



Evropská unie
Evropský sociální fond
Operační program Zaměstnanost



Metodika identifikace osob digitálně vyloučených a digitálně negramotných



DigiStrategie
2020 | rozvoj systémové
podpory digitální
gramotnosti

Metodika identifikace osob digitálně vyloučených a digitálně negramotných

Název projektu:	Rozvoj systémové podpory digitální gramotnosti
Registrační číslo projektu:	CZ.03.1.54/0.0/0.0/16_020/0005634
Publikováno:	březen 2020
Autoři:	Pracovní skupina projektu DigiStrategie 2020
Koordinace:	Josef Šmída
Poděkování:	Jiří Chábera
Grafická úprava:	Anna Lhoťanová

Toto dílo *Metodika identifikace osob digitálně vyloučených a digitálně negramotných* je licencováno pod licencí Creative Commons Uveďte původ 3.0 Česká republika. Licenční podmínky navštivte na adrese <http://creativecommons.org/licenses/by/3.0/cz/>.

Obsah

O metodice	3
Cíl metodiky	3
1. Digitální vyloučení.....	4
1.1. Definice digitálního vyloučení	4
2. Digitální gramotnost	5
2.1. Definice digitální gramotnosti	5
3. Bezpečný pohyb v digitálním světě.....	7
3.1. Rizika na internetu.....	7
3.2. Rady pro bezpečné chování.....	10
4. Skupina děti a mladiství	13
4.1. Specifika dětí a mladistvých	13
4.2. Jak pracovat s dětmi a mladistvými.....	14
4.3. Jak na sociální síť a rizika dětí a mladistvých.....	15
4.4. Další informace a pomoc.....	19
5. Skupina senioři.....	21
5.1. Specifika seniorů	21
5.2. Jak pracovat se seniory	22
5.3. Digitalizace pro stárnoucí generaci	24
6. Skupina nezaměstnaní.....	26
6.1. Úvodní rozhovor	26
6.2. Dotazník	26
6.3. Navržená opatření a podpora UoZ.....	27

0 metodice

Tento materiál je metodickým výstupem projektu **Rozvoj systémové podpory digitální gramotnosti (zkráceně DigiStrategie 2020)**, který vypracovala jeho pracovní skupina složená z odbornic a odborníků nominovaných **Ministerstvem práce a sociálních věcí a Úřadem práce ČR**. Metodické uchopení problému a hlavní editační práce byly svěřeny sociálním vědcům z **FF UK**. Kapitoly týkající se práce s mládeží a seniory byly vypracovány ve spolupráci s MPSV. Dotazník pro uchazeče o zaměstnání a scénáře k rozhovoru pro nezaměstnané byl sestaven ve spolupráci se zaměstnanci ÚP ČR, kteří s těmito skupinami dlouhodobě pracují. Následně byly odzkoušeny a zkušenosti z této zkoušky byly promítnuty do finální podoby. Koordinace tvorby a finální zhotovení tohoto metodického nástroje - **Metodiky identifikace osob digitálně vyloučených a osob digitálně negramotných** byla v gesci **FDV, metodiků projektu DigiStrategie 2020**.

Metodika je určena komukoli, koho zajímají základy tématu **digitálního vyloučení a jeho identifikace**. Především má sloužit jako **metodická pomůcka pro práci s konkrétními skupinami**. Na základě analýzy české společnosti, zkušenosti expertů a hlavně během spolupráce s lidmi z terénu byly identifikovány tři skupiny, kterých se téma týká – **uchazeči o zaměstnání, mládež a senioři**.

Cíl metodiky

Účelem tohoto metodického nástroje je **jednoduchá a rychlá identifikace problému**. Nástroj rovněž nabízí vybrané **návrhy řešení pro jeho odstranění** nebo další práci v oblasti digitálního začleňování u námi vybraných cílových skupin.

Pro všechny skupiny navrhujeme základní metodický nástroj, jak postupovat při mapování problému v práci s klienty.

Při práci s metodikou si můžete buďto **vybrat jednu z cílových skupin, anebo se něco dozvědět o problematice digitálního vyloučení a digitální gramotnosti** nebo **bezpečném pohybu v digitálním světě**.

1. Digitální vyloučení

Co je digitální vyloučení? Proč se nás týká? O uchopení, pojmenování a definici digitálního vyloučení usiluje řada mezinárodních organizací včetně OSN. V této metodice pracujeme s problematikou digitálního vyloučení jako se sociálním jevem, který má a bude mít jistě stále větší dopad na kvalitu života jedince, jeho postavení ve společnosti, svobodu a uplatnění. Můžeme tak hovořit o novém typu sociálního vyloučení, jako o nové formě strukturální chudoby. Naším cílem je pracovat s pojmem digitálního vyloučení jakožto s významným činitelem současných společenských výzev, kterým musíme čelit za účelem udržení společenské soudržnosti. Cílem tak není pokusit se tento jev staticky definovat.

1.1. Definice digitálního vyloučení

Zde se dozvíte, jak definici digitálního vyloučení chápeme my a s jakou definicí metodika pracuje.

„Digitálně vyloučená je osoba, která nemá z různých příčin možnost používat digitální technologie a služby, a tím není začleněna do moderní společnosti.“¹ Nedostatečný přístup k internetu souvisí s ekonomickou, sociální, ale i geografickou situací určitých skupin obyvatel. Více digitálně vyloučených osob bude například v zemích třetího světa, kde jsou velmi špatné sociální podmínky, chybí zde dostatečná možnost volného šíření informací a rozdíly mezi obyvateli z hlediska digitální gramotnosti jsou tedy mnohem vyšší než v jiných státech.

Digitální vyloučení se týká především: „seniorů, osob se zdravotním postižením, osob s duševním onemocněním, etnických menšin, jednotlivců i lokalit ohrožených chudobou. Nejde o kompletní výčet – digitální vyloučení se objevuje napříč celou populací, a ne vždy se váže na jasné sociodemografické charakteristiky. Také z tohoto důvodu často zůstává u jednotlivců neidentifikováno.“² Můžeme tak říci, že ohrožení jsou v určité míře všichni.

Rozdíl mezi digitálně začleněnými a vyloučenými osobami lze nazvat jako digitální propast. Myšlenka „digitální propasti“ se odvolává na rostoucí propast mezi znevýhodněnými členy společnosti, zejména chudými, venkovskými, staršími a zdravotně postiženými částmi obyvatel, kteří nemají přístup k počítačům nebo internetu; a bohatými, středními třídami a mladými lidmi žijícími v městských a příměstských oblastech, kteří k digitálním technologiím přístup mají. Digitální vyloučení vedle nízké digitální gramotnosti s sebou nese ještě znevýhodnění a také nemožnost digitální bariéry překonat (žádat někde pomoc, vyřešit životní situaci bez digitálních technologií).

My jsme se také pokusili o první segmentaci české společnosti s ohledem na jejich digitální začlenění. Segmentaci a typologii osob digitálně vyloučených a osob ohrožených digitálním vyloučením naleznete na našem portále.³

1 Pojem digitální vyloučení, DigiSlovník [online] dostupný na <http://portaldigi.cz/digislovník/>

2 Strategie digitální gramotnosti ČR 2015-2020 [online] dostupná na https://www.mpsv.cz/files/clanky/21499/Strategie_DG.pdf

3 Segmentace a typologie osob digitálně vyloučených a osob ohrožených digitálním vyloučením v ČR [online] dostupné na PortálDigi <http://portaldigi.cz/segmentace/>

2. Digitální gramotnost

Co je digitální gramotnost? Proč je důležitá? O uchopení, pojmenování a definici digitální gramotnosti usiluje řada mezinárodních organizací včetně OSN. **V této metodice pracujeme s problematikou digitální gramotnosti jako se sociálním jevem**, který má a bude mít jistě stále větší dopad na kvalitu života jedince, jeho postavení ve společnosti, svobodu a uplatnění.

2.1. Definice digitální gramotnosti

Zde se dozvíte, jak definici digitální gramotnosti chápeme my a jak s ní v metodice pracujeme.

„Digitální gramotnost je schopnost používat informační a komunikační technologie k nalezení, zhodnocení, vytvoření a sdílení informací, což vyžaduje jak kognitivní, tak technické dovednosti.“⁴

V našem **DigiSlovníku**⁵ uvádíme: „Digitální gramotnost je soubor kompetencí nutných k identifikaci, pochopení, interpretaci, vytváření, komunikování a účelnému a bezpečnému užití digitálních technologií. Tyto kompetence využívá občan za účelem udržení či zlepšení své kvality života a kvality života svého okolí, tj. např. za účelem pracovní i osobní seberealizace, rozvoje svého potenciálu a udržení či zvýšení participace na společnosti.

Referenční model **DigComp**⁶ člení kompetence digitální gramotnosti do těchto oblastí:

1. Zpracování informací
2. Komunikace a spolupráce
3. Vytváření digitálního obsahu
4. Bezpečnost
5. Řešení problémů

Podle UNESCO může být digitální gramotnost chápána jako **soubor kompetencí nutných k identifikaci, pochopení, interpretaci, vytváření, komunikování a účelnému a bezpečnému užití digitálních technologií za účelem udržení či zlepšení své kvality života a kvality života svého okolí**. To znamená jejich využití například za účelem pracovní i osobní seberealizace, rozvoje svého potenciálu a udržení či zvýšení participace na společnosti.

Co si pod pojmem digitální gramotnost můžeme představit?

