KRAJE PRO BEZPEČNÝ INTERNET

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Středočeský kraj

Vzdělávací institut Středočeského kraje

Středočeský kraj

Eva Burdová
Jan Traxler

SENIOR V KYBERPROSTORU

Publikace je financována ze státní účelové dotace MV ČR v rámci realizace projektu prevence kriminality „ Senior v kyberprostoru“, který je součástí Programu prevence kriminality Středočeského kraje na rok 2016.

Autoři: PhDr. Mgr. Eva Burdová, MBA

PhDr. Mgr. Jan Traxler

Název: **SENIOR V KYBERPROSTORU**

Vydavatel: Středočeský kraj ve spolupráci s VISK, Zborovská 11, 150 00 Praha 5

Kontaktní osoba: Mgr. Jiří Holý, e-mail: holy@visk.cz, tel.: 606 656 724

Počet stran: 40

Grafické zpracování a tisk: Tiskárna J. Krákora, Husova 635, 261 01 Příbram IV., e-mail: tisk@pb.cz, tel.: 603 427 151

Pořadí vydání: 1

Vazba: V 1

Měsíc a rok vydání: září 2016

ISBN: 978-80-905893-1-5

Vážené dámy a pánové,

právě jste otevřeli publikaci obsahující základní informace o rizicích internetu a možnostech prevence před kybernetickou kriminalitou a elektronickým násilím páchaným na seniorech. V publikaci se seznámíte s novými trendy v oblasti elektronické bezpečnosti a se zásadami bezpečného chování v kyberprostoru.

Středočeský kraj se dlouhodobě věnuje rizikům virtuální komunikace a bezpečnému užívání internetu. Realizovali jsme více než stovku seminářů pro rodiče a pedagogy, působíme preventivně ve školách a od roku 2013 jsme zapojeni do projektu Asociace krajů Kraje pro bezpečný internet. V letošním roce jsme se rozhodli, že naše aktivity rozšíříme i na další důležitou cílovou skupinu, a to na seniory.

Aktuálně totiž vzrůstá počet lidí vyššího věku, kteří využívají informační a komunikační technologie. Podle průzkumu alespoň čtvrtina lidí ve věku nad 63 let využívá internet, tedy přibližně půl milionu občanů ČR. Dá se předpokládat, že tento trend bude nadále vzrůstat.

Je skutečností, že lidé vyššího věku začínají stále více využívat sociální sítě, nakupovat on-line, využívat elektronického bankovnictví a komunikovat prostřednictvím internetu. Ať je to v souvislosti s vyšší dostupností těchto služeb nebo omezením jejich fyzických sil, každopádně se pro ně internet stává prostředkem k udržování povědomí o společenském dění, tréninku myšlení, obstarání si záležitostí jinak obtížně dostupných nebo účinnou obranou proti sociální izolaci.

Je však důležité si uvědomit, že tzv. virtuální komunikace má řadu rizik a je relativně snadné se při neopatrném jednání nebo přehnané důvěřivosti stát obětí kyberkriminality. Podle policejních zdrojů jsou u některých typů kybernetické kriminality senioři ohroženější skupinou než ostatní, a to především pro minimální nebo žádné povědomí o hrozbách a kriminalitě spojené s kyberprostorem, obecně vyšší důvěřivosti, v touze po chybějícím sociálním kontaktu apod. Senioři se stávají stále častěji obětí nejrůznějších on-line útoků (podvody, phishing, hoax, krádeže identity, malware, spam apod., výjimkou není ani kyberšikana seniorů), které jsou v této publikaci podrobně rozebrány a vysvětleny.

Pevně věřím, že Vám tato publikace umožní lépe se orientovat v problematice rizik internetu a pomůžeme Vám předcházet tomu, abyste se stali oběťmi trestné činnosti v souvislosti s používáním nových a stále se rozvíjejících komunikačních technologií.

V Praze, srpen 2016
Miloš Petera, hejtman Středočeského kraje

SENIOR V KYBERPROSTORU

Vážená paní, Vážený pane,

předkládáme Vám příručku, kde bychom se společně chtěli pokusit nahlédnout do tajů kyberprostoru a pomoci tak seniorům lépe se orientovat ve složitých vodách internetu. Rádi bychom se také zaměřili na některá úskalí a problémy, které mohou nejen na seniory v kyberprostoru čekat. Bohužel se v posledních letech setkáváme s různými „šmejdy", kteří často využívají důvěry seniorů. Jejich zranitelnosti, třeba i nemožnosti s někým různé informace či nabídky sdílet. Své podnikání tak tito „kyberšmejdi" postaví na tom, že se spolehnou, že se senioři nemohou nebo nechtějí bránit. I těchto lidí se v kyberprostoru bohužel nachází hodně a navíc se cítí ve světě internetu schovaní a anonymní. Tak anonymní zase nejsou. Pojďme si tedy povídat o tom, co pro sebe můžeme udělat, aby byl celý kyberprostor dalším úžasným místem, kde si můžeme rozšířit obzory, komunikovat se světem a hledat nové přátele. Vždyť v posledních letech seniorů připojených k internetu výrazně přibývá a spousta z nich na něm tráví dokonce i hodně času. Senioři si našli své místo i na Facebooku. Podle údajů společnosti Nielson se počet uživatelů internetu starších 65 let zvýšil za posledních 5 let celosvětově o 6 milionů. Téměř polovina z nich přitom navštívila během posledního měsíce oblíbené portály jako YouTube nebo sociální síť Facebook. Stále více seniorů je ve světě internetu aktivních. A průměrně strávený čas na internetu se v případě seniorů pohybuje okolo 58 hodin měsíčně.[1]

Internet musíme ale umět používat. Je stejně jako oheň výborný sluha, ale zlý pán. Tak se nebojme a pojďme se společně do tohoto světa podívat.

Na procházku Vás zvou Eva a Honza

[1] Zdroj: internetový magazín Lemonade Prague

BEZPEČNÝ KYBERPROSTOR

Co je kyberprostor? Je to vlastně veškeré internetové prostředí, vše, kam se na internetu můžete dostat. Existuje tedy něco takového jako bezpečný kyberprostor, není to jen vybájené místo z pohádek pro dospělé? Je vůbec možné pohybovat se po kyberprostoru bezpečně? Je to možné. Záleží to však jen a jen na uživateli a na jeho znalostech toho, co by se mohlo stát a proč je třeba některým příležitostem pro „kyberšmejdy" předcházet. Na internetu můžete najít spoustu kamarádů, kteří jsou ve Vašem věku a chtějí si povídat, můžete najít i lidi, co mají stejné zájmy jako Vy. Můžete nakupovat s tím, že Vám zboží dovezou až do domu, můžete komunikovat se zahraničím, učit se cizí jazyky, vzdělávat se, najít si spoustu informací. Podle internetu můžete vařit, najdete tam obrovské množství receptů. Můžete hledat mapy, zjišťovat, co se kde nachází, prohlížet si vzdálené země, kam byste se třeba toužili podívat. A když byste nevěděli, jak na to, není problém, máte třeba vnoučata nebo je ve Vašem okolí jiné dítě. To je nejlepší záruka toho, jak se co nejvíce dozvědět. Dnešní děti s internetem žijí takřka od narození. Ale co senioři, kteří se s ním setkávají až třeba v mnohem pokročilejším věku? Nebojte se někoho zeptat, od někoho si nechte ukázat, jaké jsou všechny možnosti. Povídejte si třeba

se svými vnoučaty, ať Vám ukážou, jak mají zabezpečený mobilní telefon a ať se podívají, zda i Vy ho máte zabezpečený. Stačí pár základních úprav, jako třeba nahrání antivirového programu, který by měl být tím úplným základem, bez kterého bychom si ani neměli dovolit jakékoli internetové aplikace spustit. S tím souvisí i výběr techniky.

