
DIGI
WELL

Co-funded by the European Union

Budovanie digitálnej odolnosti sprístupnením digitálnej pohody a bezpečnosti pre všetkých

DigiWELL

2022-2-SK01-KA220-ADU-000096888

Manuál a metodika pre budovanie digitálnej odolnosti

September, 2023

Obsah

Abstrakt

Po pandémii COVID-19 sa niektoré potreby stali životne dôležitými v dôsledku využívania digitálnych technológií a internetu, ktoré tvoria neoddeliteľnú súčasť našich životov. Najdôležitejšou z nich je schopnosť pohybovať sa v digitálnom svete bez rizika a s maximálnou bezpečnosťou. Najmä dospelí potrebujú digitálne bezpečnostné opatrenia a určité kompetencie, aby sa mohli chrániť pred kybernetickými hrozbami. Je zrejmé, že internet a digitálne technológie nielenže uľahčujú život, ale vyvolávajú aj niektoré negatívne psychologické problémy. Napríklad fenomén kyberšikany sa stal ťažko riešiteľným problémom. Zaistenie pohody v digitálnom svete sa preto v súčasných podmienkach stalo nevyhnutnosťou. V súvislosti s touto otázkou rastúce používanie digitálnych technológií a stav dosiahnutý digitálnou transformáciou priniesli do života ľudí niektoré problémy, ako je napr. digitálna únava.

Cieľom projektu DigiWELL začleniť princípy digitálnej pohody a blahobytu do vzdelávania dospelých. Projekt sa venuje otázke a riešeniu problematiky, ako technológie ovplyvňujú duševné zdravie, produktivitu a celkovú pohodu dospelých v digitálnom veku. Hlavným cieľom projektu DigiWELL je poskytnúť dospelým užívateľom informácie, schopnosti a zdroje potrebné na etický a zodpovedný pohyb v digitálnom svete. Projekt DigiWELL taktiež zahŕňa vytvorenie a realizáciu ďalších opatrení na posilnenie digitálneho povedomia u dospelých. Cieľom týchto aktivít je poskytnúť podporné prostredie, kde sa dospelí môžu podeliť o svoje skúsenosti, ťažkosti a úspechy pri dosahovaní digitálnej pohody. S ohľadom na tieto skutočnosti projekt DigiWELL predstavuje množstvo príležitostí pre jednotlivcov a organizácie, aby si uvedomili dôležitosť digitálnej pohody a o tom, ako podporovať digitálnu pohodu u dospelých ľudí, ako aj u školiteľov dospelých. Vytvorenie digitálnej pohody s holistickým prístupom je oveľa efektívnejšie, ak všetky zainteresované strany prijmú opatrenia na podporu potrieb jednotlivcov vo sfére digitálnej pohody. V dôsledku toho informácie, tipy a osvedčené postupy uvedené v tejto príručke vyzývajú ľudí a zainteresované organizácie, aby sa chopili iniciatívy smerujúcej k zlepšeniu digitálnej pohody a tiež k zodpovednejšiemu digitálnemu životu

1. Úvod

1.1. Ciele metodiky a manuálu

- Prispieť k vytvoreniu digitálnej pohody a digitálnej bezpečnosti u dospelých podporovaním a informovaním o digitálnej pohode a digitálnej bezpečnosti a o kompetenciách, ktoré sú pre nich potrebné.
- Predstaviť povedomie digitálnej odolnosti, digitálnej pohody a digitálnej bezpečnosti, zaviesť potrebnú terminológiu a najdôležitejšie výhody digitálnej pohody a digitálnej bezpečnosti medzi všetkých ľudí.

- Zabezpečiť multikulturalizmus a prispôsobiť vypracované výstupy relevantným organizáciám v partnerských krajinách.

1.2. Rámec EU DigCompu

Digitálna kompetencia v DigCompe zahŕňa „sebavedomé, kritické a zodpovedné používanie digitálnych technológií vo sfére vzdelávania, v práci a v spoločenskom živote. Je definovaná ako kombinácia vedomostí, zručností a postojov.“ (Odporúčanie Rady o kľúčových kompetenciách pre celoživotné vzdelávanie, 2018).

Rámec DigCompu identifikuje kľúčové komponenty digitálnej kompetencie v 5 oblastiach. Tieto oblasti sú uvedené nižšie:

Informačná a dátová gramotnosť: formulácia informačných potrieb, lokalizácia a získavanie digitálnych dát, informácií a obsahu. Posúdenie relevantnosti zdroja a jeho obsahu. Ukladanie, správa a organizovanie digitálnych údajov, informácií a obsahu.

Komunikácia a spolupráca: Interakcia, komunikácia a spolupráca prostredníctvom digitálnych technológií a zároveň uvedomenie si kultúrnych a generačných rozmanitostí. Zapájanie sa do spoločnosti prostredníctvom verejných a súkromných digitálnych služieb a participatívneho občianstva. Manažment vlastnej digitálnej prítomnosti, identity a reputácie.

Vytváranie digitálneho obsahu: Vytváranie a úprava digitálneho obsahu. Vylepšovanie a integrovanie informácií a obsahu do existujúceho súboru znalostí a zároveň pochopenie, ako sa majú uplatňovať autorské práva a licencie. Zadávanie zrozumiteľných pokynov pre počítačový systém.

Bezpečnosť: Ochrana zariadení, obsahu, osobných údajov a súkromia v digitálnych prostrediach. Ochrana fyzického a psychického zdravia a znalosť digitálnych technológií pre sociálnu pohodu a sociálne začlenenie. Uvedomenie si vplyvu digitálnych technológií a ich využívania na životné prostredie.

Riešenie problémov: Identifikácia potrieb a problémov a riešenie koncepčných problémov a problémových situácií v digitálnom prostredí. Používanie digitálnych nástrojov na inováciu procesov a produktov. Informovanosť o najnovšom digitálnom vývoji.

Jednou z kľúčových kompetencií v oblasti bezpečnosti je ochrana zdravia a pohody. Prostriedky na ochranu zdravia a pohody; (a) schopnosť vyhnúť sa zdravotným rizikám a ohrozeniu fyzickej a psychickej pohody pri používaní digitálnych technológií, (b) schopnosť chrániť seba a ostatných pred možnými nebezpečenstvami v digitálnom prostredí (napr. kybernetické šikanovanie) a (c) znalosť digitálnych technológií pre sociálnu pohodu a sociálne začlenenie.

1.3. Prečo by mali byť manuál a metodika dobrým zdrojom pre dospelých

Ako už bolo spomínané vyššie, po pandémii COVID-19 sa niektoré potreby stali životne dôležitými v dôsledku využívania digitálnych technológií a internetu, ktoré tvoria

neoddeliteľnú súčasť našich životov. Najdôležitejšou z nich je schopnosť pohybovať sa v digitálnom svete bez rizika a s maximálnou bezpečnosťou. Najmä dospelí potrebujú digitálne bezpečnostné opatrenia a určité kompetencie, aby sa mohli chrániť pred kybernetickými hrozbami. Je zrejmé, že internet a digitálne technológie nielenže uľahčujú život, ale vyvolávajú aj niektoré negatívne psychologické problémy. Napríklad fenomén kyberšikany sa stal ťažko riešiteľným problémom. Zaistenie pohody v digitálnom svete sa preto v súčasných podmienkach stalo nevyhnutnosťou. V súvislosti s touto otázkou rastúce používanie digitálnych technológií a stav dosiahnutý digitálnou transformáciou priniesli do života ľudí niektoré problémy, ako je napr. digitálna únava.

Táto príručka využíva čo najviac príkladov z reálneho sveta a umožňuje užívateľom, aby sami prišli na niektoré koncepty na podporu vzdelávania dospelých, Knowles (1968).

1.4. Prečo by mali byť manuál a metodika dobrým zdrojom pre školiteľov dospelých

Školenie a vzdelávanie zohrávajú kľúčovú úlohu pri zvyšovaní povedomia o digitálnej bezpečnosti takým spôsobom, že užívateľom poskytujú vedomosti, zručnosti a overené postupy potrebné na ochranu seba a svojho okolia pred kybernetickými hrozbami. Okrem toho školenie a vzdelávanie v oblasti digitálnej bezpečnosti sú základnými súčasťami budovania silného povedomia o kybernetickej bezpečnosti. Návrhom obsahu školiacich programov, ktoré sú prispôsobené špecifickým potrebám, je možné poskytnúť dospelým vedomosti a zručnosti, ktoré sú potrebné na identifikáciu kybernetických hrozieb a účinnú reakciu na ne.

Školenie pomáha jednotlivcom identifikovať rôzne typy kybernetických hrozieb, ako je napr. phishing, malware, sociálne inžinierstvo a ransomware. Identifikácia týchto hrozieb zvyšuje ostražitosť a obozretnosť pri používaní digitálnych platforiem. Vzdelávanie môže ľudí naučiť, ako spoznať phishingové e-maily, správy alebo webové stránky, identifikovať podozrivé elementy a vyhýbať sa klikaniu na škodlivé odkazy alebo poskytovaniu citlivých informácií. Toto vzdelávanie zároveň zahŕňa návody na zabezpečenie mobilných zariadení, ich ochranu pomocou prístupových kódov, používanie šifrovania a na opatrnosť pri sťahovaní aplikácií a zároveň zabezpečuje, že užívatelia sú informovaní o príslušných nariadeniach o kybernetickej bezpečnosti a požiadavkách na dodržiavanie predpisov, čo pomáha dodržiavať právne a etické normy. A napokon, prostredníctvom vzdelávania ľudia pochopia, že kybernetická bezpečnosť je spoločnou zodpovednosťou a že na udržanie bezpečného prostredia je potrebná aktívna spoluúčasť každého v rámci implementácie bezpečnostných opatrení ako v práci, tak aj v osobnom živote.

Cieľom projektu DigiWELL je riešiť problematiku digitálnej bezpečnosti a pohody u ľudí, ktorí sa nenarodili do éry internetu. Možno to dosiahnuť vytváraním a rozvíjaním flexibilných vzdelávacích príležitostí, ktoré vyhovujú špecifickým vzdelávacím potrebám dospelých. Projekt je zameraný na zvýšenie digitálnej odolnosti prostredníctvom zmiešaného vzdelávacieho prístupu. K vyššie uvedenému cieľu chce prispieť najmä táto príručka, pretože

navodzuje povedomie o digitálnej bezpečnosti, ktoré sa aktívne bráni pred kybernetickými hrozbami a chráni digitálny majetok a citlivé informácie.

Inými slovami, príručka venovaná digitálnej bezpečnosti môže zohrávať významnú úlohu pri vzdelávaní dospelých, aby sa mohli chrániť v digitálnom veku a podporovať tak bezpečnejší online zážitok pre jednotlivých užívateľov, ako aj pre spoločnosť. Projekt DigiWELL je cenným zdrojom informácií pre dospelých v oblasti vzdelávania o možných rizikách, pomáha im pochopiť dôležitosť kybernetickej bezpečnosti a ako sa chrániť v online prostredí. Nakoniec ponúka praktický návod na implementáciu opatrení v oblasti digitálnej bezpečnosti a umožňuje dospelým užívateľom pohybovať sa v digitálnom svete s istotou a slúži ako referenčná príručka, ktorú môžu títo užívatelia znovu použiť, keď sa stretnú s novými výzvami v oblasti digitálnej bezpečnosti alebo si potrebujú zopakovať určité témy.

