitu a pověst.

Tvorba digitálního obsahu: Zlepšovat a integrovat informace a obsah do stávajícího souboru znalostí a zároveň chápat, jakým způsobem je třeba uplatňovat autorská práva a licence. Umět dávat srozumitelné pokyny pro počítačový systém.

Bezpečnost: Umět chránit zařízení, obsah, osobní údaje a soukromí v digitálním prostředí. Chránit fyzické a psychické zdraví a znát digitální technologie pro sociální pohodu a sociální začlenění. Uvědomovat si dopad digitálních technologií a jejich používání na životní prostředí.

Řešení problémů: Identifikovat potřeby a problémy a řešit koncepční problémy a problémové situace v digitálním prostředí. Využívat digitální nástroje k inovaci procesů a produktů. Držet krok s vývojem digitálních technologií.

Jednou z klíčových kompetencí v oblasti bezpečnosti je ochrana zdraví a pohody. Ochrana zdraví a pohody znamená: a) umět se vyhnout zdravotním rizikům a ohrožení fyzické a psychické pohody při používání digitálních technologií, b) umět chránit sebe i ostatní před možnými nebezpečími v digitálním prostředí (např. kyberšikanou) a c) znát digitální technologie pro sociální pohodu a sociální začlenění.

1.3 Proč je M&M dobrým zdrojem pro dospělé?

Jak bylo uvedeno výše, po pandemii COVID-19 se některé potřeby staly životně důležitými díky používání digitálních technologií a internetu, které jsou v našem životě velmi rozšířené. Nejdůležitější z nich je možnost bezpečně provádět transakce v digitálním světě, aniž by došlo k jejich poškození. Zejména dospělí potřebují digitální bezpečnostní opatření a určité kompetence, aby se mohli chránit před kybernetickými hrozbami. Také internet a digitální technologie nejen usnadňují život, ale také vytvářejí některé negativní psychické problémy. Například kyberšikana se stala obtížně řešitelným problémem. V souladu s tím se zajištění pohody v digitálním světě stalo v současných podmínkách nutností. I v souvislosti s touto problematikou platí, že rostoucí využívání digitálních technologií a bod, kterého digitální transformace dosáhla, přinesly lidem některé problémy, jako je digitální únava.

Tato příručka využívá co nejvíce příkladů z reálného světa a nechává dospělé studenty, aby si sami přišli na některé pojmy, které podporují vzdělávání dospělých na základě Knowlese (1968).

1.4 Proč by měl být M&M dobrým zdrojem pro školitele dospělých?

Školení a vzdělávání hrají zásadní roli při zvyšování povědomí o digitální bezpečnosti tím, že jednotlivcům poskytují znalosti, dovednosti a osvědčené postupy potřebné k ochraně sebe i svých organizací před kybernetickými hrozbami. Školení a vzdělávání v oblasti digitální bezpečnosti jsou navíc základními složkami budování silné kultury kybernetické bezpečnosti. Vytvořením školicích programů, které jsou přizpůsobeny konkrétním potřebám a rolím, vybaví dospělé osoby znalostmi a dovednostmi potřebnými k identifikaci kybernetických hrozeb a účinné reakci na ně.

Školení pomáhá jednotlivcům porozumět různým typům kybernetických hrozeb, jako je phishing, malware, sociální inženýrství a ransomware. Díky rozpoznání těchto hrozeb mohou být jednotlivci při používání digitálních platforem ostražitější a opatrnější. Vzdělávání může jednotlivce naučit, jak rozpoznat phishingové e-maily, zprávy nebo webové stránky. Naučí se rozpoznat podezřelé prvky a vyhnout se klikání na škodlivé odkazy nebo poskytování citlivých informací. Školení zároveň zahrnuje pokyny k zabezpečení mobilních zařízení, jejich ochraně pomocí přístupových kódů, používání šifrování a obezřetnosti při stahování aplikací a zároveň zajišťuje, aby si jednotlivci byli vědomi příslušných předpisů v oblasti kybernetické bezpečnosti a požadavků na dodržování předpisů, což pomáhá zachovávat právní a etické postupy. A konečně, díky vzdělávání jednotlivci pochopí, že kybernetická bezpečnost je společnou odpovědností a že k udržení bezpečného prostředí je nutná aktivní účast všech, zatímco vštěpuje správné návyky v oblasti kybernetické bezpečnosti a podporuje jednotlivce v zavádění bezpečnostních opatření v práci i v osobním životě.

Cílem projektu DigiWELL je řešit potřeby digitální bezpečnosti a pohody dospělých, kteří se nenarodili v éře internetu. Toho dosáhne vytvářením a rozvíjením flexibilních vzdělávacích příležitostí, které uspokojí specifické vzdělávací požadavky dospělých. Projekt se zaměří na zvýšení digitální odolnosti prostřednictvím kombinovaného přístupu k učení. K výše uvedenému cíli přispívá zejména tato příručka, neboť vytváří kulturu uvědomění si bezpečnosti, která se aktivně brání kybernetickým hrozbám a chrání digitální aktiva a citlivé informace.

Jinými slovy, příručka s částí věnovanou digitální bezpečnosti může sehrát významnou roli při vybavování dospělých potřebnými dovednostmi a znalostmi, které jim umožní chránit se v digitálním věku, a podpořit tak bezpečnější a jistější online prostředí pro jednotlivce i komunity. Příručka DigiWELL je cenným zdrojem informací pro dospělé, neboť je vzdělává v oblasti potenciálních rizik a pomáhá jim pochopit význam kybernetické bezpečnosti a způsoby ochrany online. V neposlední řadě nabízí praktické pokyny k zavádění digitálních bezpečnostních opatření a posiluje dospělé, aby se mohli s důvěrou pohybovat v digitálním světě, a slouží jako referenční příručka, ke které se dospělí mohou vrátit, kdykoli se setkají s novými problémy v oblasti digitální bezpečnosti nebo si potřebují osvěžit určitá témata.

1.5 Slovník projektu DigiWELL a jeho použití

Cílem slovníku je seznámit dospělé uživatele digitálních technologií se základními pojmy a definicemi týkajícími se digitální pohody, digitální bezpečnosti a digitální odolnosti.

Klasifikace pojmů

Z hlediska obsahu obsahuje slovník 3 základní kategorie termínů;

1. Termíny a definice z oblasti informačních a komunikačních technologií (podle projektu digitální technologie).
2. Termíny a definice z oblasti informační, kybernetické a digitální bezpečnosti (digitální bezpečnost dle projektu).
3. Termíny a definice definované podle cílů projektu: digitální blahobyt a digitální odolnost. Tyto pojmy jsou relativně nové a jsou součástí desk research projektových týmů. Je třeba zdůraznit, že neexistuje jednotná definice těchto pojmů. Do této kategorie patří také termíny z oblasti duševního a fyzického zdraví, např. digitální závislost, digitální únava/vyhoření, digitální detox apod.

Pozn: V textové databázi slovníku může mít termín více než jednu definici, a to z mnoha důvodů: původní definice se v průběhu času vyvíjela, široká definice je přizpůsobená pro určitou oblast, definice pojmů jsou podobné, ale s jemnými rozdíly atd.

Termíny a definice

***Digitální* odolnost:** 1. Digitální odolnost znamená mít povědomí, dovednosti, pružnost a sebedůvěru při používání nových technologií a přizpůsobovat se měnícím se požadavkům na digitální dovednosti. Digitální odolnost zlepšuje schopnost řešit problémy a zvyšovat kvalifikaci a schopnost orientovat se v digitálních transformacích. 2. Digitální odolnost je schopnost mladých lidí rozvíjet kritické myšlení při přístupu k digitálním informacím, aby se snížila jejich zranitelnost vůči potenciálně škodlivým informacím. 3. Digitální odolnost znamená "proces dobré adaptace na digitální zdroje stresu a rozvoj dovedností pro zvládání dopadů neustále se měnícího digitálního prostředí a aplikací".

Digitální zabezpečení: Digitální bezpečnost je ochrana digitální identity, která představuje fyzickou identitu v síti nebo internetových službách. Digitální bezpečnost je soubor osvědčených postupů a nástrojů používaných k ochraně osobních údajů a online identity v online světě. Příklady nástrojů jsou: webové služby, antivirový software, SIM karty pro chytré telefony, biometrické a bezpečné osobní zařízení, správci hesel, rodičovská kontrola atd.

Digitální pohoda: 1. Digitální pohoda popisuje schopnost člověka účinně zvládat negativní dopady technologií na jeho profesní a osobní život. Cílem digitální pohody je podporovat zdravé používání technologických zařízení a digitálních služeb. 2. Stav osobní pohody zažívaný prostřednictvím zdravého používání digitálních technologií. 3. Digitální pohoda zahrnuje způsoby, jakými mohou informační technologie - včetně komunikace a senzorů - pomoci lidem žít dlouhý a zdravý život.

Digitální kompetence: Digitální kompetence: sebejisté, kritické a zodpovědné používání digitálních technologií a zapojení se do nich při učení, v práci a při zapojení do společnosti. Je definována jako kombinace znalostí, dovedností a postojů.

Digitální závislost: Digitální závislost je škodlivá závislost na digitálních médiích, zařízeních a internetu, která se vyznačuje jejich nadměrným používáním způsobem, který má negativní dopad na život uživatele.

Digitální dovednosti: Digitální dovednosti jsou jako soubor schopností používat digitální zařízení, komunikační aplikace a sítě k přístupu k informacím a jejich správě. Umožňují lidem vytvářet a sdílet digitální obsah, komunikovat a spolupracovat a řešit problémy pro efektivní a kreativní seberealizaci v životě, učení, práci a společenských aktivitách.

Kybernetická hrozba: Jakákoli okolnost nebo událost, která může mít nepříznivý dopad na organizace/jednotlivce prostřednictvím neoprávněného přístupu, zničení, vyzrazení, modifikace informací a/nebo odepření služby. Cílem je krádež/poškození dat nebo narušení digitální pohody.