- Digitální gramotnost vyžaduje aktivní znalost technologií a porozumění tomu, jak mají být užívány.
- Digitálně gramotní lidé jsou schopni komunikovat a pracovat efektivněji zvláště s těmi, kteří ovládají stejné znalosti a dovednosti jako oni.
- Digitální gramotnost zahrnuje rovněž znalost různých digitálních zařízení, jako je počíta-

⁴ <https://perpetuum.cz/2016/12/digitalni-gramotnost/>

⁵ <http://portaldigi.cz/digislovník/digitalni-gramotnost/>

⁶ <https://ec.europa.eu/jrc/en/digcomp/digital-competence-framework>

čový hardware, software, internet nebo mobilní telefon.

- Nalezení a spotřebování digitálního obsahu – umět generovat klíčová slova, procházet výsledky vyhledávačů a posoudit spolehlivost stránek či autorů.
- Vytváření digitálního obsahu – to znamená dokázat psát e-maily, blogy, příspěvky na sociálních sítích, vytvářet audia a videa a k tomu zvládnout sociální dopady tvorby, které každý takový obsah může mít
- Komunikace a sdílení informací.

Nízká digitální gramotnost je daleko více rozšířená než digitální vyloučení. To totiž zpravidla vedle nízké digitální gramotnosti s sebou nese ještě znevýhodnění a také nemožnost digitální bariéry překonat (žádat někde pomoc, vyřešit životní situaci bez digitálních technologií).

3. Bezpečný pohyb v digitálním světě

Problematika pohybu po internetu je v této kapitole dělena do dvou sekcí. První se věnuje **rizikům, které s sebou nese užívání digitálních technologií**. Druhá poskytuje **radu pro bezpečné fungování na internetu**. Problematika obsažená v této kapitole **se týká v různé míře všech osob, které se pohybují na internetu**. V tomto případě tedy nejen klientů, ale i pracovníků. Pokud pojmy a zásady z této kapitoly znáte a víte, jak na jednotlivá rizika reagovat, jak s nimi pracovat, pokračujte klidně k části textu, která se zabývá specificky vaší skupinou.

3.1. Rizika na internetu

Zde se dozvíte základní výčet rizik, které nám digitální svět aktuálně přináší. Jsou to nejčastější rizika, se kterými je nutné se nejen seznámit, ale také vypořádat, pokud se v digitálním světě chceme bezpečně pohybovat. Platí to stejně tak i pro všechny tři cílové skupiny: uchazeči o zaměstnání, děti a mladiství, senioři.

Existuje skupina rizik, která ohrožuje všechny uživatele digitálních technologií bez ohledu na jejich sociodemografické charakteristiky. V následující kapitole jsou vybrány nejčastější rizika. Pokud pojmy z této kapitoly znáte a víte, jak na jednotlivá rizika reagovat, jak s nimi pracovat, pokračujte klidně k části textu, která se zabývá specificky vaší skupinou.

3.1.1. Malware a Spyware

Malware (zkratka anglického výrazu pro škodlivý software - „malicious software“) je program, který má za úkol vniknout do systému elektronického zařízení za účelem jeho poškození, ovládnutí, odcizení dat, sledování uživatele apod. Mezi typy malwaru patří spyware (doslova špionážní software), adware, viry, trojské koně, červi, rootkity, ransomware a změny nastavení prohlížeče.

Malware se nejčastěji šíří přes internet. Do zařízení, která nejsou chráněna antimalwarovým softwarem (běžně známý spíše pod pojmem antivirus), se dostává prostřednictvím napadených webových stránek, zkušebních verzí her, stažených programů či jakýchkoli jiných stažených dat. Napadený počítač může být výrazně zpomalený, může zobrazovat různá vyskakovací okna, samovolně rozesílat spamy nebo způsobovat pády systému. Při napadení spywarem může docházet k samovolnému odesílání citlivých informací ze zařízení bez vědomí jeho majitele – např. čísel bankovních účtů, přihlašovacích údajů, seznamů navštívených stránek apod.

3.1.2. Phishing

Pod pojmem phishing rozumíme „útoky na uživatele internetu prostřednictvím podvodných emailů, které mají za cíl vylákat ze svých obětí citlivé údaje, například PINy, hesla k internetovému bankovníctví, k platebním službám jako je PayPal, PaySec, nebo k jiným účtům.“ Název odkazuje na anglický termín pro rybaření (fishing), neboť ho tyto útoky skutečně připomínají. Útočníci nachystají návnadu (mail s urgentní výzvou k zaplacení nedoplatku, vyzvednutí nových přístupových údajů apod.), rozhodí síť (rozešlou na tisíce náhodně sesbíraných adres) a čekají, až se někdo chytne.

Podvodné zprávy se snaží působit co nejvěrohodněji, obvykle se vydávají za oficiální zprávy zaslané bankovními ústavy či podobnými institucemi. Grafika podvodného emailu napodo-

buje grafiku zpráv těchto oficiálních institucí, stejně tak se útočníci snaží vytvořit co nejpodobnější emailovou adresu a webové stránky. V textu může odkaz vypadat věrohodně, ale přesto bude směřovat na podvodné stránky. Proto je třeba se podívat, kam link skutečně odkazuje. Text emailu většinou obsahuje výzvu ke změně hesla, zaplacení dluhu, aktualizaci osobních a kontaktních údajů apod.

3.1.3. Práce s informacemi

Na internetu se nachází informace záměrně matoucí a zkreslené, informace neautorizované a konečně informace podložené. Informací je na internetu nezměrné množství a člověk má často problém věrohodnost informace správně posoudit.

Zdrojem různých mýtů, lží a polopravd jsou např. sociální sítě, kde informace kolují a mnohdy jsou sdíleny pouze za účelem zvýšení sledovanosti a rozdmýchání vášní diskutujících. Mohou to být také stránky, které na první pohled vypadají věrohodně. Patří sem informace typu hoax a mají za cíl zmanipulovat čtenáře k účelovému chování.

Neautorizované informace jsou takové, se kterými se na internetu setkáváme nejčastěji, a není u nich jasné, zda jde o tvrzení autora či převzatý text. Oproti tomu u autorizovaných informací je uveden autor, zdroj informace a zároveň je jasný i důvod, proč je tato informace publikována.

Při každodenním pohybu na internetu je třeba zdravý odstup, kritické myšlení a vytváření vlastního úsudku.

Při posuzování důvěryhodnosti textu by se měl čtenář zamyslet nad tím:

1. Kdo je autorem textu?
2. Na jakém webu je text uveřejněn?
3. Jaký je obsah textu, o čem pojednává?
4. Kdy byla informace publikována?
5. Co je cílem publikování této informace?

Všechny informace je dobré si ověřovat z více zdrojů.

Rozdíl mezi dezinformacemi a misinformacemi

Ne každá mylná informace je dezinformací. Je potřeba rozlišovat mezi dezinformací a misinformací.

Misinformace je nesprávná nebo zavádějící informace, která ovšem není šířena úmyslně s cílem ovlivnit rozhodování nebo názory těch, kteří ji přijímají. Misinformace se ve sdělovacích prostředcích vyskytuje poměrně často ve formě různých faktických nepřesností a je většinou odstraněna poté, co je na ni upozorněno.

Dezinformace je naproti tomu záměrně nepravdivá, nekompletní či zavádějící informace, která je šířena s cílem ovlivnit rozhodování nebo názory těch, kterým je určena. Pojmem dezinformační kampaň se pak rozumí soubor různých dezinformací používaných cíleně a soustavně k dosažení tohoto výsledku. Dezinformace může být šířena státními či nestátními aktéry s cílem působit na cizí stát, média nebo společnost.

Cílem původce dezinformace může být např.:

- přesvědčit cílové publikum o vlastní, často alternativní „pravdě“;
- utvrdit cílové publikum v jeho přesvědčení, které koresponduje s názory původce (velmi

efektivní metoda, jelikož využívá toho, že publikum je vůči dezinformaci „dobře naladěno“);

- mást skrze relativizaci faktů (úspěšným příkladem jsou dezinformace šířené v souvislosti se sestřelením letu MH17);
- odvést pozornost od skutečné podstaty problému či jiných závažnějších problémů;
- zahltit publikum informacemi a způsobit jeho dezorientaci v problematice.

3.1.4. Nenávistné projevy na internetu

Nenávistné projevy na internetu jsou novodobým fenoménem, který zaplnil sociální sítě a internetové diskuze. Tyto projevy většinou směřují proti menšinám - především Romům, migrantům, muslimům a homosexuálům.

Nenávistný projev je takový, který podněcuje, podporuje nebo šíří nenávist vůči určité skupině osob či jednotlivci. Ačkoli existuje svoboda slova, nenávistný projev zasahuje do práv druhého člověka (narušuje jeho důstojnost, vážnost a čest), nebo může naplnit skutkovou podstatu přestupku (přestupky proti občanskému soužití) či trestného činu (tzv. nenávistné trestné činy - násilí proti skupině obyvatelů a proti jednotlivci; hanobení národa, rasy, etnické nebo jiné skupiny osob; podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod). Takové jednání je zejména nebezpečné v utvrzování předsudků a stereotypů a v eskalaci nenávisti ve společnosti. Tyto projevy nelze považovat za „normální“ jen díky jejich četnosti, neboť působí jako rozbuška sociálních nepokojů a stupňování verbálního násilí může snadno vyústit až k násilí fyzickému. V tomto směru je třeba vychovávat jak oběti, tak agresory.

Proti nenávistným komentářům je třeba se jasně vymezit. Pokud se staneme terčem takového útoku, v první řadě je důležité nahlášení závadného obsahu provozovateli daných webových stránek a požádání o smazání příspěvku. Na komentář, který by mohl být přestupkem, upozorněte obecní úřad obce s rozšířenou působností. Podezření ze spáchání trestného činu oznamte na státní zastupitelství. Úřady jsou povinny se věcí zabývat, přestože v praxi zůstávají nenávistné projevy bez postihu. Proto žádejte, aby Vás úřady písemně informovaly, jak s Vaším podáním naložily. Pokud nejste spokojeni s postupem při prověřování trestního oznámení, obraťte se na nadřízené státní zastupitelství.