1.5. Slovník DigiWELL projektu a ako ho používať

Slovník má za cieľ vysvetliť používateľom digitálnych technológií základné pojmy a definície týkajúce sa digitálnej pohody, digitálnej bezpečnosti a digitálnej odolnosti.

Klasifikácia pojmov

Obsahovo obsahuje slovník 3 základné kategórie pojmov;

1. Pojmy a definície z oblasti informačných a komunikačných technológií (digitálne technológie podľa projektu).
2. Pojmy a definície z oblasti informačnej, kybernetickej a digitálnej bezpečnosti (digitálna bezpečnosť podľa projektu).
3. Pojmy a definície definované cieľmi projektu: digitálna pohoda a digitálna odolnosť. Tieto pojmy sú relatívne nové a sú súčasťou teoretického výskumu projektových tímov. Je potrebné zdôrazniť, že neexistuje jednotná definícia týchto pojmov. Do tejto kategórie patria aj pojmy z oblasti duševného a fyzického zdravia, napr. digitálna závislosť, digitálna únava/vyhorenie, digitálny detox, atď.

Poznámka: V textovej databáze slovníka môže mať jeden výraz viac ako jednu definíciu z viacerých dôvodov: pôvodná definícia sa časom vyvíjala, široká definícia je prispôsobená na konkrétnu oblasť, definície pojmov sú podobné, ale s jemnými rozdielmi atď.

Pojmy a definície

Digitálna odolnosť: 1. Digitálna odolnosť znamená mať povedomie, zručnosti, obratnosť a sebadôveru pri používaní nových technológií a schopnosť prispôsobiť sa meniacim sa požiadavkám na digitálne zručnosti. Digitálna odolnosť zlepšuje schopnosti riešiť problémy a

zvyšovať zručnosti a orientáciu v digitálnom prostredí. 2. Digitálna odolnosť je schopnosť mladých ľudí rozvíjať kritické myslenie pri prístupe k digitálnym informáciám, aby sa znížila ich zraniteľnosť v súvislosti s potenciálne škodlivými informáciami. 3. Digitálna odolnosť znamená „proces efektívneho prispôsobenia sa digitálnym zdrojom stresu a rozvoj zručností na zvládanie vplyvu neustále sa meniacich situácií v digitálnom prostredí a aplikáciách“.

Digitálna bezpečnosť: Digitálna bezpečnosť je ochrana digitálnej identity, pretože predstavuje fyzickú identitu v sieti alebo internetových službách. Digitálna bezpečnosť je súbor osvedčených postupov a nástrojov používaných na ochranu osobných údajov a identity v online svete. Príkladmi takýchto nástrojov sú: webové služby, antivírusový softvér, SIM karty smartfónov, biometrické a zabezpečené osobné zariadenia, správcovia hesiel, rodičovská kontrola atď.

Digitálna pohoda: 1. Digitálna pohoda charakterizuje schopnosť človeka efektívne zvládať negatívne dopady technológií na svoj profesionálny a osobný život. Podstatou digitálnej pohody je podporovať racionálne používanie technologických zariadení a digitálnych služieb. 2. Stav osobnej pohody v súvislosti s racionálnym používaním digitálnych technológií. 3. Digitálna pohoda zahŕňa spôsoby, akými môžu informačné technológie – vrátane komunikácie – pomôcť ľuďom žiť dlhší a zdravší život.

Digitálna kompetencia: Sebavedomé, kritické a zodpovedné používanie digitálnych technológií a ich využívanie v rámci štúdia, v práci a v spoločnosti. Je definovaná ako kombinácia vedomostí, zručností a postojov.

Digitálna závislosť: Digitálna závislosť je škodlivá závislosť na digitálnych médiách, zariadeniach a internete, charakterizovaná ich nadmerným používaním spôsobom, ktorý má negatívny vplyv na život používateľa.

Digitálne zručnosti: Digitálne zručnosti predstavujú rozsah schopností používať digitálne zariadenia, komunikačné aplikácie a siete na prístup k informáciám a ich spravovaniu. Umožňujú ľuďom vytvárať a zdieľať digitálny obsah, komunikovať, spolupracovať a riešiť problémy pre efektívnu a tvorivú sebarealizáciu v živote, učení, práci a spoločenských aktivitách.

Kybernetická hrozba: Akákoľvek okolnosť alebo udalosť s potenciálom nepriaznivo ovplyvniť organizácie/jednotlivcov prostredníctvom neoprávneného prístupu, zničenia,

zverejnenia, úpravy informácií a/alebo odmietnutia služby. Cieľom je odcudziť /poškodiť dáta alebo narušiť digitálnu pohodu.

Kyberšikana: Pojem pre rôzne formy šikanovania v online priestore, v ktorom jeden alebo viacerí jednotlivci používajú digitálne technológie na úmyselné a opakované ubližovanie inej osobe (napr. posielanie e-mailov alebo správ, uverejňovanie komentárov na sociálnych sieťach alebo verejných fórach).

Kybernetická bezpečnosť: Kybernetická bezpečnosť je podskupinou informačnej bezpečnosti, jej cieľom je chrániť kybernetický priestor (t. j. siete, intranety, servery, informačné a počítačové systémy a infraštruktúru) pred neoprávneným prístupom, kybernetickými útokmi alebo poškodením. Kybernetická bezpečnosť sa zameriava na ochranu informácií v elektronickej/digitálnej podobe v počítačoch, úložiskách a sieťach (v kybernetickom priestore).

Digitálne súkromie: Digitálne súkromie je schopnosť jednotlivca kontrolovať a chrániť prístup k svojim osobným údajom a ich používaniu pri prístupe na internet. Digitálne súkromie pomáha jednotlivcom zostať v online anonymite tým, že chráni osobné údaje, ako sú napr. mená, adresy, rodné čísla, údaje o kreditnej karte atď.

Digitálna bezpečnosť vs. kybernetická vs. informačná bezpečnosť*:* Informačná bezpečnosť: chráni informácie (v akejkoľvek forme) a informačné systémy pred neoprávneným prístupom a použitím s cieľom zabezpečiť a zachovať súkromie dôležitých údajov. Kybernetická bezpečnosť: chráni celé siete a komunikačné systémy, počítačové systémy a ďalšie digitálne komponenty a digitálne údaje v nich uložené. Digitálna bezpečnosť: chráni online prítomnosť (identitu a súvisiace citlivé informácie).

Najlepšia prax: Osvedčené postupy, ktoré ponúkajú najefektívnejšie riešenia v danej oblasti, preukázateľne vedú k optimálnym výsledkom a sú stanovené (odporúčané) ako vhodné štandardy pre široké použitie. V oblasti digitálnej bezpečnosti sú to definované postupy na zabezpečenie ochrany jednotlivcov/organizácie v digitálnom priestore (napr. odporúčané techniky, programy, návody, manuály).

2. Digitálna pohoda

2.1. Čo je pohoda?

Pojem „**pohoda**“ popisuje stav, keď je človek spokojný, šťastný a zdravý. Zahŕňa fyzické, duševné a emocionálne blaho človeka, okrem iných oblastí jeho existencie. Pohoda sa okrem toho, že človek je bez chorôb alebo nepohodlia, zameriava aj na celkové šťastie a kvalitu života.

Fyzická pohoda je stav tela, berúc do úvahy okolnosti ako fyzická zdatnosť, strava či absencia ochorenia alebo choroby. Znamená to dodržiavanie zdravého životného štýlu prostredníctvom pravidelného cvičenia, kvalitného stravovania, dostatku spánku a zvládania stresu.

Kognitívne a emocionálne zdravie človeka súvisí s jeho **duševnou pohodou**. Znamená to mať dobrý prehľad, žiť naplno a vedieť zvládať stres a ťažkosti každodenného života. Celková všímavosť, venovanie sa koníčkom a záľubám, trávenie času s blízkymi a získanie odbornej pomoci, keď je to potrebné, to všetko môže pomôcť podporiť duševnú pohodu človeka.

Dobré sebapoznanie a schopnosť ovládať svoje emócie sa nazýva **emocionálna pohoda**. Znamená to pestovať si odolnosť, udržiavať dobré vzťahy a mať pozitívny zmysel života. Sebauvedomenie, emocionálna kontrola, efektívna komunikácia a rozvoj medziľudských vzťahov prispievajú k emocionálnej pohode.

Kvalita osobných kontaktov a pocit spolupatričnosti s komunitou sú súčasťou **sociálnej pohody**. Znamená to pestovanie trvalých väzieb s príbuznými, blízkymi, priateľmi a väčším spoločenským okruhom. Účasť na spoločenských aktivitách, spolupatričnosť ku komunite a udržiavanie kontaktov, to všetko prispieva k zlepšeniu sociálnej pohody.

Celkovo je **pohoda** komplexnou myšlienkou, ktorá zohľadňuje, ako sú navzájom prepojené rôzne aspekty života človeka. Znamená to aktívne hľadať vyrovnanú a uspokojujúcu existenciu, starať sa o svoje telesné a duševné zdravie, pestovať zdravé vzťahy a nájsť zmysel svojho života.

2.2. Pohoda a digitalizácia

Umožnením komunikácie, zvýšením efektívnosti a zlepšením prístupu k informáciám majú technológie a digitalizácia potenciál zlepšiť celkovú pohodu človeka. Ak sa človek chce pohybovať v digitálnom svete, chrániť svoje súkromie a bezpečnosť a dosiahnuť správnu rovnováhu medzi technológiami a inými aspektmi života, je dôležité, aby si uvedomil možné nevýhody a prijal potrebné preventívne opatrenia.

Technológie a digitalizácia výrazne zlepšili prístup k informáciám a službám, čo má pozitívny vplyv na pohodu. Ľudia majú teraz jednoduchý prístup k digitálnym nástrojom na osobný rozvoj, informáciám o zdravotnej starostlivosti, online podporným skupinám a vzdelávacím zdrojom. Prostredníctvom bezproblémovej komunikácie a spojenia na diaľku

technológie podporujú sociálne spojenia a znižujú pocity osamelosti. Ľudia môžu zostať v kontakte s priateľmi, rodinou a komunitami vďaka digitálnym platformám, sociálnym médiám a aplikáciám na odosielanie správ, ktoré zlepšujú sociálnu pohodu. Mnohé aspekty života sa vďaka digitalizácii stali efektívnejšími a pohodlnejšími. Pomocou digitálnych nástrojov a služieb možno teraz úlohy, ktoré si kedysi vyžadovali veľa času a úsilia, dokončiť rýchlo a bez námahy. To môže pomôcť k všeobecnej pohode tým, že ušetrí čas a zníži stres. Digitálne schopnosti sú navyše na pracovnom trhu s rozvojom technológií čoraz dôležitejšie. Získaním a využívaním týchto vymožeností možno zlepšiť zamestnateľnosť a sociálno-ekonomický blahobyt človeka. Digitálna priepasť, ku ktorej dochádza, keď niektorí ľudia alebo komunity nemajú prístup k technológiám alebo digitálnej gramotnosti, môže prehĺbiť už existujúce rozdiely.