Kyberšikana: Kyberšikana: termín pro různé formy šikany v online prostoru, při nichž jeden nebo více jedinců využívá digitální technologie k úmyslnému a opakovanému poškozování jiné osoby (např. zasílání e-mailů nebo rychlých zpráv, zveřejňování komentářů na sociálních sítích nebo veřejných fórech).

Kybernetická bezpečnost: Kybernetická bezpečnost je podmnožinou informační bezpečnosti, jejímž cílem je chránit kyberprostor (tj. sítě, intranety, servery, informační a počítačové systémy a infrastrukturu) před neoprávněným přístupem, kybernetickými útoky nebo poškozením. Kybernetická bezpečnost se zaměřuje na ochranu informací v elektronické/digitální podobě umístěných v počítačích, úložištích a sítích (v kyberprostoru).

Digitální bezpečnost vs. kybernetická bezpečnost vs. informační bezpečnost: Bezpečnost informací: chrání informace (v jakémkoli formátu a formě) a informační systémy před neoprávněným přístupem a použitím, aby bylo zajištěno a zachováno soukromí důležitých údajů. Kybernetická bezpečnost: chrání celé sítě a komunikační systémy, počítačové systémy a další digitální komponenty a v nich uložená digitální data. Digitální bezpečnost: chrání online přítomnost (identitu a související citlivé informace, aktiva.

Osvědčené postupy: Je to osvědčená metoda nebo postup, který nabízí nejefektivnější řešení v dané oblasti, který prokazatelně vede k optimálním výsledkům a je zaveden (navržen) jako vhodný standard pro široké přijetí. V oblasti digitální bezpečnosti se jedná o definované postupy pro zajištění ochrany jednotlivce/organizace v digitálním prostoru (např. doporučené techniky, programy, návody, manuály).

2 Digitální pohoda

2.1 Co je to Wellbeing?

Termín **"wellbeing"** popisuje stav, kdy je člověk spokojený, radostný a zdravý. Zahrnuje fyzickou, duševní a emocionální pohodu člověka a další oblasti jeho existence. Kromě toho, že člověk nemá žádné nemoci nebo potíže, se well-being zaměřuje na celkové štěstí a kvalitu života.

Fyzická pohoda je stav těla, který zohledňuje například fyzickou zdatnost, stravu a absenci nemocí nebo chorob. Zahrnuje udržování zdravého životního stylu prostřednictvím soustavného cvičení, výživné stravy, dostatku spánku a zvládání stresu.

Kognitivní a emocionální zdraví člověka souvisí s jeho duševní pohodou. Zahrnuje dobré vyhlídky, prožívání spokojenosti a schopnost zvládat stres a životní obtíže. K duševní pohodě mohou přispět činnosti, jako je cvičení pozornosti, věnování se koníčkům, požádání blízkých o podporu a v případě potřeby vyhledání odborné pomoci.

Dobré pochopení a schopnost ovládat své emoce se označuje jako **emoční pohoda.** Zahrnuje pěstování odolnosti, udržování dobrých vztahů a pozitivní vnímání sebe sama. K emoční pohodě přispívá sebeuvědomění, kontrola emocí, účinná komunikace a rozvoj podpůrných vztahů.

Součástí sociální pohody je i kvalita vztahů a **pocit sounáležitosti se společenstvím.** Zahrnuje pěstování trvalých vazeb s blízkými osobami, blízkými přáteli a širší sociální sítí. Účast na společenských aktivitách, přispívání komunitě a udržování pocitu spojení a sounáležitosti mohou zlepšit sociální pohodu.

Celkově je **pohoda komplexní myšlenkou**, která zohledňuje vzájemnou provázanost různých aspektů života člověka. Zahrnuje aktivní snahu o vyváženou a uspokojivou existenci, péči o tělesné a duševní zdraví, pěstování zdravých vztahů a hledání smyslu života.

2.2 Dobré životní podmínky a digitalizace

Technologie a digitalizace mají potenciál zlepšit blahobyt tím, že umožňují komunikaci, zvyšují efektivitu a zlepšují přístup k informacím. Pro řízení používání digitálních technologií, ochranu soukromí a bezpečnosti a dosažení správné rovnováhy mezi technologiemi a ostatními aspekty života je zásadní uvědomit si možné nevýhody a přijmout nezbytná opatření.

Technologie a digitalizace výrazně zlepšily přístup k informacím a službám, což má pozitivní vliv na blahobyt. Lidé mají nyní snadný přístup k digitálním nástrojům pro osobní rozvoj, informacím o zdravotní péči, online podpůrným skupinám a vzdělávacím zdrojům. Díky bezproblémové komunikaci a spojení na dálku technologie podporují sociální vazby a snižují pocity osamělosti. Lidé mohou být v kontaktu s přáteli, rodinou a komunitami díky digitálním platformám, sociálním médiím a aplikacím pro zasílání zpráv, které zlepšují sociální blaho. Mnoho aspektů života se díky digitalizaci stalo efektivnějšími a pohodlnějšími. Díky využívání digitálních nástrojů a služeb lze nyní úkoly, které dříve vyžadovaly mnoho času a úsilí, vyřídit rychle a bez námahy. To může přispět k obecnému blahobytu tím, že se uvolní čas a sníží stres. Digitální schopnosti jsou navíc s rozvojem technologií na pracovním trhu stále důležitější. Získáním a využíváním těchto schopností lze zlepšit zaměstnatelnost a socioekonomický blahobyt člověka. Digitální propast, která vzniká, když někteří lidé nebo skupiny nemají přístup k technologiím nebo nemají dostatečnou digitální gramotnost, může nicméně prohloubit již existující rozdíly.

Nesprávné nebo nadměrné používání technologií může mít škodlivé účinky na duševní zdraví, ale může mít i dobré účinky. Úzkost, zoufalství a nízké sebevědomí mohou být ovlivněny přílišným množstvím času stráveného u obrazovky, srovnáváním se sociálními médii a zneužíváním internetu. Pro ochranu duševního zdraví je zásadní udržovat zdravou rovnováhu a praktikovat uvědomělé používání technologií. Digitální prostředí má také určité problémy se soukromím a bezpečností. Kybernetické hrozby, úniky dat a online podvody mohou ohrozit finanční bezpečnost a osobní údaje lidí. Zachování celkového blahobytu v digitálním věku vyžaduje ochranu digitální bezpečnosti a soukromí.

2.3 Co je to digitální pohoda?

Rozvoj digitální odolnosti a přijetí bezpečnostních postupů vedou ke stavu optimálního zdraví a celkové pohody v digitální sféře, který se označuje jako digitální pohoda. **Digitální pohoda** vychází z konceptu blahobytu a souvisí s digitálním životem jednotlivců. Schopnost lidí přizpůsobit se, zvládat a prosperovat v digitálním světě a zároveň úspěšně řídit jak svou pohodu, tak bezpečnost se označuje jako digitální odolnost, která je kombinací digitální pohody a bezpečnosti. Základním kamenem digitální odolnosti je digitální pohoda, která klade důraz na zachování pozitivního a rozumného vztahu k technologiím. Zahrnuje omezení času stráveného u obrazovky, vysokou prioritu duševního a emocionálního zdraví, vytváření podpůrných online komunit a učení se digitální gramotnosti. V kontextu pohody pomáhá digitální odolnost lidem zvládat potíže online, jako je kyberšikana, online obtěžování nebo vystavení nebezpečnému obsahu, a zároveň zachovat jejich celkovou pohodu. Jednotlivci si mohou vybudovat silnou digitální odolnost, která jim umožní pohybovat se v digitálním světě s jistotou a odpovědností, a to díky integraci digitální pohody s digitální bezpečností. Jsou schopni lépe zvládat výzvy digitálního světa, přizpůsobovat se měnícím se nebezpečím, dělat moudré závěry, chránit své osobní údaje a udržovat si při používání internetu duševní, emocionální a fyzické zdraví. Digitální odolnost v konečném důsledku podporuje bezpečnější, zdravější a plnohodnotnější online zkušenosti lidí. digitální odolnost pomáhá lidem zvládat online obtíže, jako je kyberšikana, online obtěžování nebo vystavení nebezpečnému obsahu, a zároveň zachovává jejich celkovou pohodu. Jednotlivci si mohou vybudovat silnou digitální odolnost, která jim umožní pohybovat se v digitálním světě s jistotou a odpovědností, a to díky integraci digitální pohody s digitální bezpečností.

2.3.1 Duševní zdraví, pohoda a digitální pohoda

Celá kvalita našeho života je ovlivněna hlubokými souvislostmi mezi naším duševním zdravím a celkovou pohodou. Naše psychická a emocionální pohoda, včetně aspektů, jako jsou naše myšlenky, pocity a chování, se označuje jako duševní zdraví. Má zásadní význam pro naše celkové zdraví, je stejně důležité jako tělesná pohoda. Naopak pohoda je komplexní stav rovnováhy, naplnění a spokojenosti v životě. Vztah mezi nimi vychází z toho, že duševní zdraví člověka má významný vliv na jeho fyzické zdraví a naopak. Naše celková pohoda se zvyšuje, když pěstujeme pozitivní duševní zdraví zvládáním stresu, překonáváním překážek a budováním zdravých vztahů, což vede k plnějšímu a smysluplnějšímu životu. Na druhou stranu pocit pohody může výrazně zlepšit duševní zdraví tím, že podporuje odolnost, emoční stabilitu a vyšší schopnost vyrovnat se s životními výzvami. Šťastný a prosperující život si můžeme vytvořit tím, že se zaměříme na vztah mezi naším duševním zdravím a pohodou.

Vzhledem k rychlému zdokonalování technologií a jejich všudypřítomné integraci do našeho každodenního života nabývá duševní zdraví v digitálním věku komplexní a dynamické povahy. V kontextu digitálního věku se duševní a emocionální pohoda člověka označuje jako "digitální duševní zdraví". Zahrnuje soci-

ální média, online interakce, psychologické účinky digitálních technologií a neustálé propojení, které definuje moderní život. Přestože technologie přinesly mnoho výhod a příležitostí, vytvořily také značné potíže pro duševní zdraví. Navzdory neustálému virtuálnímu kontaktu může digitální věk vést k problémům, jako je závislost na internetu, kyberšikana, informační přetížení, sociální srovnávání a pocity izolace. Poskytuje však také nejmodernější přístupy ke zvládání duševního zdraví, jako jsou aplikace pro duševní zdraví, online terapie a virtuální podpůrné skupiny. Při procházení spletitostí digitálního věku je nezbytné udržovat zdravou rovnováhu mezi online a offline životem, uvědomovat si, kolik digitálních médií konzumujeme, a aktivně vyhledávat digitální nástroje, které mohou zlepšit naši duševní pohodu, a zároveň se chránit před možnými nástrahami.