VÝBĚR TECHNIKY, NA ČEM ZÁLEŽÍ A K ČEMU TO POTŘEBUJETE?

Dostali jste od svých známých, dětí nebo příbuzných počítač, tablet, notebook nebo telefon? Je důležité vědět, co které zařízení umí a co neumí. Jak se ovládá a k čemu ho vlastně můžete používat. Je velmi důležité uvědomit si, že každé zařízení Vám může v mnoha situacích pomoci, ale někdy také i ublížit. Než tedy začnete uvedenou techniku používat, měli byste zvážit, k jakým činnostem ji budete využívat. Určitě není na škodu zeptat se svých známých, dětí nebo odborníků, k čemu všemu lze toto zařízení používat. Leckdy mají o mnoho více zkušeností, a tak Vám mohou pomoci s orientací a využitím.

Dalším důležitým faktorem je, jak dokážete ve světě kyberprostoru ochránit svou identitu. Na ulici také nestojíte s lístečkem, kdo jste, kde bydlíte, jaké máte konto apod.

INFORMACE, KTERÉ O SOBĚ POSKYTUJETE

Využívání výpočetní techniky a mobilů s sebou nese možnost a riziko o sobě uvádět mnoho informací, které jsou následně umístěny v síti internetu a za určitých podmínek jsou tyto informace dostupné komukoli. Skutečně komukoli na celém světě. Ne pouze jedincům, kterým chcete, ale všem. A tyto informace o Vás, které jste tam uvedli nebo i někdo jiný za Vás, se pak nechají různým způsobem využívat, ale i zneužívat. Důrazně proto doporučujeme nikde a nikdy o sobě neuvádět žádné bližší informace, na základě kterých byste mohli být identifikováni a následně třeba kontaktováni. Není žádnou ostudou nebo hanbou nechat si poradit od někoho zkušenějšího.

PO TELEFONU – MARKETING: CO DĚLAT V PŘÍPADĚ VOLÁNÍ TELEMARKETINGU, VÝZKUMNÍKŮ...

Pokud jste někde uvedli své jméno, telefonní číslo, e-mail nebo adresu, nemůžete se pak divit, že se stáváte cílem mnohých reklamních a i různě podvodných firem, které Vás kontaktují za účelem např. prodeje svých výrobků a služeb. Nestačíte se pak divit, co takto volající společnosti již o Vás vědí a že Vám nabízejí věci, které by se Vám mohly hodit. Jak se v tomto případě správně zachovat? Bylo by dobré vypátrat, kde na Vás zjistili kontakt. A v případě, že ho nemají od Vaší známé osoby, doporučujeme hovor ukončit. Ve většině případů je snahou volají-

cích Vám něco prodat nebo nabídnout, popř. zjistit o Vás další informace, které ještě nemají, aby v příštím kontaktu s Vámi byli úspěšnější.

Už se Vám stalo, že Vám po telefonu nebo e-mailu sdělili, že jste něco vyhráli anebo že máte jistotu výhry v případě, že například od nich objednáte nějaké zboží nebo se dostavíte na osobní schůzku? Nenechte se zbytečně oklamat různými marketingovými triky a nabídkami. V drtivě většině jen budete přinuceni si zakoupit předražené a ve finále pro Vás nepotřebné a neupotřebitelné zboží. Tyto nabídky se vyznačují velmi často tím, že Vám slibují něco zdarma za něco, když uděláte. Dále pak tím, že na rozhodnutí máte jen omezený čas a tím Vás nutí se rychle rozhodnout a moc o celé věci nepřemýšlet a hlavně nemoci se s někým poradit. Buďte vždy ve střehu a tyto nabídky raději odmítejte. Získejte dostatek času si to promyslet a zvážit. Na tom není nic špatného, že každý nákup je důležité si promyslet.

ZVEDAT ČI NEZVEDAT NEZNÁMÁ TELEFONNÍ ČÍSLA?

Stává se Vám, že Vám volají telefonní čísla, která neznáte, nebo nemáte uložená v adresáři? Je jen na Vás, zda tento hovor přijmete nebo ne. Zvažte možná rizika přijetí těchto volání. Mnohdy se můžete stát obětí už je díky tomu, že zvednete neznámé telefonní číslo a budete s volajícím diskutovat a sdělovat různé osobní údaje. Své nejbližší máte pravděpodobně uložené v paměti telefonu, a tak pokud volají, hned vidíte jejich jméno.

SOS tlačítko - mnohé z telefonních přístrojů dnes obsahují SOS tlačítko, které slouží k informování Vámi nadefinovaných kontaktů, že máte

nějaký problém. Lze si do tohoto seznamu uložit čísla svých známých, příbuzných a kamarádů, kteří Vám v případě problému mohou a můžou pomoci. Rozhodně doporučujeme se s funkcí toho tlačítka seznámit předem. Mobilní telefony, kde není toto tlačítko integrováno, ale podobnou funkci umí také. Jen je potřeba tuto funkci najít v menu a aktivovat si ji. Nejčastěji se jedná o potřebu stisknout kombinaci dvou tlačítek. Telefon umí vyslat předdefinovanou SMS zprávu, ale také informaci o Vaší poloze, kde se právě nacházíte, a to pomocí GPS lokátoru nebo třeba i Wi-Fi sítě, kde jste připojeni. Zároveň bývá také přenesena zvuková a obrazová informace, která se v okamžiku stisknutí tlačítka nahraje a odešle. Můžete tedy i sdělit to, co se právě děje, popřípadě udělat i fotografii místa, kde se momentálně nacházíte.

CO ZAPÍNAT A NEZAPÍNAT V TELEFONU, V POČÍTAČI (GPS, ODESÍLÁNÍ ZPĚTNÝCH VAZEB)

Při používání mobilního telefonu, počítače, tabletu nebo smartphonu je vhodné jej správě nastavit, než jej začnete používat. Pokud si nejste jistí správným nastavením, požádejte své známé, kamarády, či příbuzné o pomoc. Správné nastavení na začátku Vám může ušetřit mnoho nepříjemných chvilek.

CO SI INSTALOVAT?
JAK OVĚŘIT NEZÁVADNOST?

Do elektronických zařízení si můžete nainstalovat mnoho užitečných programů, které Vám často mohou pomoci. Přesto je na místě vědět několik důležitých informací. Je vhodné vědět, za jakým účelem chcete daný program nebo aplikaci využívat, a zda to tento program či aplikace skutečně umí. Měli byste se zajímat i o licenční podmínky dané aplikace. Mnoho aplikací je dnes bezplatných. To je určitě obrovská výhoda, ale je třeba zmínit, že většina těchto aplikací Vás pak obtěžuje reklamou, které se Vám objevují na displeji. Některé aplikace mohou být bohužel i podvodné a mohou obsahovat funkci, která bez Vašeho vědomí odesílá důležité informace. Proto doporučujeme, než si nějakou aplikaci instalujete, pokusit se o ní zjistit veškeré dostupné informace. Nejlepší je doporučení od známých, kteří třeba danou aplikaci již používají. Dále jsou to různé recenze, kde mnoho uživatelů píše své osobní zkušenosti s danou aplikací a Vy pak máte možnost posoudit její vhodnost nebo nevhodnost pro Vaši potřebu. V neposlední řadě je nutné mít na každém IT zařízení nainstalovaný antivirový program, který je schopen Vás z velké části dobře ochránit před instalací a využíváním podezřelé nebo závadné aplikace.

