SENIOŘI

BEZPEČNĚ na internetu

APSS ČR

MPSV

INSTITUT VZDĚLÁVÁNÍ APSS ČR

PhDr. Jana Pšejová, Ondřej Fara

Senioři bezpečně na internetu

Vydala Asociace poskytovatelů sociálních služeb ČR
Vančurova 2904, 390 01 Tábor
Vyšlo v roce 2024
První vydání

Aktivity projektu Senioři bezpečně na internetu jsou podpořeny z dotačního programu „Podpora veřejně účelných aktivit seniorských a proseniorských organizací s celostátní působností“.

OBSAH

1 Úvod do kybernetické bezpečnosti 6

2 Základy bezpečného chování na internetu 10

3 Dopady na každodenní život 14

4 Tipy na bezpečné používání e-mailů a sociálních sítí 18

5 Klíčem k našim osobním údajům je heslo 22

6 Fake news – falešné zprávy a dezinformace 26

7 Bezpečné používání mobilů a tabletů 30

8 Bezpečné prohlížení internetu 34

9 Praktické rady pro bezpečné používání technologií 38

10 Specifika práce se seniory 42

11 Závěrečné desatero 44

Přílohy příručky 46

ÚVOD DO KYBERNETICKÉ BEZPEČNOSTI

1


Ctrl

ÚVOD DO KYBERNETICKÉ BEZPEČNOSTI

CO JE KYBERNETICKÁ BEZPEČNOST?

Kybernetická bezpečnost je při používání počítače, tabletu nebo mobilu zásadní stejně jako zamykání domova, kdykoliv odcházíte ven. Určitě máte doma cenné věci. Nejsou to jen peníze, ale hlavně rodinné fotografie, důležité dokumenty, šperky, cenné vzpomínky na milé lidi a místa. Zamykáte dveře, aby se k nim nedostal nikdo nepovolaný.

Kybernetická bezpečnost má podobný cíl, jen místo fyzického prostoru chrání vaše digitální zařízení a data před zloději a podvodníky na internetu. Je to soubor opatření a postupů, které zajišťují, že vaše osobní a citlivé informace zůstanou v bezpečí a chráněné před neautorizovaným přístupem.

PROČ JE PRO SENIORY DŮLEŽITÁ?

Senioři jsou v dnešní době uživatelé digitálních technologií jako všichni ostatní. Využívají počítače, mobily i tablety. Do světa internetu se odvažují vstoupit čím dál častěji. Přesto pro ně tyto technologie mají svá úskalí. S digitálním světem rozhodně nedrží krok od narození, a proto si některé vlastnosti techniky potřebují osvojit vědomě. Pokud se zamyslíme nad seniorskou skupinou ve vztahu k bezpečnému chování v digitálním světě, měli bychom mít stále na mysli, že senioři obecně:

- **Mají méně zkušeností s technikou:** Senioři nemají tolik zkušeností a mohou se snadněji stát obětí podvodu. Nejsou zvyklí na triky, které podvodníci používají, jako jsou phishingové e-maily nebo falešné webové stránky, které vypadají důvěryhodně.

- **Jsou důvěřivější:** Starší lidé mohou uvěřit podvodným e-mailům nebo zprávám, které vypadají, jako by je posílala jejich banka nebo přátelé. Podvodníci toho rádi využívají. Umí vzbudit obavu, naději nebo lítost a útočí na emoce seniora tak, aby ho mohli zneužít.

- **Hůře čelí negativním psychologickým dopadům:** Kybernetické útoky mohou vážně narušit duševní pohodu seniorů. Strach a úzkost spojené s pocitem, že byl člověk podveden nebo ohrožen, mohou negativně ovlivnit celkové psychické rozpoložení. Tento stres může způsobit, že se senioři technologiím začnou vyhýbat, a tak může dojít k jejich izolaci od důležitých sociálních a informačních zdrojů.

- **Mohou být závislí na technologiích využívaných pro komunikaci:** Pro mnoho seniorů jsou technologie hlavním způsobem, jak zůstat v kontaktu s rodinou a přáteli.

- **Často běžně využívají internet k vyhledávání různých informací,** ale také k nakupování a výběru různých služeb. Podvodníci mohou využít falešné webové stránky nebo škodlivé odkazy k tomu, aby ukradli osobní a finanční údaje nejen seniorů.

- **Používají internet k přístupu k lékařským informacím a službám:** Únik těchto citlivých informací může mít vážné následky a ohrozit jejich zdraví.

ZÁKLADY BEZPEČNÉHO CHOVÁNÍ NA INTERNETU

2

ZÁKLADY BEZPEČNÉHO CHOVÁNÍ NA INTERNETU

Bezpečné chování na internetu je naprosto klíčové, pokud chceme ochránit osobní údaje a zajistit, že online aktivity zůstanou soukromé. Internet je skvělý nástroj, který umožňuje mnohé – zůstat v kontaktu s rodinou a přáteli, získávat nové informace, nakupovat z pohodlí domova, ale také hrát si a bavit se. Je to proměnlivý svět plný možností a příležitostí, kde stejně jako v reálném světě číhají různá rizika a hrozby.

Na začátek malé doporučení – nebojte se nových, neznámých slov. Je nejvyšší čas si na ně zvyknout, zařadit je do slovníku a jít s dobou. Jako pomůcka je pro vás na konci brožurky připravený přehledný slovníček.

PŘEHLED ZÁKLADNÍCH RIZIK A HROZEB

- **Phishing:** Představte si, že dostanete e-mail od banky, který vás žádá o potvrzení vašich přihlašovacích údajů. Tento e-mail je ale falešný a jeho cílem je ukrást vaše informace. Phishingové útoky jsou velmi časté a podvodníci se stále zdokonalují v tom, jak napodobit důvěryhodné instituce. Proto je důležité být vždy opatrný a nikdy neposkytovat své citlivé údaje prostřednictvím e-mailu nebo odkazu, který vám přijde neočekávaně a který jste si nevyžádali.

- **Ransomware:** Ransomware je typ malwaru, který zašifruje vaše soubory a požaduje výkupné za jejich odemčení. Představte si, že všechny vaše fotografie, dokumenty a další důležité soubory jsou zablokovány a vy k nim nemáte přístup. Útočníci často požadují platbu v kryptoměnách, aby zůstali anonymní. Nejlepší obranou proti ransomware je pravidelné zálohování důležitých souborů na externí disk nebo do cloudu.