V současnosti existuje složitý vztah mezi duševním zdravím a digitální pohodou. Psychická a emocionální pohoda jednotlivců, která zahrnuje faktory, jako jsou nálada, myšlenky, pocity a chování, se označuje jako jejich duševní zdraví. Na druhé straně digitální pohoda popisuje rovnováhu a harmonii, kterou člověk pociťuje při používání technologií a zapojení do digitálních vztahů. Digitální éra přináší mnoho výhod, umožňuje konektivitu, přístup k informacím a šance na osobní rozvoj. Nadměrné používání technologií, neustálá oznámení, tlak sociálních médií a informační přetížení však mohou mít negativní dopad na duševní zdraví tím, že způsobují napětí, obavy a pocit odtržení od reality. Na druhou stranu může mít příznivý dopad na duševní zdraví, pokud je digitální pohoda upřednostňována stanovením limitů, pravidelnými přestávkami od obrazovek a pozorností vůči digitální spotřebě. Za účelem podpory duševního zdraví i digitální pohody a zaručení harmonického soužití mezi naším virtuálním a reálným životem je nezbytné nastolit zdravou rovnováhu mezi digitálním zapojením a offline aktivitami. Smysluplnějšího a vyváženějšího života v digitálním věku lze dosáhnout vědomým využíváním technologií a digitálních nástrojů k posílení duševního zdraví.

2.3.2 Proč potřebujeme digitální pohodu?

Klíčovými faktory digitální pohody jsou kvalita života, komunikace, produktivita a úspěch, duševní a fyzické zdraví. Protože zahrnuje celkový stav člověka, který je zdravý, šťastný a spokojený, je digitální pohoda důležitá. Vztahuje se k celkovému zdraví lidí a komunit a zohledňuje jejich sociální, psychické a fyzické aspekty. Nadměrné nebo nezdravé používání mobilních telefonů, sociálních médií a videoher může být škodlivé pro duševní zdraví. Úzkost, zoufalství, osamělost a nízké sebevědomí mohou být zhoršeny nadměrným časem stráveným u obrazovky, častým srovnáváním s ostatními na sociálních sítích nebo kyberšikanou. V tomto ohledu je digitální pohoda způsobem, jak mít kontrolu nad vlastním životem. Pro dobré duševní zdraví a digitální pohodu je zásadní mít zdravý vztah k technologiím. Součástí toho může být nastavení limitů pro používání gadgetů, zapojení do digitálního detoxu, účast na offline aktivitách a upřednostňování péče o sebe a osobních interakcí. Musíme si být vědomi dopadu, který mají digitální technologie na naše duševní zdraví, a přijmout proaktivní opatření k zajištění jejich rozumného používání.

Digitální pohoda se v digitálním věku stala základní lidskou potřebou, zejména v souvislosti s pandemií Covid-19. Naše závislost na digitálních platformách vzrostla, protože technologie stále pronikají do všech oblastí našeho každodenního života, od komunikace a vzdělávání až po zaměstnání a zábavu. Epidemie způsobila, že digitalizace postupuje nebývalým tempem, vyžaduje práci na dálku, online školství a více virtuálních vztahů. V důsledku toho je udržování naší digitální pohody zásadní pro vedení plnohodnotného a zdravého života. V tomto rychle se měnícím **digitálním prostředí** můžeme technologie využívat svědomitě a zodpovědně, abychom zajistili, že budou náš život spíše zlepšovat, než aby ohrožovaly naši celkovou pohodu, a to tak, že digitální pohodu uznáme jako základní lidskou potřebu.

2.3.3 Dobrá a špatná digitální pohoda

Digitální wellbeing je komplexní pojem, který zahrnuje řadu aspektů z digitálního světa. Zabývá se tím, jak jsou jednotlivci fyzicky, psychicky a sociálně zdraví a jednak se cítí digitálně uvědomělí, vyrovnaní, v bezpečí, spokojení a zdraví. Jak je vidět, význam připisovaný pojmu "digitální pohoda" směřuje většinou k příznivé stránce digitalizace, která odkazuje na dobrou digitální pohodu. Naopak jednotlivci, kteří zažívají nedostatek digitální pohody, odkazují na špatnou digitální pohodu. S ohledem na tuto skutečnost lze tvrdit, že mezi hlavní ukazatele dobré digitální pohody patří následující aspekty:

- Digitální bezpečnost: Zajištění digitální bezpečnosti významně přispívá k digitální pohodě člověka. Zahrnuje ochranu vaší online přítomnosti, včetně vaší identity, dat a aktiv.
- Digitální bezpečnost: Zahrnuje povědomí jednotlivců o potenciálních rizicích v digitálním světě a souvisí se schopností jednotlivců kriticky identifikovat a zvládat různé hrozby v digitálním prostředí.
- Digitální rovnováha: Týká se cílevědomého využívání technologií a digitálního světa. Digitální rovnováha má co do činění s využíváním digitálního světa, digitálních nástrojů a vybavení pro oblasti života, nikoli pro všechno. Pravidelná a konzistentní rovnováha online/offline a vyhýbání se přílišné závislosti na technologiích jsou známkami dobré digitální rovnováhy.
- Digitální nezávislost: Je to schopnost kontrolovat čas strávený online a vyhnout se tomu, aby se digitální svět soustředil na každodenní život. Trávení příliš mnoho času online a plánování méně společenských aktivit kvůli nadměrnému používání internetu jsou některé známky digitální závislosti.
- Digitální spokojenost: Týká se dosažení spokojenosti a pocitu potěšení při používání digitálních nástrojů a vybavení a propojení s technologiemi.
- Digitální příležitosti: Zabývá se využíváním technologií a digitalizace s cílem otevřít nové možnosti související s šířením digitálních technologií a získat nové kompetence pro vytváření nových příležitostí.
- Kritické a odpovědné používání technologií: Technologie spolu se svými příležitostmi vyžadují, aby uživatelé jednali zodpovědně a chránili svá vlastní práva a respektovali práva ostatních, jednali odpovědně a obezřetně a kriticky přemýšleli o jakémkoli obsahu v digitálním světě.

Tyto aspekty by také mohly být považovány za jeden z dimenzí digitálního blahobytu. Pokud má někdo relativně vyšší úroveň digitálního zabezpečení, bezpečnosti, rovnováhy, nezávislosti, spokojenosti, příležitostí a/nebo kritického a odpovědného používání technologií při používání digitálních nástrojů a zařízení, může být považován za osobu s dobrým digitálním blahobytem. Naopak, pokud někomu chybí některé z výše uvedených složek, znamená to, že má špatnou digitální pohodu. Je třeba si uvědomit, že fyzicky, psychicky a sociálně zdravý člověk také odkazuje na dobrou digitální pohodu a další aspekty mohou potenciálně přispět k digitální pohodě jednotlivců a celkové pohodě.

2.3.4 Podpora digitálního blahobytu jednotlivců: potenciální zisky pro všechny a pro vzdělávání dospělých

Podpora digitální pohody ve vzdělávání dospělých nebo posílení pohody dospělých a digitální pohody poskytuje mnoho příležitostí. Blahobyt je v první řadě základní lidskou potřebou. Zejména po pandemii COVID-19 tráví většina lidí mnohem více času online a jsou více vystaveni technologiím a jejich rizikům a

hrozbám. Ať už si to lidé záměrně přejí nebo ne, vnášejí do práce celé své já, konkrétně je zde jasná souvislost mezi vlastní pohodou lidí a atmosférou v pracovním prostředí. Potenciální opatření na podporu blahobytu a digitální pohody jednotlivců tedy přispívají jak k nim jako lidským bytostem, tak k organizacím, pro které pracují. Z organizačního hlediska podpora digitální pohody pracovníků přispívá, ale neomezuje se pouze na výkonnost týmu, odhodlání, inovace a spokojenost. Digitální pohoda umožňuje jednotlivcům stát se soustředěnějšími, angažovanějšími a produktivnějšími, což přispívá ke zdravějšímu životu v pracovním prostředí i mimo něj. Osvojení si digitálních wellness postupů zaměstnancům umožňuje být méně vyčerpaní a rozptýlení. Podpora podpůrných opatření pro digitální pohodu posiluje rovnováhu mezi pracovním a soukromým životem jednotlivců. Kromě toho eliminuje negativní dopady nadměrného vystavení digitalizaci, což umožňuje zažívat méně úzkosti, zoufalství, stresu a tak dále.

Myšlenka well-beingu v kontextu vzdělávání dospělých přesahuje konvenční představy o akademických úspěších a zahrnuje celkové zdraví a naplnění studentů. Koncept "digitální pohody" nabyl na významu s příchodem digitální éry, zejména pro digitální nomády, kteří se při mobilním životním stylu do značné míry spoléhají na technologie. Ve vzdělávání dospělých se termín "digitální well-being" vztahuje k tomu, že studentům poskytuje schopnosti a informace, které potřebují k rozumnému a etickému používání internetu.