Antivirová kontrola - každé IT zařízení a zejména to, které je připojeno k internetové síti, je nutné si chránit alespoň antivirovým programem. Řada těchto programů je k dispozici ve free verzi, to znamená, že jsou to bezplatné programy, které Vám zaručí alespoň tu základní ochranu. Máte na výběr z velkého počtu výrobců těchto programů a není jednoduché doporučit, který je ten nejlepší. Opět platí pravidlo přečíst si recenze na daný produkt, a pak se rozhodnout. Nebo si nechat doporučit od zkuše-

nějšího uživatele. Rozhodně se ale vyplatí mít nainstalovaný antivirový program.

ELEKTRONICKÉ BANKOVNICTVÍ, HESLA – VÝZNAM, TVORBA A UCHOVÁNÍ V TAJNOSTI, PLATEBNÍ KARTY (PIN)

Mnozí uživatelé dnes využívají výpočetní techniku a i mobilní telefony k elektronickému bankovnictví. V Česku je elektronické bankovnictví dobře chráněno a je relativně bezpečné ho používat, pokud i Vy jako uživatel dodržujete všechny zásady bezpečného ovládání. K těm patří např. používání antivirového programu na svém zařízení. K ovládání elektronického bankovnictví doporučujeme používat jiné zařízení než to, na které Vám je zasílána autorizace případné transakce, většinou se jedná o SMS. Dále pak záleží na internetovém připojení. Nedoporučujeme se rozhodně připojovat na veřejných místech, jako jsou restaurace, kavárny apod. Zde hrozí riziko zneužití, které souvisí s bezdrátovým přenosem Wi-Fi. Další neméně důležitou zásadou je, že nikdy a za žádných okolností nikomu nesdělujte své heslo. To, že si držíte heslo v tajnosti, by mělo být naprostou samozřejmostí. Je to něco jako klíč od domu. Kdybyste ho někomu jen tak půjčili, nemohli byste se pak divit, že byste mohli najít vykradený dům. Samotné heslo by také mělo být silné. To v dnešním světě znamená, že by mělo obsahovat kombinaci více znaků a mělo by mít nějakou minimální délku. Doporučujeme nepoužívat heslo slovníkového typu nebo vlastních jmen (např. koloběžka, Lenka, 12345 apod.). Heslo by mělo mít alespoň 8 znaků a mělo by obsahovat velká a malá písmena, číslice a nestandardní znak (tečku, čárku, paragraf...).

Také používání platebních karet k placení na internetu má svá pravidla a člověk by je měl znát a dodržovat. Nikdy byste neměli platební kartu dávat z ruky. Hrozí zde možnost zneužití karty na internetu při placení, protože u nezabezpečené platební karty je potřeba znát pouze její číslo, platnost a z druhé strany karty CVV/CVC kód (3 číslice). Pokud již platební kartu používáte, měli byste si v elektronickém bankovnictví nebo na pobočce ověřit, zda je funkce plateb na internetu povolena nebo zakázána a případně si nastavit nějaké finanční limity. Zároveň je důležité nastavit si vyšší stupeň zabezpečení při placení kartou, a to třeba pomocí zaslání kontrolní SMS zprávy. Pokud vše nastavíte správně a budete se chovat obezřetně, lze říci, že i placení platební kartou na internetu je relativně bezpečné.

Nedostali jste zboží, co teď? Nebo máte jiný problém s nakoupeným zbožím? Můžete se obrátit např. na Evropské spotřebitelské centrum při ČOI, Štěpánská 15, 120 00 Praha 2.

ZNEUŽITÍ SENIORA V KYBERPROSTORU

Je třeba si uvědomit, že kyberprostor je odrazem našeho současného světa. To, co se

děje zde mezi námi, děje se také ve virtuálním světě na internetu. Tak jako jsou v okolí Vašeho bydliště lidé hodní a zlí, přesně takoví lidé jsou i na internetu. Každý z Vás se musí chovat obezřetně, předvídat a počítat s tím, že ne každý má dobré úmysly. Je dobré s tímto vším počítat a nebýt přehnaně důvěřivý. Velice často se stává, že někteří lidé s nekalými úmysly záměrně vyhledávají seniory, protože věří, že je lépe dokážou přesvědčit svými „fintami" tak, aby se k nim dostali co nejvíce blízko, případně se vloudili až do jejich bytu. Všichni jistě už znáte triky těchto pochybných individuí, před kterými jste pravidelně varováni Policií ČR i svými blízkými. Jsou to např. otřepané fráze typu: „Já jsem zaměstnanec energetické společnosti." Nebo: „Prosím, prosím, potřebuji navštívit WC." Či: „Jsem starý známý, Vy si na mě nepamatujete? Pracovali jsme spolu, kamarádil jsem s Vaším synem." Nebo se vydávají za příbuzného, synovce tetičky z pátého kolene apod. Také brousí nože, prodávají deky, přístroje, nádobí apod. To všichni znáte a dáváte si jistě pozor.

Může se Vám něco podobného stát na internetu? Odpověď je jednoznačná. Může. Nebude to vypadat úplně takto, ale scénář je hodně podobný. Základem je vloudit se do přízně seniora, zjistit co nejvíce informací, a pak s těmi informacemi nakládat. I na internetu se musíte chránit před okradením, snažit se vyhýbat podvodům a podvodným nabídkám a chránit sebe i svůj majetek. Nemusíte se hned bát a raději se s nikým nebavit či nenakupovat, je jen třeba dodržovat pár základních pravidel a umět si ověřit, s kým komunikujete a vybrat si správné a ověřené servery ke svým nákupům. Důležité i zde je hlavně vědět a znát.

JAK SI OVĚŘIT IDENTITU DRUHÉHO ČLOVĚKA V KYBERPROSTORU?

V kyberprostoru - v počítačovém světě je vždy nutností vědět, s kým opravdu komunikujete. Ne to, za koho se ten „druhý“ vydává. Na internetu, ale i v telefonu se můžete vydávat, za koho chcete, můžete si o sobě uvádět záměrně nepravdivé nebo zkreslující informace. Proto ověření si identity, ověření si informací o daném člověku v počítačovém světě, je hodně důležité. Nikdy nemůžete předem vědět, co ten „druhý“ má skutečně v plánu, a kdo to vlastně je. Za relativně jednoduché, a přesto v dnešní době velmi účinné, považujeme ověřit si identitu dané osoby např. video komunikací pomocí webové kamery a mikrofonu. To má dnes každý notebook, každý smartphone. Při tomto hovoru máte možnost vidět toho, kdo s Vámi komunikuje, slyšet ho, ale také máte příležitost si vhodnou formou ověřit údaje, které o sobě uvádí. To, že komunikujete s daným člověkem, kterého právě teď vidíte a slyšíte, lze například tím, že jej požádáte, aby si v tento okamžik vzal papír a na něj napsal např. dnešní datum a Vaše jméno a tento papír Vám ukázal do kamery. Pokud by se daná osoba začala vymlouvat, že to není možné nebo že nemá kameru nebo funkční mikrofon, prosím, zbystřete. S velkou pravděpodobností se může jednat o nějakého podvodníka, který se vydává za někoho jiného, než ve skutečnosti je. Doporučujeme ihned komunikaci ukončit.

JAK NAKUPOVAT NA E-SHOPU? JAK SI OVĚŘIT DŮVĚRYHODNOST?