- **Malware:** Malware je škodlivý software, který může napadnout váš počítač nebo telefon. Může zpomalit vaše zařízení, ukrást vaše data, nebo dokonce zablokovat přístup k vašim souborům. Malware se často šíří prostřednictvím infikovaných příloh v e-mailech, škodli-

vých webových stránek nebo falešných aktualizací softwaru. Je proto důležité být na pozoru a všímat si věcí, které nejsou standardní. Pro větší jistotu je možné nainstalovat antivirový program, který pomůže rozpoznat většinu hrozeb. Je však nutné používat známé a ověřené antivirové programy.

- **Sociální inženýrství:** Sociální inženýrství je technika, kterou podvodníci používají k manipulaci s lidmi, aby získali přístup k citlivým informacím. Může se jednat o telefonní hovor, e-mail nebo osobní setkání, při kterém se podvodník vydává za někoho, kdo potřebuje vaši pomoc nebo informace. Například se může vydávat za technickou podporu a požádat vás o přihlašovací údaje k vašemu účtu. Důležité je být vždy obezřetný a ověřovat si identitu lidí, kteří od vás žádají citlivé informace. Nejlépe tak, že zavěsíte a zavoláte sami na ověřené telefonní číslo. Víte, že případným útočníkům můžete dát přihlašovací údaje k dispozici i tím, že je máte napsaná na viditelných nebo snadno dostupných místech, případně je sdílíte s kolegy či rodinou? Mějte stále na paměti, že s hesly je potřeba zacházet úplně stejně jako s fyzickými klíči a dobře je opatrovat.

- **Dezinformace:** Dezinformace jsou falešné nebo zavádějící informace šířené za účelem manipulace. Jednoduše řečeno – jsou to nejčastěji obyčejné lži nebo pomluvy. Dezinformace mohou být šířeny prostřednictvím sociálních sítí, e-mailů nebo webových stránek. Je tedy důležité používat to, čemu se dnes moderně říká kritické myšlení – důležité je ověřovat si informace z důvěryhodných zdrojů, být skeptický vůči zprávám, které vypadají podezřele nebo příliš dramaticky a u nichž je zjevné, že chtějí v lidech vyvolat strach nebo překvapení. Při šíření dezinformací mohou útočníci kombinovat různé typy hrozeb. Například mohou zveřejňovat dezinformace na stránkách, které vypadají jako běžné zpravodajské portály, aby zmátli čtenáře a vytvořili dojem, že informace pocházejí z ověřeného zdroje. Na těchto stránkách mohou útočníci požadovat i platební údaje, díky kterým si ohromnou šokující zprávu budete moct přečíst celou. Touto cestou si do svého zařízení můžete nechtěně nainstalovat vir, který poté šíří dezinformace mezi další lidi – například z vašeho účtu na sociálních sítích. Nenechte sebou manipulovat. Zapojte selský rozum a všímejte si odkazů, na které klikáte.

DOPADY NA KAŽDODENNÍ ŽIVOT

3

DOPADY NA KAŽDODENNÍ ŽIVOT

PŘÍKLAD: JAK TO TAKÉ MŮŽE VYPADAT?

Špatně zvládnutá situace

Pan Novák obdržel e-mail, který vypadal jako zpráva od jeho banky. V e-mailu si přečetl, že jeho účet byl kompromitován a že musí okamžitě kliknout na odkaz a přihlásit se, aby potvrdil svou totožnost. E-mail vypadal velmi důvěryhodně, měl správné logo banky a byl v něm použit profesionální styl jazyka. Pan Novák na odkaz klikl a byl přesměrován na webovou stránku, která vypadala (skoro) přesně jako stránky jeho banky. Zadáním svých přihlašovacích údajů však ve skutečnosti poskytl své údaje podvodníkům. Do několika hodin byly z jeho účtu vybrány peníze, dřív, než si uvědomil, že byl podveden.

Skvěle zvládnutá situace

Pan Novák obdržel e-mail, který vypadal jako zpráva od jeho banky, v němž stálo, že jeho účet byl kompromitován. V e-mailu „banka" požadovala, aby okamžitě klikl na odkaz a přihlásil se, aby potvrdil svou totožnost. Pan Novák si všiml, že e-mail obsahuje naléhavé varování, což mu připadalo podezřelé. Na odkaz proto neklikl, ale zavolal přímo do své banky na oficiální telefonní číslo uvedené na jejích webových stránkách. Operátor banky mu potvrdil, že žádný takový e-mail neposlali a že se jedná o phishingový útok. Pan Novák tímto správným postupem ochránil své údaje a předešel finanční ztrátě.

Útočníci nemusí člověka zkoušet zneužít jen prostřednictvím e-mailu, ale také např. pomocí vishingu (spojení slov „voice" – hlas – a „phishing"), což je forma útoku, kdy člověku zavolají jménem banky s tím, že si potřebují ověřit další údaje k žádosti např. o půjčku a žádají nejen osobní údaje (rodné číslo, bydliště…), ale také třeba přihlašovací údaje do banky. Nikdy nikomu nesdělujte žádné své údaje po telefonu. Pokud obdržíte podezřelý telefonát, zavěste a zavolejte na oficiální číslo vaší banky, abyste ověřili pravost hovoru.

JAKÁ OHROŽENÍ JSOU DŮLEŽITÁ?

- **Krádež peněz:** Podvody a kybernetické útoky mohou vést k významným finančním ztrátám. Peníze mohou „zmizet" z bankovních účtů, dojde na podvodné platby kreditními kartami nebo placení výkupného za odemčení zašifrovaných souborů.

- **Ztráta osobních údajů:** Únik citlivých informací, jako jsou rodná čísla, čísla účtů nebo zdravotní záznamy, může vést až ke zneužití identity a následným dalším podvodům. Ztráta těchto údajů může mít dlouhodobé následky a způsobit mnoho problémů.

- **Poškození dobrého jména:** Dezinformace a kybernetické útoky mohou poškodit pověst. Falešné informace šířené o vás nebo vašich blízkých mohou vážně poškodit osobní i profesionální vztahy. Proto je opravdu důležité být při sdílení informací online opatrný a pečlivě zvažovat, jaké informace o sobě sdělujete třeba na sociálních sítích.