Úspěšná integrace digitální pohody do vzdělávání dospělých vyžaduje pečlivou a důkladnou strategii, protože se jedná o složitý a neustálý proces. Prvním a nejdůležitějším krokem je poskytnout dospělým účastníkům vzdělávání školení, aby si byli vědomi hodnoty digitální pohody a toho, jak ovlivňuje jejich celkové zdraví a produktivitu. Díky této výuce získají potřebné praktické dovednosti, aby se mohli rozumně a bezpečně orientovat v digitálním světě. Druhou fází je úprava učebních materiálů tak, aby osnovy odrážely koncepty digitální pohody. To zahrnuje začlenění myšlenek, jako je kontrola digitálních rušivých vlivů, soukromí online, digitální etiketa a digitální gramotnost. Dospělí studenti mohou lépe pochopit výhody a nevýhody technologií a naučit se, jak je efektivně používat, začleněním těchto funkcí do kurzů. Je vytvořeno podpůrné prostředí, kde mohou studenti sdílet zkušenosti, vyměňovat si techniky a znovu potvrzovat svůj závazek k digitální pohodě tím, že navrhují další akce na podporu posílení, jako jsou semináře a rozhovory. Aby bylo vzdělávání dospělých relevantní a účinné při podpoře dobrých životních podmínek v digitální éře, musí se neustále vyvíjet, aby udrželo krok s rychle se měnícím digitálním prostředím. Aby bylo vzdělávání dospělých relevantní a účinné při podpoře dobrých životních podmínek v digitální éře, musí se neustále vyvíjet, aby udrželo krok s rychle se měnícím digitálním prostředím.

3 Digitální zabezpečení

3.1 Digitální bezpečnost a kybernetická bezpečnost

Podle Organizace pro hospodářskou spolupráci a rozvoj (OECD) je **digitální bezpečnost** zásadní pro důvěru v digitálním věku. OECD od počátku 90. let 20. století usnadňuje mezinárodní spolupráci a vypracovává politické analýzy a doporučení v oblasti digitální bezpečnosti. Cílem práce v této oblasti je rozvíjet a podporovat politiky, které posilují důvěru, aniž by omezovaly potenciál informačních a komunikačních technologií (ICT) podporovat inovace, konkurenceschopnost a růst. Digitální bezpečnost se týká ekonomických a sociálních aspektů kybernetické bezpečnosti, na rozdíl od čistě technických aspektů a aspektů souvisejících s vymáháním trestního práva nebo národní a mezinárodní bezpečností. Pojem "digitální" je v souladu

s výrazy, jako jsou digitální ekonomika, digitální transformace a digitální technologie. Tvoří základ pro konstruktivní mezinárodní dialog mezi zúčastněnými stranami, které usilují o posílení důvěry a maximalizaci příležitostí plynoucích z informačních a komunikačních technologií[1].

Digitální bezpečnost a kybernetická bezpečnost spolu souvisejí, ale nejsou totožné. Obě zahrnují ochranu digitálních aktiv a informací před neoprávněným přístupem, použitím nebo poškozením, ale liší se rozsahem a zaměřením.

Digitální bezpečnost označuje praxi ochrany digitálních dat, informací a aktiv před neoprávněným přístupem, krádeží nebo poškozením. Zahrnuje širší škálu bezpečnostních opatření, která chrání data a informace na různých digitálních platformách a zařízeních, včetně počítačů, chytrých telefonů, tabletů a dalších digitálních technologií.

Digitální bezpečnostní opatření mohou zahrnovat:

- Ochrana heslem: Vytváření silných a jedinečných hesel pro online účty a zařízení.
- Šifrování dat: Šifrování dat, které zabraňuje neoprávněnému přístupu nebo narušení dat.
- Zabezpečená komunikace: Používání šifrovacích protokolů pro bezpečný přenos dat.
- Řízení přístupu: Zavedení oprávnění a omezení pro omezení přístupu k citlivým datům.
- Zabezpečení zařízení: Využití funkcí, jako je zámek obrazovky a vzdálené vymazání ztracených nebo odcizených zařízení.

Kybernetická bezpečnost je podmnožinou digitální bezpečnosti a zaměřuje se konkrétně na ochranu digitálních aktiv před kybernetickými hrozbami a útoky. Zahrnuje obranu proti neoprávněnému přístupu, poškození nebo narušení digitálních systémů, sítí a infrastruktur.

Opatření kybernetické bezpečnosti mohou zahrnovat:

- Ochranu firewallem: Nastavení bariér, které brání neoprávněnému přístupu do sítě.
- Systémy detekce narušení: Monitorování sítí z hlediska podezřelých aktivit a potenciálních hrozeb.
- Ochrana proti malwaru: Použití antivirového softwaru k detekci a odstranění škodlivého softwaru.
- Plánování reakce na incidenty: Vypracování protokolů pro účinnou reakci na kybernetické bezpečnostní incidenty.
- Zpravodajství o kybernetických hrozbách: Shromažďování a analýza informací za účelem předvídání kybernetických hrozeb a jejich prevence.

Digitální bezpečnost zahrnuje širší škálu postupů, které chrání data a informace v digitální oblasti, zatímco kybernetická bezpečnost je specializovaná oblast zaměřená na obranu proti kybernetickým hrozbám a útokům v digitálních systémech a sítích. Obě tyto oblasti představují klíčové součásti pro zajištění celkové bezpečnosti a ochrany digitálních aktiv a informací.

[1] HTTPS://WWW.OECD.ORG/DIGITAL/DIGITAL-SECURITY/

3.2 Kybernetické bezpečnostní hrozby, kterým čelí dospělí

Dospělí čelí v dnešním digitálním světě široké škále kybernetických bezpečnostních hrozeb. Zde jsou uvedeny některé běžné hrozby kybernetické bezpečnosti, se kterými se dospělí často setkávají:

- **Phishingové útoky:** Phishing je technika, kterou kyberzločinci používají k tomu, aby jednotlivce přiměli k poskytnutí citlivých informací, jako jsou přihlašovací údaje, čísla kreditních karet nebo osobní údaje. Phishingové e-maily, zprávy nebo webové stránky se mohou tvářit jako z důvěryhodných zdrojů, ale jejich cílem je oklamat uživatele a přimět ho, aby prozradil své údaje.
- **Malware:** Malware je škodlivý software určený k infiltraci, poškození nebo získání neoprávněného přístupu do počítačových systémů. Mezi typy malwaru patří viry, ransomware, spyware a trojské koně. Malware se může šířit prostřednictvím škodlivých e-mailových příloh, infikovaných webových stránek nebo napadeného softwaru.
- **Krádež identity:** Kyberzločinci mohou ukrást osobní údaje, jako jsou čísla sociálního pojištění, data narození nebo finanční údaje, a spáchat tak krádež identity. Tyto informace jsou často získávány prostřednictvím úniků dat nebo pokusů o phishing.
- **Online podvody:** Existuje mnoho online podvodů zaměřených na dospělé, například podvody s loteriemi, milostné podvody, podvody s falešnou technickou podporou a podvodné investiční programy. Podvodníci používají různé taktiky, aby jednotlivce zmanipulovali k zaslání peněz nebo poskytnutí osobních údajů.
- **Úniky dat:** K narušení bezpečnosti údajů dochází, když jsou odhaleny nebo odcizeny citlivé informace, které mají společnosti nebo organizace k dispozici. Jako dospělý člověk můžete být únikem dat postiženi, pokud jsou vaše osobní údaje uloženy v dotčených subjektech.
- **Sociální inženýrství:** Sociální inženýrství zahrnuje manipulaci osob, aby sdělily důvěrné informace nebo provedly určité akce. Kyberzločinci mohou používat techniky sociálního inženýrství k získání neoprávněného přístupu do systémů nebo účtů.
- **Útoky na hesla:** Slabá hesla nebo opakované používání hesel mohou vést k útokům na hesla, jako jsou útoky hrubou silou nebo slovníkové útoky, kdy se kyberzločinci pokoušejí uhodnout nebo prolomit hesla, aby získali neoprávněný přístup.
- **Rizika spojená s veřejnou sítí Wi-Fi:** Používání veřejných sítí Wi-Fi může dospělé vystavit bezpečnostním rizikům, protože tyto sítě mohou být nedostatečně šifrované a náchylné k odposlechu ze strany útočníků.
- **Hrozby zevnitř:** Vnitřní hrozby zahrnují zaměstnance nebo osoby s oprávněným přístupem k systémům nebo datům, kteří úmyslně nebo neúmyslně způsobí škodu nebo únik citlivých informací.
- **Zranitelnosti internetu** věcí: Rostoucí rozšíření zařízení internetu věcí (IoT) může vytvářet rizika pro kybernetickou bezpečnost, protože mnohá z těchto zařízení mohou mít nedostatečná bezpečnostní opatření a mohou být zneužita kyberzločinci.

Dospělí by měli dodržovat zásady kybernetické bezpečnosti, včetně používání silných a jedinečných hesel, vícefaktorového ověřování, aktualizace softwaru a zařízení, obezřetnosti vůči podezřelým e-mailům a odkazům a obezřetnosti vůči informacím, které sdílejí online. Pravidelná školení o kybernetické bezpečnosti mohou také pomoci jednotlivcům zůstat informováni o nových hrozbách a osvědčených postupech, jak zůstat v bezpečí online. V následující části jsou podrobně představeny některé nejdůležitější postupy

digitální bezpečnosti pro dospělé, které snižují riziko, že se stanou obětí kybernetických hrozeb, a chrání jejich digitální identitu a majetek.