Vždy je třeba uchovávat všechny důkazy – screenshot obrazovky, video, komunikaci s pachatelem a veškeré údaje, které o něm máte k dispozici. Zároveň je nutné dbát na svoji bezpečnost, odstranit z internetu veškeré informace o své osobě a nedávat pachateli žádná vodítka, podle kterých by vás mohl reálně vystopovat.

3.1.5. Hoax

Jedná se o falešné, poplašné a řetězové zprávy, které mají varovný/naléhavý charakter. Mnohým se může zdát, že šíření hoaxů nemůže být škodlivé. Při bližším pohledu na problém zjistíme opak. Velké množství hoaxů rozesílají uživatelé tím nejhorším způsobem tzn. předávají je dál na všechny adresy. Kvůli lavinovitému šíření zprávy nemůžete vědět, komu v dalších úrovních bude e-mail doručen.

Také šíření nepravdivých, polopravdivých nebo zkreslených informací o různých společnostech jim mohou způsobit různé nepříjemnosti. Například poškození dobrého jména, ale také zbytečné zahlcení zákaznických linek, kam lidé na základě falešné zprávy zbytečně volají. V současnosti se již považuje za prokázané, že hoaxy slouží také jako nástroj pro

ovlivňování výsledků voleb a jsou svou povahou a podobou považovány za porušování pravidel férové soutěže politických stran. Jestliže nemáte jistotu, zda obdržená zpráva je hoax, prohlédněte si nejdříve některý ze seznamů hoaxů.

Databázi hoaxů a další informace o této problematice je možné dohledat na stránkách hoax.cz a manipulatori.cz.

3.2. Rady pro bezpečné chování

Zde se dozvíte, jaké jsou základy pro bezpečný pohyb v digitálním světě. Důraz je zde kladen zejména na osobní kyberbezpečnost, práci s hesly a práci s informacemi.

Rady pro zvýšení kybernetické bezpečnosti:

1. **Pravidelně aktualizujte** – Kybernetičtí útočníci často využívají již známou zranitelnost systémů.
2. **Zálohujte** – S nadsázkou se někdy říká, že se většina uživatelů naučí zálohovat až ve chvíli, kdy o data přijde. Zálohovací zařízení by mělo být po zkopírování dat odpojeno od sítě, protože škodlivý software obvykle umí napadnout i data umístěná v záloze. „Pokud doma přijdete o fotografie z dovolené či vaši sbírku vtipů, je to zcela jistě velmi nepříjemné. Nicméně se nejedná o kritickou situaci. Pro podnikání ale může nedostupnost dat znamenat velké ztráty, nebo i ohrožení jejího fungování. Proto je důležité zálohovat celý systém,“ říká Milan Habrcetl, bezpečnostní expert společnosti Cisco.
3. **Pozor na emailové přílohy** – Podle studie Cisco 2017 Annual Cybersecurity Report je každou vteřinu na světě posláno 3 500 spamů. Přitom 8 % až 10 % z nich je infikováno nebezpečným softwarem. Nemusí se ale jednat jen o nevyžádanou poštu. Často se objevují také cílené útoky využívající sociálního inženýrství. „Takový email se jeví jako úkol od ředitele firmy, který zadal a poslal na účetní oddělení společnosti. Falešný email přijde z adresy jan.novak@quallcart.cz, namísto ze správné jan.novak@quallcart.cz. Zbytek emailu vypadá jako originál – podpis, logo i firemní písmo. Ve zprávě, která je adresována účetní pak stojí, že je nutné urgentně proplatit přiloženou fakturu. Pokud ale účetní peníze odešle, pak již nenávratně zmizí na zahraničním účtu,“ popisuje Milan Habrcetl.
4. Neklikejte na **podezřelé odkazy** a weby – Může to znít jako samozřejmost, ale ne každý má toto pravidlo zažité. Pokud uživatel spěchá a hledá nějakou informaci, může ztratit pozornost a otevřít podezřelou webovou stránku. Stejně tak by uživatelé rozhodně neměli klikat na bannery, které jim slibují finanční odměnu, nový smartphone zdarma či jinou výhru.
5. **Bud'te opatrní i u stránek s ikonkou zámečku** – Mezi lidmi často koluje mýtus, že pokud se připojujete k webovým stránkám přes HTTPS (většinou zvýrazněné zelenou ikonkou zámku před názvem internetové adresy), pak jim nic nehrozí. To ale nemusí být pravda. Dnes útočníci dokážou vytvořit stránky se stejným zabezpečením, které ale využívají k šíření nebezpečného softwaru. I v tomto případě je nutná zvýšená pozornost uživatelů.
6. **Nepodceňujte nevyžádané programy zobrazující reklamu**, mohou být předzvěstí útoku. Mnoho uživatelů, ale i organizací, bere tzv. adware, tedy program zobrazující nevyžádanou internetovou reklamu, na lehkou váhu a vnímá jej spíše jako obtěžující. Nicméně tyto programy mohou být nebezpečné. „Útočníci je často využívají jako nástroj k přípravě útoku. Navíc tyto programy často předávají data o uživateli a komunikují se vzdálenými servery, které mohou sloužit jako brána útočníků,“ říká Habrcetl.

7. **Nikomu neposílejte citlivé údaje** – Pokud uživatele emailem kontaktuje banka s požadavkem na přeposlání přihlašovacích údajů, pak se takřka jistě jedná o podvod. Stejně tak se může vymstít zadávání svých bankovních údajů na neznámé webové stránky. Někteří útočníci například pronikli k účtům uživatelů sociálních sítí a následně kontaktovali jejich známé s prosbou o převod peněz.

3.2.1. Práce s hesly

Lidé si často neuvědomují, jak snadno se mohou stát terčem digitálního útoku. Jednou z forem takového útoku je nabourání se do účtů pomocí prolomení přístupových hesel. Těch má každý člověk v dnešní době mnoho a jsou různě důležitá. Heslo je jako klíč – zatímco klíč od skříňky s pastelkami není tolik významný, klíč od bytu bychom určitě nikomu cizímu nedali.

Je velkou chybou, pokud používáme jedno heslo všude. Pokud máme jedno heslo pro e-mail, finanční služby, diskuzní fóra, sociální sítě, e-shopy a hry, je to velice riskantní, protože dříve či později se některá z těchto služeb může stát obětí útoku. Možná dokonce některá ze služeb ukládá hesla nešifrovaná. Pak je lhostejné, jak silné bylo vaše heslo, v momentě, kdy dojde k jeho prolomení, dostane útočník zároveň přístup i k dalším účtům, které by jinak byly v bezpečí. Nejvíce bychom tedy měli chránit ta nejdůležitější hesla – pro e-mail a pro služby, kde jde o peníze či citlivé údaje. K prolomení hesla se používají různé techniky (např. útok hrubou silou, kdy se jedná o systematické zkoušení různých přístupových údajů, dokud není nalezena ta správná kombinace znaků, slovníkový útok pomocí připraveného seznamu slov aj.).

Při vytváření bezpečného a silného hesla je důležité se držet zásady nezjistitelnosti a zapamatovatelnosti. Heslo by mělo obsahovat malá a velká písmena, číslice a další znaky (tečka, čárka). Délka hesla by měla být alespoň 7 znaků. Rovněž lze použít velmi dlouhou neodhadnutelnou kombinaci slov, která zdánlivě nedávají smysl (např. popisují určitý příběh, který zná jen majitel hesla, tudíž si je snadno zapamatuje).

Existují také **webové aplikace**, např. LastPass, které se integrují do prohlížeče, používaná hesla ukládají šifrovaná, sledují i změny hesel, případně nová hesla pomáhají generovat. Uživatel tak může používat stovky bezpečných hesel, aniž by si je musel pamatovat, s výjimkou hlavního hesla. Bezpečné je také provázání programu s otiskem prstu, kterým by měl být zabezpečen i mobilní telefon (jedná se o výrazně bezpečnější formu zabezpečení než je například odemykání pomocí gesta).

Pravidla pro práci s hesly:

1. **Nikdy nepoužíváme krátká a průhledná hesla** (jména osob a zvířat, heslo podobné přihlašovacímu jménu, jednoduché číselné řady typu 123456, heslo, které má s námi úzkou spojitost - např. jméno, příjmení, datum narození, e-mail, rodné číslo, číslo OP atd., „heslo“, „heslo“ apod.);
2. **heslo by nemělo být slovo ze slovníku;**
3. **na různých účtech máme unikátní hesla;**
4. **heslo nikdy nikomu nesdělujeme;**
5. **hesla si nikam nezapisujeme;**
6. **při opuštění počítače se odhlásíme;**
7. **pokud pracujeme na veřejném počítači, po ukončení práce vymažeme cookies a uložená hesla;**

8. **na veřejných počítačích si nikdy neukládáme hesla** do webového prohlížeče, rovněž na svých přenosných počítačích jsme velmi opatrní - k počítači se může dostat někdo jiný;
9. opatrnost je na místě **i doma** - heslo může zneužít i sourozenec, nebo návštěva - i děti by si proto měly dobře zabezpečit své uživatelské účty a nenechat nikoho, aby pracoval pod jejich přihlášením;
10. pokud to služba umožňuje, **používejte dvoufaktorové ověření** (přes mobilní telefon);
11. **heslo jednou za čas doporučujeme změnit**, cca 1x za 3 měsíce.