- **Dopady do soukromí:** Strach a úzkost spojené s kybernetickými útoky mohou mít vážný dopad na duševní pohodu. Pocit narušení soukromí nebo podvodu umí způsobit velký stres. Je důležité mít někoho, s kým lze tyto pocity sdílet, a hledat podporu. Strach a špatná zkušenost totiž mohou způsobit, že budete k používání technologií skeptičtí, což může vést až k sociální izolaci.

Jednoduše řečeno, stačí používat „digitální zámky" a selský rozum. Nedělat to, co byste nedělali ani v reálném světě – tedy nechodit na podezřelá, „temná" místa a nevěřit hned cizím lidem.

TIPY NA BEZPEČNÉ POUŽÍVÁNÍ E-MAILŮ A SOCIÁLNÍCH SÍTÍ

4

TIPY NA BEZPEČNÉ POUŽÍVÁNÍ E-MAILŮ A SOCIÁLNÍCH SÍTÍ

BEZPEČNÉ POUŽÍVÁNÍ E-MAILŮ

E-maily a sociální sítě jsou důležitými nástroji pro komunikaci, sdílení informací a udržování kontaktů s rodinou a přáteli. Mají-li online aktivity zůstat bezpečné, je důležité věnovat se bezpečnému chování i v této části digitálního světa. Jaké jsou tedy naše tipy pro bezpečné používání e-mailů a ochranu soukromí na sociálních sítích?

1. **Ověřujte odesílatele:** Před otevřením e-mailu nebo kliknutím na odkaz vždy ověřte, kdo je skutečným odesílatelem. Podvodníci totiž mohou snadno vytvořit falešné e-maily, které vypadají jako od důvěryhodných institucí nebo osob. Tuto skutečnost nejlépe zjistíte e-mailovým nebo telefonickým dotazem na ověřené číslo. Stačí se zeptat, jestli vám podezřele vypadající e-mail skutečně poslali. Je důležité být obezřetný také u e-mailů od blízkých osob. I jejich účty mohou být někdy napadeny. Všímejte si například neobvyklých slovních spojení nebo špatného slovosledu, který by mohl napovídat, že se jedná o překlad. Pokud obdržíte neobvyklý e-mail od někoho, koho znáte, raději se s ním nejdříve spojte jiným způsobem, například telefonicky, a ověřte si, že vám e-mail skutečně poslal on.

2. **Nikdy nesdílejte citlivé údaje přes e-mail:** Důvěryhodné instituce nikdy nepožadují vaše hesla, čísla platebních a kreditních karet nebo jiné citlivé údaje prostřednictvím e-mailu. Pokud takovou žádost obdržíte, jedná se nejspíš o podvod. Nejrozumnější je stáhnout si přímo do mobilu ověřenou aplikaci své banky a sledovat zprávy (notifikace) přímo v této aplikaci.

3. **Buďte opatrní při otevírání příloh:** Přílohy v e-mailech mohou obsahovat škodlivý software. Otevírejte pouze přílohy od důvěryhodných zdrojů a pokud si nejste jisti, raději je neotevírejte, případně odesílateli oznamte, že neznámé přílohy otevírat jednoduše nebudete.

OCHRANA SOUKROMÍ NA SOCIÁLNÍCH SÍTÍCH

Pokud používáte sociální sítě, sledujte své nastavení soukromí. Sdílejte informace pouze s lidmi, které znáte a kterým důvěřujete. Nebojte se vytvořit si různé skupiny tak, abyste mohli zvlášť komunikovat se svými nejbližšími, zvlášť se známými a zvlášť s lidmi, které neznáte. Především s nimi na sociálních sítích komunikujte obezřetně. Níže přinášíme základní, jednoduché rady, jak si ochránit soukromí na sociálních sítích:

1. **Buďte opatrní na to, co sdílíte:** Pečlivě si promyslete, než něco zveřejníte. Informace, které sdílíte online, mohou být viděny mnoha lidmi, přičemž se mezi nimi mohou najít tací, kteří vámi zveřejněné informace zneužijí nebo překroutí. Naprosto bez výjimek se vyhněte sdílení osobních údajů, jako jsou adresa, telefonní číslo nebo dokonce informace ohledně financí. Příkladem může být sdílení fotek z dovolené – pokud jste pryč a nikdo u vás doma není, raději fotografie z dovolené nesdílejte. Fotografie mohou být signálem pro zloděje, který tak u vás doma může spáchat trestnou činnost.

2. **Ověřujte žádosti o přátelství:** Žádosti o přátelství přijímejte pouze od lidí, které skutečně znáte. Domů také nepozvete každého, kdo u vás zaklepe na dveře.

3. **Pozor na podvody:** I sociální sítě jsou místem, kde se mohou objevovat podvody. Pokud obdržíte zprávu od někoho, koho neznáte, nebo pokud zpráva vypadá podezřele, buďte opatrní. Nikdy neklikejte na odkazy nebo neotevírejte přílohy od neznámých osob. Buďte opatrní při nákupech na nejrůznějších internetových bazarech. Osobní a platební údaje je v těchto případech rozhodně lepší nesdílet. **Nikdy nereagujte na žádosti o poslání peněz, a to ani v případě, že by se mohlo zdát, že tato žádost je od vašich přátel nebo někoho z rodiny.**

KLÍČEM K NAŠIM OSOBNÍM ÚDAJŮM JE HESLO

5

KLÍČEM K NAŠIM OSOBNÍM ÚDAJŮM JE HESLO

Dobrá hesla jsou důležitá, abyste zajistili dostatečnou bezpečnost vašich online účtů a digitálních aktivit. Jak je tedy potřeba nad hesly přemýšlet a jak si je správně vytvořit, vysvětlí následující část brožury. Dozvíte se také, co je dvoufaktorové ověřování, které vám můžeme doporučit.

TVORBA SILNÝCH HESEL

Jaká jsou doporučení pro tvorbu pořádného hesla? Jak to udělat, aby vaše hesla byla rovnocennou obdobou vašeho svazku klíčů, kterými pečlivě chráníte svůj fyzický majetek?

Délka: Heslo by mělo mít minimálně 10 znaků. Čím delší heslo, tím obtížnější je ho prolomit.

Kombinace znaků: Používejte kombinaci velkých a malých písmen, číslic a speciálních znaků (např. !, @, #, $).

Nepoužívejte osobní informace: Vyhněte se používání jmen, dat narození nebo jiných osobních údajů, které mohou být snadno zjistitelné.