3.3 Digitální bezpečnostní postupy pro dospělé

Digitální bezpečnostní postupy jsou pro dospělé zásadní, aby mohli chránit své osobní informace, data a online účty před kybernetickými bezpečnostními hrozbami. Zde jsou uvedeny některé důležité postupy digitálního zabezpečení, které by dospělí měli dodržovat:

- **Používejte silná a jedinečná hesla:** Dospělí by si měli pro své online účty vytvářet silná a jedinečná hesla. Vyvarujte se používání snadno uhodnutelných hesel, jako je "123456" nebo "heslo". Zvažte používání správce hesel, který umožňuje bezpečně generovat a ukládat složitá hesla.
- **Zapněte vícefaktorové ověřování (MFA):** Pokud je to možné, zapněte na svých online účtech vícefaktorové ověřování. MFA přidává další vrstvu zabezpečení tím, že kromě hesla vyžaduje i druhou formu ověření, například jednorázový kód zaslaný na mobilní zařízení.
- **Udržujte software a zařízení aktualizované:** Pravidelně aktualizujte operační systém, webové prohlížeče a softwarové aplikace. Aktualizace často obsahují bezpečnostní záplaty, které řeší známé zranitelnosti.
- **Buďte obezřetní u e-mailů a odkazů:** Při otevírání e-mailů od neznámých odesílatelů nebo klikání na podezřelé odkazy buďte opatrní. Obzvláště opatrní buďte u e-mailů, které požadují citlivé informace nebo vás přesměrují na přihlášení na falešné webové stránky.
- **Zabezpečte svou domácí síť:** Změňte výchozí heslo na domácím směrovači Wi-Fi a zapněte šifrování WPA2 nebo WPA3, abyste ochránili svou bezdrátovou síť. Vyhněte se používání veřejných sítí Wi-Fi pro citlivé činnosti, pokud nepoužíváte virtuální privátní síť (VPN).
- **Pravidelně zálohujte data:** Pravidelně zálohujte důležité soubory a data na externí pevný disk, do cloudového úložiště nebo na zabezpečenou zálohovací službu. V případě ztráty dat nebo útoku ransomwaru vám zálohování zajistí, že budete moci své soubory obnovit.
- **Používejte zabezpečenou Wi-Fi a HTTPS:** Při přístupu na citlivé webové stránky se ujistěte, že používají šifrování HTTPS. V adresním řádku prohlížeče hledejte symbol visacího zámku, abyste si ověřili zabezpečení webové stránky.
- **Dávejte pozor na sociální média:** Buďte obezřetní, pokud jde o informace, které sdílíte na platformách sociálních médií. Vyvarujte se zveřejňování osobních údajů, jako je vaše adresa, telefonní číslo nebo cestovní plány, protože tyto informace mohou být zneužity k útokům sociálního inženýrství.
- **Nainstalujte si antivirový a bezpečnostní software:** Používejte na svých zařízeních renomovaný antivirový a bezpečnostní software, který vás ochrání před malwarem a dalšími hrozbami. Udržujte software aktualizovaný, abyste zajistili optimální ochranu.
- **Vzdělávejte se v oblasti kybernetické bezpečnosti:** Informujte se o nejnovějších hrozbách kybernetické bezpečnosti a osvědčených postupech čtením renomovaných zdrojů, účastí na webových seminářích nebo v programech pro zvyšování povědomí o kybernetické bezpečnosti (viz dostupné zdroje o digitální bezpečnosti pro dospělé).

Začleněním těchto postupů digitální bezpečnosti do každodenní rutiny mohou dospělí výrazně snížit riziko, že se stanou obětí kybernetických bezpečnostních hrozeb, a ochránit svou digitální identitu a majetek.

3.4 Zdroje digitální bezpečnosti dostupné pro dospělé

Středisko pro vzdělávání v oblasti kybernetické bezpečnosti (CEH)[2] na Kalifornské státní univerzitě v San Marcosu nabízí zdroje a pokyny pro snahy kampusu a komunity o zvýšení vzdělávání a povědomí o digitální bezpečnosti. CEH je společným úsilím kanceláře pro informační bezpečnost kampusu, vysokých škol pro vědu a matematiku a obchodní administrativu.

CEH se snaží zajistit, aby se vzdělávací programy v oblasti digitální bezpečnosti na univerzitě zabývaly širokými otázkami souvisejícími s aktuálním děním v oblasti digitální bezpečnosti, a poskytuje příležitosti k začlenění témat digitální bezpečnosti do kurzů vyučovaných na celé univerzitě. CEH také nabízí zdroje studentům, studentským organizacím a široké veřejnosti. Podporuje a usnadňuje komunikaci a spolupráci se vzděláváním v oblasti digitální bezpečnosti v celé komunitě. Poskytla výukové materiály k tématům, jako je soukromí a sociální média, kybernetická bezpečnost pro studenty, kybernetická bezpečnost v současnosti a koncepty kybernetické bezpečnosti.

Kromě toho byly v roce 2008 představeny školicí materiály agentury ENISA[3] týkající se kybernetické bezpečnosti. Od té doby byly rozšířeny o nové oddíly obsahující zásadní informace pro úspěch v oblasti kybernetické bezpečnosti. ENISA obsahuje školicí materiály, jako jsou příručky pro učitele, sady nástrojů pro studenty a virtuální snímky, které doplňují praktická školení.

4 Osvědčené postupy budování digitální bezpečnosti pro dospělé

Digitální bezpečnost je v naší propojené společnosti stále důležitější a starší lidé jsou jednou z nejzranitelnějších skupin online. S rozvojem technologií se zvyšují i kybernetické hrozby. Je proto důležité zavést opatření a pokyny na ochranu starších dospělých v digitálním prostředí. Níže uvádíme několik osvědčených postupů a úspěšných opatření zavedených v několika zemích, které mohou sloužit jako reference pro ostatní.

Strategie kybernetické bezpečnosti Evropské unie zastoupené ve zprávách, které jsou všechny k dispozici na oficiálních internetových stránkách Evropské komise a poskytují cenné poznatky o osvědčených postupech pro zlepšení digitální bezpečnosti v Evropě.

4.1 Klíčové otázky pro budování digitální bezpečnosti

Může se zdát, že tento oddíl je opakováním oddílu 3.3. Praktiky digitálního zabezpečení pro dospělé, ale obsahuje více reálných scénářů a příkladů.

[2] https://www.csusm.edu/cybersec-hub/index.html

[3] https://www.enisa.europa.eu/topics/training-and-exercises/trainings-for-cybersecurity-specialists/online-training-material

Silná hesla: Pomozte jim vytvořit silná a jedinečná hesla pro každý účet. Hesla musí být dlouhá a obsahovat velká a malá písmena, číslice a speciální znaky. Hesla musí být dlouhá (alespoň 8 znaků), obsahovat velká a malá písmena, číslice a speciální znaky. Nepoužívejte předvídatelné osobní údaje, jako jsou jména nebo data narození. Připomeňte jim, aby svá hesla nikomu nesdělovali a pravidelně je měnili.

Silným heslem může být například "P@ssw0rd2023!", které kombinuje velká písmena, malá písmena, číslice a speciální znaky. Vyvarujte se používání předvídatelných osobních údajů, jako jsou jména nebo data narození, například "John1980" nebo "MarySmith123".

Vzdělávání a osvěta: Informujte je o online rizicích a hrozbách, jako je phishing, malware a krádež identity. Pomozte jim pochopit, jak tyto situace rozpoznat a jak se jim vyhnout. Je důležité je poučit o online rizicích, jako je phishing (pokus o podvodné získání důvěrných informací), malware (škodlivý software) a krádež identity. Naučte se rozpoznat tyto varovné signály a vyhněte se tomu, abyste se dostali do těchto pastí. Vysvětlete možné negativní dopady a způsoby ochrany.

Vysvětlete například, že phishingové e-maily se mohou tvářit jako e-maily z legitimních zdrojů a vyzývat ke kliknutí na odkazy a zadání citlivých informací. Ukažte jim příklady podezřelých e-mailů a návod, jak je rozpoznat. Poskytněte informace o běžných typech škodlivého softwaru, jako jsou falešné antivirové programy nebo vyskakovací okna, a o tom, jak se jim vyhnout.

Dvoufaktorové ověřování (2FA): Pomozte jim zavést dvoufaktorové ověřování, kdykoli je to možné. To přidá vašim účtům další úroveň zabezpečení. Dvoufaktorové ověřování přidává další vrstvu zabezpečení. Pokud je to možné, pomozte jim tuto funkci na jejich účtech povolit. 2FA vyžaduje kromě standardního hesla další způsob ověření, například kód textové zprávy, autentikátor nebo otisk prstu.

Například po zadání hesla obdrží textovou zprávu s ověřovacím kódem, který musí zadat, aby získali přístup ke svému účtu. To přidává další vrstvu zabezpečení a ztěžuje přístup neoprávněných uživatelů k jejich účtům.

Bezpečné používání mobilních zařízení: Pomozte jim nastavit zámky obrazovky, rozpoznávání obličeje nebo otisky prstů pro ochranu jejich mobilních zařízení. Připomeňte jim, aby svá zařízení nesdíleli s lidmi, které neznají, a aby byli opatrní při stahování aplikací z nespolehlivých zdrojů.

Ukažte jim například, jak povolit PIN nebo použít otisk prstu k odemknutí smartphonu. Připomeňte jim, aby svá zařízení nesdíleli s lidmi, které neznají, a aby byli opatrní při stahování aplikací z nespolehlivých zdrojů.

Aktualizace softwaru: Ujistěte se, že vaše zařízení (počítače, tablety, chytré telefony) mají nainstalovány nejnovější bezpečnostní záplaty a aktualizace. Aktualizace často obsahují opravy známých zranitelností, takže udržování zařízení v aktuálním stavu je pomáhá chránit.

***Nakupování online*:** Připomeňte jim, aby nakupovali pouze na spolehlivých a bezpečných webových stránkách a používali bezpečné platební metody. Naučte je hledat zámek v adresním řádku a používat bezpečné platební metody, například kreditní karty s dodatečnými bezpečnostními opatřeními.

Bezpečné používání e-mailu: Upozorněte je na phishing a poraďte jim, aby neklikali na odkazy nebo nestahovali přílohy od neznámých odesílatelů. Upozorněte je na e-mailový phishing, kdy se podvodníci snaží získat citlivé informace tím, že se vydávají za legitimní odesílatele. Zdůrazněte, že je důležité neklikat na odkazy ani nestahovat přílohy z podezřelých e-mailů nebo od neznámých odesílatelů. Vyzývá vás, abyste si před odesláním důvěrných informací ověřili legitimitu e-mailů u odesílatele.

Sociální média: Pomozte jim upravit nastavení soukromí na jejich sociálních médiích, aby měli kontrolu nad tím, kdo vidí jejich příspěvky, a vyhnuli se sdílení citlivých osobních informací. Naučte je, aby na sociálních sítích nesdíleli veřejně citlivé informace, jako jsou telefonní čísla, adresy nebo finanční informace.

Proveďte je například nastavením soukromí na Facebooku, abyste omezili počet osob, které mohou zobrazovat jejich příspěvky, pouze na přátele. Zdůrazněte, že je důležité být opatrný při sdílení informací, jako jsou telefonní čísla, adresy nebo finanční údaje, na platformách sociálních médií.