V dnešní době je moderní, rychlejší a často i levnější nakupovat zboží na internetu. Ale ani tato činnost se nemusí obejít bez problémů a

rizik. Je dobré dát si pozor na několik věcí. Pokud jste již nalezli na internetu dané zboží, není vždy nejlepší kupovat jej v obchodě, kde je nejlevnější. Nejlevnější nákup s sebou může přinášet rizika. Také placení zakoupeného zboží předem může být rizikové. A to hlavně v případě, že s daným internetovým obchodem nemáte osobní zkušenost. Nebo alespoň někdo z mých známých. Může se stát, že si vyberete a zaplatíte zboží, a to Vám pak nedorazí. Někdy se také stává, hlavně u neznámých obchodníků, že objednané zboží pošlou na dobírku, ale v balení se pak nenachází objednaná věc, ale jiná nebo třeba i kus cihly. I zde platí přísloví: „Nejsem tak bohatý, abych si kupoval nejlevnější věci." Než nakoupíte u daného obchodníka, doporučujeme si zjistit o daném internetovém obchodě co nejvíce informací. A to od známých, příbuzných nebo na internetových stránkách. Dobrým vodítkem Vám může být certifikace daného obchodu. Podívejte se např. na www.apek.cz. Dalšími znaky dobrého obchodu by měly být dostupné veškeré údaje o obchodníkovi (název firmy nebo obchodníka, IČ, adresa, telefonní a jiné kontakty…). Dále pak reklamační řád, kompletní a přehledný ceník dopravy. Také pokud obchod používá reálné, vlastní fotografie prodávaného zboží, lze toto považovat za klad. Měli byste také vědět, že pokud nakoupíte zboží přes internet, máte nárok na odstoupení od kupní smlouvy, a to 14 dní. Potřeba je toto odstoupení učinit písemně, např. e-mailem. Za lepší variantu považujeme doporučený dopis nebo dodejku. Následně nepoužité zboží, ideálně v neporušeném obalu (platí např. pro CD a DVD) zaslat zpět prodejci. Ten Vám musí do 30 dní vrátit finanční plnění.

JAK SE CHRÁNIT PŘED OKRADENÍM

Pokud komunikujete s ostatními lidmi, které neznáte, například se s nimi seznámíte na sociálních sítích, nevyprávějte jim hned, co vše doma máte. Někdy podvodníci chtějí zjistit, zda jste majitelem nějakých cenností či starožitností tím, že nadhodí udičku a sami se začnou chlubit a vyprávět, co vše mají oni. Nikdy nevyprávějte o tom, jak jste doma sami, nebo že někam odjíždíte a byt necháváte celé léto zamčený a prázdný. Vyvolejte zdání, že Vás stále někdo navštěvuje. Také dejte pozor na webovou kameru, která často může prozradit, co vše je v bytě nebo domě za vybavení tak, že ji pustíte a ostatním ukážete celý svůj byt. Někdy můžete být vyzváni, ať otočíte tabletem či notebookem, popojdete o kus dál, protože Vám sluníčko dopadá do obličeje a ten, kdo si s Vámi povídá, na Vás špatně vidí. Pokud spouštíte webovou kameru, je dobré, když sedíte u zdi a za Vámi je z pokoje vidět pouze holá zeď.

Často jste ostatními uživateli internetu vyzýváni k tomu, abyste fotili vše, co děláte. Někteří si fotí jídlo, vyvěsí, co jedli a komentují. Někteří popisují, jak si koupili novou televizi, jak byli venku, jak se koupali, prostě cokoli. Někteří lidé žijí více ve virtuálním světě a popisují vše ostatním a s ostatními to sdílejí. Nenechte se strhnout, vždy přemýšlejte, co ukazujete, a co si chcete opravdu zachovat jako vlastní soukromí. Tím také často předcházíte i riziku přepadení.

CÍLENÉ TECHNIKY MANIPULACE

Věřte, že podvodníci často využívají různé záminky a lsti, na které může naletět kdokoli, nejen senior. Někdy si s Vámi píší a komunikují opravdu dlouho a už od počátku je jejich záměr

rem vylákat z Vás informace či peníze působením na Vaše emoce a city. Těmto jedincům se říká kyberpredátoři, jejich působení je opravdu promyšlené do posledního detailu, proto se mu říká sociální inženýrství. Neberte to tak, že Vy jste ten, kdo naletěl, spoustu lidí si to pak vyčítá, ale nejedná se jen o seniory. Případů je spousty i mezi ostatními lidmi. Někteří to ani nenahlásí, protože se stydí, že naletěli.

Velice krátké příklady:

Právnička, velice schopná a znalá žena, ve své profesi úspěšná a značně vytížená. Neměla čas se někde s někým seznamovat, přesto nechtěla být sama a na sociální síti se seznámila s úžasným okouzlujícím mužem. Každý den si spolu psali, posílal jí své fotografie, byl to opravdu fešák s krásným autem. Také právník, mluvil česky, ale žil v Americe. Zamilovala se do něj. Toužila se s ním setkat, on s ní také. Snažil se pro to udělat vše, ale měl spoustu práce. Velice rád by přiletěl, ale špatně investoval a teď nemá na letenku, protože zbylé peníze má na termínovaném vkladu. Poslala mu tolik peněz, kolik chtěl, hlavně aby ho už viděla. Co na tom, že to bylo mnohem víc, než stojí letenka. Potřeboval další peníze, důvodů bylo spousta. Až když byl její účet o 160 tisíc lehčí, došlo jí, že asi nikdy nepřiletí. Říkáte hloupé? Ano, ale milovala ho, věřila mu, chtěla ho potkat a nechtěla být už sama…

Senior, 72 let, již několik let ovdovělý, uznávaný lékař. Děti jsou už dávno dospělé, úspěšné, syn žije v Kanadě, dcera se provdala do Německa. Vídá je občas. Také je mu smutno. Má úplně vše, ale nikoho, s kým by trávil svůj čas. Tohoto pána, který není žádný nemohoucí, si našla na internetu kyberpredátorka, 29 let. Její manipulace byla na velice vysoké úrovni, rok zvládala předvádět neuvěřitelné schopnosti. Nejprve pouze po internetové síti, později se se-

niorem setkala. Nakonec se scházeli v jeho bytě, potvrdila si, že se nespletla, byl opravdu majetný. Ona byla okouzlující, bude se o něj starat do konce života, bezmezně ho miluje. Omládl, nabral spoustu nové síly a energie, byl šťastný. Přepsal na ni těsně před svatbou všechen svůj majetek. Svatba se nekonala, žena zmizela.

Zranitelný je každý, ale nejvíce ten, kdo není poučen a není připraven na to, že v kyberprostoru se může setkat s kyberpredátorem a není opatrný. Pokud opatrní jste, můžete si na internetu najít i opravdové přátele a nemusíte se cítit ohrožení. Spoustu mladých, ale dnes i starších lidí si na internetu našli partnera pro život a jsou s ním šťastni.

JAK TAKOVÁ MANIPULACE VYPADÁ:

1. Profilování - v této fázi si Vás útočník hledá, zkouší, získává dostupné informace. Hlavně z Vašich profilů na sociálních sítích, z toho, co o Vás na internetu je. Někdy byste se divili. Pokud jste byli za svého profesního života v organizaci, která se prezentovala na internetu, a to je dnes téměř každá, zjistí si o Vás útočník, co jste dělali, jak jste byli úspěšní, čím jste se zabývali apod. Pokud k tomu přidáte pár informací na svém profilu, má dokonalý obrázek o Vaší sobě. Je dobré dát si občas do některého běžného vyhledávače své jméno a zjistit, co vše o Vás na internetu je.

2. Navázání kontaktu, falešná identita - útočník Vás osloví a začne si s Vámi povídat, často se vydává již v této fázi za někoho jiného a neříká o sobě pravdu.