Unikátnost: Pro každý účet používejte jiné heslo. Tím minimalizujete riziko, že pokud bude jedno heslo prolomeno, útočníci získají přístup k dalším účtům.

Pokud stále tápete, jaké vhodné heslo zvolit, podívejte se na závěrečné stránky této brožury. Najdete tam pár užitečných tipů.

DVOUFAKTOROVÉ OVĚŘOVÁNÍ

Dvoufaktorové ověřování (MFA) je dalším krokem ke zvýšení bezpečnosti vašich účtů. Jak už jsme zmínili, MFA přidává další stupeň zabezpečení tím, že vyžaduje nejen heslo, ale také další způsob ověření. Tím může být kód zaslaný na váš telefon, otisk prstu nebo jiné bezpečnostní opatření.

Jak tedy může vypadat takové MFA přihlášení? Jako obvykle nejprve zadáte své uživatelské jméno a silné heslo. Poté budete požádáni o další způsob ověření, jako je jednorázový kód nebo biometrické ověření.

Používání MFA výrazně zvyšuje bezpečnost vašich účtů a snižuje riziko, že někdo získá přístup k vašim citlivým informacím. Je to velmi podobné tomu mít na dveřích dva zámky nebo rovnou dvoje dveře. Pokud chcete vědět, jak na to, pročtěte si doporučení v závěru této brožury.

FAKE NEWS – FALEŠNÉ ZPRÁVY A DEZINFORMACE

6


FAKE

FAKE NEWS – FALEŠNÉ ZPRÁVY A DEZINFORMACE

V dnešní době, kdy internet a sociální sítě hrají v našem každodenním životě velkou roli, je stále důležitější umět rozpoznat, které informace jsou pravdivé a ověřené, abychom se na ně mohli spolehnout, a co jsou takzvané dezinformace nebo fake news. V českém prostředí je označujeme jako falešné zprávy. Mohou totiž vážně narušit nejen klid a pohodu jednotlivců, ale dokonce ovlivnit celou společnost.

JAK ROZPOZNAT DEZINFORMACE

- **Přehnané titulky:** Dezinformační články často používají dramatické a přehnané titulky, které mají za cíl upoutat vaši pozornost. Buďte opatrní, pokud se vám zdá, že titulek je příliš šokující nebo z něj přímo sálá senzačnost.

- **Nedostatek zdrojů:** Důvěryhodné zprávy vždy uvádějí své zdroje. Pokud článek neobsahuje žádné zdroje nebo vám přijdou podezřelé, je dobré k článku přistupovat obezřetně.

- **Chyby v textu:** Dezinformační články často obsahují pravopisné a gramatické chyby, což může naznačovat, že článek nenapsal profesionální novinář.

- **Překvapivá a neuvěřitelná tvrzení:** Pokud něco zní příliš dobře (nebo špatně) na to, aby to byla pravda, pravděpodobně to pravda není. Dezinformace často využívají lidskou zvědavost a tendenci věřit šokujícím zprávám. Pracují s nadšením, nebo naopak se strachem. Silná emoce je totiž velký hnací motor. Často také na člověka vyvíjejí tlak kvůli nedostatku času – „sdílejte rychle, než to smažou“. V takovém případě jste se s vysokou pravděpodobností setkali s fake news.

Dezinformace v nás mohou vyvolat pocit, že se není čeho obávat, opak je ale pravdou. Mohou podněcovat nenávist a skutečně dokážou velmi úspěšně rozdělovat lidi a zasahovat do jejich vztahů. Nesouhlas a nenávist tak může vážně narušit vztahy v rodinách, skupinách přátel, pracovních týmech i celé společnosti. Dezinformace mohou ovlivňovat názory, např. na volby, zdravotní péči nebo mezinárodní vztahy. Nezapomínejme ani na to, že falešná zpráva může poškodit pověst jednotlivců nebo organizací, což může negativně ovlivnit jejich osobní, resp. profesionální život.

BEZPEČNÉ POUŽÍVÁNÍ MOBILŮ A TABLETŮ

7

BEZPEČNÉ POUŽÍVÁNÍ MOBILŮ A TABLETŮ

Přenosná zařízení se stala nedílnou součástí našeho každodenního života. Tato zařízení mohou být nejen prostředkem, který zajišťuje komunikaci, ale také zdrojem zábavy a praktickým nástrojem pro udržování kontaktu s rodinou a přáteli, přístup k informacím a službám. Na co tedy myslet, aby bylo jejich používání bezpečné?

ZAMYKÁNÍ OBRAZOVKY

Proč je to důležité? Pokud ztratíte svůj telefon nebo tablet, zamčená obrazovka zabrání cizím lidem v přístupu k vašim informacím.

Jak na to: Nastavte zámek obrazovky pomocí hesla, PIN kódu, otisku prstu nebo rozpoznání obličeje.

AKTUALIZACE TELEFONU I APLIKACÍ

Proč je to důležité? Aktualizace často obsahují opravy bezpečnostních chyb, které mohou chránit vaše zařízení před novými hrozbami.

Jak na to: Sledujte, zda jsou váš operační systém a aplikace aktuální. Můžete si nastavit automatické aktualizace.

STAHOVÁNÍ APLIKACÍ

Proč je to důležité? Škodlivé aplikace mohou ohrozit bezpečnost vašich osobních údajů.

Jak na to: Stahujte aplikace jen z oficiálních obchodů jako Google Play nebo App Store. Před instalací si přečtěte recenze a hodnocení ostatních uživatelů.

ZÁLOHOVÁNÍ DAT

Proč je to důležité? Zálohování dat vám umožní obnovit vaše informace v případě ztráty nebo poškození zařízení.

Jak na to: Pravidelně nebo automaticky zálohujte své fotografie, kontakty a další důležité údaje do cloudového úložiště nebo na externí disk.

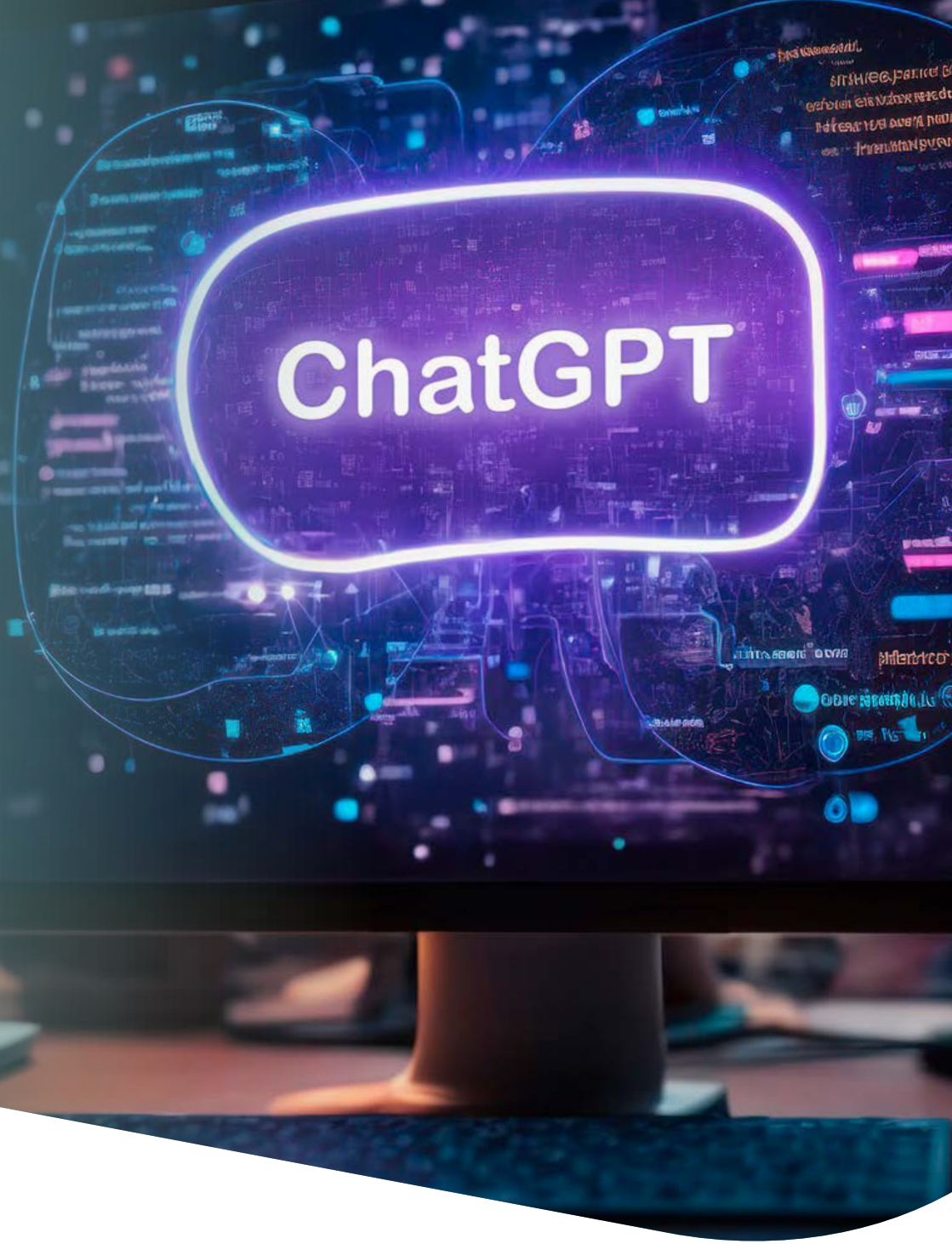
SLEDOVÁNÍ ZAŘÍZENÍ:

Proč je to důležité? Pokud ztratíte své zařízení, možnost sledování vám může pomoci ho najít.

Jak na to: Aktivujte funkci „Najdi moje zařízení". Tyto služby vám umožní sledovat polohu zařízení a případně jej vzdáleně uzamknout nebo vymazat.

BEZPEČNÉ PROHLÍŽENÍ INTERNETU

8


ChatGPT

BEZPEČNÉ PROHLÍŽENÍ INTERNETU

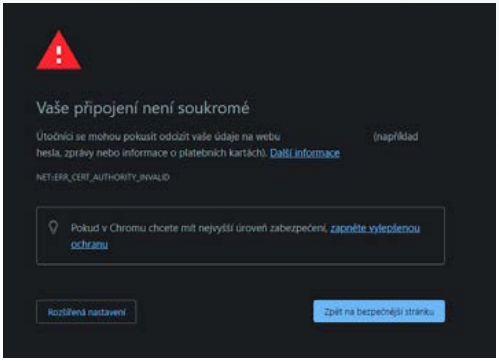
Prohlížení internetu je činnost, která se stala součástí každodenních aktivit lidí všech generací. Aby bylo prohlížení internetu bezpečné, je důležité dodržovat několik základních pravidel a opatření.

JAK BEZPEČNĚ PROHLÍŽET INTERNETOVÉ STRÁNKY

Používejte důvěryhodné webové stránky

Proč je to důležité? Důvěryhodné webové stránky nebývají tak často infikovány škodlivým softwarem nebo podvodným obsahem.

Jak na to: Navštěvujte webové stránky, které znáte a kterým důvěřujete. Ověřujte, zda webová adresa začíná „https://" – písmeno „s" znamená, že stránka je zabezpečená. Poznáte to také podle zámečku v adresním řádku prohlížeče.



V případě, kdy stránka nemá platný certifikát (není zabezpečená), všechny prohlížeče před načtením stránky uživatele upozorní, že je na stránce něco špatně. Na takové stránky byste nikdy neměli zadávat jakékoliv osobní, platební ani přihlašovací údaje.

Mějte však na paměti, že i podvodná stránka může mít platný certifikát a tvářit se, že je bezpečná. Je důležité si při otevření odkazu zkontrolovat, zda nás stránka někam nepřesměrovala, a ověřit, zda je URL[1] stránky správná.

VYHNĚTE SE PODEZŘELÝM ODKAZŮM

Proč je to důležité? Kliknutí na podezřelé odkazy může vést k infikaci škodlivým softwarem nebo krádeži vašich osobních údajů.

Jak na to: Neklikejte na odkazy v e-mailech nebo zprávách od neznámých odesílatelů. Pokud odkaz vypadá podezřele, raději ho neotevírejte a zeptejte se odesílatele na jeho obsah jiným způsobem – např. mu můžete zavolat.

PŘI POUŽÍVÁNÍ VEŘEJNÝCH WI-FI SÍTÍ

Vyhněte se citlivým operacím

Proč je to důležité? Veřejné Wi-Fi sítě mohou být nezabezpečené a útočníci je mohou snadno využít k zachycení vašich dat.