Bezpečné procházení: Naučte se rozpoznávat tyto bezpečné webové stránky ("https" a "lock") a vyhněte se klikání na podezřelé odkazy nebo stahování neznámých souborů. Naučte je rozlišovat bezpečné webové stránky tak, že v adresním řádku zkontrolujete, zda na nich není zámek a zda jsou spuštěny. "http" místo "https". Vysvětlete, že je důležité vyhýbat se klikání na podezřelé odkazy nebo stahování souborů z neznámých zdrojů, protože mohou obsahovat malware nebo vás přesměrovat na podvodné webové stránky.

Zabezpečení sítě Wi-Fi: Ujistěte se, že v domácí síti Wi-Fi používají silná hesla a že se nepřipojují k veřejným nebo neznámým sítím Wi-Fi. Vysvětlete jim, že je důležité používat v domácí síti Wi-Fi silná hesla a nepřipojovat se k veřejným nebo neznámým sítím Wi-Fi. Nezabezpečené sítě Wi-Fi mohou být potenciálně napadeny nebo zachyceny za účelem špionáže dat.

Neaktivní účty: Pomozte jim zrušit nebo odstranit online účty, které již nepoužívají, abyste snížili bezpečnostní riziko. Neaktivní účty mohou být zranitelné vůči útokům, zejména pokud obsahují osobní údaje.

Pozor na podezřelé hovory a zprávy: Naučte je, aby na neočekávané telefonáty a zprávy nesdělovali osobní nebo finanční údaje. Naučte je, aby byli opatrní při sdělování osobních nebo finančních informací na nečekané hovory nebo textové zprávy. Vyzvěte odesílatele, aby si před sdělením citlivých informací ověřil svou totožnost. Uveďte například příklady běžných podvodů, jako jsou falešné telefonáty na technickou podporu nebo oznámení o výhře v loterii.

Dohled a podpora: Nabídněte jim pomoc při pravidelných kontrolách online účtů a pomoc v případě podezření na podezřelé aktivity nebo problémů s bezpečností. Udržujte si přehled o nejnovějších online hrozbách a poskytujte jim průběžné poradenství a podporu. Ukažte jim například, jak zkontrolovat jejich nedávnou aktivitu na účtu a přihlášení na různých platformách.

Osobní údaje: V případě, že se vám podaří získat osobní údaje, můžete se obrátit na tzv: Naučte je, aby byli opatrní při sdílení osobních informací online a aby omezili množství informací, které zveřejňují. Omezte množství informací, které zveřejňují, například adresy, telefonní čísla nebo informace o škole. Podpoří soukromí a důležitost ochrany své online identity.

Zálohujte důležitá data: Pravidelně zálohujte důležitá data, abyste zabránili jejich ztrátě v případě narušení bezpečnosti nebo selhání zařízení.

4.2 Osvědčené postupy ve světě

4.2.1 Kybernetická Evropa

Agentura ENISA pořádá od roku 2010 Cyber Europe[4] , sérii cvičení v oblasti kybernetických incidentů a krizového řízení, která obsahují zajímavé scénáře inspirované skutečnými událostmi a vypracované evropskými odborníky na kybernetickou bezpečnost. Každé dva roky spolupracují veřejný a soukromý sektor ze zemí EU a EHP a evropské instituce, orgány a agentury, aby posílily své stávající technické a operační schopnosti.

Cvičení Cyber Europe probíhá dva dny a simuluje rozsáhlé kybernetické bezpečnostní incidenty, které přerůstají v kybernetické krize s dopadem na celou EU. Účastníci tohoto cvičení budou schopni analyzovat pokročilé technické kybernetické bezpečnostní incidenty, řešit složité situace v oblasti kontinuity provozu a krizového řízení, které vyžadují koordinaci a spolupráci od místní úrovně až po úroveň EU.

Cílem série cvičení Cyber Europe je zlepšit připravenost Evropy na řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí tím, že účastníkům umožní otestovat a zlepšit jejich připravenost v celé EU, vybudovat důvěru v rámci ekosystému kybernetické bezpečnosti EU a poskytnout příležitosti ke školení.

Účast na konferenci Cyber Europe je skvělou příležitostí k:

- Zvyšování povědomí o kybernetické bezpečnosti
- Vytvořit a/nebo vyzkoušet postupy pro řešení kybernetických krizí
- Zlepšit komunikaci v rámci řetězce kybernetické reakce
- Vytvořit společný jazyk a zlepšit vzájemné porozumění
- Rozvíjet různé individuální a kolektivní schopnosti a dovednosti v oblasti odolnosti.
- Analyzovat složité technické kybernetické bezpečnostní incidenty; zvládat složité situace v oblasti kontinuity podnikání a krizového řízení.

4.2.2 Přizpůsobení rozhraní a technologie

Japonsko je průkopníkem v přizpůsobování technologií a zařízení tak, aby byly přístupnější starším lidem. Například některé japonské chytré telefony a tablety mají jednodušší uživatelské rozhraní a vylepšené funkce přístupnosti, což usnadňuje jejich používání lidem s omezenými digitálními dovednostmi.

[4] https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme

Ostatní země a výrobci technologií mohou přijmout taková opatření, aby zajistili, že starší lidé budou moci digitální zařízení používat bezpečně a efektivně. Přijetí těchto postupů jinými zeměmi a výrobci technologií může zajistit, že starší dospělí budou mít přístup k uživatelsky přívětivějším digitálním zařízením, což pomůže zlepšit jejich bezpečnost a účast na internetu.

Na evropském území existuje několik kurzů zaměřených na zvyšování povědomí o používání těchto nástrojů staršími lidmi. Například sdružení ACDA v Paříži nabízí levné kurzy, které starším lidem přibližují svět technologií. Kurzy tohoto sdružení nabízejí možnost naučit se od základů ovládat počítač. Objevování počítačových jednotek, aplikací, formátů souborů. Poté mohou účastníci získat pokročilejší dovednosti, jako je správa a organizace vlastní poštovní schránky a naučit se používat word, jak zpracovat písemný dokument[5].

4.2.3 Linky pomoci a specializovaná podpora

Singapur zřídil vlastní linku pomoci pro seniory, kteří se potýkají s problémy v oblasti digitální bezpečnosti. Tato linka důvěry nabízí poradenství a technickou pomoc při řešení problémů s kybernetickou bezpečností. Ostatní země mohou zvážit zavedení podobných služeb, aby poskytly přímý a bezpečný komunikační kanál pro seniory, kteří potřebují online pomoc. Tyto služby poskytují starším lidem přímý a bezpečný komunikační kanál pro získání pomoci při problémech s kybernetickou bezpečností, jako jsou například online podvody nebo malware. Zavedení podobných služeb v jiných zemích může být důležitou podpůrnou sítí pro ochranu starších lidí v digitálním světě.

Například na evropském území se sdružení AGE UK[6] prioritně zaměřuje na podporu starších lidí nejvíce ohrožených digitálním vyloučením.

Kromě poskytování služeb starší populaci se kurzy zaměřují konkrétně na pomoc vysoce rizikové skupině při přístupu do digitálního světa. Přestože základní složky programu zůstanou při práci s těmito vysoce rizikovými skupinami do značné míry nezměněny, bude pravděpodobně nutné provést určité úpravy, aby program zůstal dostupný a účinný pro ty, kteří jej nejvíce potřebují.

Vysoce rizikové služby v rámci programu Digitální šampion se zaměří na starší osoby, které:

- trpí demencí a/nebo ztrátou paměti
- mají nízký příjem
- žijí osaměle
- mají problémy s mobilitou
- jsou odkázáni na domácnost.

4.2.4 Osvětové kampaně a vzdělávání

Země, jako je Austrálie a Kanada, zavedly pro starší dospělé kampaně a vzdělávací programy v oblasti kybernetické bezpečnosti a digitální bezpečnosti. Tyto kampaně poskytují informace o běžných kybernetických hrozbách, tipy, jak se chránit před podvody na internetu, a o důležitosti aktualizace zařízení. Vlády mohou spolupracovat s místními organizacemi, komunitními centry a dobrovolnickými skupinami, aby oslo-

[5] http://www.aucoursdesages.fr/cours.php

6 https://www.ageuk.org.uk/our-impact/programmes/digital-skills/digital-champions/

vily starší obyvatele a poskytly jim školení o digitálních dovednostech. Cílem těchto informačních a vzdělávacích kampaní je posílit postavení starších lidí prostřednictvím vzdělávání v oblasti digitální bezpečnosti. Učí je, jak rozpoznat a vyhnout se podvodům na internetu, chránit své osobní údaje a používat bezpečnostní nástroje, jako jsou antivirové programy a silná hesla. Jsou také informováni o rizicích spojených s používáním sociálních médií a o důležitosti správného nastavení soukromí na internetu. Výše uvedená asociace ACDA v Paříži nabízí také kurzy digitální bezpečnosti.

Dalším sdružením, které se zaměřuje na digitální osvětu, je nadace Orange, která informuje křehké skupiny o nejnovějších technologiích a vede je k bezpečnějšímu používání digitálních technologií[7].

Kromě toho nadace Orange pořádá po celé Francii řadu bezplatných kurzů digitální výchovy pro mladé lidi a ženy, kteří jsou často nezaměstnaní, nemají kvalifikaci a někdy se nacházejí v nejistých situacích. Školením těchto lidí v digitálních dovednostech jim pomáhají znovu se socializovat, hledat si práci, osvojit si profesionální využití digitálních technologií, rozvíjet podnikání, nebo dokonce učinit digitální technologie svou profesí.