Nesprávne alebo nadmerné používanie digitálnych technológií môže mať škodlivé účinky na duševné zdravie. Úzkosť, zúfalstvo a nízke sebavedomie môžu byť spôsobené príliš dlhým časom stráveným pred obrazovkou, v priestore sociálnych médií alebo online zneužívaním. Na ochranu duševného zdravia je dôležité udržiavať zdravú rovnováhu a technológie využívať rozumne. Digitálne prostredie má určité riziká spojené so súkromím a bezpečnosťou. Kybernetické hrozby, úniky údajov alebo online podvody môžu ohroziť finančnú bezpečnosť a súkromné dáta ľudí. Udržanie celkovej pohody v digitálnom veku si vyžaduje ochranu digitálnej bezpečnosti a súkromia.

2.3. Čo je digitálna pohoda?

Rozvoj digitálnej odolnosti a prijatie bezpečnostných opatrení vedú k stavu optimálneho zdravia a všeobecnej pohody v digitálnej sfére, ktorá sa označuje ako **digitálna pohoda.** Digitálna pohoda pochádza z konceptu pohody ako takej a súvisí s digitálnym životom jednotlivcov. Schopnosť ľudí prispôsobiť sa, existovať a prosperovať v digitálnom svete a zároveň úspešne manažovať svoju pohodu a bezpečnosť sa označuje ako **digitálna odolnosť**, ktorá je kombináciou digitálnej pohody a bezpečnosti. Základným kameňom digitálnej odolnosti je digitálna pohoda, ktorá kladie dôraz na zachovanie prínosného a racionálneho využívania technológií. Znamená to obmedzenie času stráveného pred obrazovkou, kladenie vysokej priority na duševné a emocionálne zdravie, vytváranie podporných online komunít a učenie sa digitálnej gramotnosti. V kontexte pohody digitálna odolnosť pomáha ľuďom zvládať online nástrahy, ako je napr. kyberšikana, online obťažovanie alebo vystavenie nebezpečnému obsahu. Jednotlivci si môžu vybudovať silnú digitálnu odolnosť, ktorá im umožní pohybovať sa v digitálnom svete s istotou a zodpovednosťou prostredníctvom integrácie digitálnej pohody a digitálnej bezpečnosti. Sú schopní lepšie zvládať výzvy digitálneho sveta, prispôsobovať sa meniacim sa nebezpečenstvám, robiť racionálne úsudky, chrániť svoje osobné informácie a udržiavať si svoje duševné, emocionálne a fyzické zdravie pri používaní internetu. Digitálna odolnosť v konečnom dôsledku podporuje bezpečnejšie, zdravšie a plnohodnotnejšie online prostredie pre ľudí.

2.3.1. Duševné zdravie, pohoda a digitálna pohoda

Celkovú kvalitu nášho života ovplyvňujú hlboké prepojenia medzi duševným zdravím a celkovou pohodou. Naša psychická a emocionálna pohoda, vrátane aspektov, ako sú myšlienky, pocity a správanie, sa označuje ako naše duševné zdravie. Je základom nášho celkového zdravia, rovnako ako aj fyzické zdravie. Je to komplexný stav rovnováhy, naplnenia a spokojnosti v živote. Vzťah medzi nimi je založený na tom, aký významný vplyv má duševné zdravie človeka na jeho fyzické zdravie a naopak. Naša celková pohoda sa zvyšuje, keď si vytvárame pozitívne duševné zdravie ovládaním stresu, prekonávaním prekážok a budovaním zdravých vzťahov, čo vedie k plnohodnotnejšiemu a zmysluplnejšiemu životu. Na druhej strane, pocit pohody môže výrazne zlepšiť duševné zdravie tým, že podporuje odolnosť, emocionálnu stabilitu a vyššiu schopnosť vyrovnať sa s výzvami v živote. Môžeme si vytvoriť šťastný a prosperujúci život tým, že sa zameriame na vzťahy medzi naším duševným zdravím a duševnou pohodou.

Vďaka rýchlemu pokroku v technológii a jej všadeprítomnej integrácii do nášho každodenného života nadobúda duševné zdravie v digitálnom veku komplexný a dynamický charakter. V kontexte digitálneho veku sa o duševnej a emocionálnej pohode človeka hovorí ako o „digitálnom duševnom zdraví“. Zahŕňa sociálne médiá, online interakcie, psychologické účinky digitálnych technológií a neustály kontakt, ktoré definujú moderný život. Hoci technológie vytvorili mnoho výhod a príležitostí, spôsobili aj značné ťažkosti pre duševné zdravie. Napriek neustálemu virtuálnemu kontaktu môže digitálny vek spôsobiť problémy, ako je napr. závislosť na internete, kyberšikana, informačné preťaženie, sociálne porovnávanie a pocity izolácie. Poskytuje však aj vynikajúce prístupy k manažmentu vlastného duševného zdravia, ako sú aplikácie pre duševné zdravie, online terapie či virtuálne podporné skupiny. Udržiavanie zdravej rovnováhy medzi životom online a offline, uvedomovanie si toho, koľko a ako často digitálne médiá používame a aktívne hľadanie digitálnych nástrojov, ktoré môžu zlepšiť našu duševnú pohodu a zároveň chrániť pred potenciálnymi hrozbami, sú nevyhnutné, pre život a prácu v úskaliach digitálneho prostredia.

V súčasnosti existuje zložitý vzťah medzi duševným zdravím a digitálnou pohodou. Psychologická a emocionálna pohoda, ktorá zahŕňa faktory ako nálada, myšlienky, pocity a správanie, sa označuje ako duševné zdravie. Na druhej strane, digitálna pohoda popisuje rovnováhu a harmóniu, ktorú človek pociťuje pri používaní technológií a zapájaní sa do sveta digitálnych vzťahov. Digitálna éra má mnoho výhod, umožňuje byť neustále v kontakte, poskytuje prístup k informáciám a príležitosti na osobný rozvoj. Nadmerné používanie technológií, neustále notifikácie, tlak sociálnych médií a preťaženie informáciami však môžu mať negatívny vplyv na duševné zdravie tým, že spôsobujú napätie, obavy a pocit odlúčenia od reality. Na druhej strane môže mať aj priaznivý vplyv na duševné zdravie, a to vtedy, keď si človek stanoví limity, pravidelné prestávky pri práci s technológiami a kontroluje si digitálnu spotrebu. Za účelom podpory duševného zdravia a digitálnej pohody a zaručenia harmonickej vyváženosti medzi našim virtuálnym a skutočným životom je nevyhnutné dosiahnuť zdravú

rovnováhu medzi digitálnym svetom a offline aktivitami. Zmysluplnejší a vyváženejší život v digitálnom veku možno dosiahnuť používaním digitálnych nástrojov za účelom lepšenia duševného zdravia.

2.3.2. Prečo potrebujeme digitálnu pohodu?

Kľúčovými faktormi digitálnej pohody sú kvalita života, komunikácia, produktivita, úspech, duševné a fyzické zdravie. Digitálna pohoda je dôležitá, pretože zahŕňa celkový stav zdravia, šťastia a spokojnosti. Vzťahuje sa na celkové zdravie ľudí, berúc do úvahy ich sociálne, psychologické a fyzické aspekty. Nadmerné alebo nezdravé používanie mobilných telefónov, sociálnych médií a videohier môže byť škodlivé pre duševné zdravie. Nadmerný čas strávený pred obrazovkou, časté porovnávanie sa s ostatnými na sociálnych sieťach alebo kyberšikana môžu spôsobovať úzkosť, zúfalstvo, osamelosť a nízke sebavedomie. V tomto ohľade je digitálna pohoda spôsob, ako mať kontrolu nad svojim životom. Na podporu dobrého duševného zdravia a digitálnej pohody je dôležité mať zdravý vzťah k technológiám. Súčasťou toho môže byť nastavenie limitov pre používanie aplikácií, zapájanie sa do digitálnych detoxov, do offline aktivít, vyhľadávanie osobných kontaktov a venovanie starostlivosti o seba samého. Musíme si byť vedomí vplyvu digitálnych technológií na naše duševné zdravie a prijať proaktívne opatrenia na zabezpečenie ich rozumného používania.

Digitálna pohoda sa stala základnou ľudskou potrebou v digitálnom veku, najmä v dôsledku pandémie Covid-19. Naša závislosť od digitálnych platforiem rastie, keďže technológie neustále prenikajú do každej oblasti nášho života, od komunikácie a vzdelávania až po zamestnanie a zábavu. Epidémia spôsobila výrazný posun v digitalizácii, čoho ukážkou je práca na diaľku, online vzdelávanie a viac virtuálnych kontaktov. V dôsledku toho je udržiavanie našej digitálnej pohody kľúčové pre plnohodnotný a zdravý život. Môžeme využívať technológie zmysluplným a zodpovedným spôsobom za účelom uľahčenia a zlepšenia života, a nie tak, aby predstavovali hrozbu pre našu všeobecnú pohodu, ktorú v tomto rýchlo sa meniacom digitálnom prostredí považujeme za základnú ľudskú potrebu.

2.3.3. Dobrá a nedostatočná digitálna pohoda

Digitálna pohoda je komplexný pojem, ktorý zahŕňa rôzne aspekty digitálneho sveta. Zaoberá sa tým, či sú jednotlivci fyzicky, psychicky a sociálne zdraví a na druhej strane či sa cítia digitálne uvedomelí, vyrovnaní, v bezpečí a spokojní. Ako vidno, význam pripisovaný výrazu „digitálna pohoda“ sa väčšinou týka pozitívnej stránky digitalizácie, teda dobrej digitálnej pohody. Naopak, u jednotlivcov, ktorí majú nedostatok digitálnej pohody, sa stav označuje ako nedostatočná alebo zlá digitálna pohoda. Vzhľadom k tomu by sa nasledovné aspekty mohli považovať za hlavné ukazovatele dobrej digitálnej pohody:

- Digitálne zabezpečenie: Záruka digitálneho zabezpečenia predstavuje významný príspevok k digitálnej pohode človeka. Zahŕňa ochranu v čase online prítomnosti vrátane osobnej identity, údajov a aktív.
- Digitálna bezpečnosť: Zahŕňa to, že si jednotlivci uvedomujú potenciálne riziká v digitálnom svete a súvisí so schopnosťou jednotlivcov kriticky identifikovať a eliminovať rôzne hrozby v digitálnom prostredí.
- Digitálna rovnováha: Vzťahuje sa na účelné využívanie technológií a digitálneho sveta. Digitálna rovnováha súvisí s využívaním digitálneho sveta, digitálnych nástrojov a zariadení pre rôzne oblasti života, rozhodne však nie pre všetky. Pravidelná a konzistentná online/offline rovnováha a vyhýbanie sa veľkej závislosti od technológií sú znakmi dobrej digitálnej rovnováhy.
- Digitálna nezávislosť: Je to schopnosť kontrolovať čas strávený online a vyhnúť sa úplnému vtiahnutiu digitálneho sveta do každodenného života. Tráviť príliš veľa času online a plánovať menej spoločenských aktivít v dôsledku nadmerného používania internetu sú niektoré z príznakov digitálnej závislosti.
- Digitálna spokojnosť: Vzťahuje sa na dosiahnutie spokojnosti a pocitu potešenia a radosti pri využívaní digitálnych nástrojov, zariadení a technológií.
- Digitálna príležitosť: Zaoberá sa využívaním technológií a digitalizácie s cieľom otvoriť nové možnosti súvisiace so šírením digitálnych technológií a so získavaním ďalších kompetencií na vybudovanie nových príležitostí.
- Kritické a zodpovedné používanie technológií: Technológie vyžadujú, aby používatelia konali zodpovedne, chránili svoje vlastné práva a rešpektovali práva iných, aby konali zodpovedne a obozretne a kriticky premýšľali o akomkoľvek obsahu v digitálnom svete.