Jak na to: Nepřistupujte k citlivým informacím, jako jsou bankovní účty nebo e-mailové účty, když používáte veřejnou Wi-Fi síť.

[1] URL (zkratka z anglického Uniform Resource Locator) neboli jednotná adresa zdroje, která se používá pro přesnou identifikaci dokumentů na internetu.

PRAKTICKÉ RADY PRO BEZPEČNÉ POUŽÍVÁNÍ TECHNOLOGIÍ

9

PRAKTICKÉ RADY PRO BEZPEČNÉ POUŽÍVÁNÍ TECHNOLOGIÍ

JAK BEZPEČNĚ NAKUPOVAT ONLINE

Nakupování online je pohodlné a často nabízí širší výběr produktů než kamenné obchody. Můžete nakupovat z pohodlí domova, srovnávat ceny a číst recenze ostatních zákazníků, díky čemuž si vyberete tu nejlepší nabídku a ušetříte, navíc se vyhnete frontám v obchodě.

Mnoho online obchodů nabízí doručení domů přímo až ke dveřím, což je obzvlášť příjemné pro seniory nebo osoby s omezenou pohyblivostí. Internetové nakupování také umožňuje snadné vyhledávání specifických produktů a porovnávání různých značek a modelů.

Při nakupování online je však důležité být obezřetný a chránit své osobní a finanční údaje. Nakupujte pouze na známých a ověřených webových stránkách. Připravili jsme pro vás pár rád:

1. Přečtěte si vždy před nákupem recenze a hodnocení obchodu od ostatních zákazníků. Zkontrolujte, zda je webová adresa zabezpečená, tzn. začíná „https://“, a to zejména v případech, kdy zadáváte své platební údaje.

2. Vyhněte se neobvyklým a podezřelým nabídkám, které vypadají příliš dobře na to, aby byly pravdivé. Podezřele nízké ceny mohou být známkou podvodu. Při nakupování používejte silná a jedinečná hesla pro každý online obchod a pokud je to možné, zapněte dvoufaktorové ověřování, což útočníkům ztíží přístup k vašim účtům.

3. Platťe pomocí bezpečných platebních metod (debetními/kreditními kartami) nebo např. přes PayPal, což je jedna ze služeb nabízejících ochranu kupujících. Pokud vám vyhovuje platit převodem z účtu, zvažte, zda si nepořídit jeden účet pouze pro online nákupy. Pak stačí, když na něj převedete potřebnou částku a případný útočník se nedostane k vašemu „hlavnímu“ účtu, kde máte své finanční prostředky a třeba i úspory.

4. Ověřujte důvěryhodnost online obchodů. Hledejte kontaktní informace, jako je telefonní číslo, e-mail a fyzická adresa. Pokud je nenajdete, buďte opatrní. Zkontrolujte recenze a zkušenosti jiných nakupujících. Pokud jste je nenašli, vyberte si raději jiný online obchod.

5. Používejte pro stahování a instalaci aplikací pro online nakupování pouze oficiální služby, jako je Google Play nebo App Store. Před instalací si přečtěte recenze a hodnocení ostatních uživatelů, abyste se ujistili, že aplikace je důvěryhodná a bezpečná.

Nakupování online může být skvělým zážitkem, pokud dodržíte několik základních pravidel bezpečnosti:

- Buďte obezřetní.
- Chraňte své osobní údaje.
- Užívejte si pohodlí a výhody, které online nakupování nabízí.

SPECIFIKA PRÁCE SE SENIORY

10

SPECIFIKA PRÁCE SE SENIORY

Nebojte se zdánlivě složité technologické koncepty komunikovat jednoduše. Práce s lidmi ve vyšším věku vyžaduje v oblasti digitální bezpečnosti specifický přístup. Je důležité si uvědomit, že senioři jsou často velmi zkušení, moudří a chytří lidé, kteří se úspěšně orientují v mnoha jiných oblastech života. Potřebují pouze pomoct osvojit si nové dovednosti – práci s moderními technologiemi a problematiku digitální bezpečnosti. Při práci s touto skupinou je užitečné zohlednit následující doporučení:

- **Podpořte snížení ostychu a obav** – Jedná se o důležitý aspekt práce se seniory. Senioři se často mohou při používání nových technologií cítit nejistě nebo nervózně. Empatie a trpělivost jsou klíčové pro vytváření bezpečného a podporujícího prostředí. Poslouchejte jejich obavy a otázky bez přerušování a poskytněte jim dostatek času, aby nové koncepty pochopili. Ukažte, že jste tam pro ně a že jim chcete pomoci. Vyjádřete jim respekt uznáním jejich celoživotních zkušeností a moudrosti, na kterou mohou prací s digitálními technologiemi navázat.

- **Zjednodušujte terminologii** – Komplexní technické pojmy a jazyk mohou být matoucí. Jednoduché a srozumitelné vysvětlení usnadňuje seniorům pojmy pochopit a zapamatovat si je. Používejte běžné výrazy a přirovnání, které jsou blízké jejich každodennímu životu. Například dvoufaktorové ověřování můžete vysvětlit jako „zamčení dveří a kontrolu občanského průkazu před vstupem do letadla".

- **Fanděte jejich učení** – Povzbuzování a pozitivní zpětná vazba mohou výrazně zvýšit sebevědomí seniorů a motivovat je k dalšímu učení. Ukažte jim, že každý krok vpřed je důležitý a hodnotný. Chvalte je a oceňujte, aby měli větší chuť pokračovat ve vzdělávání.

- **Zkoušejte, hrajte si** – Praktické ukázky a cvičení umožňují seniorům vyzkoušet si nové dovednosti v bezpečném prostředí. Po každém vysvětlení seniory nechte, aby si danou činnost vyzkoušeli sami, a buď-

te připraveni jim pomoci, pokud budou mít potíže. Nebojte se zkoušet nové přístupy či postupy na zajímavých tématech, která konkrétního jednotlivce nebo skupinu zajímají. Podpořte jejich hravost, bavte se.

- **Využijte malé skupiny** – Individuální přístup je nezbytný, protože každý senior má jiné zkušenosti a schopnosti, a proto je potřebné výuku přizpůsobit jejich možnostem a tempu. Zjistěte, jaké mají zkušenosti s technologiemi a jaké jsou jejich cíle. Zajistěte, aby se cítili pohodlně a mohli se efektivně učit. Zajímavé je také učení v malých skupinkách, kde mohou sdílet svoji práci s vrstevníky, dělit se o znalosti, ale i o nejistotu. Věřte, nebo nevěřte, ale tímto způsobem se učí nejen samotná skupina, ale také její lektor.

- **Použití většího písma a dalších pomocných prvků** může seniorům, kteří mají problémy se zrakem nebo jemnou motorikou, značně usnadnit práci s digitálními zařízeními. Ukažte jim, jak na jejich zařízeních nastavit větší písmo, používat zvětšovací funkce nebo hlasové ovládání. Můžete jim také doporučit ergonomické pomůcky, jako jsou stylusy nebo stojánky na tablety, které usnadní manipulaci se zařízením.

- **Vysvětlujte, vysvětlujte a potom vysvětlujte** – Představování přínosů technologií seniorům je pro ně dalším motivujícím faktorem. Senioři mohou být motivovanější k učení, pokud vidí konkrétní přínosy používání technologií. Ukažte jim, jak technologie mohou jejich každodenní život zlepšit – např. jak komunikovat s rodinou přes videohovory, nakupovat online nebo vyhledávat zdravotní informace. Tímto způsobem jim ukážete, že technologie nejsou jen složité a nepochopitelné, ale mohou být také velmi užitečné a přínosné. Že jim mohou až neuvěřitelně přiblížit celý svět.

ZÁVĚREČNÉ DESATERO

DOPORUČENÍ PRO VŠECHNY

1. Aktualizujte svůj software.
2. Používejte silná hesla.
3. Zapněte dvoufaktorové ověřování.
4. Buďte při otevírání e-mailů opatrní.
5. Stahujte aplikace jen z důvěryhodných zdrojů.
6. Buďte opatrní při používání veřejných Wi-Fi sítí.

DOPORUČENÍ PRO LEKTORY

7. Buďte při práci se seniory trpěliví a empatičtí.
8. Vysvětlujte seniorům technologie a jejich používání jednoduše a srozumitelně.
9. Pomáhejte seniorům překonat překážky – nastavte větší písmo a vyšší kontrast.
10. Povzbuzujte seniory a nezapomeňte ocenit jejich pokroky.

PŘÍLOHY PŘÍRUČKY

PŘÍLOHA Č. 1: SLOVNÍČEK ODBORNÝCH POJMŮ

Antivirový program – software, který chrání váš počítač před škodlivým softwarem.

Cloudové úložiště – služba, která ukládá vaše data online, aby k nim bylo možné přistupovat odkudkoli.

Dvoufaktorové ověřování (MFA) – bezpečnostní proces, který vyžaduje dvě formy identifikace (např. heslo a kód z mobilu).

Fake news – záměrně nepravdivé nebo zavádějící informace.

Heslo – tajný kód, který chrání vaše účty.

Malware – škodlivý software, který může poškodit váš počítač nebo z něj ukrást data.

Phishing – podvodná technika, kdy se útočníci vydávají za důvěryhodnou instituci a snaží se získat vaše údaje.

Ransomware – typ malwaru, který zašifruje vaše soubory a požaduje výkupné za jejich odemčení.

Sociální inženýrství – manipulace lidí s cílem získat citlivé informace.

Spam – nevyžádané e-maily nebo zprávy, často reklamní nebo podvodné.

Úložiště – místo, kde jsou ukládána data, může být jak fyzické (disk), tak online (cloud).

Zálohování – vytváření kopie vašich dat pro případ ztráty nebo poškození.

PŘÍLOHA Č. 2: TIPY NA TVORBU SILNÝCH HESEL

1. **Použijte oblíbenou frázi**
   - Vyberte si oblíbenou větu nebo citát z knihy, filmu nebo písně – např. „Každý den je nový začátek".
   - Vezměte první písmena každého slova – „Kdjnz".
   - Přidejte čísla a speciální znaky – „Kdjnz2024!".

2. **Zvolte osobní příběh**
   - Vyberte si příběh z vašeho života, který si dobře pamatujete – např. „Moje první auto bylo červené".
   - Vezměte první písmena každého slova – „Mpabc".
   - Přidejte čísla a speciální znaky – „Mpabc1980!".

3. **Použijte kombinaci slov**
   - Vyberte si dvě nebo tři nesouvisející slova – např. „Kočka" a „Hvězda".
   - Spojte je dohromady a přidejte čísla a speciální znaky – „KockaHvezda@45".

4. **Vytvořte si rým**
   - Vyberte si dvě nebo tři slova, která se rýmují – např. „Kniha" a „Dýha".
   - Spojte je dohromady a přidejte čísla a speciální znaky – „KnihaDyha+88".

5. **Použijte oblíbené místo**
   - Vyberte si oblíbené místo nebo destinaci – např. „Praha Karlův most".
   - Vezměte první písmena každého slova – „PKm".
   - Přidejte čísla a speciální znaky – „PKm@2024!".

6. **Kombinujte oblíbené věci**
   - Vyberte si dvě oblíbené věci – např. „Čokoláda" a „Káva".
   - Spojte je dohromady a přidejte čísla a speciální znaky – „CokoladaKava#12".

7. **Použijte oblíbený sport nebo tým**
   - Vyberte si oblíbený sport nebo tým – např. „Hokej Sparta".
   - Vezměte první písmena každého slova – „HS".
   - Přidejte čísla a speciální znaky – „HS2023!".

PŘÍLOHA Č. 3: MULTIFAKTOROVÉ OVĚŘOVÁNÍ

Dvoufaktorové ověřování (MFA) je bezpečnostní opatření, které přidává další stupeň ochrany. Kromě hesla potřebujete ještě jeden způsob ověření, například kód zaslaný na váš telefon. Zde je jednoduchý příklad, jak MFA funguje:

Jak to funguje?

1. Přihlášení k účtu

- Otevřete webovou stránku nebo aplikaci, ke které se chcete přihlásit.
- Zadejte své uživatelské jméno a heslo jako obvykle.

2. Ověření

- Po zadání hesla budete vyzváni k vyplnění druhého ověřovacího kroku.
- Tento krok může být kód zaslaný na váš mobilní telefon prostřednictvím SMS, generovaný ve speciální aplikaci, případně zaslaný na váš e-mail.

3. Přijetí kódu

- Na váš telefon dorazí SMS zpráva s kódem nebo aplikace vygeneruje jednorázový kód.
- Pokud jste zvolili, aby vám na e-mail přišel kód, zkontrolujte si vaši e-mailovou schránku.