4.2.5 Programy finanční ochrany

Země jako Velká Británie a USA[8] zavedly politiky na ochranu důchodců před internetovými finančními podvody. Tyto politiky zahrnují limity odpovědnosti pro oběti podvodu a opravné prostředky k získání zpět odcizených finančních prostředků. Ostatní země mohou tyto iniciativy prozkoumat a přizpůsobit je svým finančním systémům, aby ochránily seniory před možnými finančními ztrátami. Finanční ochrana starších osob je důležitou součástí digitální bezpečnosti. Programy speciálně určené k prevenci a zmírnění finančních podvodů online mohou této populaci poskytnout vyšší úroveň bezpečnosti. Stanovení limitů odpovědnosti obětí podvodů a vytvoření mechanismů pro vymáhání odcizených peněz jsou kroky, které lze podniknout. Tato opatření nejen chrání finanční blaho starších dospělých, ale také vysílají jasný signál, že jejich blaho a finanční bezpečnost jsou brány vážně.

V Evropě je zásadním aspektem ochrany finančního blahobytu starších osob stanovení omezení odpovědnosti obětí podvodů. Pokud jsou oběti podvodu činěny odpovědnými za finanční ztráty, které utrpěly, může to vést k závažným důsledkům, včetně finančního zruinování a citového strádání. Zavedením politik, které stanoví přiměřené limity odpovědnosti, společnost uznává jedinečnou zranitelnost starších dospělých a snaží se zmírnit zátěž, která je na ně kladena. Toto opatření představuje záchrannou síť, která zajišťuje, aby starší dospělí nebyli nespravedlivě zatěžováni následky podvodných činností. Stanovení limitů odpovědnosti obětí podvodů je klíčovým aspektem ochrany finančního blahobytu starších osob. Na evropské půdě se ochraně starších osob, které se často stávají oběťmi podvodů na internetu, které nemají dostatečnou informovanost a mohou utrpět finanční ztráty, věnuje mnoho sdružení. Jedním z takových sdružení je Marketing Management IO (MMIO), certifikovaná agentura ve Španělsku a Francii[9].

Pokud jsou oběti podvodu pohnány k odpovědnosti za své finanční ztráty, může to mít závažné důsledky. Proto je důležitá informovanost. Zavedením politik, které stanoví přiměřené hranice odpověd-

[7] https://fondationorange.com/en/digital-solidarity

[8] https://www.bankofamerica.com/signature-services/elder-financial-services/

[9] https://www.marketing-management.io/blog/formation-digital-marketing

nosti, společnost uznává jedinečnou zranitelnost starších osob a snaží se jim ulehčit. Toto opatření poskytuje záchrannou síť a zajišťuje, aby starší osoby nebyly nespravedlivě zatíženy důsledky podvodných činností.

Marketingový management IO (MMIO) zahrnuje témata, jako jsou internetové příležitosti, přirozené odkazování, zviditelnění na internetu, obsahový marketing a zvyšování prodeje. Pojmy jsou zjednodušené a akce jsou zdarma. K dispozici jsou také bonusové zdroje.

Kurz obsahuje 5 lekcí s videi. Facebook nabízí platformu s bezplatným přístupem k více než 70 online kurzům. Tyto kurzy se zaměřují konkrétně na využití Facebooku ke zlepšení online prezentace a prodeje firmy, na bezpečnost a informovanost.

4.2.6 Spolupráce s technologickým průmyslem

Některé země, například Spojené státy, navázaly spolupráci s technologickými společnostmi, aby řešily problémy digitální bezpečnosti spojené se stárnutím populace. Tato spolupráce může zahrnovat zdokonalování bezpečnostního softwaru, zlepšování odhalování podvodů a zavádění bezpečnostních prvků do digitálních produktů a služeb. Spolupráce s technologickým průmyslem může být účinným způsobem, jak udržet krok s nejnovějšími bezpečnostními hrozbami a řešeními, jako je zavádění pokročilých bezpečnostních technologií, zlepšování odhalování podvodů a podpora bezpečnostních postupů u digitálních produktů a služeb určených pro starší osoby. Spolupráce s technologickým průmyslem zajišťuje rychlejší a aktuálnější reakci na digitální hrozby.

V jiných zemích, například ve Francii a Anglii, probíhají kurzy digitální bezpečnosti, které pomáhají starším lidem porozumět obranným technologiím; nabízené kurzy jim umožňují vybudovat si základy digitalizace a pochopit, jak se bezpečně pohybovat na internetu.

Například společnost Konexio[10] nabízí školení v oblasti digitálních dovedností – od těch nejzákladnějších až po nejpokročilejší – na podporu sociální a profesní integrace. Inovativní, založené na praktických případových studiích a s velkým důrazem na průřezové a vztahové dovednosti či měkké dovednosti, naše vzdělávací kurzy mají za cíl umožnit každému, aby se zapojil do digitalizace společnosti. Nabízejí různé formace: digitální dovednosti, webový designér, technik systémů a sítí, digitální pomocník. Program se zaměřuje na osvojení měkkých dovedností a sociálních kódů profesního světa prostřednictvím workshopů. Nabízí také možnosti přímého propojení s profesionálním světem prostřednictvím naší sítě. Nabízí pravidelnou následnou a individuální podporu, která našim žákům pomáhá dělat pokroky a řešit případné potíže.

4.2.7 Mezinárodní zdroje, zprávy a iniciativy

Tyto zdroje poskytují cenné pokyny a osvědčené postupy pro zlepšení digitální bezpečnosti ve vzdělávání dospělých v EU.

Otevřený, bezpečný a zabezpečený kyberprostor: Tato zpráva poskytuje přehled o strategii kybernetické bezpečnosti EU, jejímž cílem je podporovat otevřený, bezpečný a zabezpečený kyberprostor v Evropě. Zpráva obsahuje osvědčené postupy pro zlepšení kybernetické bezpečnosti, včetně řízení rizik, reakce na incidenty a partnerství veřejného a soukromého sektoru.

[10] https://www.konexio.eu/formations.html

Zpráva agentury ENISA o prostředí hrozeb: Tato zpráva Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) poskytuje přehled současného prostředí kybernetických hrozeb v Evropě, včetně nejčastějších typů kybernetických útoků a nejvíce ohrožených odvětví. Zpráva obsahuje osvědčené postupy pro prevenci a zmírnění kybernetických útoků, včetně školení o bezpečnostním povědomí, řízení zranitelností a plánování reakce na incidenty.

Směrnice o bezpečnosti sítí a informací a akt EU o kybernetické bezpečnosti: Tato zpráva poskytuje přehled právního rámce EU pro kybernetickou bezpečnost, včetně směrnice o sítích a informačních systémech a aktu EU o kybernetické bezpečnosti. Zpráva obsahuje osvědčené postupy pro dodržování zákonných požadavků, jako je hlášení incidentů a řízení rizik.

Rámec EU pro certifikaci kybernetické bezpečnosti: Tato zpráva poskytuje přehled rámce EU pro certifikaci kybernetické bezpečnosti, jehož cílem je zvýšit bezpečnost a důvěryhodnost digitálních produktů a služeb. Zpráva obsahuje osvědčené postupy pro získání a udržení certifikace kybernetické bezpečnosti, včetně zabezpečení již od návrhu, testování a hodnocení a průběžného monitorování a hodnocení.

Kybernetická bezpečnost pro malé a střední podniky: Tato zpráva obsahuje pokyny a osvědčené postupy pro malé a střední podniky (MSP), jak zlepšit jejich kybernetickou bezpečnost. Zpráva obsahuje rady týkající se řízení rizik, školení v oblasti povědomí o bezpečnosti, vývoje bezpečného softwaru a plánování reakce na incidenty.

Digitální dovednosti u dospělé populace: Tato zpráva Evropské komise poskytuje přehled digitálních dovedností dospělé populace v EU. Obsahuje oddíl o digitální bezpečnosti, který zdůrazňuje, že dospělí musí mít základní znalosti a dovednosti, aby se mohli chránit před kybernetickými hrozbami.

Digitální dovednosti pro celoživotní vzdělávání: Tato zpráva Evropské komise obsahuje pokyny a osvědčené postupy pro rozvoj digitálních dovedností dospělých. Obsahuje oddíl o digitální bezpečnosti, který poskytuje rady týkající se řízení rizik, bezpečného prohlížení, správy hesel a ochrany údajů.

Projekt Kybernetická bezpečnost pro digitální vzdělávání: Tento projekt sítě European Schoolnet poskytuje zdroje a školení o kybernetické bezpečnosti pro učitele a studenty v Evropě. Projekt zahrnuje řadu materiálů, včetně online kurzů, plánů výuky a hodnotících nástrojů, které jsou zaměřeny na zlepšení digitální bezpečnosti ve vzdělávání.

Projekt Digitální bezpečnost pro seniory: Tento projekt Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) poskytuje zdroje a školení o kybernetické bezpečnosti pro seniory. Projekt zahrnuje řadu materiálů, včetně online kurzů, příruček a videí, které jsou zaměřeny na zlepšení digitální bezpečnosti starších osob.

Koalice pro digitální dovednosti a pracovní místa: Cílem této iniciativy Evropské komise je zlepšit digitální dovednosti Evropanů, aby se mohli plně zapojit do digitální ekonomiky. Zahrnuje řadu zdrojů a možností školení, mimo jiné v oblasti digitální bezpečnosti.

4.3 Osvědčené postupy vzdělávání dospělých v oblasti digitální bezpečnosti

***Program* ENISA pro školení školitelů**

Všechny online školicí materiály a školicí kurzy v sekci "Školicí kurzy pro odborníky na kybernetickou bezpečnost" vycházejí z filozofie "Train the Trainer". Cílem programu a filozofie "Train the Trainer" je rozšířit síť školitelů a podpořit lepší výměnu informací. To bude sloužit několika účelům, mj:

- Sdílení školicích materiálů s cílem ušetřit čas a peníze na školení,
- vytváření regionálních školení,
- Podpora spolupráce mezi různými poskytovateli školení,
- Propagace osvědčených školicích postupů,
- omezení konkurence a duplicity.

Online školicí materiály agentury ENISA budou obsahovat Příručku pro školitele, sadu nástrojů pro studenty a virtuální stroje ke stažení. To umožní potenciálním školitelům připravit se na kurz a Příručka jim pomůže při vedení studentů v kurzu. Bude obsahovat kontrolní listy, případné malé testy, které umožní zjistit, zda studenti pochopili důležité poznatky z kurzů, a doplňující informace nebo cvičení, které může školitel použít, aby kurz učinil zajímavějším nebo náročnějším.