Tieto aspekty by bolo možné považovať za dimenzie digitálnej pohody. Ak niekto má alebo si dokáže zabezpečiť digitálnu bezpečnosť na relatívne vyššej úrovni, ďalej rovnováhu, nezávislosť, spokojnosť, a/alebo kritické a zodpovedné využívanie technológií, digitálnych nástrojov a zariadení, možno ho považovať za osobu s dobrou digitálnou pohodou. Naopak, ak niekomu chýbajú niektoré z vyššie uvedených skutočností, znamená to, že má nedostatočnú digitálnu pohodu. Stojí za zmienku, že byť fyzicky, psychicky a sociálne zdravý znamená mať aj dobrú digitálnu pohodu a tieto aspekty môžu potenciálne prispievať k digitálnej pohode ako aj k celkovej pohode jednotlivcov.

2.3.4. Podpora digitálnej pohody jednotlivcov: potenciálne benefity pre všetkých a pre vzdelávanie dospelých

Podpora digitálnej pohody vo vzdelávaní dospelých alebo posilňovanie pohody a digitálnej pohody u dospelých poskytuje mnoho príležitostí. V prvom rade je pohoda základnou ľudskou potrebou. Najmä po COVID-19 väčšina ľudí trávi oveľa viac času online a sú viac vystavení technológiám spolu s ich rizikami a hrozbami. Či ľudia chcú alebo nie, prenášajú

do práce celé svoje ja, a teda existuje jasná súvislosť medzi pohodou ľudí a pracovnou atmosférou. Teda okolnosti podporujúce pohodu a digitálnu pohodu jednotlivcov prispievajú k dobrej pracovnej atmosfére a pohode na pracovisku. Z organizačného hľadiska podpora digitálnej pohody pracovníkov prispieva k tímovému výkonu, odhodlaniu, inováciám a celkovej spokojnosti. Digitálna pohoda umožňuje ľuďom stať sa sústredenejšími, angažovanejšími a produktívnejšími, čo prispieva k zdravšiemu životu v pracovnom prostredí aj mimo neho. Osvojenie si praktík digitálnej pohody u zamestnancov umožňuje, aby boli menej vyčerpaní a viac sústredení. Podporné akcie pre digitálnu pohodu posilňujú rovnováhu medzi pracovným a súkromným životom jednotlivcov. Okrem toho eliminujú negatívne dopady nadmerného vystavenia sa digitalizácii, čo umožňuje menej prežívať úzkosť, zúfalstvo, stres a pod.

Myšlienka pohody v kontexte vzdelávania dospelých presahuje konvenčné predstavy o akademickom vzdelávaní a zahŕňa celkové zdravie a duševné naplnenie učiacich sa. Pojem „digitálna pohoda“ nadobudol dôležitosť s príchodom digitálnej éry, najmä pre digitálnych nomádov, ktorí sa vo veľkej miere spoliehajú na technológie a zároveň žijú mobilným životným štýlom. Vo vzdelávaní dospelých sa pojem „digitálna pohoda“ vzťahuje na poskytovanie informácií študujúcim, ktoré potrebujú na rozumné a etické využívanie internetu. Podpora digitálnej pohody je kľúčová pre vytvorenie úspešného vzdelávacieho prostredia, pretože digitálni nomádi sa často stretávajú s konkrétnymi ťažkosťami, ako je napríklad žonglovanie medzi osobným a pracovným životom a prekonávanie pocitov osamelosti. Začlenenie digitálnej pohody do vzdelávania dospelých znamená naučiť ľudí, ako správne tráviť čas strávený pred obrazovkou, budovať pozitívne online komunity a nadobudnúť znalosti o správnom využívaní digitálnych technológií. Zahŕňa tiež témy ako sú kybernetická bezpečnosť, digitálna únava a ochrana osobných údajov. V dnešnom digitálne riadenom svete môžu školitelia zabezpečiť pozitívne a obohacujúce vzdelávanie tým, že sa zamerajú na potrebu posilnenia digitálnej pohody vo vzdelávaní dospelých a poskytnú digitálnym nomádom a iným študentom nástroje na udržanie zdravej rovnováhy medzi ich digitálnymi interakciami a celkovou pohodou.

Úspešná integrácia digitálnej pohody do vzdelávania dospelých si vyžaduje starostlivú a dôkladnú stratégiu, pretože sa jedná o komplikovaný a dlhodobý proces. Prvým a najdôležitejším krokom je poskytnúť dospelým užívateľom školenie, aby si boli vedomí hodnoty digitálnej pohody a toho, ako táto pohoda ovplyvňuje ich celkové zdravie a produktivitu. Vďaka takémuto školeniu získavajú potrebné praktické zručnosti pre rozumný a bezpečný pohyb v digitálnom svete. Druhou fázou je úprava učebných materiálov tak, aby tieto materiály zahŕňali koncepciu digitálnej pohody. To znamená začlenenie problematiky, ako je kontrola digitálneho prostredia, online súkromia, digitálnej etikety a digitálnej gramotnosti. Dospelí užívatelia môžu takto lepšie pochopiť výhody a nevýhody technológií a naučiť sa, ako ich efektívne využívať. Vytvára sa tak podporné prostredie, kde si užívatelia môžu vymieňať skúsenosti, poznatky, zručnosti a opakovane sa uisťovať v otázkach problematiky digitálnej pohody prostredníctvom ďalších podujatí, ako sú stretnutia, semináre

a diskusie. Aby bolo vzdelávanie dospelých zmysluplné a efektívne pri podpore pohody v digitálnej ére, musí sa neustále vyvíjať tak, aby držalo krok s rýchlo sa meniacim digitálnym prostredím.

3. Digitálna bezpečnosť

3.1 Digitálna a kybernetická bezpečnosť

Podľa Organizácie pre hospodársku spoluprácu a rozvoj (OECD) je **digitálna bezpečnosť** nevyhnutná pre budovanie dôveryhodnosti v digitálnom veku. Od začiatku 90. rokov OECD podporuje medzinárodnú spoluprácu a rozvíja politiku analýz a odporúčaní v oblasti digitálnej bezpečnosti. Aktivity v tejto oblasti sa zameriavajú na rozvoj a podporu opatrení, ktoré posilňujú dôveryhodnosť bez toho, aby obmedzovali potenciál informačných a komunikačných technológií (IKT) v oblasti podpory inovácií, konkurencieschopnosti a rastu. Digitálna bezpečnosť sa vzťahuje na ekonomické a sociálne aspekty kybernetickej bezpečnosti, na rozdiel od čisto technických aspektov súvisiacich s presadzovaním trestného práva alebo národnou a medzinárodnou bezpečnosťou. Pojem „digitálny“ je v súlade s výrazmi ako digitálna ekonomika, digitálna transformácia a digitálne technológie. Tvorí základ pre konštruktívny medzinárodný dialóg medzi zainteresovanými stranami, ktoré sa snažia posilniť dôveryhodnosť a maximalizovať výhody plynúce z IKT.

Digitálna bezpečnosť a **kybernetická bezpečnosť** spolu súvisia, ale nepredstavujú to isté. Obidva pojmy zahŕňajú ochranu digitálnych dát a informácií pred neoprávneným prístupom, použitím alebo poškodením, líšia sa však rozsahom a zameraním.

Digitálna bezpečnosť sa vzťahuje na ochranu digitálnych údajov, informácií a aktív pred neoprávneným prístupom, odcudzením alebo poškodením. Zahŕňa širšiu škálu bezpečnostných opatrení, ktoré chránia údaje a informácie na rôznych digitálnych platformách a zariadeniach vrátane počítačov, smartfónov, tabletov a iných digitálnych technológií**.**

Digitálne bezpečnostné opatrenia môžu zahŕňať:

- Ochranu heslom: Vytváranie silných a jedinečných hesiel pre online účty a zariadenia.
- Šifrovanie údajov: Kódovanie údajov, aby sa zabránilo neoprávnenému prístupu alebo úniku údajov.
- Bezpečnú komunikáciu: Používanie šifrovacích protokolov pre bezpečný prenos údajov.
- Riadenie prístupu: Implementácia povolení a obmedzení pre prístup k citlivým údajom a informáciám.
- Zabezpečenie zariadenia: Využívanie funkcií, ako sú zámky obrazovky a vzdialené vymazanie stratených alebo odcudzených zariadení.

Kybernetická bezpečnosť je podmnožinou digitálnej bezpečnosti a zameriava sa konkrétne na ochranu digitálnych aktív pred kybernetickými hrozbami a útokmi. Zahŕňa ochranu proti neoprávnenému prístupu, poškodeniu alebo narušeniu digitálnych systémov, sietí a infraštruktúr.

Opatrenia kybernetickej bezpečnosti môžu zahŕňať:

- Firewall ochranu: Nastavenie bariér na zabránenie neoprávnenému prístupu do siete.
- Systémy detekcie narušenia: Monitorovanie sietí zamerané na podozrivé aktivity a potenciálne hrozby.
- Ochranu pred malwarom: Používanie antivírusového softvéru na detekciu a odstránenie škodlivého softvéru.
- Plánovanie reakcií na incidenty: Vývoj protokolov pre efektívnu reakciu na incidenty v oblasti kybernetickej bezpečnosti.
- Informácie o kybernetických hrozbách: Zhromažďovanie a analýza informácií s cieľom predvídať kybernetické hrozby a predchádzať im.

Digitálna bezpečnosť zahŕňa širšiu škálu postupov, ktoré chránia dáta a informácie v digitálnej sfére, pričom kybernetická bezpečnosť je špecializovaná oblasť zameraná na obranu pred kybernetickými hrozbami a útokmi v digitálnych systémoch a sieťach. Obe sú kľúčovými komponentmi pri zabezpečovaní celkovej bezpečnosti a ochrany digitálnych aktív a dát.

3.2. Kybernetické hrozby, ktorým čelia dospelí užívatelia

Dospelí užívatelia čelia v dnešnom digitálnom svete širokej škále hrozieb v oblasti kybernetickej bezpečnosti. Tu je niekoľko bežných ohrození kybernetickej bezpečnosti, s ktorými sa dospelí často stretávajú:

- ***Phishingové útoky***: Phishing je technika používaná počítačovými zločincami na oklamanie jednotlivcov, aby poskytli citlivé informácie, ako sú prihlasovacie údaje, čísla kreditných kariet alebo osobné údaje. Phishingové e-maily, správy alebo webové stránky sa môžu zdať, že pochádzajú z dôveryhodných zdrojov, no ich cieľom je oklamať používateľov, aby prezradili svoje informácie.
- ***Malware****:* Malware je škodlivý softvér určený na infiltráciu, poškodenie alebo získanie neoprávneného prístupu do počítačových systémov. Medzi typy malwaru patria vírusy, ransomware, spyware a trójske kone. Škodlivý softvér sa môže šíriť prostredníctvom škodlivých e-mailových príloh, infikovaných webových stránok alebo napadnutého softvéru.
- ***Krádež identity***: Kyberzločinci môžu ukradnúť osobné informácie, ako sú rodné čísla, dátumy narodenia alebo údaje o kreditných kartách, aby spáchali krádež identity. Tieto informácie sa často získavajú prostredníctvom úniku údajov alebo pokusov o phishing.