4. Skupina dětí a mladiství

Tato část pojednává o problémech, kterým čelí především **děti a mládež**. Vlivem technologického pokroku už není tolik problém fyzický přístup, ale **vyloženě nízká digitální gramotnost** a s tím spojené nežádoucí jevy.

I z toho důvodu jsme se v této části zaměřili na typická, relativně častá rizika spojená s užíváním internetu. A protože je většina z nich velmi citlivé povahy, nebylo by vhodné jít např. cestou metodického tázání pomocí dotazníku.

A proto následující text nabízí **základní přehled současných rizik a následuje okruh otázek, na které je vhodné při rozhovoru zaměřit pozornost**. Málokdy mladiství čelí všem níže popsaným rizikům. Proto jsou v této části textu propojeny popisy rizik rovnou s okruhy modelových otázek.

Tato kapitola vznikla především díky dlouholeté praxi získané v organizaci Česká asociace streetworkingu. Vychází z materiálů, které v přehledné a především aktualizované podobě lze nalézt na webu orientovaném přímo na mládež.

4.1. Specifika dětí a mladistvých

Každá skupina má svá specifika a není tomu jinak ani u dětí a mladistvých. Zde se dozvíte aktuální trendy mezi dětmi a mladistvými v digitálním světě. Metodika cílí zejména na rizika, bezpečný pohyb a chování „na internetech“.

Kdo je nejvíce ohrožený a čím?

Již roku 2009 ukázala zpráva mezinárodního projektu EU Kids Online, že rizikům digitálního světa jsou nejčastěji vystaveny děti z rodin s nižším společenským postavením.

Přetrvává rizikové chování jako je poskytování osobních informací či sledování pornografie. Dalším rizikem je **konzumace násilného nebo nenávistného obsahu, kyberšikana nebo obdržení nechtěných sexuálních komentářů a podnětů.**

Reálné setkání s člověkem, se kterým se děti seznámily přes internet, se zdá být nejméně častým, nicméně nejnebezpečnějším rizikem. U chlapců je mnohem pravděpodobnější, že se setkají s rizikovým chováním (nebo ho sami vytvářejí), dívky se častěji setkávají s riziky, která se týkají obsahu a kontaktu.

Není nikterak nadnesené, když současnou generaci dětí a mladých lidí nazveme online generací. S internetem se setkávají již od útlého dětství, nejkuli od narození.

Vycházíme z předpokladu, že **ve věkové kategorii 10-18 let**, na niž se v následujícím textu zaměříme, má přístup k počítači či chytrému telefonu a k internetu velká většina dětí a mladých lidí. Existují samozřejmě i takové děti a dospívající, kteří přístup k počítači a na internet nemají, těch je však výrazně méně a pravděpodobně se bude jednat o děti pocházející z rodin ohrožených sociálním vyloučením, nebo děti rodičů, kteří z důvodu víry, náboženského vyznání nebo světonázoru technologie striktně odmítají.

Důležité je, že počítačové dovednosti se žáci (a především dívky) v zásadní míře naučili ve škole.

Na druhém stupni základní školy (a v odpovídajících ročnících víceletého gymnázia) je

povinnost zařadit vzdělávací oblast Informační a komunikační technologie do výuky, avšak v minimálním rozsahu pouze 1 hodina týdně. Výuka je zaměřena na vyhledávání, zpracování a využití informací a komunikaci. Nejde tedy o komplexní ani jednotnou výuku k digitální gramotnosti, očekávané výstupy nejsou Rámcovým vzdělávacím programem pro základní vzdělávání jasné definovány. (ICILS 2013. Shody a rozdíly v počítačové a informační gramotnosti mezi vybranými evropskými zeměmi.)

Z terénního šetření je dále patrné, že úroveň počítačové gramotnosti žáků úzce koreluje s dosaženým vzděláním a sociálním statusem jejich rodičů. Úroveň vzdělání rodičů žáků s nejlepšími výsledky je obecně vyšší. Žáci, jejichž rodiče mají nižší vzdělání a sociální status, měli zároveň výrazně horší výsledky při posuzování věrohodnosti informačních zdrojů, než děti vzdělaných a úspěšných rodičů. S tímto úkolem však měly české i evropské děti obecně problém.

4.2. Jak pracovat s dětmi a mladistvými

Zde se dozvíte námi navrženou metodu, jak s touto skupinou pracovat s cílem posilování bezpečí a eliminaci rizik v digitálním světě.

Pro tuto skupinu jsme zvolili **metodu strukturovaného rozhovoru**. Ten by měl vedle rizik obecných (viz první kapitola) zahrnovat především rizika specifická pro tuto skupinu.

Rizika jsou velmi často vázána na kontext jak lokální, tak osobní. Z toho důvodu postupujeme **spíše než návrhem striktního schématu rozhovoru nabídkou tematických okruhů jim přidružených otázek**.

U každé otázky také rozepisujeme poznatky k riziku vztažené. **Málokdy se totiž stane, že děti nebo mladiství čelí všem rizikům.** Většinou jde o konkrétní situace z kategorie špatné zkušenosti.

Jak a na co se ptát? Jako východisko k hovoru můžete použít komiksový příběh a otázky:

- „Co si o tomto příběhu myslíš, stávají se takové věci?“
- „Stalo se ti nebo někomu známému něco podobného?“
- „Co bys udělal/a, kdybys byl/a v roli hlavního hrdiny/hrdinky příběhu?“
- „Jak by ses cítil/a, kdyby tohle provedl?“
- „Komu by ses svěřil/a s takovým problémem?“
- „Jakým způsobem si ověřuješ, s kým komunikuješ na internetu?“
- „Co si myslíš o sdílení intimních fotografií a videí skrze internet nebo mobilní telefon?“
- „Jak máš zabezpečený svůj mobilní telefon/účet na sociálních sítích/počítač?“ atd.

Primárně je důležité zjistit, zda má dotyčný **přístup na internet a odkud se připojuje**. Pokud bude tvrdit, že přístup nemá, je potřeba se ujistit, zda se opravdu nepřipojuje občas alespoň ze školy, od kamaráda, z volně přístupné Wi-Fi.

Důležité také je, jestli má tzv. chytrý telefon s datovým připojením. Jestli má přístup nějak omezený anebo neomezený. Jestli používá e-mail a k čemu.

Jestli umí pracovat s počítačem i jinak, než být jen na sociálních sítích. Zda jej využívá např. ke vzdělávání, studiu atp. To vám může navodit předběžný obrázek, jak na tom dotyčný je.

Další otázky je možné položit již s orientací na konkrétní riziková témata.

V dalším kroku vás provedeme ukázkou otázek, které se vztahují ke konkrétním rizikům.

4.3. Jak na sociální sítě a rizika dětí a mladistvých

Zde se dozvíte více o specifických rizicích typických pro danou skupinu. Každý, kdo s touto skupinou pracuje, by se měl orientovat alespoň v základních problémech, které v současnosti přinášejí zejména sociální sítě a jejich bezhraniční využívání právě nezletilými.

Obzvláště děti a mládež poměrně málo řeší na internetu své **soukromí a zabezpečení svých osobních informací**. Mladí také tolik neuvažují nad tím, zda je o nich zveřejněné informace nemohou poškodit v budoucnosti například při hledání zaměstnání. V dnešní době je již běžné, že si personalisté prověřují uchazeče nejen podle zaslaného životopisu, ale vyhledávají informace o uchazeči komplexně, a to právě za pomoci sociálních sítí a internetových vyhledávačů.

Problémem je také samotná obranyschopnost dítěte. Děti často vstupují do světa sociálních sítí nadšené. Nechájí se jimi pohltnout. Setkání se s něčím negativním může dítě vysoce poznamenat po psychické stránce.

Chyby někdy bohužel pramení i z nedostatečného přístupu rodičů. **Role rodičů je ve výchově v digitálním světě klíčová.** Pokud dítě dostane nové kolo, rodiče si spíše ověřují, zda dítě může vyrazit do provozu na silnici. V případě nového počítače se způsobilost dítěte k jeho používání neprověřuje až tak často. Někteří rodiče bývají naopak rádi, že dítě je doma, v bezpečí, a ne na nebezpečné ulici.

4.3.1. Kybergrooming

- Co je to kybergrooming?
- Povídáš si přes internet s někým, koho neznáš?
- S někým koho jsi nikdy neviděl?
- Co by měl každý vědět, než se s někým seznámí přes internet?

Při kybergroomingu se jedná o manipulaci nejčastěji s dětskou obětí za účelem sjednání schůzky a následného vydírání, sexuálního zneužití či ublížení na zdraví.

Kybergrooming je jednou z metod takzvaného sociálního inženýrství (způsob manipulace lidí za účelem provedení určité akce nebo získání informace), kdy si útočník vytvoří falešnou identitu, postupně si získá důvěru oběti, vytvoří si s ní vztah a později (někdy až po několika měsících) si s ní domluví osobní schůzku.

Právě seznamování pomocí internetu a sociálních sítí rapidně proměňuje způsoby socializace ve společnosti a zejména u mladých. Internetové seznamky a chaty jsou plné mladých lidí, kteří se chtějí seznámit.

Výzkum rizikového chování českých dětí v prostředí internetu 2013 pro bezpečnýinternet.cz provedla Pedagogická fakulta UPOL. Výzkumu se účastnilo 21 372 dětí z více jak 4 000 škol ve věku 11-14 let (69 %) a 15-17 let (31 %), a je tak nejrozsáhlejším výzkumem, který se kdy u dětí na toto téma realizoval. Výzkum ukázal, že děti jsou ochotny si nejen psát, ale také se osobně potkat s lidmi, které neznají z jiného než on-line prostředí.

Podle výzkumu si s lidmi, které nezná z reálného světa, povídá on-line 53 % dotázaných dětí. 27 % respondentů uvedlo, že by si na vyžádání přidal cizího člověka mezi osoby, se kterými může komunikovat, např. v rámci sociální sítě.