3. Vzbuzování důvěry, zrcadlení, prohlubování vztahu využívá již informací, které o Vás na internetu získal, pro Vás je až překvapivé, jak je

skvělý, má podobné zájmy, často úplně stejné jako Vy (technika zrcadlení), prohlubuje vztah s Vámi.

4. Vábení nebo vydírání - slibuje, jak Vám bude pomáhat, kdykoli to budete potřebovat, bude pořád s Vámi, bude Vám nablízku, nebo Vás miluje. Chce být s Vámi, vezme Vás někam, kam jste už dávno chtěli. Splní Vám vše, co si přejete, nalezne toho, koho hledáte. Nebo ve Vás vyvolává pocity, že jen Vy mu dokážete pomoci, že potřebuje zachránit, Vy budete užitečný, ochranitelský, záchranář apod. Tím vyláká peníze či další věci, dokonce i nemovitost. Nebo nastupuje tvrdší kalibr, pokud na Vás z Vaší předešlé komunikace získal nějaké diskriminující informace a osobní údaje, a začíná vydírání. I v této fázi využívá techniky cílené manipulace. Pozor na to, že ochota svěřit se neznámému člověku na internetu je díky zdánlivé anonymitě podstatně vyšší, než je tomu v reálném životě. Na internetu totiž neneseme bezprostřední důsledky, které může naše sdělení vyvolat (v reálném světě důsledky svého chování neseme). Útočník ochotu oběti svěřit se s důvěrnými informace využívá vždy ve svůj prospěch.

5. Izolace oběti - v této fázi útočník začne oběť izolovat od okolí. Když to senior bude někomu vyprávět, je vysoká pravděpodobnost, že někdo z okolí tuto hru či manipulaci prohlédne, protože už bude informován. To se útočníkovi nemůže hodit. Proto začne opět cílenou manipulací vymýšlet všechny možné důvody, aby se senior nikomu nesvěřoval s tím, co spolu sdílejí, že je určitě někdo bude chtít rozdělit a důvodů najde tisíce.

6. Osobní schůzka - pokud má kyberpedátor pocit, že oběť dostatečně zmanipuloval a že už necouvne, pokusí se o osobní schůzku. Většinou již má tento jedinec dostatek informací a citli-

vých materiálů, které může využívat. I na schůzce může být okouzlující. To je přece záměr. Vše může být velice rychlé.

Pozor!!! Závažná rozhodnutí o vašem majetku konzultujte s právníkem, nechte si poradit od dalších věrohodných osob. Většina institucí a nevládních organizací, která poskytuje pomoc seniorům, nabízí i bezplatnou právní poradnu.

KYBERŠIKANA

I senioři mohou a často i zažívají kyberšikanu, přestože se o ní ve společnosti mluví převážně v souvislosti s dětmi.

Už ze samotného názvu kyberšikana je celkem jasné, že se jedná o nějaký jiný druh šikany. Na rozdíl od klasické šikany, která probíhá tváří v tvář - útočník versus oběť, je kyberšikana trochu odlišná a agresorům jsou k dispozici nejen jiné nástroje ubližování, ale i zvláštnosti virtuálního prostředí. Na toto často senior není připraven, a o to více to pro něj může být šokující.

CO SI POD TÍM MÁTE PŘEDSTAVIT? CO DO KYBERŠIKANY PATŘÍ?

- Zasílání výhrůžných a krutých e-mailů a SMS zpráv, výhrůžné telefonáty nebo obtěžování přes různé sociální sítě. Někdo má Vaši e-mailovou adresu, Vaše číslo telefonu a tímto se jen baví. Je spokojený, že ve Vás vyvolává strach a napětí.

- Další způsob kyberšikany, poškození Vašeho jména, zničení vašich kontaktů a přátel jsou situace, kdy agresoři získají hesla a identifikační údaje k Vašim virtuálním účtům - chatu, sociální síti, e-mailu a pod Vaším jménem zasílají ostat-

ním vulgární, obtěžující zprávy, fotografie, videa.

- Kyberšikanou je i provokování a napadání uživatelů v on-line komunikaci (především v rámci veřejných chatů a diskuzí).

- Kyberšikanou je i zveřejňování cizích tajemství s cílem poškodit oběť (např. v rámci sociálních sítí, blogů nebo jiných webových stránek, pomocí SMS zpráv apod.). Cíl je jasný. Poškodit Vás, znemožnit, pomlouvat.

- Kyberšikana je i vyloučení z virtuální komunity (např. ze skupiny přátel v rámci sociální sítě).

- Do kyberšikany patří i obtěžování (např. opakovaným prozváněním, voláním nebo psaním zpráv).

Méně časté projevy kybešikany v souvislosti se seniory, využívané spíše k vydírání oběti, v souvislosti s tím, co si pomyslí ostatní apod.:

- Fotografování, nahrávání oběti, kdy jsou pořízené záběry upravovány a je vyhrožováno zasíláním vlastním dětem, příbuzným apod. Někdy se jedná už přímo o vyvěšení upravených obrázků, fotografií a video nahrávek on-line, kde je oběť často zesměšňována a znemožňována.

- Vyvěšení pornografických fotografií s tváří oběti na internetu, různé fotomontáže.

- Vytváření webových stránek, které různými způsoby (verbálně, graficky, zvukově…) oběť šikany uráží a zesměšňují.

JAK SE CHRÁNIT:

- Chovejte se k ostatním slušně, s úctou, nevyvolávejte konflikty.

- Nedůvěřujte hned každému. Výzkumy ukazují, že většina lidí ve virtuální komunikaci lže.

- Nikomu nesdělujte citlivé informace, které by mohly být zneužity (osobní údaje, osobní fotografie, své problémy, hesla k elektronickým účtům atd.).

- Seznamujte se s pravidly používání služeb internetu a GSM sítí, i když jsou dlouhá a nechtějí se nám číst.

VE CHVÍLI, KDY KE KYBERŠIKANĚ JIŽ DOCHÁZÍ:

- UKONČIT - nekomunikovat s tím, kdo Vás napadá či na Vás útočí, nemstít se.

- BLOKOVAT - zamezit šikanujícímu přístup k Vašemu profilu i k dané službě (kontaktovat poskytovatele služby, zablokovat si přijímání útočníkových zpráv nebo hovorů v telefonu, nastavit si blacklist, v případě nutnosti i změnit svou virtuální identitu).

- OZNÁMIT – nebát se a oznámit útok Policii ČR, případně na webu Policie ČR viz dále, schovat si důkazy pro vyšetřování (např. zprávy, videozáznamy, odkazy na weby, blogy).

- NEBÝT NEVŠÍMAVÝ - pokud se něco podobného děje jinému seniorovi, povědět mu o tom, co to je.[2]

Co dělat, když máte pocit, že jste se stali terčem nějakého podvodu či jiného nežádoucího chování v prostředí internetu? Mluvit o tom s někým, radit se, ohlásit to…

- Pokud narazíte na něco, co Vám není příjemné nebo Vás vyděsí, opusťte webovou stránku a s někým o tom mluvte, případně můžete nahlásit na stránkách Policie ČR kliknutím na ikonu vpravo - HLÁŠENÍ KYBERKRIMINALITY.

- Pokud Vás někdo pronásleduje pomocí virtuálních technologií, páchá tzv. kyberstalking.

[2] Upraveno z přehledový list, Registrační číslo CZ.1.07/1.3.13/02.0040. www.e-nebezpeci.cz

Opakovaně Vás obtěžuje, snaží se Vás opakovaně dlouhodobě kontaktovat (pomocí dopisů, e-mailů, telefonátů, SMS zpráv, zasíláním vzkazů na ICQ, Skype, v chatu, zasíláním různých zásilek s dárky apod.), mluvte o tom s někým blízkým, nenechávejte si to pro sebe, navštivte Policii ČR, poraďte se s odborníky.