- ***Online podvody***: Existuje mnoho online podvodov zameraných na dospelých užívateľov, ako sú lotériové podvody, vzťahové podvody, podvody v súvislosti s technickou podporou a podvodné investičné schémy. Podvodníci používajú rôzne taktiky za účelom manipulácie jednotlivcov, aby posielali finančné prostriedky alebo poskytovali osobné informácie.
- ***Únik údajov***: Únik údajov nastane vtedy, keď dôjde k odhaleniu alebo krádeži citlivých informácií, ktoré sú v správe spoločností alebo organizácií. Ako osobu vás môže postihnúť únik údajov, ak vaše osobné údaje uchovávajú dotknuté subjekty.
- ***Sociálne inžinierstvo***: Sociálne inžinierstvo zahŕňa manipuláciu jednotlivcov s cieľom odhaliť dôverné informácie alebo vykonať určité akcie. Kyberzločinci môžu používať techniky sociálneho inžinierstva na získanie neoprávneného prístupu k systémom alebo účtom.
- ***Útoky heslom***: Slabé heslá alebo opätovné použitie hesiel môžu viesť k útokom na heslá, ako sú útoky hrubou silou alebo slovníkové útoky, pri ktorých sa počítačoví zločinci pokúšajú uhádnuť alebo prelomiť heslá, aby získali neoprávnený prístup.
- ***Riziká spojené s verejnou Wi-Fi sieťou***: Používanie verejných Wi-Fi sietí môže vystaviť požívateľov bezpečnostným rizikám, pretože týmto sieťam môže chýbať správne šifrovanie a sú náchylné na odpočúvanie útočníkmi.
- ***Interné hrozby***: Interné hrozby sa týkajú zamestnancov alebo jednotlivcov s autorizovaným prístupom k systémom alebo údajom, ktorí úmyselne alebo neúmyselne spôsobujú škodu alebo únik citlivých informácií.
- ***Zraniteľnosť internetu vecí***: Rastúce zavádzanie zariadení internetu vecí (IoT) môže vytvárať riziká kybernetickej bezpečnosti, keďže mnohé z týchto zariadení môžu mať nedostatočné bezpečnostné opatrenia a môžu ich zneužiť kyberzločinci.

Na ochranu pred týmito hrozbami by užívatelia mali dodržiavať potrebné opatrenia v oblasti kybernetickej bezpečnosti, vrátane používania silných a jedinečných hesiel, umožnenia viacfaktorovej autentifikácie, udržiavania softvérov a zariadení v aktualizovanom stave, dávať si pozor na podozrivé e-maily a odkazy a zvažovať informácie, ktoré zdieľajú online. Pravidelné školenia v oblasti kybernetickej bezpečnosti môžu ľuďom poskytnúť informácie o nových hrozbách a osvedčených postupoch, ako zostať v online bezpečí. V ďalšej časti sú podrobne uvedené niektoré z najdôležitejších oblastí digitálnej bezpečnosti, ktoré môžu pomôcť znížiť riziko, že sa užívatelia stanú obeťou hrozieb kybernetickej bezpečnosti, a môžu dopomôcť k ochrane ich digitálnej identity.

3.3. Odporúčania v oblasti digitálnej bezpečnosti pre užívateľov

Pravidlá digitálnej bezpečnosti sú pre užívateľov nevyhnutné na ochranu ich osobných údajov, informácií a online účtov pred hrozbami v oblasti kybernetickej bezpečnosti. Tu je niekoľko dôležitých oblastí digitálneho zabezpečenia, ktoré by užívatelia mali dodržiavať:

- ***Používajte silné a jedinečné heslá***: Užívatelia by si mali vytvárať silné a jedinečné heslá pre svoje online účty. Nepoužívajte ľahko uhádnuteľné heslá ako „123456“ alebo „heslo“. Zvážte použitie správcu hesiel na bezpečné generovanie a ukladanie zložitých hesiel.
- ***Povoľte viacfaktorovú autentifikáciu (MFA):*** Kedykoľvek je to možné, povoľte na svojich online účtoch viacfaktorové overenie. MFA pridáva ďalšiu vrstvu zabezpečenia tým, že okrem hesla vyžaduje aj druhú formu overenia, ako je napríklad jednorazový kód odoslaný na vaše mobilné zariadenie.
- ***Udržujte softvér a zariadenia aktualizované***: Pravidelne aktualizujte svoj operačný systém, webové prehliadače a softvérové aplikácie. Aktualizácie často obsahujú bezpečnostné záplaty, ktoré riešia známe zraniteľnosti.
- ***Buďte opatrní pri e-mailoch a odkazoch***: Buďte opatrní pri otváraní e-mailov od neznámych odosielateľov alebo pri klikaní na podozrivé odkazy. Dávajte si pozor najmä na e-maily, ktoré požadujú citlivé informácie alebo vás nasmerujú na prihlásenie na falošnú webovú stránku.
- ***Zabezpečte svoju domácu sieť***: Zmeňte predvolené heslo na domácom smerovači Wi-Fi a povoľte šifrovanie WPA2 alebo WPA3 na ochranu vašej bezdrôtovej siete. Nepoužívajte verejné siete Wi-Fi na citlivé aktivity, pokiaľ nepoužívate virtuálnu súkromnú sieť (VPN).
- ***Pravidelne zálohujte dáta***: Pravidelne zálohujte dôležité súbory a dáta na externý pevný disk, cloudové úložisko alebo službu bezpečného zálohovania. V prípade straty údajov alebo ransomware útokov, zálohovanie zaisťuje, že budete môcť obnoviť svoje súbory.
- ***Používajte zabezpečenú Wi-Fi sieť a HTTPS***: Pri prístupe na citlivé webové stránky sa uistite, že používajú šifrovanie HTTPS. Ak chcete overiť bezpečnosť webovej stránky, vyhľadajte v paneli s adresou prehliadača symbol visiaceho zámku.
- ***Buďte opatrní pri sociálnych médiách***: Buďte opatrní pri informáciách, ktoré zdieľate na platformách sociálnych médií. Vyhnite sa zverejňovaniu osobných údajov, ako je vaša adresa, telefónne číslo alebo cestovateľské plány, pretože tieto informácie môžu byť použité na útoky v kontexte sociálneho inžinierstva.
- ***Nainštalujte si antivírusový a bezpečnostný softvér***: Na ochranu pred škodlivým softvérom a inými hrozbami používajte na svojich zariadeniach renomovaný antivírusový a bezpečnostný softvér. Udržujte softvér aktuálny, aby ste zaistili optimálnu ochranu.
- ***Vzdelávajte sa v oblasti kybernetickej bezpečnosti***: Buďte informovaní o najnovších hrozbách v oblasti kybernetickej bezpečnosti a osvedčených postupoch ochrany čítaním renomovaných zdrojov, navštevovaním webinárov alebo účasťou na programoch zameraných na zvyšovanie povedomia o kybernetickej bezpečnosti (Pozrite si zdroje o digitálnej bezpečnosti dostupné pre užívateľov).

Začlenením týchto pravidiel digitálnej bezpečnosti do každodennej rutiny môžu užívatelia výrazne znížiť riziko, že sa stanú obeťou hrozieb kybernetickej bezpečnosti, a tak ochrániť svoju digitálnu identitu.

3.4. Zdroje o digitálnej bezpečnosti dostupné pre užívateľov

Centrum vzdelávania v oblasti kybernetickej bezpečnosti (CEH) na Kalifornskej štátnej univerzite v San Marcos ponúka zdroje a usmernenia pre akademické a komunitné snahy o zvýšenie vzdelávania a informovanosti v oblasti o digitálnej bezpečnosti. CEH predstavuje kolektívnu spoluprácu Úradu pre informačnú bezpečnosť, technických a prírodovedných vysokých škôl a obchodnej správy.

CEH sa snaží zabezpečiť, aby vzdelávacie programy v oblasti digitálnej bezpečnosti riešili široké otázky súvisiace so súčasným dianím v oblasti digitálnej bezpečnosti a poskytuje príležitosti na začlenenie tém o digitálnej bezpečnosti do kurzov vyučovaných na celej univerzite. CEH ponúka zdroje študentom, študentským organizáciám a širokej verejnosti. Podporuje a uľahčuje komunikáciu a spoluprácu pri vzdelávaní v oblasti digitálnej bezpečnosti v celej komunite. Poskytuje učebné materiály na témy ako súkromie a sociálne médiá, kybernetická bezpečnosť pre študentov, kybernetická bezpečnosť dnes a koncepty kybernetickej bezpečnosti.

Okrem toho boli v roku 2008 zavedené školiace materiály ENISA o kybernetickej bezpečnosti. Odvtedy boli rozšírené o nové sekcie obsahujúce dôležité informácie v oblasti kybernetickej bezpečnosti. ENISA obsahuje školiace materiály, ako sú príručky pre učiteľov, súpravy nástrojov pre študentov a virtuálne obrázky, ktoré dopĺňajú praktické školenia.

4. Osvedčené postupy pre budovanie digitálnej bezpečnosti pre dospelých užívateľov

Digitálna bezpečnosť je v našej spoločnosti čoraz dôležitejšia a starší ľudia sú jednou z najzraniteľnejších skupín v online priestore. S napredovaním technológií napredujú aj kybernetické hrozby. Je preto dôležité zaviesť opatrenia a usmernenia na ochranu starších ľudí v digitálnom prostredí. Nižšie sú uvedené niektoré osvedčené postupy a úspešné opatrenia implementované v niekoľkých krajinách, ktoré môžu slúžiť ako referenčný rámec pre ostatných.

Stratégia kybernetickej bezpečnosti Európskej únie je uvedená v správach, ktoré sú všetky dostupné na oficiálnej webovej stránke Európskej komisie a poskytujú cenné informácie o osvedčených postupoch pre zlepšenie digitálnej bezpečnosti v Európe.

4.1. Kľúčové odporúčania pri budovaní digitálnej bezpečnosti

Táto časť sa môže zdať zopakovaním časti 3.3. Odporúčania v oblasti digitálnej bezpečnosti pre užívateľov, obsahuje však viac scenárov a príkladov z reálneho sveta.

Silné heslá: Pomôžte im vytvoriť silné a jedinečné heslá pre každý účet. Heslá musia byť dlhé (najmenej 8 znakov) a musia obsahovať veľké a malé písmená, čísla a špeciálne znaky. Vyhnite sa používaniu predvídateľných osobných údajov, ako sú mená alebo dátumy narodenia. Zdôraznite im, aby svoje heslá s nikým nezdieľali a pravidelne ich menili.

Silné heslo môže byť napríklad „P@ssw0rd2023!“ ktorý kombinuje veľké písmená, malé písmená, čísla a špeciálne znaky. Vyhnite sa používaniu predvídateľných osobných informácií, ako sú mená alebo dátumy narodenia, ako napríklad „John1980“ alebo „MarySmith123“.