Na otázku, zda by šly děti na schůzku s neznámým člověkem, odpovědělo 36 % z nich kladně. Pozitivní ale je, že 59 % by se v takovém případě svěřilo kamarádům nebo sourozencům či rodičům (41 %). Učitelům by se svěřila pouhá 3 % dotázaných.

Děti si kolikrát neuvědomují, že místo internetového kamaráda na ně může čekat někdo úplně jiný a celá situace může skončit tragicky. Zarážející je, že 76 % dotázaných dětí považuje osobní setkání s člověkem, kterého znají jen z internetového prostředí, za riskantní a nebezpečné, a přesto by 55 % z nich na takovou schůzku stejně šlo.

Co by mělo dítě vědět předtím, než se rozhodne seznámat se po internetu, či při kontaktu s novou osobou, která dítě osloví?

- Dítě by mělo být opatrné a uvědomit si, že na druhém konci nemusí být vždy ta osoba, za kterou se daný uživatel vydává.
- S tímto souvisí i střídmost při vyplňování profilu na sociální síti. Veřejně viditelné údaje jako jméno, fotografie, adresa, název školy a kontaktní údaje, jsou pro dítě nebezpečné. U dětí je tedy především namístě, aby sledovaly své digitální stopy.
- Pokud se dítě rozhodne komunikovat s neznámou osobou, mělo by si ověřit pravou identitu svého protějšku a požadovat zaslání aktuální fotky. Tedy takové, kde protějšek drží před sebou papír, na němž je napsán rukou unikátní vzkaz, který dítě zadá. Pokud bude reakce taková, že protějšek nemá webkameru, fotoaparát ani mobil, aby vše mohl vyfotit, je v tom již cosi podezřelého, jelikož tyto technologie dnes vlastní každý.
- Pokud se dítě rozhodne pro schůzku, vždy by o tom mělo říct blízké osobě, nejlépe rodičům nebo staršímu sourozenci, kamarádovi. Na schůzku by nejlépe nemělo chodit samo, a už vůbec ne na nějaká opuštěná místa atp. Schůzka by měla proběhnout na veřejném místě plném lidí.

4.3.2. Kyberšikana

- Co je kyberšikana?
- Jak se liší od šikany? Znáš někoho, koho na internetu šikanují?
- Co se dá dělat, když máš podezření na kyberšikanu?
- Jak se preventivně bránit, aby ses nestal obětí?

Kyberšikana je šikana realizovaná prostřednictvím moderních informačních technologií.

Může jít například o vydírání, ubližování, ztrapňování, obtěžování, ohrožování nebo zastrašování přes internet nebo mobilní zařízení. Aby se jednalo o kyberšikanu, musí být toto nevhodné chování opakované.

Kyberšikana je bohužel častým jevem. Obětí bývají především děti, které se určitými rysy odlišují od ostatních (osvojené děti, děti z neúplných rodin, sociálně slabší a podobně). Již zmiňovaný výzkum UPOL (2013) mezi více než 21 tisíci dětmi ve věku 11-17 let ukázal, že **téměř 51 % dětí do 18 let má zkušenost s nějakou formou kyberšikany.**

Mezi nejčastější druhy kyberšikany, se kterými se dotazované děti setkaly, patří verbální útoky (33 %), obtěžování za pomoci prozvánění (24 %) a vyhrožování či zastrašování (17 %). Mezi jevy, které mají rok od roku rostoucí tendenci, patří nejčastěji vydírání a krádež identity. Ve všech těchto případech ale musí existovat i útočník. Samy děti se ve výzkumu přiznávaly, že jsou mnohdy autory kyberšikany vůči jiným dětem. Přiznaly se, že se nejčastěji uchylují k verbálním útokům (11 %) a obtěžování prozváněním (6 %).

Server Šance Dětem vytvořil **seznam vlastností kyberšikany**, kvůli kterým je obzvlášť nebezpečná, zde některá z nich:

- Je snadné stát se útočníkem – urážlivý nebo posměšný vzkaz je vždy lehčí napsat, než ho říci dotyčnému do očí.
- Anonymita – oběť nemusí vždy vědět, kdo je útočníkem. Stačí si pouze založit falešný profil a z něj na oběť útočit.
- Obtížněji rozpoznatelná – chybí fyzické příznaky, například modřiny.

Pokud byste se setkali s obětí kyberšikany, Ministerstvo školství, mládeže a tělovýchovy navrhuje několik kroků, které byste jí měli doporučit:

1. **Ukončete komunikaci:** nekomunikujte s útočníkem, nesnažte se ho žádným způsobem odradit od jeho počínání, nevyhrožujte, nemstěte se. Cílem útočníka je vyvolat v oběti reakci, ať už je jakákoli.
2. **Blokujte útočníka:** zamezte útočníkovi přístup k vašemu účtu nebo telefonnímu číslu a je-li to v dané situaci možné, i k nástroji či službě, pomocí které své útoky realizuje (kontaktujte poskytovatele služby).
3. **Oznamte útok, poraďte se s někým blízkým, vyhledejte pomoc:** svěřte se blízké osobě. Pro uchování důkazů oslovte někoho, kdo má vyšší IT gramotnost. Kontaktujte školu a specializované instituce (policii, intervenční služby specializující se na řešení kyberšikany, psychology apod.).
4. **Uchovejte důkazy:** uchovejte a vystopujte veškeré důkazy kyberšikany (SMS zprávy, e-mailové zprávy, zprávy z chatu, uložte www stránky apod.). Na základě těchto důkazů může být proti útočníkovi či útočníkům zahájeno vyšetřování.

4.3.3. Kyberstalking

- Co je kyberstalking?

Kyberstalking znamená nebezpečné pronásledování oběti prostřednictvím moderních informačních technologií.

Oběť je sledována například skrze sociální sítě, e-mail, internetová fóra nebo SMS. Útočník může svou oběť obtěžovat nebo dokonce zastrašovat či vydírat. Dochází k bombardování různými vzkazy nebo ke zneužití citlivých informací či fotografií. Toto chování se objevuje opakovaně, dlouhodobě, systematicky a obvykle se postupně stupňuje.

Pronásledování může mít různé podoby:

- oběť může být urážena;
- mohou jí být poškozována data či vybavení (například pomocí posílání počítačového viru);
- útočník o ní může shromažďovat osobní data;

- může se za oběť ve virtuálním prostředí vydávat;
- může o ní zveřejňovat nepravdivé informace či například podporovat jiné lidi, aby oběť obtěžovali (například zveřejněním falešného inzerátu o oběti, kde údajně nabízí prostituci).

Kyberstalking je vážný a nebezpečný zločin v zákoně nazýván jako nebezpečné pronásledování a může být potrestán odnětím svobody. Proto je důležité obrátit se při podezření na kyberstalking na policii.

4.3.4. Sexting

- Co je sexting?
- Poslal jsi někdy někomu své intimní fotky anebo video přes internet?
- Chatuješ s někým pomocí webkamery?
- Víš, že se to dá snadno zneužít?

Pojem sexting souhrnně označuje sdílení textového či audiovizuálního obsahu se sexuálním podtextem.

Ať už mladí lidé posílají takovýto obsah například svým vrstevníkům pouze z legrace nebo i někomu dalšímu, koho dostatečně neznají, ne vždy si uvědomují, že takto **sdílený materiál už nebudou nikdy schopni uhlídat** a že se může zcela nekontrolovatelně šířit dál.

Někdy se může jednat původně jen o soupeření mezi kamarády, o předvádění se. Ovšem v kombinaci s nízkým zajištěním osobních dat může často dojít k nechtěnému a nekontrolovatelnému úniku těchto citlivých osobních dat. Často se jedná o nechtěný únik tzv. nude pictures.

S pojmem „sexting“ jsou nejčastěji skloňovány následující trestné činy:

- omezování osobní svobody (§ 171);
- znásilnění (§ 185), Sexuální nátlak (§ 186);
- pohlavní zneužití (§ 187);
- výroba a jiné nakládání s dětskou pornografií (§ 192);
- zneužití dítěte k výrobě pornografie (§ 193);
- ohrožování výchovy dítěte (§ 201);
- nebezpečné pronásledování (§ 354) aj.

Každopádně setkání se se „sextingem“ může zanechat vážné následky na oběti. Je proto důležité zamezit dalšímu takovému jednání.

Oběť sextingu by se měla svěřit blízké osobě. Společně by měli vyhledat odbornou pomoc.

Doporučit můžete například Dětské krizové centrum (DKC), které se specializuje na psychosociální pomoc dětem ohroženým Syndromem CAN, tedy dětem zneužívaným, zanedbávaným a týraným.

Také je možné využít krizovou linku DKC. Kontakty zde: www.ditekrize.cz

4.3.5. Happy slapping

- Víš, co znamená happy slapping?
- Víš, že je to protizákonné?

Tento závažný jev se poprvé vyskytl v r. 2005 ve Velké Británii v jižní části Londýna v hiphopové subkultuře „ganga teenagerů“ a odtud se rozšířil do celého světa, ČR nevyjímaje.

Happy slapping spočívá v tom, že si agresori vyberou oběť (dítě nebo dospělého člověka), kterou následně fyzicky napadnou (slapping = fackování).

Obětí může být prakticky kdokoli, kdo se zrovna vyskytuje na daném místě. Bohužel, brutalita takových útoků se stále stupňuje, oběť je nejen fackována, ale také bita pěstí, kopána, případně znásilněna, svlečena, pomočena, nebo jinak zostuzena. V některých případech dokonce útoky skončily smrtí oběti.

Celý tento násilný akt je jedním z party agresorů nahráván na mobilní telefon a následně zveřejněn na internetu za účelem „pobavení“. Uveřejnění a šíření těchto videí vedlo v některých případech až k sebevraždě oběti.

Důležité je také o happy slappingu mluvit a důrazně takové chování odmítnout. Někteří mladí lidé mají tendenci se takovým činům obdivovat a napodobovat je. Z internetu mohou nabýt dojmu, že jsou nepostihnutelní.

Při rozhovoru s potenciálními agresory bychom tak měli tyto mladé lidi informovat o legislativě a hrozcích sankcích a dalších společenských následcích, které z takového jednání pro ně plynou (viz digitální stopa). Jejich nepostihnutelnost je totiž pouze iluzorní a ten, kdo by rád takové jednání vyzkoušel, by si měl uvědomit, že takové chování splňuje podstatu trestného činu vědomého ublížení na zdraví.

4.4. Další informace a pomoc

Zde se dozvíte více, zejména pokud vás téma zajímá do hloubky a rádi byste se mu věnovali.

Více informací o kyberšikaně, kybergroomingu, sextingu a obecně o bezpečnosti na internetu si mohou dospívající vyhledat na portálu www.jdidoklubu.cz.

Jde o internetovou obdobu nízkoprahového zařízení pro děti a mládež. O dané problematice si zde mohou děti a dospívající chatovat s odborně proškolenými pracovníky. Najdete zde i komiksově zpracované příběhy, které slouží jako jednoduchý nástroj pro rychlejší a snadnější vhled do problematiky. Dospívající mohou v příbězích snadno rozpoznat rizika a chyby hlavních postav, nebezpečí popisovaných situací atp.

Ideální je, se čtenářem komiksu celý příběh rozebrat, nechat jeho samotného popsat co vidí a jak by se v podobných situacích zachoval on.

Komiksy jsou skvělou příležitostí, jak celé téma bezpečného chování na internetu otevřít a jak se o něm začít nenásilnou formou bavit. Příběhy jsou někdy záměrně překombinované. Autoři se snažili dostat do těch několika políček co nejvíce situací a případů rizikového chování. Příběhy ale vycházejí ze skutečného života a mnohdy se inspirovali příběhem

konkrétního dítěte.

Například komiks s názvem „*Virtuální realita*“ je příběhem Ryana Patricka Halligana. Ryan (18. prosince 1989 - 7. října 2003) byl americký teenager z Essexu ve Vermontu, který spáchal sebevraždu poté, co byl šikanován svými spolužáky jak v reálném životě, tak kyberšikanován v online prostoru. Bylo mu pouhých 13 let. Příběh „*Virtuální realita*“ v sobě nese prvky kyberšikany, ale i sextingu.

Další komiks „*Nudíš se, všichni Tě pruděj*“ představuje portál Jdidoklubu.cz.

Příběh „*To nevysvětlíš*“ zpracovává, jak je důležité věnovat se zabezpečení svého telefonu, hesel a jak nepříjemná může být ztráta identity v internetovém prostředí.

Poslední komiks „*Co se může stát*“ zpracovává téma sextingu a kybergroomingu.



Zdroje pro tuto cílovou skupinu:

Jdidoklubu.cz

<https://www.e-bezpeci.cz/index.php/temata/kyberikana/87-71>

www.ditekrize.cz

www.bezpecnyinternet.cz

www.portaldigi.cz

5. Skupina senioři

Přezkoumáním míry znalostí, vědomostí a praxe ve využívání digitálních technologií dospějeme k zjištění, jakou potřebu má cílová skupina seniorů. Klíčová je motivace a chuť se dál vzdělávat. Dále pak dostupnost a přístup k digitálním technologiím. Chcete-li vést rozhovor o využívání moderních technologií se seniorem, a identifikovat překážky pro rozvoj digitální gramotnosti, nabízíme jeho strukturovaný dotazník ke stažení v kroku s názvem „jak pracovat se seniory“.

5.1. Specifika seniorů

5.1.1. Jaké jsou hlavní příčiny nevyužívání digitálních technologií pro skupinu seniorů?

- **Chybí fyzický přístup včetně nepřipojení k internetu** (ekonomické bariéry, chybějící technologie v nejbližším životním prostoru jedince).
- **Chybí motivace** (nedostatek zkušeností, rezistence a obavy z nových technologií, nedostatečné vnímání přínosů v důsledku aktuální praxe jako je eGovernment, e-Health apod.).
- **Digitální negramotnost** (nedostatek příležitostí k digitálnímu vzdělání).

Velmi individuální je motivace. Ta negativní může být spojena se zásadním negativním postojem k inovacím a novým technologiím jako takovým nebo k vybraným technologiím a prostředkům..

5.1.2. Indikátory digitálního vyloučení

- Indikátory digitálního vyloučení, resp. ohrožení digitálním vyloučením mohou být:
- ekonomická situace jednotlivce;
- fyzická přítomnost technologií a služeb v nejbližším prostředí;
- dostupnost internetového připojení v místě;
- postoj k digitálním technologiím;
- zdroj a zprostředkující faktor informací o digitálních technologiích a jejich možnostech.
- stávající vybavení a praxe (využívání služeb) v digitálních technologiích;
- dosažené formální vzdělání a přítomnost problematiky informačních a komunikačních technologií a digitálních technologií v něm;
- praxe v zaměstnání a povolání, případně ve společenském životě z hlediska kontaktu s problematikou informačních a komunikačních technologií a digitálními technologiemi v jejím průběhu včetně.

Chcete-li vést rozhovor o využívání moderních technologií se seniorem, nabízíme jeho strukturu v (pdf) příloze. Několik příkladů, které lze použít k motivaci, najdete tamtéž.

5.1.3. Motivace

Pro cílovou skupinu seniorů, která je ohrožena digitální negramotností a digitálním vyloučením se jeví jako nejdůležitější **faktor motivace**. Aktuálně většina seniorů v okolním prostředí najde přístup k digitálním technologiím (telefon, tablet, počítač) s připojením na

internet, bude schopna se naučit jednoduché digitální technologie ovládat a smysluplně využívat, často i k překonání sociálního vyloučení, naplnění svých specifických potřeb a k reálnému zlepšení kvality života. Musí však – a týká se to zejména těch, kteří nemají potřebné informace o digitálních technologiích a o možnostech, které jsou jim schopny zprostředkovat nebo se jejich využívání obávají – dostat sociálně přijatelnou formou informace, které je budou motivovat k zájmu o digitální technologie jako takové a o jejich využívání.

Přitom tato věc zůstává svobodou volby od naprostého odmítnutí až k všeobecné akceptaci a mezitím široké škály, v níž jednotlivec nastaví své hranice, které však nemusí být neměnné. Tento proces je součástí sociální práce.

Přirozeným motivačním impulzem se může stát rozvoj elektronických nástrojů veřejné správy a veřejných služeb anebo další aspekty osobního života. Dnes již existuje celá řada možností, jak využít digitální technologie a nástroje nebo internet. Ať už se jedná o **osobní situace, osobní potřeby k naplnění sociálních a kulturních potřeb nebo vzájemné komunikaci.**

5.1.4. Individuální právo a svoboda

Je třeba vnímat, že digitální gramotnost a ngramotnost jsou volbou a že každý občan má na takovou volbu právo, včetně stanovení vlastní hranice, kam nebo kam až ve svém životě digitální technologie vpustí a kam nikoliv. Připojení se pomalu, avšak s jistotou jednou stane právem. Nesmíme ale zapomínat i na právo být offline a respektovat osobní rozhodnutí.

Nakládání s touto svobodou volby je zásadním etickým rozměrem sociální práce a má přednost před byť i nejskvělejšími dobrými úmysly ve veřejném zájmu.

Pochopitelně, tato volba může být ovlivněna nedostatkem informací o možnostech, které digitální technologie poskytují např. v oblasti vzájemné komunikace k překonání osamělosti nebo k řešení osobních situací, nebo také negativní zkušeností z dosavadní vlastní praxe nebo zprostředkovaných informací o negativních jevech, o zneužitích, které přitom ani nemusí být s novými digitálními technologiemi spojeny, ale jsou prostě aktuální (např. šmejdi).

5.2. Jak pracovat se seniory

Zde se dozvíte, jak specificky pracovat s cílovou skupinou seniorů. Motivace, aspekt zdraví, společenský kontakt, péče. To jsou všechno oblasti, které již nyní podléhají digitalizaci a stárnoucí generace se s tím musí vypořádat.

U seniorů s nulovým nebo velmi malým, letným potenciálem **vztahu k digitálním technologiím je nejdůležitější ve vzájemné interakci najít motivaci**, která bude na straně seniora přispívat k překonávání všech překážek způsobujících digitální vyloučení. Při individuálním pohovoru to znamená, zabývat se prvky podstatnými pro sociální vyloučení či začlenění jedince na všech úrovních od rodiny přes místo, kde bydlí či převážně pobývá, až po komunitu a dostupné instituce.

Na základě individuální diagnostiky a analýzy příčin digitálního vyloučení můžeme postupně překonávat a řešit jednotlivé důvody digitálního vyloučení. Nelze tak činit jednostranně, protože má-li to být v zájmu jedince, musí být do řešení aktivně zapojen, poskytovat součinnost v míře, které je schopen.

Zásadní odmítnutí ze strany seniora může být důsledkem obav a zejména nulové motivace k nabytí potřebných kompetencí. Motivační složka je tedy při komunikaci se seniory zcela zásadní.

5.2.1. Aspekt zdraví

Vzhledem k tomu, že v šetřeních prováděných ČSÚ mezi lidmi staršími 65 let uvádějí senioři za zdroj největších obav vlastní bezpečí včetně rizik plynoucích ze zdravotního stavu, je zřejmé, že silným motivačním prvkem pro nabytí digitálních kompetencí **může být zájem o některé z asistivních technologií a s nimi souvisejících služeb od stávající tísňové péče až po perspektivní služby asistovaného života včetně monitoringu některých charakteristik zdravotního stavu.**

Na to navazuje možnost **elektronického zdravotnictví** sloužícího ke zvýšení zdravotní bezpečnosti sdílením zdravotnické dokumentace a historie i současnosti preskripce léků s registrujícími a dalšími ošetřujícími lékaři a zdravotnickými zařízeními, které se na péči podílejí.

5.2.2. Aspekt společenský kontakt a kontakt s rodinou

Významné jsou u této cílové skupiny také pocity osamění. Proto významným motivujícím prvkem může být pro tyto osoby **zprostředkování kontaktu a komunikace s osobami blízkými nebo v rámci vytvořené komunity s využitím informačních a komunikačních technologií**, případně dostupnost informací o možnostech aktivizace a společenského života v dané komunitě.

Hledání motivace může být u některých starších jedinců složité a pracné, otvírá však cestu k možnosti řešit prostřednictvím digitálních kompetencí aktivizaci seniorů a jejich **začlenění do společenského života**, tedy zároveň základní atributy kvality života. Nejvíce to bude platit pochopitelně u samostatně žijících jedinců.

5.2.3. Aspekt pečující

Správná motivace se **týká jak členů cílové skupiny, tak samotných aktérů**, jejichž úkolem je prostřednictvím sociální práce a následného učení, resp. vzdělávání se s digitální negramotností seniorů poprat. V konkrétní situaci a prostředí k práci se skupinou si musí **stanovit reálné postupné cíle a indikátory**, jejichž plnění bude měřítkem dosaženého úspěchu. Neplnění některých indikátorů pak bude mít povahu upozornění, že některé cíle nebo prostředky nebyly v daných souvislostech zvoleny správně. Včasná změna může být prevencí pozdějšího zklamání.

Níže si můžete **stáhnout dotazník**, který vám pomůže rámovat daný problém u dané skupiny. **Součástí dokumentu je pak sada příkladů dobré praxe**, které mohou sloužit jako vodítko v případě motivačních rozhovorů s představiteli dané cílové skupiny.



Ke stažení:

[Dotazník jak pracovat se seniory \(.docx\)](#)

5.3. Digitalizace pro stárnoucí generaci

Zde se dozvíte, jaké mohou být konkrétní příklady digitalizace, které se široce dotýkají naší stárnoucí generace. Jsou to zejména asistivní technologie a digitalizace českého zdravotnictví.

5.3.1. Asistivní technologie na pomoc seniorům a OZP

Definice Asistivní technologie (AT):

Jakýkoliv nástroj, zařízení, software nebo systém, využívající zpravidla moderní technologie (zejména senzory, aktuátory, informační a komunikační technologie).

Cíle AT:

- posílit, udržet nebo zlepšit funkční schopnosti jedinců se speciálními potřebami;
- usnadnit každodenní život;
- zlepšit kvalitu života, samostatnost a soběstačnost.

Velká část asistivních technologií je založena na digitálních technologiích. **Asistivní technologie nalézají využití ve zdravotních a sociálních službách**, v podpoře samostatného života seniorů a OZP ve vlastním domácím prostředí.

Existence asistivních technologií může motivovat seniory a OZP k nabývání digitálních kompetencí a k digitální gramotnosti za účelem možnosti pochopit funkce technologie, která má zlepšit kvalitu jeho života, a jejího ovládání a plného využití.

Užívání některých asistivních technologií je podmíněno digitální gramotností (např. hlasem ovládaný počítač pro osoby s tělesným hendikepem).

Souborné zpracování informací o asistivních technologiích a o možnostech, potenciálu i překážkách rozvoje jejich využití naleznete:

- <http://www.podporaprocesu.cz/aktivita13/>
- http://www.podporaprocesu.cz/wp-content/uploads/2016/03/V%C3%BDstup_1.pdf

5.3.2. Digitalizace českého zdravotnictví

Pro seniory a jejich motivaci k užívání moderních technologií je také dobré seznámit se s postupem digitalizace českého zdravotnictví. To přispívá se zlepšení dostupnosti, kvality, ale i bezpečí zdravotnictví. Proto zde uvádíme několik zdrojů k nahlédnutí.

Zásadní pro pacienty je **bezpečné sdílení zdravotní dokumentace a elektronická preskripce umožňující sdílet informace o aktuálně i historicky předepsaných lécích, poskytování informací o kontraindikacích, nesnášenlivosti nebo o vzájemných interakcích (již nyní je dostupná aplikace Znáám své léky).**

Smyslem musí být kvalita a bezpečnost zdravotní péče a odpovědnost na straně zdravotníků i pacientů.

Při dosavadních zkušenostech s elektronizací nebo digitalizací českého zdravotnictví se může zdát zařazení tohoto tématu do metodiky digitální gramotnosti pro seniory jako zbytečné

nebo minimálně předčasné. Pohled na aktuální dění přináší indicie, že se do prostoru elektronického zdravotnictví vrací privátní iniciativa. A to na mnohem vyšší odborné úrovni.

Pokud se již dnes podíváme na inovovaný produkt zdravotní knížky Zdravel a pro sportovce ALL-IMP a podporu, kterou tvoří těmto produktům Institut pro podporu elektronizace zdravotnictví, z. ú., je zřejmé, že stát bude mít na tomto poli silného konkurenta a že ho bude muset přinejmenším respektovat.

Pro pacienty – seniory nevyjímaje – je to velká šance na cestě ke kvalitě a bezpečnosti zdravotní péče.

6. Skupina nezaměstnaní

Tato skupina je velmi dobře definovatelná a i její problémy se dají velmi dobře standardizovat. Je zde i **jasně specifikovaná potřeba - zprostředkovat adekvátní zaměstnání. Z toho důvodu jsme pro práci s touto skupinou zformulovali dotazník.** Ten má za úkol rozlišit, jaké míře a povaze problému čelí každý z testovaných uchazečů o práci a nabídnout tak pracovníkům ÚP ČR jednoduchý nástroj pro identifikaci problému.

Dotazník je ke stažení v podkapitole s názvem „dotazník“.

6.1. Úvodní rozhovor

Zde se dozvíte, jak z pozice pracovníka kontaktního pracoviště Úřadu práce (KoP ÚP) přistoupit k úvodnímu pohovoru na téma digitální gramotnosti s uchazečem o zaměstnání. To vše s pomocí námi přiloženého dotazníku.

Při pohovoru s uchazečem o zaměstnání (dále jen „UoZ“) nad dotazníkem doporučujeme následující postup.

1. Seznamte se s dotazníkem a typy otázek.
2. Pokud osoba nemá fyzický přístup k internetu, nemá smysl v dotazníku dále pokračovat. Namísto kladení otázek z dotazníku se doporučujeme zeptat na následující tři okruhy:
 - Kde jsou bariéry v přístupu (finanční, technická, motivace...)?
 - Má se osoba na koho obrátit při řešení situací, kde je třeba znalost ICT?
 - Jaké konkrétně má UoZ zkušenosti s ICT (má děti/kamarády, kteří zkušenosti mají)? Zkoušel někdy sám?
3. Pokud osoba má fyzický přístup k internetu, pokračujte v dotazníku a odpovědi následně vyhodnoťte. Vodítko pro vyhodnocení je součástí dotazníku.

Dotazník s vyhodnocením je v následující podkapitole přiložen ke stažení.

6.2. Dotazník

Zde se dozvíte, jak dotazník vyhodnotit a jak s uchazečem jeho problém ukotvit.

Prostřednictvím odpovědí v dotazníku je UoZ „zařazen“ do jedné z následujících skupin:

1) *Bezproblémoví*

Nevykazují žádný problém, jsou stabilně fyzicky připojeni, mají nadprůměrné dovednosti a zkušenosti.

2) *Malý problém (digitálně nekvalifikovaní)*

Skórují všude nadprůměrně, vykazují problémy s fyzickým připojením, jejich kompetence mohou být zastaralé a/nebo nedostatečné v souvislosti s trhem práce.

3) *Střední problém (digitálně negramotní)*

Pohybují se pod průměrem skóre, spíše nižší až nulové zkušenosti s využíváním IT. Mají přístup k internetu a/nebo ICT (např. smartphone).

4) **Vážný problém (digitálně vyloučení)**

1. **Nízká digitální gramotnost**

Podprůměrné dovednosti, nízká zkušenost, ale také problémy s motivací k dalšímu vzdělávání v oblasti ICT. Nemusí mít závažné problémy s připojením. Mají na koho případně delegovat ICT úkoly.

2. **Digitální vyloučení**

Spojení problematického fyzického přístupu, nízkých zkušeností, vnímaného problému s ICT při dosahování cílů. ICT úkoly ani nelze delegovat na sociální prostředí.

Rozdělení do skupin vám umožní část vyhodnocení přiloženého dotazníku. Na základě přidělení skupiny navrhujte uchazeči o zaměstnání v danou chvíli dostupná řešení - dalšího vzdělávání, rekvalifikací nebo naopak pomoci uchazeči o podtrhnutí jeho digitálních dovedností při hledání nového zaměstnání. Důležité je, v případě uchazeče, uvědomění si svých limitů nebo naopak předností. Často se stává, že si lidé digitální své kompetence neuvědomují nebo je nepovažují za důležité.

Motivací pro uchazeče pak mohou být i konkrétní a lukrativní nabídky práce, které vyžadují digitální kompetence, avšak takové kompetence a dovednosti, které si lze prostřednictvím programů ÚP snadno doplnit. Více se dozvíte v dalším kroku.