Můžete to také nahlásit na stránkách Policie ČR kliknutím na ikonu vpravo - HLÁŠENÍ KYBERKRIMINALITY.

- Pokud Vás někdo podvedl a Vy jste následkem jeho podvodného jednání přišel o peníze, majetek či jinou újmu, mluvte o tom s někým blízkým, nenechávejte si to pro sebe. Navštivte Policii ČR, poraďte se s odborníky nebo to můžete nahlásit na stránkách Policie ČR kliknutím na ikonu vpravo - HLÁŠENÍ KYBERKRIMINALITY.

Důležité je nenechat volný prostor pro pachatele, zastavit jeho jednání tím, že to oznámíte a ochráníte tak možné další oběti. A také pomáhá nebýt na to sám.

NETIKETA

Pojem netiketa vznikl ze dvou slov: net jako internet a etiketa. Všichni víme, co etiketa je, je to jakýsi soubor nepsaných zásad slušného chování. Netiketa je tedy soubor pravidel slušného chování na internetu. Je jedno, zda se připoju-

jete přes počítač, tablet či notebook nebo chytrý telefon. Přemýšlejte o tom, jak byste se chovali v běžném normálním životě, v běžné komunikaci, a podle toho se zkuste chovat tak i na internetu. Dětem se často říká jednoduchá poučka: „Nepiš a neříkej to, co bys neřekl své babičce." Podobně k tomu zkuste přistoupit i Vy, jen si uvědomte pár jednoduchých pravidel v souvislosti s počítači:

1. Nezapomínejte, že i když v ruce držíte tablet, telefon, či jste na počítači a nikdo s Vámi v místnosti není, tak že na druhém konci Vaší komunikace je opět člověk. To, co mu píšete, byste mu možná nikdy neřekli do očí. Představte si, že sedí vedle Vás. S tím souvisí i to, co se v internetové komunikaci nazývá flaming - v překladu hoření. Jde o nepřátelské chování některých lidí, které se odehrává ve virtuálním světě. Nejčastěji v diskuzních fórech, chatu, sociálních sítích, ale i v e-mailu. Útočník urážlivým způsobem napadá oběť tím, že do kyberprostoru umisťuje vzkazy, ve kterých ji hrubým způsobem uráží a zesměšňuje. Své chování útočník postupně stupňuje. Častým motivem je, že útočník nesouhlasí s názory oběti a tu pak uráží a argumentuje svými přesvědčeními. *Výzkumy ukazují, že „flaming"* jako agresivní chování ve formě slovního napadání *je v prostředí virtuální reality až čtyřikrát častější než v reálném životě.*[3] Nejjednodušší je v těchto případech vůbec nereagovat, nesnažit se tomu člověku cokoli vysvětlovat ani ho přesvědčit, že je to jinak. Nejlepší je nenechat se vyprovokovat k žádné další odpovědi ani další komunikaci. Ukončit komunikaci, a to co nejrychleji. V krajním případě je možné změnit virtuální identitu (založit si jiný účet nebo profil). Někdy flaming přeroste v tzv. flame war (česky doslova plamenná válka, též svatá válka, příliš ohnivá diskuse apod., někdy jen flame - pla-

[3] ŠMAHEL, David. Psychologie a internet: děti dospělými, dospělí dětmi. Praha: Triton, 2003, 158 s. Psychologická setkávání, s.13

men), což je používané označení pro plamenné internetové diskuse, které naprosto překročí únosnou mez slušného chování. Z diskuse se stává hádka, při které se účastníci navzájem urážejí a často končí osobním napadáním a už dávno není o obsahové stránce dané komunikace. Často se jedná o emotivní kontext naprosto vyhrocené komunikace, z které člověku není dobře. Může s sebou nést psychické, ale i fyzické následky, které mohou být pro seniora značně destruktivní. Proto přemýšlejte a snažte se takovou komunikaci ukončovat, případně než pošlete jakoukoli emotivní odpověď, vyčkejte raději do druhého dne. Teď se odpojte, vyspěte se, ráno moudřejší večera a pokračovat můžete druhý den. Emoce již budou zklidněné.

2. Z předchozího bodu vychází to, co je již napsáno výše, ale považujeme to za důležité zopakovat. Snažte se dodržovat obvyklá pravidla slušnosti respektovaná v normálním životě. Co považujete za nevhodné v každodenním životě, je naprosto samozřejmě nevhodné i ve virtuálním světě a virtuální komunikaci na internetu.

3. Protože můžete komunikovat v cizích jazycích a v podstatě po celém světě, je dobré uvědomit si, s kým mluvíte. V různých zemích světa může platit i jiná morálka. Velký pozor byste si v současném světě měli dát na politická a náboženská témata a jim podobné problémy. Nejenže některé názory mohou být trestné, mohou být ale i značně provokační a mohou vést k tomu, že si Vás účastník diskuse bude chtít vyhledat. Proto byste se těmto tématům měli vyhýbat, či by měly být diskutovány s maximálním taktem a v mezích slušnosti.

4. Pozor na to, že člověk, se kterým hovoříte, nemusí mluvit cizím jazykem, přesto si nemusíte rozumět, protože mezi Vámi chybí neverbální komunikace (gesta, mimika apod.). Ten člověk

na druhém konci může být jinak osobnostně nastaven, může mít jiný smysl pro humor, může jinak chápat. Pozor na ironii a na sarkasmy.

5. Když píšete delší texty, používejte malá i velká písmena, diakritiku. Pokud píšete pouze velká písmena, může to vypadat, jako když křičíte. Zároveň díky tomu, že v psaném textu chybí neverbální projevy emocí, začaly se používat k jejich vyjadřování tzv. emotikony nebo jinak smajlíci. Není třeba s nimi plýtvat, ale můžeme je do komunikace vkládat.

6. Zde uvádíme základní přehled nejčastěji používaných, ale je jich mnohem více:

VYJADŘOVÁNÍ EMOCÍ – EMOTIKONY:

:) ☺ :-)	základní - nejčastěji používaní smajlíci, které použijete v případě vtipného komentáře
;) ;-)	úsměv s mrknutím
:(☹ :-(	jsem smutný nebo se mi nelíbí něco, co někdo řekl
:>	sarkastická poznámka
@=	bomba!!!
:o() ;o* :-*	líbající smajlík, pusinka
:D :-D	velký smích
d:)	pohoda
:P	vyplazený jazyk
I-o	zívající smajlík
:-V	křičící smajlík
:-7	úšklebek
8-(	smutně koukám
=o)	dobrá nálada
3-)	trojitý úsměv
:-[	stydím se

7. Berte ohled na druhé. Ten člověk třeba už nechce odpovídat, je noc a spí nebo nemá tak rychlé připojení, může se zabývat zrovna jinou činností a teď hned se nemůže věnovat Vám. Takže pokud napíšete SMS, neprozvánějte apod.