Vzdelávanie a povedomie: Informujte ich o online rizikách a hrozbách, ako je phishing, malware a krádež identity. Pomôžte im naučiť sa, ako tieto situácie rozpoznať a vyhnúť sa im. Je dôležité poučiť ich o online rizikách, ako je phishing (pokusy o podvodné získanie dôverných informácií), malware a krádež identity. Naučte ich rozpoznať varovné signály a vyhnúť sa pádu do nastražených online pascí. Vysvetlite im možné negatívne dopady a aj to, ako sa chrániť.

Vysvetlite im napríklad, že phishingové e-maily môžu pôsobiť, že pochádzajú z legitímnych zdrojov a žiadajú ich, aby klikli na odkazy a zadali citlivé informácie. Ukážte im príklady podozrivých e-mailov a možnosti, ako ich identifikovať. Poskytnite im informácie o bežných typoch malwaru, ako sú falošný antivírusový softvér alebo vyskakovacie okná, a ako sa im vyhnúť.

Dvojfaktorové overenie (2FA): Pomôžte im implementovať dvojfaktorové overenie vždy, keď je to možné. Dvojfaktorová autentifikácia pridáva ďalšiu vrstvu zabezpečenia. Ak je to možné, pomôžte im povoliť túto funkciu vo všetkých účtoch. 2FA vyžaduje okrem štandardného hesla aj inú metódu autentifikácie, ako je kód textovej správy, autentifikátor alebo odtlačok prsta.

Napríklad po zadaní hesla im príde textová správa s overovacím kódom, ktorý je potrebné zadať pre prístup k svojmu účtu. To pridáva ďalšiu vrstvu zabezpečenia a sťažuje neoprávneným používateľom prístup k ich účtom.

Bezpečné používanie mobilných zariadení: Pomôžte im nastaviť zámky obrazovky, rozpoznávanie tváre alebo odtlačky prstov na ochranu mobilných zariadení. Pripomeňte im, aby nezdieľali svoje zariadenia s ľuďmi, ktorých nepoznajú, a aby boli opatrní pri sťahovaní aplikácií z nespoľahlivých zdrojov.

Ukážte im napríklad, ako povoliť PIN alebo použiť odtlačok prsta na odomknutie smartfónu. Pripomeňte im, aby nezdieľali svoje zariadenia s ľuďmi, ktorých nepoznajú, a aby boli opatrní pri sťahovaní aplikácií z nespoľahlivých zdrojov.

Aktualizácie softvéru: Zaistite, aby zariadenia (počítače, tablety, smartfóny) mali nainštalované najnovšie bezpečnostné záplaty a aktualizácie. Aktualizácie často obsahujú opravy známych zraniteľností, takže pravidelná aktualizácia zariadení ich pomáha chrániť.

Online nakupovanie: Zdôraznite im, aby nakupovali iba na spoľahlivých a bezpečných webových stránkach a používali bezpečné spôsoby platby. Naučte ich hľadať zámok v paneli s adresou a používať bezpečné spôsoby platby, ako sú kreditné karty s dodatočnými bezpečnostnými opatreniami.

Bezpečné používanie e-mailu: Upozornite ich na phishing a na to, aby sa vyhýbali klikaniu na odkazy alebo sťahovaniu príloh od neznámych odosielateľov. Upozornite ich na e-mailový phishing, kedy sa podvodníci snažia získať citlivé informácie tváriac sa ako legitímni odosielatelia. To poukazuje na dôležitosť neklikania na odkazy alebo nesťahovania príloh z podozrivých e-mailov alebo od neznámych odosielateľov.

Sociálne médiá: Pomôžte im upraviť nastavenia ochrany osobných údajov na sociálnych médiách tak, aby mali kontrolu nad tým, kto vidí ich príspevky, a aby sa vyhli zdieľaniu citlivých osobných údajov. Naučte ich, aby sa vyhýbali zdieľaniu citlivých informácií, ako sú telefónne čísla, adresy alebo finančné informácie na verejných sociálnych sieťach.

Preveďte ich napríklad nastaveniami súkromia na Facebooku tak, aby ste obmedzili sledovanie ich príspevkov iba pre priateľov. Zdôraznite dôležitosť opatrnosti pri zdieľaní informácií, ako sú telefónne čísla, adresy alebo finančné podrobnosti na platformách sociálnych médií.

Bezpečné prehliadanie: Naučte ich rozpoznávať zabezpečené webové stránky ("https" a "lock") a vyhýbať sa klikaniu na podozrivé odkazy alebo sťahovať neznáme súbory. Naučte ich rozlišovať zabezpečené webové stránky tak, že si skontrolujú zámok v paneli s adresou a či je spustené „https“ namiesto „http“. Vysvetlite im, aké je dôležité vyhýbať sa klikaniu na podozrivé odkazy alebo sťahovať súbory z neznámych zdrojov, pretože môžu obsahovať malware alebo ich môžu presmerovať na podvodné webové stránky.

Zabezpečenie Wi-Fi siete: Uistite sa, že vo svojej domácej Wi-Fi sieti používajú silné heslá a upozornite ich, aby sa vyhýbali pripájaniu k verejným alebo neznámym Wi-Fi sieťam.

Vysvetlite dôležitosť používania silných hesiel v domácej sieti Wi-Fi a dôležitosť vyhýbania sa pripájaniu k verejným alebo neznámym sieťam Wi-Fi. Nezabezpečené siete Wi-Fi môžu byť potenciálne napadnuté alebo odpočúvané za účelom špionáže údajov.

Neaktívne účty: Pomôžte im zrušiť alebo odstrániť online účty, ktoré už nepoužívajú, aby sa znížilo bezpečnostné riziko. Neaktívne účty môžu byť zraniteľné, najmä ak obsahujú osobné informácie.

***Pozor na podozrivé volania a správy*:** Naučte ich, aby nezverejňovali osobné alebo finančné údaje pri neočakávaných volaniach alebo správach. Naučte ich byť opatrní pri prezrádzaní osobných alebo finančných informácií pri nečakaných volaniach alebo SMS správach. Poraďte im, aby si overili totožnosť druhej strany. Uveďte príklady bežných podvodov, ako sú falošné telefonáty technickej podpory alebo oznámenia o výhre v lotérii.

Dohľad a podpora: Ponúknite pomoc s pravidelnými kontrolami online účtov a pomôžte im, ak majú podozrenie na podozrivé aktivity alebo majú problémy so zabezpečením. Buďte v obraze s najnovšími online hrozbami a poskytujte nepretržité poradenstvo a podporu. Ukážte im napríklad, ako si skontrolovať nedávnu aktivitu účtu a prihlásenia na rôznych platformách.

Osobné informácie: Naučte ich, aby boli opatrní pri zdieľaní osobných údajov online a obmedzili množstvo informácií, ktoré zverejňujú a aby obmedzili množstvo informácií takého druhu, ako sú adresy, telefónne čísla alebo informácie o škole. Podporuje to súkromie a dôležitosť ochrany online identity.

Zálohovanie dôležitých údajov: Pravidelne je potrebné zálohovať dôležité údaje, aby sa predišlo strate v prípade narušenia bezpečnosti alebo zlyhania zariadenia***.***

4.2. Osvedčené postupy v rámci celého sveta

4.2.1. Cyber Europe

ENISA od roku 2010 organizuje akciu Cyber Europe[1], sériu cvičení zameranú na kybernetické hrozby a krízový manažment, ktoré prezentujú scenáre inšpirované skutočnými udalosťami a sú vyvinuté európskymi odborníkmi na kybernetickú bezpečnosť. Každé dva roky verejný a súkromný sektor z krajín EÚ a EHP, ako aj európske inštitúcie, orgány a agentúry spolupracujú na posilnení svojich existujúcich technických a operačných možností a schopností.

Cvičenie Cyber Europe prebieha počas dvoch dní a simuluje rozsiahle incidenty v oblasti kybernetickej bezpečnosti, ktoré eskalujú do kybernetických kríz zasahujúcich celú EÚ. Účastníci tohto cvičenia budú schopní analyzovať pokročilé technické incidenty v oblasti kybernetickej bezpečnosti, riešiť zložité situácie súvisiace s kybernetickou bezpečnosťou a krízovým manažmentom, ktoré si vyžadujú koordináciu a spoluprácu od regionálnej úrovne až po úroveň EÚ.

Séria cvičení Cyber Europe má za cieľ zlepšiť pripravenosť Európy na riešenie rozsiahlych incidentov a kríz v oblasti kybernetickej bezpečnosti tým, že účastníkom umožní otestovať a zlepšiť svoju pripravenosť v rámci celej EÚ, vybudovať dôveryhodnosť v systéme kybernetickej bezpečnosti EÚ a poskytnúť príležitosti na ďalšie vzdelávanie.

Účasť na Cyber Europe poskytuje vynikajúce príležitosti na:

- Zvyšovanie kybernetického povedomia
- Vytvorenie a/alebo otestovanie postupov kybernetického krízového manažmentu
- Zlepšenie komunikácie v rámci reťazca kybernetickej odozvy
- Vytvorenie spoločného jazyka a zlepšenie vzájomného porozumenia
- Rozvíjanie rôznych individuálnych a kolektívnych schopností a zručností v kontexte digitálnej odolnosti
- Analýza zložitých technických incidentov v oblasti kybernetickej bezpečnosti; zvládnutie zložitých situácií v kontexte kontinuity podnikania a krízového manažmentu.

4.2.2. Adaptácia užívateľského rozhrania a technológie

Japonsko bolo priekopníkom v prispôsobovaní technológií a zariadení takým spôsobom, aby boli prístupnejšie pre starších ľudí. Napríklad niektoré japonské smartfóny a tablety majú jednoduchšie používateľské rozhrania a vylepšené funkcie dostupnosti, vďaka čomu ich môžu ľahšie používať ľudia s obmedzenými digitálnymi zručnosťami. Iné krajiny a výrobcovia technológií môžu prijať podobné zásady, aby tým zabezpečili, že starší užívatelia budú môcť používať digitálne zariadenia bezpečne a efektívne. Prijatie týchto zásad inými krajinami a výrobcami technológií môže zabezpečiť, že starší užívatelia budú mať prístup k užívateľsky prívetivejším digitálnym zariadeniam, čo pomôže zlepšiť ich online bezpečnosť a pohodu.

Na európskom území existuje niekoľko kurzov zameraných na zvýšenie informovanosti starších ľudí o používaní týchto nástrojov. Napríklad združenie ACDA v Paríži ponúka cenovo dostupné kurzy, aby starším ľuďom predstavila svet digitálnych technológií. Kurzy tohto združenia ponúkajú možnosť naučiť sa od základov ovládať počítač, počítačové jednotky, aplikácie alebo formáty súborov. Potom môžu účastníci získať pokročilejšie zručnosti, ako je správa a organizácia poštových schránok a naučiť sa používať Word pri spracovávaní písomného dokumentu[1].

4.2.3. Linky pomoci a špecializovaná podpora

Singapur zriadil vlastnú linku pomoci pre seniorov, ktorí čelia problémom s digitálnou bezpečnosťou. Táto linka pomoci ponúka rady a technickú pomoc pri riešení problémov s kybernetickou bezpečnosťou. Iné krajiny môžu zvážiť zavedenie podobných služieb, aby poskytli priamy a bezpečný komunikačný kanál pre seniorov, ktorí potrebujú online pomoc. Tieto služby poskytujú starším ľuďom priamy a bezpečný komunikačný kanál na získanie pomoci s problémami v oblasti kybernetickej bezpečnosti, ako sú napr. online podvody alebo malware. Zavedenie podobných služieb v iných krajinách môže byť dôležitou podporou na ochranu starších ľudí v digitálnom svete.

Napríklad na európskom území združenie AGE UK[2] uprednostňuje podporu starších ľudí, ktorí sú najviac zraniteľní digitálnym prostredím.

Okrem poskytovania služieb pre staršiu populáciu sa kurzy zameriavajú najmä na pomoc vysokorizikovej skupine pri prístupe do digitálneho sveta. Hoci základné komponenty programu zostávajú pri práci s týmito vysoko rizikovými skupinami do značnej miery nezmenené, pravdepodobne budú potrebné určité úpravy, aby sa zabezpečilo, že program zostane dostupný a efektívny pre tých, ktorí ho najviac potrebujú.

Služby v programe Digital Champion sa zameriavajú na starších ľudí, ktorí:

- Majú demenciu a/alebo stratu pamäti
- Majú nízky príjem
- Žijú sami
- Majú problémy s mobilitou
- Sú viazaní na domácnosť.

4.2.4. Kampane na zvyšovanie informovanosti a vzdelávania

Krajiny ako Austrália a Kanada zaviedli kampane pre kybernetickú bezpečnosť a vzdelávacie programy v oblasti digitálnej bezpečnosti pre starších užívateľov. Tieto kampane poskytujú informácie o bežných kybernetických hrozbách, tipy, ako sa chrániť pred online podvodmi, a o tom, aké dôležité je udržiavať svoje zariadenia aktualizované. Vlády môžu spolupracovať s miestnymi organizáciami, komunitnými centrami a dobrovoľníckymi skupinami, aby oslovili staršiu populáciu a poskytli školenie o digitálnych zručnostiach. Cieľom týchto informačných a vzdelávacích kampaní je posilniť sebavedomie starších ľudí prostredníctvom vzdelávania v oblasti digitálnej bezpečnosti. Učia sa, ako identifikovať a vyhnúť sa online podvodom, chrániť svoje osobné údaje a používať bezpečnostné nástroje, ako sú antivírus a silné heslá. Sú tiež informovaní o rizikách spojených s používaním sociálnych médií a o dôležitosti správneho nastavenia online súkromia. Združenie ACDA v Paríži, uvedené vyššie, ponúka aj kurzy digitálnej bezpečnosti.

Ďalším združením, ktoré sa zameriava na digitálne povedomie, je Nadácia Orange, ktorá informuje zraniteľné skupiny o najnovších technológiách a smeruje ich k bezpečnejšiemu využívaniu digitálneho sveta [2].

Okrem toho Nadácia Orange organizuje celý rad bezplatných digitálnych školiacich kurzov po celom Francúzsku pre mladých ľudí a ženy, ktoré sú často nezamestnané, nemajú potrebnú kvalifikáciu a niekedy sa nachádzajú v zložitých životných situáciách. Trénovanie takejto skupiny ľudí v digitálnych zručnostiach im pomáha resocializovať sa, hľadať si prácu, osvojiť si profesionálne využitie digitálnych technológií, rozvíjať podnikanie alebo dokonca venovať sa tejto problematike profesionálne.

4.2.5. Programy finančnej ochrany

Krajiny ako Spojené kráľovstvo a USA[2] zaviedli opatrenia na ochranu dôchodcov pred online finančnými podvodmi. Tieto opatrenia zavádzajú limity zodpovednosti pre obete podvodu a opravné prostriedky na spätné získanie odcudzených finančných prostriedkov. Iné krajiny môžu preskúmať tieto iniciatívy a prispôsobiť ich svojim podmienkam, aby ochránili seniorov pred možnými finančnými stratami. Finančná ochrana starších užívateľov je dôležitou súčasťou digitálnej bezpečnosti. Programy špeciálne navrhnuté na prevenciu a zmiernenie online finančných podvodov môžu poskytnúť tejto časti populácie vyššiu úroveň bezpečnosti. Potrebné je stanovenie limitov zodpovednosti pre obete podvodov a vytvorenie mechanizmov na vymáhanie odcudzených peňazí. Tieto opatrenia nielen chránia finančnú pohodu starších užívateľov, ale vysielajú aj jasný odkaz, že ich pohoda a finančné zabezpečenie sa berú vážne.

V Európe je stanovenie limitov zodpovednosti pre obete podvodov dôležitým aspektom ochrany finančnej pohody starších užívateľov. Keď sú obete podvodu brané na zodpovednosť za finančné straty, ktoré utrpia, môže to viesť k vážnym následkom vrátane finančného krachu a emocionálneho utrpenia. Uplatňovaním opatrení, ktoré stanovujú primerané limity zodpovednosti, spoločnosť berie do úvahy možné zraniteľnosti, ktorým čelia starší užívatelia, a snaží sa zmierniť záťaž, ktorá je na nich kladená. Tieto opatrenia poskytujú záchrannú sieť, ktorá zabezpečuje, aby starší užívatelia neboli nespravodlivo zaťažovaní dôsledkami podvodných činností. Stanovenie hraníc zodpovednosti pre obete podvodov je kľúčovým aspektom ochrany finančnej pohody starších ľudí. Na európskej pôde sa veľa združení venuje ochrane starších ľudí, ktorí sú často obeťami online podvodov, pretože nemajú dostatok znalostí a môžu utrpieť finančné straty. Jednou z takýchto asociácií je Marketing Management IO (MMIO), certifikovaná agentúra v Španielsku a Francúzsku[2].

Keď sú obete podvodu brané na zodpovednosť za svoje finančné straty, môže to viesť k vážnym následkom. Preto je dôležitá informovanosť. Uplatňovaním opatrení, ktoré stanovujú primerané limity zodpovednosti, spoločnosť uznáva možné zraniteľné miesta starších ľudí a snaží sa zmierniť ich záťaž. Tieto opatrenia poskytujú záchrannú sieť, ktorá zabezpečuje, aby starší ľudia neboli nespravodlivo zaťažovaní následkami podvodných činností.

Marketing Management IO (MMIO) zahŕňa témy ako internetové príležitosti, prirodzené referencie, online viditeľnosť, obsahový marketing a zvyšovanie predaja. Koncepty sú zjednodušené a prístupy sú bezplatné. K dispozícii sú aj bonusové zdroje.

Kurz obsahuje 5 lekcií s videami. Facebook ponúka platformu s bezplatným prístupom k viac ako 70 online kurzom. Tieto kurzy sa konkrétne zameriavajú na používanie Facebooku na zlepšenie online aktivít, predaja, bezpečnosti a celkového online povedomia.

4.2.6. Spolupráca s technologickým priemyslom

Niektoré krajiny, ako napríklad Spojené štáty americké, uzavreli partnerstvo s technologickými spoločnosťami s cieľom riešiť problémy digitálnej bezpečnosti v súvislosti so staršou populáciou. Táto spolupráca môže zahŕňať zlepšenie bezpečnostného softvéru, zlepšenie detekcie podvodov a implementáciu bezpečnostných funkcií v digitálnych produktoch a službách. Spolupráca s technologickým priemyslom môže predstavovať jednak efektívny spôsob, ako čeliť najnovším bezpečnostným hrozbám a jednak riešenia, ako sú implementácia pokročilých bezpečnostných technológií, zlepšenie detekcie podvodov a podpora bezpečnostných postupov pre digitálne produkty a služby zamerané na starších ľudí. Spolupráca s technologickým priemyslom zabezpečuje rýchlejšiu a adekvátnejšiu reakciu na digitálne hrozby.

Iné krajiny ako napr. Francúzsko a Anglicko majú kurzy digitálnej bezpečnosti, ktoré pomáhajú starším ľuďom pochopiť obranné technológie; ponúkané kurzy im umožňujú vybudovať základy v oblasti digitalizácie a naučiť sa, ako sa bezpečne pohybovať na internete.

Napríklad Konexio[2] ponúka školenia v oblasti digitálnych zručností – od najelementárnejších po najpokročilejšie – na podporu sociálnej a profesionálnej integrácie. Školiace kurzy sú inovatívne, založené na praktických prípadových štúdiách a so silným dôrazom na prierezové a vzťahové zručnosti alebo mäkké zručnosti, a majú za cieľ umožniť každému zapojiť sa do digitálnej spoločnosti. Ponúkajú rôzne formáty: digitálne zručnosti, webdizajnér, systémový a sieťový technik, digitálni pomocníci. Program sa zameriava na osvojenie si mäkkých zručností a sociálnych kódexov profesionálneho sveta prostredníctvom workshopov. Ponúkajú tiež možnosti priameho prepojenia s profesionálnym svetom prostredníctvom vlastnej siete a pravidelné sledovanie a personalizovanú podporu, aby pomohli klientom napredovať a vyriešiť akékoľvek ťažkosti, s ktorými sa môžu stretnúť.

4.2.7. Medzinárodné zdroje, správy a iniciatívy

Tieto zdroje poskytujú cenné usmernenia a osvedčené postupy na zlepšenie digitálnej bezpečnosti vo vzdelávaní dospelých v EÚ.

Otvorený a bezpečný kybernetický priestor: Táto správa poskytuje prehľad stratégie pre kybernetickú bezpečnosť EÚ, ktorej cieľom je podporovať otvorený a bezpečný kybernetický priestor v Európe. Správa obsahuje osvedčené postupy na zlepšenie

kybernetickej bezpečnosti vrátane riadenia rizík, reakcií na incidenty a na zefektívnenie spolupráce verejno-súkromných sektorov.

Správa ENISA o hrozbách: Táto správa Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) poskytuje prehľad o súčasnom stave kybernetických hrozieb v Európe vrátane najbežnejších typov kybernetických útokov a najviac ohrozených sektorov. Správa obsahuje osvedčené postupy na predchádzanie a zmierňovanie kybernetických útokov, vrátane školení o bezpečnosti, riadenia zraniteľnosti a plánovania reakcií na incidenty.

Smernica NIS a zákon EÚ o kybernetickej bezpečnosti: Táto správa poskytuje prehľad právneho rámca EÚ o kybernetickej bezpečnosti, vrátane smernice o sieťových a informačných systémoch (NIS) a zákona EÚ o kybernetickej bezpečnosti. Správa obsahuje osvedčené postupy na dodržiavanie zákonných požiadaviek, ako je hlásenie incidentov a riadenie rizík.

Certifikačný rámec kybernetickej bezpečnosti EÚ: Táto správa poskytuje prehľad certifikačného rámca o kybernetickej bezpečnosti EÚ, ktorého cieľom je zlepšiť bezpečnosť a dôveryhodnosť digitálnych produktov a služieb. Správa obsahuje osvedčené postupy na získavanie a udržiavanie certifikátov kybernetickej bezpečnosti už od návrhu, testovania, hodnotenia a priebežného monitorovania.

Kybernetická bezpečnosť pre MSP: Táto správa poskytuje malým a stredným podnikom (MSP) usmernenia a osvedčené postupy, ako zlepšiť ich postavenie v oblasti kybernetickej bezpečnosti. Správa obsahuje rady pre prevenciu rizík, rady pre školenia o bezpečnosti, vývoj bezpečného softvéru a plánovanie reakcií na incidenty.