Ke stažení:

[Dotazník uchazeče o zaměstnání \(.docx\)](#)

6.3. **Navržená opatření a podpora UoZ**

Zde se dozvíte konkrétní navržená opatření pro uchazeče o zaměstnání navržené Úřadem práce ČR, jejichž cílem je bojovat proti digitálnímu vyloučení na jedné straně a na straně druhé posilovat jeho digitální gramotnost a kompetence.

Na základě tohoto rozdělení jsou níže uvedeny možnosti zapojení uchazeče o zaměstnání do aktivit/činnosti/podpory poskytované Úřadem práce ČR. Cílem těchto aktivit je snížit či zabránit digitálnímu vyloučení uchazeče o zaměstnání („UoZ“). Navržené aktivity/činnosti či podpora však vždy musí vycházet ze schopností a individuálních požadavků každého jednotlivce.

6.3.1. **Charakterizace skupin uchazečů o zaměstnání**

Uchazeči o zaměstnání jsou prostřednictvím interaktivní osobní diskuze s kompetentním pracovníkem ÚP a s pomocí výsledků písemného dotazníku dle této metodiky rozdělení do následujících skupin:

1) **Digitálně vyloučení (vážný problém)**

UoZ se zásadními (vážnými) problémy v oblasti motivace k využívání digitálních technologií a ke vzdělávání v této oblasti. Pro tyto uchazeče je charakteristické odmítání digitálních technologií z řady často smyšlených důvodů a silná neochota k jejich využívání. Velice často (nikoli vždy) mají osoby digitálně vyloučené velice nízké povědomí o možnostech digitálních technologií a neumí si ani představit, jak a k čemu je mohou v osobním i pracovním životě využívat. Obvykle (nikoli vždy) je digitální vyloučení spojeno s nulovou digitální gramotností, resp. s nulovými nebo mizivými digitálními kompetencemi. K digitálním technologiím mají obvykle z různých důvodů omezený přístup, stejně tak nemají ve svém okolí lidi, kteří by

mohli představovat pomoc či osobní stimulaci.

2) Digitálně negramotní (střední problém)

UoZ s velice nízkými, někdy s nulovými digitálními kompetencemi. Těmto lidem nechybí představa, k čemu by mohli digitální technologie používat, pokud by s nimi uměli smysluplně pracovat. Jsou schopni se vzdělávat pouze s interaktivní pomocí okolí. Mají obvykle k dispozici mobilní technologie, jsou schopni využívat několik nejběžnějších služeb internetu, ale o digitálních kompetencích potřebných pro trh práce nemají žádné konkrétní představy. V jejich okolí jsou lidé, kteří je udržují v kontaktu s digitálními technologiemi a jsou schopni jim v základních věcech poradit, často ovšem na zcela amatérské úrovni.

3) Digitálně nekvalifikovaní (malý problém)

UoZ, kteří tvrdí, že s digitálními technologiemi nemají problém a působí dojem, že jsou zběhlými uživateli těchto technologií. Jejich pohled na digitální technologie ale zahrnuje většinou pouze mobilní technologie připojené na internet. Jsou schopni relativně rutinně používat různé služby internetu, komunikovat a používat sociální média, ale v oblasti digitálních technologií využívaných na trhu práce se neorientují nebo mají pouze povrchní představy a digitální kompetence v této oblasti. Obvykle nevlastní stolní počítač nebo notebook nebo nepoužívají žádné desktopové aplikace.

4) Bezproblémoví (žádný nebo minimální problém)

Pokud UoZ nevykazuje žádný problém, je stabilně fyzicky připojen, má nadprůměrné dovednosti a zkušenosti s využíváním ICT, projednají se s ním v rámci individuálního poradenství možnosti dalšího rozvoje jeho ICT dovedností a dalšího rozšíření jeho zkušeností s využíváním ICT, popř. možnosti trvalého udržení úrovně stávajících digitálních kompetencí, a to vše s přihlédnutím k jeho individuálním potřebám (např. zařazení do poradenského programu zaměřeného na příslušnou tematiku a rozvíjejícího další příslušné dovednosti atd.).

6.3.2. Možná opatření ÚP

Pro uchazeče o zaměstnání zařazené do příslušné skupiny navrhnou kompetentní pracovníci ÚP vhodná opatření, tj. aktivity, činnosti, vzdělávání nebo podporu, jejichž cílem může být digitální začlenění, zamezení digitálního vyloučení, zvýšení digitálních kompetencí na úroveň digitální gramotnosti nebo zvýšení digitálních kompetencí na úroveň tzv. digitální kvalifikace, tj. digitálních kompetencí potřebných pro vstup na trh práce. Jakékoli aktivity, činnosti, vzdělávání nebo podpora však vždy musí vycházet ze schopností, možností a individuálních potřeb každého uchazeče o zaměstnání.

1) Digitálně vyloučení (vážný problém)

Nezbytně nutným opatřením pro digitální začlenění uchazečů o zaměstnání zařazených v této skupině jsou jakékoli aktivity ÚP, které povedou ke změně postoje uchazeče k digitálním technologiím. To je hlavní cíl digitálního začleňování. Nejjednodušší takovou aktivitou může být pohovor se zkušeným praktikem – motivátorem. Pokud jde o oblast digitálního vzdělávání, pak mezi takovéto aktivity patří vzdělávací kurzy zaměřené na digitální začleňování, resp. na odstranění digitálního vyloučení, překonání digitální propasti a podobně. V širším pohledu jde o tzv. motivační kurzy. Typickým zástupcem motivačních kurzů je např. mezinárodně standardizovaný kurz pro digitální začleňování e-Citizen, ale existují i další, méně sofistikované kurzy tohoto druhu. Zásadně chybné je posílat digitálně vyloučené uchazeče o zaměstnání na kompetenční nebo rekvalifikační kurzy.

2) *Digitálně negramotní (střední problém)*

Pro tuto skupinu uchazečů o zaměstnání je možné vybrat ze širšího spektra aktivit, resp. vzdělávacích kurzů. Pro typické uchazeče z této skupiny je vhodné použít prakticky jakékoli vzdělávací, tzv. kompetenční kurzy zaměřené na využívání digitálních technologií, zejména mobilních, a to především ve spojení se službami internetu. Příkladem mohou být vzdělávací kurzy patřící do kategorie „Základy obsluhy PC“ nebo „Počítačová gramotnost podle konceptu ECDL Core“, které akredituje MŠMT v rámci rekvalifikací. Vzdělávací obsah těchto kurzů musí být v souladu s podmínkami akreditace uzpůsoben tak, aby se týkal nejméně těch oblastí digitálních technologií, které jsou úzce spojeny s obsahem pojmu digitální gramotnost (rámeček DIGCOMP, sylaby ECDL). Jde zejména o následující oblasti:

- Základy práce s počítačem a správa souborů
- Základy práce s internetem a komunikace
- Vyhledávání, vyhodnocování a zpracování informací z internetu
- Spolupráce a výměna informací na internetu
- Bezpečné používání informačních technologií

Pro uchazeče s nulovými digitálními kompetencemi je možné také použít jednodušší kurzy pro digitální začleňování, v tomto případě ale kurzy nejméně na obdobné úrovni, jakou má program e-Citizen.

Pro dosažení žádané účinnosti kompetenčních kurzů je naprosto zásadní zakončení těchto kurzů objektivním ověřením (změřením) výsledků vzdělávání, což je v případě využití kurzů akreditovaných MŠMT v rámci rekvalifikací nebo mezinárodně standardizovaného kurzu e-Citizen zajištěno.

3) *Digitálně nekvalifikovaní (malý problém)*

Tato skupina uchazečů o zaměstnání je vhodnou skupinou pro rekvalifikace v oblasti digitálních technologií. Z nabídky akreditovaných rekvalifikačních kurzů, které pokrývají přenositelné digitální kompetence se pro tuto skupinu uchazečů o zaměstnání hodí pouze kurzy patřící do kategorie „Obsluha PC“ nebo „Počítačová gramotnost podle konceptu ECDL“. Vzdělávací obsah těchto kurzů musí být v souladu s podmínkami akreditace uzpůsoben tak, aby se týkal těch oblastí digitálních technologií, které úzce souvisí s běžnými digitálními dovednostmi vyžadovanými trhem práce. Jde zejména o následující oblasti:

- Vyhledávání, vyhodnocování a zpracování informací z internetu
- Bezpečné používání informačních technologií
- Zpracování textu
- Práce s tabulkami
- Použití databází
- Prezentace
- ... a další oblasti (např. dle rámce DIGCOMP nebo Sylabů ECDL)

Součástí všech rekvalifikačních kurzů jsou ze zákona závěrečné zkoušky zakončené získáním osvědčení o absolvování rekvalifikačního kurzu, v případě rekvalifikačních kurzů využívajících koncept ECDL pak navíc některým z mezinárodně platných certifikátů ECDL.

6.3.3. Princip návaznosti opatření ÚP

Hranice mezi skupinami uchazečů o zaměstnání nejsou ostré a jednotlivé skupiny na sebe z pohledu svých postojů a schopností, rozsahu a hloubky digitálních kompetencí plynule navazují. Totéž lze říci o vzdělávacích kurzech, takže veškerá opatření ÚP by měla (zjednodušeně) sledovat následující princip:

Digitálně vyloučení → Motivační kurzy → Digitálně negramotní, ale motivovaní uchazeči o zaměstnání → Kompetenční kurzy → Digitálně gramotní, ale digitálně nekvalifikovaní uchazeči → Rekvalifikační kurzy → Rekvalifikovaný uchazeč připravený pro vstup na trh práce.