8. Neposílejte žádné zbytečně velké e-mailové zprávy ani je nepřeposílejte dále. Když chci někomu poslat obrázek nebo fotku, zmenším ji, dnes to již e-maily umožňují samy. Různé servery a sociální sítě umožňují využít například funkci náhledu obrázku. V této souvislosti přemýšlejte i o tom, zda opravdu vše musíte přeposlat. Nepřeposílejte dále hoaxy, kdy Vás odesílatel nutí k přeposlání všem známým apod. Získávají se tím jen tzv. „živé aktuální“ adresy uživatelů internetu. Hoax znamená v překladu poplašná zpráva, kanadský žertík, vtípek. Ve své podstatě jde o šíření e-mailových zpráv pomocí internetové sítě, které jsou nepravdivé, poplašné anebo třeba jen řetězové. Ty nejen že člověka obtěžují, ale mohou v něm vyvolat i pocity strachu, viny nebo příjemce jinak mystifikovat. Nejčastěji se můžete setkat se zprávami, které Vás „varují“ před nebezpečím například počítačového viru nebo jiné situace, která Vás může poškodit. Častým hoaxem je také zpráva, která Vás žádá o pomoc při řešení např. zdravotního problému jiného člověka s tím, že máte tento e-mail přeposlat co největšímu počtu svých známých a zdravotně postiženému budou za tuto činnost zaslány poskytovatelem internetu nějaké finanční prostředky. Také řetězové dopisy „štěstí“ jsou častým hoaxem a jejich přeposílání může být nebezpečné. Hoax Vás především obtěžuje. Zatěžuje Vaše internetové připojení a celou internetovou síť. Uvede Vás v omyl a Vy se pak řídíte nepravdivou informací. Tímto pak můžete neúmyslně poškodit i jiné

osoby. Můžete být pomocí poplašné zprávy vyzváni k navštívení webových stránek se závadným kódem (virem) a můžete si tak infikovat počítač. Značná část lidí také tento e-mail-hoax skutečně přepošle svým známým a tím vlastně může šířit poplašnou zprávu a s největší pravděpodobností i osobní údaje (e-mailové adresy) jiných uživatelů, které nesmazal nebo je nedal do skryté kopie. Tyto adresy jsou pak nejčastěji používány k zasílání spamu, který opět Vás a ostatní obtěžuje. Odesláním hoaxu snižujete také vlastní důvěryhodnost. (Více informací naleznete např. na www.hoax.cz.)

9. Nerozesílejte žádné spamy ani reklamy, ani podivné nabídky čehokoli, již tak jsou jimi schránky zahlceny a Vaši známí a přátelé je určitě nechtějí. Kdyby se o dané věci něco chtěli dozvědět, budou si to jistě sami hledat na internetu.

10. Nešiřte internetem to, co není Vaše, týká se to i fotografií, obrázků, písniček, filmů a čehokoli jiného, k čemu Vy sami nemáte autorská práva. Na porušování autorských práv si musíme dávat pozor úplně všude, ale na internetu nám často toto uniká.

11. Chraňte své soukromí, ale respektujte i soukromí ostatních uživatelů. Může se Vám stát, že Vám přišla SMS zpráva, e-mail či jiné sdělení, které vyhodnotíte tak, že Vám určitě nepatří. V tomto případě je správné tuto informaci smazat a taktně upozornit toho, kdo zprávu napsal, že došla někomu jinému. Třeba na tu zprávu někdo zoufale čeká a nikdy by se k němu nedostala. Známe všichni Pošťáckou pohádku ☺.

Určitě bychom našli společně spoustu dalších pravidel netikety a na internetu jich také hodně najdete, pokud zapátráte. Pokusili jsme se

shrnout jen základní nástřel, abyste si všichni dokázali představit, co to taková netiketa může být.

ZÁKLADNÍ PRAVIDLA BEZPEČNÉHO POUŽÍVÁNÍ A CHOVÁNÍ SE NA INTERNETU:

Na toto téma existuje již mnoho „desater". Můžete si na internetu najít i jiná a zkusit si je porovnat či přidat další informace:

- Vždy používejte IT techniku k předem stanovenému cíli.
- Chovejte se tak, abyste svými činy neubližovali jinému a zároveň se sami chraňte před možným nebezpečím.
- Používejte techniku, které rozumíte a nesnažte se zbytečně jen „zkoušet", zda se něco podaří.
- Instalujte jen předem ověřené a známé programy. Neotevírejte soubory, které neznáte nebo které přišly v nevyžádané e-mailové poště.
- Používejte kvalitně zabezpečený počítač, notebook, telefon.
- Pamatujte, že silné heslo by mělo obsahovat velké písmeno, malé písmeno, číslici a nestandardní znak. Délka by měla být alespoň 8 znaků.

Heslo slovníkového typu např. sluníčko je snadno rozluštitelné – hackeři si s ním poradí v horizontu několik minut.

- Nezapomínejte na veškeré aktualizace operačního systému, který používáte.

- Mějte nainstalované vhodné programy, které chrání Vaše bezpečí a Vaše zařízení před útočníkem.

- Nedůvěřujte všem informacím, které na internetu naleznete – nejsou vždy pravdivé.

- Nešiřte informace, které nejsou pravdivé a jejichž pravdivost nemáte dostatečně ověřenou.

- Udržujte svá hesla v naprosté tajnosti a nikdy je nikomu nesdělujte.

- Komunikujte ve virtuálním světě jen s tím, s kým chcete Vy sám.

- Nebojte se nevhodnou komunikaci ukončit a říci jasné NE.

- Za žádných okolností nikomu nesdělujte své osobní údaje (jméno, příjmení, bydliště, datum narození, rodné číslo, telefonní číslo, heslo, PIN, apod.).

- Uvědomte si, že informace, které máte o sobě vyplněné v profilech na sociálních sítích, jsou de facto přístupné všem. Útočník je vždy o krok napřed před postupným zabezpečováním.

- Nenechte se oklamat sliby virtuálních útočníků (mohou vám slibovat lásku, pokračování vztahu v reálném světě, peníze, dárky apod.). Uvědomte si, že lidé na internetu mohou lhát!

- Všímejte si nesrovnalostí v komunikaci s kyberútočníky (útočník například udává různý věk, mění informace, které Vám o sobě sdělil dříve apod.).

- Uvědomte si, proč by někdo chtěl za každou cenu udržet internetový vztah nebo obsah komunikace v tajnosti. Sdělení typu: „Neříkejte to

synovi, dceři, chtěli by nám vztah zničit.“ apod.).

- Ve virtuálním prostředí nikomu nesdělujte své osobní informace (zejména své fotografie a už vůbec ne intimní).

- Nikdy nechoďte na osobní schůzku, aniž by o ní věděli Vaši přátelé a měli jste s nimi domluvené „jištění“ (sedí u stolu vedle, zavolají Vám apod.). Uvědomte si, co všechno se Vám na schůzce může stát a jak může být schůzka riskantní. Nikoho si po první schůzce nevoďte domů a neukazujte mu, co doma máte.

- Dejte si pozor na to, s kým se bavíte a o čem. Internetová komunikace vypadá jako anonymní, ale není. Nechcete přece, aby Vás „internetový známý“ např. vystopoval v reálném světě nebo aby Vás nutil dělat něco, co dělat nechcete.

- Nikdy neodpovídejte na neslušné, hrubé nebo vulgární e-maily a vzkazy.

Pamatujte si, že opatrný surfař na internetu, je inteligentní surfař!

SLOVNÍČEK POJMŮ S VYSVĚTLENÍM A MOŽNÝMI RIZIKY:

Aplikace - počítačový program, který instalujete do počítače, notebooku, tabletu nebo chytrého telefonu. Řada aplikací je zdarma. Některé jsou placené a je vždy nutné si ověřit, zda nepoužíváte daný program/aplikaci v rozporu s licenčními podmínkami. Nebezpečí u aplikací je možnost nakažení Vašeho IT zařízení virem a následné zneužití informací získaných z Vašeho zařízení.