Digitálne zručnosti u dospelej populácie: Táto správa Európskej komisie poskytuje prehľad o digitálnych zručnostiach dospelej populácie v EÚ. Zahŕňa časť o digitálnej bezpečnosti, ktorá zdôrazňuje potrebu, aby dospelí mali základné znalosti a zručnosti na ochranu pred kybernetickými hrozbami.

Digitálne zručnosti pre celoživotné vzdelávanie: Táto správa Európskej komisie poskytuje usmernenia a osvedčené postupy pre rozvoj digitálnych zručností u dospelých. Zahŕňa časť o digitálnom zabezpečení, ktorá poskytuje rady týkajúce sa riadenia rizík, bezpečného prehliadania, správy hesiel a ochrany údajov.

Projekt Kybernetická bezpečnosť pre digitálne vzdelávanie: Tento projekt Európskej školskej siete Schoolnet poskytuje zdroje a školenia o kybernetickej bezpečnosti pre učiteľov a študentov v Európe. Projekt zahŕňa celý rad materiálov vrátane online kurzov, plánovania a nástrojov hodnotenia, pričom všetky sú zamerané na problematiku zlepšenia digitálnej bezpečnosti vo vzdelávaní.

Projekt Digitálna bezpečnosť pre seniorov: Tento projekt Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) poskytuje zdroje a školenia o kybernetickej bezpečnosti pre starších občanov. Projekt zahŕňa celý rad materiálov vrátane online kurzov, sprievodcov a videí, ktoré sú všetky zamerané na problematiku zlepšenia digitálnej bezpečnosti medzi staršími užívateľmi.

Koalícia digitálnych zručností a pracovných miest: Cieľom tejto iniciatívy Európskej komisie je zlepšiť digitálne zručnosti Európanov, aby sa mohli plne zapojiť do digitálneho hospodárstva. Zahŕňa celý rad zdrojov a príležitostí na školenie, a to aj v oblasti digitálnej bezpečnosti.

4.3. Osvedčené postupy vzdelávania dospelých v oblasti digitálnej bezpečnosti

ENISA program "Učiť školiteľa"

Všetky online školiace materiály a školiace kurzy v sekcii 'Školenia pre špecialistov na kybernetickú bezpečnosť' sú založené na filozofii 'Učiť školiteľa'. Cieľom programu a filozofie „Učiť školiteľa" je rozšíriť sieť školiteľov a podporiť lepšiu výmenu informácií. Bude to mať niekoľko účelov, napr.:

- zdieľanie školiacich materiálov s cieľom ušetriť čas a peniaze na školenia,
- vytváranie regionálnych vzdelávacích združení,
- podpora spolupráce medzi rôznymi poskytovateľmi školení,
- propagácia osvedčených tréningových postupov,
- obmedzenie konkurencie a duplicity.

Online školiace materiály agentúry ENISA budú zahŕňať príručku pre školiteľov, sadu nástrojov pre študentov a virtuálne nástroje na stiahnutie. To umožňuje potenciálnym školiteľom pripraviť kurz a príručka im pomôže viesť študentov v kurze správnym spôsobom. Bude obsahovať rôzne cvičenia a malé testy, aby sa zistilo, či študenti pochopili dôležité lekcie z kurzov, a ďalšie informácie alebo cvičenia, ktoré môže školiteľ použiť na to, aby bol kurz zaujímavejší alebo náročnejší.

Vzájomné učenie sa zo svojich úspechov a neúspechov umožňuje začínajúcim aj skúseným školiteľom lepšie navrhovať a viesť školenia, vďaka čomu budú úspešnejšie, „zábavnejšie" a s lepšími a trvácnejšími výsledkami.

TiK – Technológia v skratke

Projekt sleduje medzigeneračný prístup prostredníctvom školení, ktoré ponúkajú mladí dobrovoľníci (vo veku 16 až 30 rokov) ako takzvaní „Tablet-Tréneri", ktorí vzdelávajú podľa špeciálneho študijného plánu pre „tabletové" vzdelávanie. Kurzy sa vyznačujú množstvom metód, flexibilných úloh a osobitným nasadením mladých trénerov. Ďalší rozvoj kurzov podporuje aj spätná väzba od účastníkov a lektorov, ktorí vypracovali aj vlastné špeciálne učebné materiály pre seniorov. Kurzy sú pre záujemcov ľahko dostupné a veľká pozornosť sa venuje širokej geografickej distribúcii „TiK modulov" a informáciám na www.digitaleseniorinnen.at. Účastníkmi kurzov sú najmä ekonomicky znevýhodnené ženy na nízkej vzdelanostnej úrovni. Do konca roka 2018 sa v týchto moduloch učilo viac ako 2000

osôb a ďalších 1000 osôb sa zúčastnilo na kurze. Najstarší účastník, ktorý sa práve zúčastňuje kurzu, má 97 rokov a vzdeláva sa u mladého muža v detskom domove. Projekt bol niekoľkokrát ocenený na federálnej a regionálnej úrovni.

5. Školenie dospelých: Ako si vybudovať digitálnu odolnosť

Andragogika ako štúdium vzdelávania dospelých vznikla v Európe v 50. rokoch 20. storočia, ale až v 70. rokoch bol priekopníkom tejto teórie a modelu vzdelávania dospelých Malcolm Knowles, americký praktik a teoretik vzdelávania dospelých, ktorý definoval andragogiku ako „umenie a vedu pomáhať dospelým učiť sa“ (Fidishun 2000). Fidishun (2000) odporúčal, aby sa pri navrhovaní online vzdelávania použili andragogické princípy za účelom uľahčenia „flexibility a schopnosti študentov pohybovať sa cez lekcie kedykoľvek, kdekoľvek a vlastným tempom“.

5.1. Štyri princípy andragogiky

Vzhľadom k tomu, že dospelí majú svoj vlastný, špecifický spôsob učenia sa, existujú 4 hlavné princípy, na základe ktorých možno čo najefektívnejšie prispôsobiť vzdelávanie pre nich.

• Pokiaľ ide o učenie sa, dospelí chcú alebo musia byť zapojení do toho, ako sa ich školenie plánuje, poskytuje a realizuje. Chcú mať pod kontrolou, čo, kedy a ako sa učia.

• Dospelí získajú viac, keď môžu preniesť minulé skúsenosti do procesu učenia sa. Môžu čerpať z toho, čo predtým poznali, aby dodali svojmu učeniu širší kontext.

• Memorovanie faktov a informácií nie je pre dospelých správny spôsob učenia sa. Potrebujú riešiť problémy, uvažovať a argumentovať, aby čo najlepšie spracovali informácie, ktoré sú im prezentované.

• Dospelí chcú vedieť „Ako môžem teraz použiť tieto informácie?“. To, čo sa učia, musí byť použiteľné v živote a musí byť okamžite implementované.

5.2. Ako budú školitelia dospelých implementovať andragogiku

Umožnenie samoriadeného učenia sa

V minulosti bolo učenie sa často povinnosťou vykonávanou v určitom čase. Teraz s využitím technológií, ako je napr. systém riadenia vzdelávania, môžeme pre dospelých vytvoriť oveľa samostatnejšie a nezávislejšie vzdelávacie prostredie. Môžeme im umožniť školiť sa kedy a kde chcú, ponúknuť im výber kurzov, do ktorých sa môžu prihlásiť, a umožniť im, aby mali svoje vlastné vzdelávacie ciele.

Používanie príkladov z reálneho sveta

Ako uvádza teória, dospelí chcú vedieť, aké bude mať ich školenie okamžité uplatnenie a prínos. Pri vytváraní obsahu kurzu je potrebné doňho vložiť čo najviac príkladov z reálneho sveta.

Keď sa školia dospelí o digitálnej pohode a/alebo digitálnej bezpečnosti, treba ich previesť krok za krokom pracovným postupom, ktorý budú skutočne používať a explicitne uviesť ako, kedy a prečo ho majú používať. Treba uviesť, ako im školenie pomôže, a potom použiť na školenie skutočné príklady.

Nechajte dospelých, aby na to prišli sami

Keďže dospelí uprednostňujú riešenie problémov pred samotnými faktami, pri vytváraní obsahu je vhodné nezverejniť hneď všetky odpovede. Prečo sa radšej nezaoberať kreativitou a nevybudovať kurzy, ktoré rozhýbu mozgy študentov?

Môžeme to urobiť niekoľkými jednoduchými spôsobmi, vrátane pridania odhadov a simulácií, ktoré načrtnú špecifické problémy, s ktorými sa môžu skutočne stretnúť, a potom ich primäť k tomu, aby používali nadobudnuté zručnosti na ich prekonanie.

6. Záver

Digitálna bezpečnosť starších ľudí je kľúčovým problémom, ktorý si vyžaduje pozornosť a konanie zo strany vlád ako aj spoločnosti ako celku. Zavedením vyššie uvedených osvedčených postupov môžu krajiny zlepšiť digitálnu ochranu a pohodu u svojho staršieho obyvateľstva. Zvyšovanie povedomia, vzdelávanie, špecializovaná podpora, technologická adaptácia a priemyselná spolupráca sú kľúčovými piliermi na zabezpečenie bezpečnej a pozitívnej online skúsenosti pre starších dospelých.

Cieľom projektu DigiWELL je začleniť princípy digitálnej pohody do vzdelávania dospelých. Jeho iniciatívy smerujú k zlepšovaniu celkových postupov organizácií v oblasti vzdelávania dospelých. Projekt chápe, aké dôležité je riešiť skutočnosť ako technológie ovplyvňujú duševné zdravie, produktivitu a celkovú pohodu dospelých v digitálnom veku. Hlavným cieľom projektu DigiWELL je poskytnúť dospelým užívateľom informácie, schopnosti a zdroje potrebné na etický a zodpovedný pohyb v digitálnom svete. Projekt DigiWELL tiež zahŕňa vytvorenie a realizáciu ďalších aktivít na posilnenie digitálneho povedomia dospelých užívateľov. Cieľom týchto aktivít je poskytnúť podporné prostredie, kde sa dospelí môžu podeliť o svoje skúsenosti, ťažkosti a úspechy pri získavaní digitálnej pohody. S ohľadom na túto skutočnosť projekt DigiWELL predstavuje množstvo príležitostí pre jednotlivcov a organizácie, aby si uvedomili dôležitosť digitálnej pohody a o tom, ako podporovať digitálnu pohodu u dospelých jednotlivcov, pedagógov a školiteľov dospelých. Implementácia digitálnej pohody s holistickým prístupom je oveľa viac možná, ak všetky príslušné strany prijmú

opatrenia na podporu potrieb jednotlivcov v tejto oblasti. V dôsledku toho informácie, tipy a osvedčené postupy uvedené v tejto príručke vyzývajú ľudí a zainteresované organizácie, aby sa chopili iniciatívy za účelom zlepšenia digitálnej pohody a digitálneho života nás všetkých.

7. Referencie

Pri príprave slovníka boli použité voľne dostupné online zdroje: online slovníky, vedecké články a literatúra z oblasti informačnej bezpečnosti, digitálnych technológií a služieb, digitálnej pohody a digitálnej odolnosti, ako aj pojmy a definície z oblasti Informačnej bezpečnosti. Všetky zdroje sú uvedené v textovej databáze pracovnej verzie slovníka.

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