Vzájemné učení se z úspěchů a neúspěchů umožňuje začínajícím i zkušeným školitelům lépe navrhovat a vést školení, aby byla úspěšnější, "zábavnější" a s lepšími a dlouhodobějšími výsledky.

TiK – Technologie ve zkratce

Projekt zaměřený na špičkové technologie sleduje mezigenerační přístup prostřednictvím vzdělávání mladých dobrovolníků (ve věku od 16 do 30 let), kteří se vzdělávají podle speciálních učebních osnov pro výuku tabletů. Kurzy se vyznačují množstvím metod a flexibilních návodných otázek a zvláštním nasazením mladých školitelů. Nízkoprahové kurzy nabízejí dobrovolně pouze za malý příspěvek na náklady. Další rozvoj kurzů zajišťuje zpětná vazba účastníků a lektorů, kteří pro ně vypracovali i vlastní speciální materiály a bezbariérové pomůcky pro seniory. Kurzy jsou pro zájemce snadno dosažitelné a velká pozornost je věnována širokému geografickému rozšíření "TiKmodulů" a informací na www.digitaleseniorinnen.at. Účastníky kurzů jsou osoby a zejména ekonomicky znevýhodněné ženy na nízké úrovni vzdělání. Do konce roku 2018 se s moduly seznámilo více než 2000 osob a dalších 1000 osob se zúčastnilo kurzů-programů. Nejstaršímu účastníkovi, který se právě účastní kurzu, je 97 let, vzdělává se u mladého muže v domově důchodců. Projekt byl několikrát oceněn na spolkové i zemské úrovni.

5 Školení dospělých: Jak budovat digitální odolnost

Andragogika jako nauka o vzdělávání dospělých vznikla v Evropě v 50. letech 20. století, ale jako teorii a model vzdělávání dospělých ji jako průkopník představil až v 70. letech 20. století Malcolm Knowles, americký praktik a teoretik vzdělávání dospělých, který andragogiku definoval jako "umění a vědu o pomoci dospělým učit se" (Fidishun 2000). Fidishun (2000) navrhl, aby byly andragogické principy využívány při koncipování online výuky s cílem usnadnit "flexibilitu a možnost studentů procházet výukou kdykoli, kdekoli a svým vlastním tempem".

5.1 Čtyři principy andragogiky

Vzhledem k tomu, že dospělí mají svůj vlastní, jedinečný způsob učení, existují 4 ústřední principy, které vysvětlují, jak pro ně nejlépe připravit školení.

- Pokud jde o učení, dospělí se chtějí nebo potřebují podílet na tom, jak je jejich školení plánováno, prováděno a realizováno. Chtějí mít kontrolu nad tím, co, kdy a jak se budou učit.
- Dospělí získají více, když mohou do procesu učení zapojit své minulé zkušenosti. Mohou čerpat z toho, co již dříve znali, a dodat tak svému učení větší kontext.
- Memorování faktů a informací není pro dospělé ten správný způsob učení. Potřebují řešit problémy a používat uvažování, aby si co nejlépe osvojili předkládané informace.
- Dospělí chtějí vědět: "Jak mohu tyto informace nyní použít?". To, co se učí, musí být použitelné v jejich životě a musí to být možné okamžitě aplikovat.

5.2 Jak budou školitelé dospělých uplatňovat andragogiku

Umožnění sebeřízeného učení

V minulosti bylo učení často povinnou činností prováděnou v určitou dobu. Nyní díky technologiím, jako je systém řízení výuky, můžeme pro dospělé studenty vytvořit mnohem samostatnější a nezávislejší prostředí pro učení. Můžeme jim umožnit, aby se vzdělávali, kdy a kde chtějí, nabídnout jim výběr kurzů, které si mohou zvolit, a umožnit jim mít vlastní odlišné vzdělávací cíle.

Využití příkladů učení z reálného světa

Jak uvádí teorie, dospělí rádi vědí, jak pro ně bude mít školení bezprostřední uplatnění a přínos. Při tvorbě obsahu kurzů bychom mu tedy měli vštípit co nejvíce příkladů z reálného světa.

Při školení dospělých účastníků o digitální pohodě a/nebo digitální bezpečnosti je krok za krokem proveďte pracovním postupem, který budou skutečně používat, a výslovně uveďte, jak a proč jej budou používat. Uveďte, jak vám školení pomůže, a pak při školení použijte skutečné příklady.

Nechat dospělé studenty, aby si na to přišli sami

Vzhledem k tomu, že dospělí dávají přednost řešení problémů před pouhým sdělováním faktů, je dobré při vytváření obsahu nepředkládat hned všechny odpovědi. Proč místo toho nebýt kreativní a nevytvořit kurzy, které zapojí mozek vašich studentů?

Toho můžeme dosáhnout několika jednoduchými způsoby, včetně přidání hodnocení a simulací, které nastíní konkrétní problémy, s nimiž se může účastník kurzu skutečně setkat, a následně přimějí dospělé účastníky kurzu, aby využili své dovednosti k jeho překonání.

6 Závěr

Digitální bezpečnost starších lidí je klíčovým problémem, který vyžaduje pozornost a opatření ze strany vlád a celé společnosti. Zavedením výše uvedených osvědčených postupů mohou země zlepšit digitální ochranu a blahobyt své stárnoucí populace. Zvyšování povědomí, vzdělávání, specializovaná podpora, technologická adaptace a spolupráce s průmyslem jsou klíčovými pilíři pro zajištění bezpečných a pozitivních zkušeností starších osob na internetu.

Cílem projektu DigiWELL je začlenit zásady digitální pohody do vzdělávání dospělých. Jeho iniciativy směřují k přispění k celkové praxi organizací, sítí a iniciativ v oblasti vzdělávání dospělých. Projekt si uvědomuje, jak zásadní je zabývat se tím, jak technologie ovlivňují duševní zdraví, produktivitu a celkovou pohodu dospělých v digitálním věku. Hlavním cílem projektu DigiWELL je poskytnout dospělým účastníkům vzdělávání informace, schopnosti a zdroje potřebné k etické a svědomité orientaci v digitálním světě. Projekt DigiWELL zahrnuje také vytvoření a realizaci dalších iniciativ pro posílení postavení dospělých studentů. Cílem těchto aktivit je poskytnout podpůrné prostředí, ve kterém mohou dospělí sdílet své zkušenosti, potíže a úspěchy při podpoře digitální pohody. S ohledem na to projekt DigiWELL představuje mnoho příležitostí pro jednotlivce a organizace dospělých, aby si uvědomili a poučili se o významu digitální pohody a o tom, jak podporovat digitální pohodu dospělých jednotlivců a vzdělavatelů a školitelů dospělých. Umožnění digitální pohody s holistickým přístupem je mnohem více možné, pokud všechny příslušné strany přijmou opatření na podporu potřeb digitální pohody jednotlivců. Informace, tipy a osvědčené postupy uvedené v této příručce proto vyzývají lidi a zainteresované organizace, aby se chopili iniciativy, díky níž bude mít více z nás lepší digitální pohodu a také silnější digitální život.

7 Odkazy

Při přípravě slovníku byly použity volně dostupné online zdroje: online slovníky, vědecké články a literatura z oblasti informační bezpečnosti, digitálních technologií a služeb, digitální pohody a digitální odolnosti, jakož i termíny a definice z oboru Informační bezpečnost. Všechny zdroje jsou uvedeny v textové databázi pracovní verze slovníku.

1 BAI. Committee on National Security Systems (CNSS) Glossary (2015). In *BAI Information Security Consulting & Training [online]*. Retrieved from: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf

2 *Capterra Glossary*. Capterra. (n.d.). https://www.capterra.com/glossary/

3 CSRC. (n.d.). *Glossary*. Computer Security Resource Center. https://csrc.nist.gov/glossary/

4 *Cybersecurity glossary of terms*. Global Knowledge. (n.d.). https://www.globalknowledge.com/ca-en/topics/cybersecurity/glossary-of-terms/

5 *Glossary*. DigitalHealthEurope. (n.d.). https://digitalhealtheurope.eu/glossary/

6 *Glossary*. The Digital Wellness Lab. (2022). https://digitalwellnesslab.org/parents/glossary/

7 ISO. (n.d.). *ISO/IEC 27032:2023(en) Cybersecurity — Guidelines for Internet security*. Online browsing platform (OBP) - ISO. https://www.iso.org/obp/ui/iso

8 Jirásek, P., Novák, L., Požár, J., & Vavruška, K. (2022). *Výkladový Slovník kybernetické bezpečnosti = Cyber security glossary*. *Fifth edition.* Praha: Česká pobočka AFCEA, 2022. p. 352, ISBN 978-80-908388-4-0

9 Kissel, R. L. (2019, July 16). *Glossary of key information security terms*. NIST. https://www.nist.gov/publications/glossary-key-information-security-terms-1

10 MF SR. (n.d.). *Metodický pokyn na použitie odborných výrazov pre oblasť informatizácie spoločnosti - CSIRT.SK*. CSIRT.SK. http://www.csirt.gov.sk/wp-content/uploads/2021/08/Metodicky_pokyn_glosar_pojmov.pdf

11 Paulsen, C., & Byers, R. D. (2021). *Glossary of key information security terms*. NIST. Retrieved from: https://www.nist.gov/publications/glossary-key-information-security-terms-2

12 Stallings, W., & Brown, L. V. (2015). *Computer security: Principles and practice*. *Third edition.* Boston, MA: Pearson, 2015. p.838. ISBN 978-0-13-377392-7. Pearson.

13 *TVETipedia Glossary*. UNSECO-UNEVOC. (n.d.) https://unevoc.unesco.org/home/TVETipedia+Glossary

14 Fidishun, D. (2000). Teaching adult students to use computerized resources: Utilizing Lawler's keys to adult learning to make instruction more effective. *Information technology and libraries*, *19*(3), 157-157.

15 European Commission, Directorate-General for Education, Youth, Sport and Culture, Key competences for lifelong learning, Publications Office, 2019, https://data.europa.eu/doi/10.2766/569540