4. Zadání kódu

- Zadejte zaslaný kód na webové stránce nebo v aplikaci, kde jste se přihlašovali.

5. Úspěšné přihlášení

- Po zadání správného kódu budete přihlášeni do svého účtu.

Jak už bylo řečeno, MFA poskytuje další stupeň ochrany. Přestože někdo může vaše heslo zjistit, bez druhého faktoru, tzn. bez ověření, se k vašemu účtu přihlásit nemůže. Můžete si to představit, jako byste měli dva zámky na dveřích místo jednoho – i když někdo otevře první zámek (heslo), stále potřebuje klíč k druhému zámku (kód).

Asociace poskytovatelů sociálních služeb ČR

www.apsscr.cz

APSS ČR je největší profesní organizací sdružující poskytovatele sociálních služeb v České republice. Sdružuje více než 1300 organizací a téměř 3000 registrovaných služeb.

Asociace v rámci své činnosti:

- zastupuje a hájí zájmy svých členů u státních a ostatních zainteresovaných institucí, zejména předkládáním odborných stanovisek, kvalifikovanou oponenturou a iniciací a podporou žádoucí právní regulace sociálních služeb;
- zprostředkovává rozšiřování vědeckých a výzkumných poznatků do činnosti poskytovatelů sociálních služeb a předávání tuzemských i zahraničních odborných zkušeností svým členům;
- vyvíjí studijní, dokumentační, vzdělávací a expertní činnost;
- organizuje kongresy, odborné konference a vzdělávací programy;
- je pořadatelem již tradičního Týdne sociálních služeb ČR, spolupořadatelem ocenění Národní cena – Pečovatel/ka roku, držitelem licence E-Qalin pro ČR (model měření a zvyšování kvality) a správcem Značky kvality (systém externí certifikace zařízení).

Sekce a svazy Asociace:

Činnost sekcí a svazů probíhá na základě specifických potřeb členů Asociace.

Sekce:

• sekce terénních služeb;
• sekce ambulantních služeb APSS ČR;
• sekce sociálních služeb pro osoby bez domova;
• sekce adiktologických služeb;
• sekce služeb péče o ohrožené dítě;
• sekce služeb pro rodinu;
• sekce nadregionálních poskytovatelů sociálních služeb;
• sekce nestátních poskytovatelů pobytových sociálních služeb.

Svazy:

• Profesní svaz sociálních pracovníků v sociálních službách;
• Profesní svaz zdravotnických pracovníků v sociálních službách.

APSS ČR je členem:

Institut vzdělávání APSS ČR

Společně za vzděláním!

Jsme největší vzdělávací organizací v České republice v oblasti dalšího vzdělávání pracovníků sociálních služeb. Chceme se podílet na rozvoji systému celoživotního vzdělávání a být jedním z článků přispívajících ke zvyšování kvality nabízených sociálních služeb.

OTEVŘENÉ SEMINÁŘE

Institut vzdělávání nabízí širokou škálu akreditovaných kurzů ve školicích místnostech v Praze, Brně, Ostravě a Táboře. Kurzy připravujeme pro pracovníky sociálních služeb na všech pozicích. Naší snahou je, aby kurzy byly co nejvíce zaměřené na praxi a byly interaktivní.

- Široká škála akreditovaných kurzů.
- Školicí místnosti v Praze, Brně, Ostravě a Táboře.
- Akreditované on-line školení.
- Kurzy pro pracovníky sociálních služeb na všech pozicích.
- Interaktivní kurzy zaměřené na praxi.
- Aktuální témata školení.
- Výměna zkušeností a dobré praxe mezi účastníky z různých organizací.

Nabídka kurzů na www.institutvzdelavani.cz / Otevřené kurzy

SEMINÁŘ „NA KLÍČ“ PRO ORGANIZACE

Zrealizujeme pro Vaši organizaci kurz až pro 25 účastníků na jakékoli téma z naší nabídky. Nemusíte složité posílat své zaměstnance na školení, lektor přijede přímo k Vám. Kurzy realizujeme i v odpoledních hodinách nebo v sobotu.

- Finanční úspora při větších skupinách.
- Eliminace roztříštěnosti péče díky jednotnému vzdělávání zaměstnanců.
- Přesnější zasazení vzdělávání do prostředí poskytované služby.
- Vyšší efektivita vzdělávání díky individuálnímu přístupu.
- Výhodnější ceny při dlouhodobější spolupráci s Institutem vzdělávání.
- Časová úspora.
- Možnost naplánování kurzu s ohledem na časové a personální možnosti organizace.
- Upevnění týmové spolupráce.

Nabídka kurzů na www.institutvzdelavani.cz / Kurzy na klíč

Kontakt: www.institutvzdelavani.cz | Tel.: +420 724 940 126 | Email: institut@apsscr.cz

Život Plus, z.ú.

NADREGIONÁLNÍ POSKYTOVATEL TERÉNNÍCH SOCIÁLNÍCH SLUŽEB PRO SENIORY, OSOBY SE ZDRAVOTNÍM POSTIŽENÍM, OSOBY S CHRONICKÝM ONEMOCNĚNÍM A NEFORMÁLNĚ PEČUJÍCÍ OSOBY

Život+

Chcete žít **plnohodnotný život** v přirozeném prostředí?

NABÍDKA SLUŽEB

Tísňová péče

- Poskytnutí tísňového zařízení „SOS tlačítka“
- Spojení s dispečinkem nepřetržitě 24 hodin denně
- Zprostředkování pomoci v krizové situaci
- Poskytnutí pomoci a podpory ve Vaší životní situaci

Odborné sociální poradenství

- Jak pečovat v domácím prostředí
- Kde a jak žádat o příspěvky
- Kde a jak žádat o kompenzační pomůcky
- Poskytnutí psychologické podpory

Pořádáme besedy, přednášky a kurzy pro veřejnost.
Více o nabídce služeb se dozvíte na www.zivotplus.cz

Zanechte nám kontakt, ozve se Vám zpět sociální pracovník
operator@zivotplus.cz

NONSTOP LINKY

724 182 325 / 327 532 900

Život Plus, z.ú.,
Benešova 632, 284 01 Kutná Hora

Pobočka pro Jihočeský kraj:
Špidrova 47/42, 385 01 Vimperk

2024
www.apsscr.cz