E-mail - elektronická pošta. Umožňuje přijímat a odesílat textové i jiné informace prostřednictvím internetové sítě. Výhody e-mailové komu-

nikace jsou v tom, že uživatel nemusí být aktuálně přihlášení v počítači nebo jiném zařízení a e-mail na Vás „počká“. Také tento způsob komunikace s touto časovou prodlevou počítá. Každý e-mail obsahuje adresáta (jeho e-mailovou adresu), předmět zprávy a pak vlastní tělo – obsah zprávy. K jednotlivým e-mailům lze přikládat přílohy (obrázky, videa, zvukové nebo i jiné soubory). Velikost zprávy bývá někdy omezena určitou velikostí, aby se internet nezatěžoval přenosem a ukládáním objemných dat. Zranitelnost opět vidíme v obsahu dané komunikace mezi jednotlivými uživateli.

Facebook - jedna z největších společenských sítí na internetu. Slouží ke komunikaci mezi jednotlivými uživateli. Můžete si psát, posílat obrázky a videa. Zároveň tyto soubory můžete sdílet s jinými uživateli nebo i skupinami uživatelů. V dnešní době je možné se pomocí facebookového profilu přihlašovat i k různým aplikacím a hrám. Riziko je v množství a citlivosti údajů, informací, fotek a videí, které tam uživatelé vkládají a ostatním je tímto zpřístupní.

GPS - Global Positioning Systém - česky globální polohovací systém. Tento systém slouží k určení geografické polohy na světě, a to s přesností na několik metrů. Využívá se v navigačních systémech dopravních prostředků, ale i třeba při použití SOS tlačítka na Vašem telefonu. Sledování polohy daného zařízení lze samozřejmě i zneužít. Pokud máte GPS zapnuté, může se stát, že Vás někdo pomocí tohoto lokátoru může za určitých okolností sledovat. Může pak vědět, zda jste nebo nejste doma, nebo kde se nacházíte.

Hoax - jde o nepravdivou informaci, která se šíří nejčastěji pomocí e-mailové komunikace. Do této kategorie spadají i řetězové e-maily, které Vás nabádají k tomu, abyste je poslali svým známým. V krajním případě může být šíření hoaxu kvalifikováno jako protiprávní jednání. Pro ověření podezřelého e-mailu navštivte www.hoax.cz.

ICQ - jedná se o program, který umožňuje komunikaci na internetu mezi jednotlivými uživateli. V dnešní době velmi podobné aplikaci Skype. Obliba ICQ pomalu klesá. Riziko přináší daný obsah komunikace. Opětovně upozorňujeme na obsah komunikace a skutečné ověření si dané osoby, se kterou komunikujete.

Kyberprostor - jde o virtuální svět na internetu. V tomto světě mohou uživatelé anonymně komunikovat, sdílet své fotografie, zprávy, videa a jiná data. Lze zde hrát hry, seznamovat se, diskutovat v různých diskuzních skupinách, nakupovat, obchodovat a využívat elektronické bankovnictví.

Kyberstalking - jde o takové jednání pachatele, při kterém Vás neustále obtěžuje a kontaktuje ve virtuálním světě. A to nejčastěji pomocí SMS, e-mailů, telefonu a i on-line komunikace v kyberprostoru. Pachatel od Vás chce získat informace nebo Vás chce donutit k osobní schůzce pomocí slibů, dárků a později vyhrožováním a vydíráním.

Kyberšikana - šikana, která se odehrává v kyberprostoru při využití výpočetní techniky. Jejími účastníky (agresorem nebo obětí) se může stát kterýkoli uživatel internetové sítě na celém

světě. Kyberšikana má různé podoby (viz dřívější text). Důsledky kyberšikany bývají velmi často tragické. Boj proti kyberšikaně je obtížný, neboť oběť se často nesvěří nebo to, co se jí děje, nepovažuje v prvotní fázi za problematické.

Skype - jedná se o program, který umožňuje internetové volání, komunikaci mezi jednotlivými počítači. Volání mezi zařízeními s programem Skype je zdarma a je hojně využíváno. Komunikace mezi volajícími může být i formou video hovorů. K tomu je potřeba pouze webkamera (dnešní notebooky a mobilní telefony ji již mají v základní výbavě). Komunikace přes Skype je nyní relativně bezpečná díky šifrovanému přenosu. Rizika spojená s využíváním jsou na naší straně. Jde hlavně o to, co a komu pomocí této komunikace sdělujeme. Skutečně víte s jistotou, kdo je druhý člověk, se kterým komunikujete?

Smartphone - chytrý mobilní telefon. Toto zařízení lze používat jako malý počítač. Má vlastní operační systém (Android, iOS, WindowsPhone, BlackBerry,…). Do tohoto zařízení je pak možné si instalovat různé programy/aplikace a ty následně využívat. V dnešní době je nevýhodou krátká doba použitelnosti vzhledem k malé kapacitě baterie a možnost zneužití tohoto zařízení např. pomocí virů. Zařízení pak bez Vašeho vědomí a souhlasu může odesílat důležité a soukromé informace třetí osobě, která je následně může zneužít.

YouTube - patří mezi největší prostor pro sdílení videosouborů. Uživatelé na tento webový server vkládají svá videa, a tím je zpřístupní ostatním uživatelům. Ti je pak mohou prohlížet,

komentovat a hodnotit. Rizika opět vidíme v obsahu daných videí a s tím spojených komentářů a hodnocení.

Webkamera - webová kamera. Jde o periferní zařízení připojené k počítači, pomocí kterého je zaznamenáván obraz a v dnešní době i zvuk. Ty je pak možné si buď jen uložit, nebo i v reálném čase (on-line) zpřístupňovat ostatním uživatelům internetu. Využívá se velmi často k video telefonování nebo i monitorování osob a prostor. Riziko webových kamer spočívá v tom, co za obraz a video snímají a komu ho zpřístupňují. Pozor na ztrátu soukromí.

WhatsApp - jedná se o komunikační program mezi uživateli chytrých mobilních telefonů. Umožňuje nejen komunikaci, video komunikaci, ale také sdílení souborů a informací obsažených v telefonu včetně veškerých telefonních a jiných kontaktů. Uživatelé mohou sdílet i svoji geografickou polohu pomocí GPS. Aplikace je vázána na telefonní číslo uživatele. Riziko opět vidíme v obsahu komunikace a sdílení polohy s ostatními uživateli.

Wi-Fi - bezdrátové připojení k internetu. Velmi rozšířené a oblíbené. Dnešní Wi-Fi připojení dosahuje poměrně velké přenosové rychlosti internetu a je tedy používáno nejen v domácnostech, ale i ve firemním prostředí. Jeho zranitelnost spočívá především v možném „odposlechu“ komunikace mezi Wi-Fi přípojným bodem a Vaším zařízením. A to hlavně v případě, pokud dané Wi-Fi připojení není šifrované a k jeho připojení se nepoužívá heslo. Také není zcela bezpečné se připojovat k Wi-Fi v obchodních centrech apod.

LITERATURA A ODKAZY K VYUŽITÍ:

ŠMAHEL, David.
Psychologie a internet:
děti dospělými, dospělí dětmi.
Praha: Triton, 2003, 158 s. Psychologická setkávání, sv. 6. ISBN 80-725-4360-1.

www.hoax.cz

www.e-nebezpeci.cz

www.e-bezpeci.cz

www.prvok.upol.cz

http://www.bezpecne-online.cz/surfuj-bezpecne/komunikace-se-svetem/netiketa.html

http://www.chovani.eu/netiketa/c56

http://svetsenioru.cz/blogy/redakce/seniori-internet-dve-perlicky-ze-sveta-senioru-z-kyberprostoru

POZNÁMKY: