Bezpečně na internetu

Eva Burdová
Jan Traxler

PREVENCE SE MUSÍ VYPLATIT
MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
Středočeský kraj
Vzdělávací institut Středočeského kraje
Středočeský kraj

Vážení přátelé,

internet a virtuální komunikace se staly neodmyslitelnou součástí našich životů a pro mnohé z nás i součástí každodenní práce.

Ne všichni se dokážeme v dynamickém, spletitém a neustále se měnícím světě internetu dobře orientovat a vypořádávat se s riziky, která tento virtuální svět, komunikace a pohyb v něm, přináší. Součástí tohoto světa jsou i naše děti. A tak jako tomu bylo vždy v minulosti, je realitou v současnosti a bude i v budoucnu, děti a mladí lidé se do nových věcí a nových příležitostí pouštějí velmi rychle a spontánně, a často bez uvědomění si rizik s tím spojených. Je na nás, dospělých, abychom se snažili je před těmito riziky co nejvíce ochránit.

Informační a komunikační technologie jsou fascinujícími nástroji, které umožňují navazovat virtuální vztahy, vytvářet virtuální skupiny lidí, kteří by se v běžném „reálném" životě nesetkali. Ne každý uživatel internetu je však důvěryhodný. Díky anonymitě uživatelů internetu lze jen velmi obtížně odhadnout, s kým komunikujeme. Počítačová kriminalita se stala, bohužel, realitou, a tak jak se rychle rozvíjí samotný internet, stejně rychle se vyvíjí počítačová kriminalita ve svých nejrůznějších podobách.

Středočeský kraj, s vědomím závažnosti této problematiky, rozhodl v roce 2014 zařadit do programu prevence kriminality a programu primární prevence rizikového chování téma počítačové kriminality a rozhodl se zároveň zaměřit tuto prevenci nejenom na žáky a pedagogické pracovníky škol, ale i na

Publikace je financována ze státní účelové dotace MV ČR v rámci realizace projektu prevence kriminality „Bezpečně na internetu", který je součástí Programu prevence kriminality Středočeského kraje na rok 2014.

Autoři: Mgr. Burdová Eva, MBA, PhDr. Mgr. Traxler Jan
Název: **Bezpečně na internetu**
Vydavatel: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK)
Zborovská 11, Praha 5
Kontaktní osoba: Mgr. Jiří Holý- ředitel VISK
Počet stran : 44
Jazyková korektura: Mgr. Magdaléna Hardyn
Odborná korektura: RNDr. Jan Jirátko, Jan Kelyman
Tisk: Tiskárna PRIMA spol. s r. o. , Březohorská 253, Příbram VII
Pořadí vydání: 1.
Měsíc a rok vydání: září 2014

ISBN: 978 -80-904864-9-2

rodiče žáků plnících povinnou školní docházku. Protože právě žáci základní škol jsou jednou z nejohroženějších skupin, chceme dát Vám, jejich rodičům, maximum informací nejenom k získání základní orientace v rizicích internetu, ale i informací ke způsobům a formám ochrany dětí před nimi.

V minulém roce Středočeský kraj pilotně ověřil realizaci několika specializovaných seminářů věnovaných bezpečnosti na internetu, které byly určeny pro rodiče žáků základních škol. Semináře měly velmi dobrou odezvu, a proto jsme v letošním roce, s podporou MV ČR, připravili sérii několika desítek těchto seminářů a zároveň jsme vytvořili prostor pro vydání příručky o bezpečnosti na internetu, kterou právě teď držíte v rukou. Dozvíte se z ní řadu informací nejen o rizicích, která internet přináší, ale i o možnostech, jak děti ochránit, jak řešit situace, kdy jsou akutně ohroženy nebo již přímo do některé z forem počítačové kriminality vtaženy. O aktuálnosti těchto rizik svědčí jak řada odborných analytických údajů, tak i informací z více než pětiny základních škol v kraji, které již počítačovou kriminalitu musely řešit.

Pevně věřím, že Vám tato publikace umožní lépe se orientovat v problematice rizik virtuální komunikace a pomůže Vám předcházet tomu, abyste se ani Vy a ani Vaše děti nestali oběťmi trestné činnosti v souvislosti s používáním nových komunikačních technologií.

V Praze, srpen 2014

Ing. Miloš Petera
hejtman Středočeského kraje

Příručka o nástrahách internetu nejen pro rodiče

Dnešní doba přináší obrovské množství nástrah, jedním z rizik, která si snad ani většina lidí neuvědomuje, je i internet. Stejně jako u ohně je internet velice dobrý sluha, ale zlý pán. Mnoho rodičů ani netuší, s čím se jejich potomek na internetu může setkat a jaká rizika nám informační technologie mohou přinášet. V žádném případě nechceme v této příručce hořekovat nad tím, jak by bez internetu bylo lépe. To určitě ne! Chceme ale poukázat na to, jak je důležité věnovat se dítěti i v této oblasti. A zrovna tak, jak dítě učíme bezpečí v každodenním životě, je třeba, abychom jej naučili i bezpečnému užívání internetu. Je nemyslitelné, že bychom dítě pustili samotné do vody, pokud by neumělo plavat, učíme dítě rozhlížet se na přechodu, aby jej nepřejelo auto, ale často posadíme dítě k počítači a o jeho bezpečí se nestaráme a o bezpečném chování mu nic nesdělíme. Je to stejné jako neplavce nechat vprostřed rybníka či malé dítě uprostřed silnice. Pojďme si tedy povídat o tom, co dělat, aby internet byl pro nás i naše děti bezpečným místem plným informací, nadšení a zážitků a abych jako dospělák i jako dítě věděl, co mám dělat, jak se mám chovat, s čím se mohu setkat, a pokud už se s něčím rizikovým setkám, jak mám reagovat.

Cílem naší příručky je co nejsrozumitelnější formou poukázat na nejčastější rizika spojená s využíváním informačních technologií. Určitě si neklademe za cíl vypracovat příručku pro odbornou veřejnost, to by bylo zbytečné, odborníci tato rizika znají. Chceme co nejsrozumitelnější formou oslovit rodiče, jako běžného uživatele internetu, a budeme se snažit mluvit řečí, které bude rozumět každý a ne jen hrstka vyvolených IT specialistů.

Příručka je určená především všem rodičům, kteří chtějí být informováni a díky tomu se odhodlají pár

chvil číst, nebo jen prolistovávat příručkou a zjistit tak, co vše může na jejich děti, a ne jen na ně, číhat na vlnách internetu.

Z hlediska internetu a jeho rizik je nutný komplexní přístup v oblasti preventivních aktivit. Za velmi důležité považujeme působit preventivně na všechny zúčastněné osoby. Děti jsou často poučeny již ve škole od pedagogů, lektorů primární prevence nebo ostatních spolužáků. Avšak rodič je ten, který tyto informace může postrádat. A právě v rodině je nutné těmto rizikům předcházet, protože nejvíce času na internetu děti tráví právě doma ve svém volném čase.

Není žádným tajemstvím, že naše děti ovládají počítač, mobilní telefon nebo tablet lépe než my dospělí. Pro ně je ovládání intuitivní záležitostí, počítač a internet jsou hrou i výzvou vyzkoušet nepoznané. Na internetu se můžeme setkat se vším, co nás jen napadne, jsou zde všechny možné dětské servery, hry pro děti, ale zrovna tak lehce se dají najít stránky s pornografickým obsahem či popisem výroby bomby. Lze zde najít věci prospěšné úplně stejně jako cokoli pro děti nevhodné. Internet je odrazem celosvětové společnosti, je to jakési zrcadlo vyspělého světa. Nás by ale mělo zajímat, do jaké míry je čas strávený dítětem na internetu bezpečný a co je pro naše děti vhodné. Jaké je to „ve vodách" českého internetu? Podle statistik Policie ČR za loňský rok se lidé na internetu mohli nejčastěji setkat *s nejrůznějšími podvody (1740x). Mezi další nejčastější trestné činy páchané na celosvětové počítačové síti loni patřily poškození a zneužití záznamu na nosiči informací (206x), mravnostní trestné činy (182x) a porušování autorských práv (173x). Výjimkou nejsou ani různé úvěrové podvody (113x). Internetová kriminalita je navíc na vzestupu. Zatímco v roce 2011 bylo spácháno 1502 skutků, v roce 2012 jich bylo již 2195. A loňský rok statistiku rozhodně nevylepšil - policie zaznamenala 3108 činů.*[1]

Jak tedy zajistit svým vlastním dětem „počítačové" bezpečí? Stoprocentně to nikdy nejde. Vy sami se můžete co nejvíce jako rodiče snažit, mít perfektně technicky zabezpečený počítač, tablet či mobilní telefon dětskými zámky, sledováním historie a filtrováním nevhodného obsahu mnoha počítačovými programy. To je jistě prospěšné a je výborné, pokud rodič do této problematiky alespoň trochu nahlédne a počítač zabezpečí minimálně kvalitními antivirovými programy, firewally a klade důraz na složitá, kombinovaná a nesnadno dešifrovatelná hesla k emailovým schránkám, elektronickým účtům a dalším aplikacím.

Ovšem za mnohem důležitější faktor v dnešním světě považujeme prevenci již od útlého dětství, informovanost rodičů i dětí z hlediska osobního bezpečí na internetu. Hned od počátku používání internetu je přínosné naučit děti několik důležitých zásad bezpečného pohybu ve virtuálním prostoru. To jistě v dnešní době patří do základních dovedností, do elementární gramotnosti, kterou rodiče dětem mohou dát úplně stejně, jako je naučí hygienickým návykům, čištění zubů, přecházení silnice apod. Můžeme mít perfektně technicky zabezpečený počítač, mohli bychom popisovat spoustu programů, které zestárnou s vývojem počítače a budou už možná nepoužitelné po vytisknutí této příručky. Ovšem univerzálnější a déle použitelnější jsou informace a nácvik jednoduchých dovedností důležitých i v dalším životě dítěte. Pokud se mi toto jako rodiči podaří, mám vyhráno. Vždyť dítě se s počítačem nemusí setkat jen doma. Právě když doma budu mít filtrovány všechny závadné obsahy, vše perfektně zabezpečeno, bude dítě vyhledávat počítač jinde. Vždyť zakázané ovoce nejlépe chutná.

[1] *[online]. [cit. 2014-07-15]. Dostupné z: http://www.novinky.cz/internet-a-pc/327263-netolismus-a-dalsi-stinne-stranky-internetu.html*

A tuším já jako rodič, jak mají zabezpečený počítač ostatní spolužáci? Aby dítě otevřelo počítač někde jinde, tomu se neubráním. Musím ho prostě varovat a naučit se na internetu bezpečně pohybovat.

Měli bychom se také zajímat o to, jaké jsou varovné signály toho, že se něco děje a že je něco v nepořádku. Jak to zjistit a co následně dělat, kam se obrátit o pomoc, je snahou této příručky.

Pro začátek jen několik drobných dotazů k zamyšlení pro každého rodiče:

- *Víte, kolik hodin Vaše dítě tráví v zajetí informačních technologií?*
- *Víte, s kým si Vaše dítě píše a s kým komunikuje?*
- *Víte, jaké informace o sobě a vaší rodině dítě sděluje?*
- *Víte, kolikrát se Vaše dítě sejde s osobou, kterou zná jen z virtuální reality?*

Tyto a další otázky nás jistě napadnou, pokud se chvíli budeme zabývat jen několika riziky spojenými s používáním internetu. Zdaleka nemůžeme popsat vše, co se může stát. Nicméně je podstatné uvědomit si alespoň to nejdůležitější. Internet je lákadlo, děti zde hledají hry, hudbu, komunikují, navazují virtuální přátelství, hledají kamarády. Nejdříve si hrají samy, později hrají hry s ostatními, sdílejí data, posílají si fotky, komunikují o všem, co dělají, komunikují s kýmkoli a kdykoli. Internet vnímají jako kouzelný svět plný zábavy a většina z nich si jakákoli rizika neuvědomuje. I mnoha rodičům v dnešním „zlém" světě připadá mnohem bezpečnější, když jejich dítě raději sedí u počítače v teple domova a není venku, kde by se mu mohlo něco přihodit. Jak mylná je tato myšlenka, bohužel zjišťují až ve chvíli, kdy nastává problém.

Z výzkumu, který byl proveden v ČR v roce 2014, vyplývá:

- *s problematikou kyberšikany se setkalo 50,90% dětí*
- *rodičům by se svěřilo 61,76% dětí s vydíráním*
- *rodičům by se svěřilo 50,19% dětí s vyhrožováním nebo zastrašováním*
- *nejčastějším problémem je průnik na účet a to v 34,80%*
- *s verbálními útoky se setkalo 34,33% dětí*
- *s obtěžováním pomocí prozvánění na telefonu se setkalo 26,36% dětí*
- *13,70% se setkalo s ponižováním, ztrapňováním a šířením fotografie*
- *17,84% se setkalo s vyhrožováním a zastrašováním*
- *11,82% se setkalo s krádeží virtuální identity*
- *většina dětí se svěří svému rodiči. Na druhém místě pak učiteli*
- *v 76,99% děti zveřejňují na internetu jméno a příjmení*
- *v 56,41% děti zveřejňují na internetu fotografii obličeje*
- *55,72% dětí zveřejní na internetu svojí e-mailovou adresu*
- *29,80% dětí bylo svým internetovým známým nebo kamarádem požádáno o zaslání své fotografie obličeje a 54,67% z nich této žádosti vyhovělo*
- *7,81% na internet umístilo svojí sexy fotografii nebo video*
- *12,14% dětí svoji sexy fotografii nebo video zaslalo internetem nebo mobilním telefonem svému známému*

- *54,30% dětí komunikuje na internetu s neznámými lidmi*
- *26,92% dětí bylo požádáno, aby udržely jejich komunikaci v tajnosti*
- *40,22% dětí by bylo ochotno jít na osobní schůzku s „kamarádem" z internetu*
- *43,56% dětí bylo požádáno přes internet o osobní schůzku*
- *54,91% dětí skutečně na tuto schůzku dorazilo*[2]

Právě na tato zjištění se pokouší náš text reagovat a ukázat Vám, jak k daným problémům dochází, co vašemu dítěti a nejen jemu hrozí a co je možné proti tomu učinit. Věnujeme se jen některým problémům, které se pokoušíme co nejsrozumitelnější formou vysvětlit a ukázat rizika, která skrývají.

Jaké jsou varovné signály pro rodiče, na co by měl rodič dát pozor?

Z psychologického hlediska jsou u většiny následně popisovaných rizikových situací podobné varovné signály. Dítě začne měnit své chování v souvislosti s počítačem. Notebook či tablet odnáší při práci z dosahu rodičů, začne se s počítačem zavírat sám v pokoji, odmítá s rodiči komunikovat o tom, co na počítači dělá, nechce se vůbec bavit o čemkoli souvisejícím s počítačem. Zdatnější jedinci začnou vymazávat historii ve svém počítači, dítě můžete nachytat při lži, mlží, odpovídá vyhýbavě, najednou může potřebovat více peněz, nečekaně odchází za kamarády, může být ustrašené.

Toto jsou nejčastější signály, ovšem může se jednat i o jinak změněné chování, dítě může mít zhoršený prospěch ve škole, unikat do fantazie, trávit na počítači čím dál více času, být unavené, protože se počítači věnuje i v noci, může přijít o kamarády apod. Tyto příznaky jsou převážně znaky počítačové závislosti. Nepochybujeme o tom, že vnímavý rodič, který se svým dítětem normálně komunikuje, naslouchá mu a zajímá se o něj, změnu chování velice dobře a včas odhalí. Pokud je navíc informovaný, nemá problém, aby návodnými otázkami mohl zjistit, co se děje.

Jakmile rodič zjistí cokoli, co se mu nelíbí, nebo se mu dítě svěří se zhlédnutím závadného obsahu, s navázáním kontaktu s vulgárním člověkem či jinou rizikovou situací, neměl by nikdy reagovat unáhleně, zbrkle či značně pohoršeně. Rodič by měl dítěti situaci klidně vysvětlit, mluvit s ním o tom, říci dítěti, že ono za to nemůže, že na internetu se mohou objevit i takovéto věci a dokonce i zlí lidé a že nejjednodušší je okamžitě se odpojit. Dítě nesmí ztratit v rodiči důvěru, je důležité, aby se příště nebálo svěřit.

Časté formy rizikového chování spojené s užíváním internetu

Kyberšikana - v překladu šikana, která se odehrává ve světě informační a telekomunikační techniky

Jde o takové jednání, které má oběť záměrně ohrozit nebo jí ublížit prostřednictvím prostředků informační a telekomunikační techniky. Nejčastěji se setkáte se zneužitím mobilního telefonu a internetu. Podle loňského výzkumu má každé druhé dítě na českém internetu zkušenosti s kyberšikanou. Rozsáhlý výzkum ukázal, že mezi nejčastější druhy kyberšikany patří verbální útoky (33%), obtěžování za pomoci prozvánění (24%) a vyhrožování či zastrašování (17%). Děti se navíc přiznaly k tomu, že v nezanedbatelné míře jsou samy autory kyberšikany vůči svým vrstevníkům.

[2] *[online]. [cit. 2014-07-20]. Dostupné z: http://www.e-bezpeci.cz/index.php/tiskove-zpravy/884-ahoj-potkame-se-osobne-40-deti-na-internetu-by-souhlasilo*

Kyberšikana má svá specifika oproti „klasické“ šikaně. Rozdíly jsou především ve velké anonymitě. Pachatel se cítí bezpečně, neboť si myslí, že se o něm nikdo nedozví. Některé děti-agresoři ani nevědí, že páchají kyberšikanu, berou to za jakousi formu uvolnění svých vlastních tenzí a nespokojeností, někteří potřebují demonstrovat svou sílu, vyvolat strach, někdy sami v reálném světě strachem trpí, či jsou oběťmi klasické šikany. Častým spouštěcím faktorem takovéhoto jednání může být pouhá nuda, hádka s kamarády, konflikty se spolužáky, pomsta.

Většina obětí se nedozví, kdo je agresorem kyberšikany, což je velice nepříjemné a pocit strachu se tím zvyšuje i v reálném světě. Dalším rozdílem je doba trvání. Ke kyberšikaně může docházet kdykoli (365 dní v roce/24 hodin denně). Ale může také proběhnout pouze jednou a následky mohou trvat po zbytek života oběti, k SMS se můžeme kdykoli vrátit a neustále ji číst dokola, jakákoli zpráva pomocí ICT technologií „visí“ v kyberprostoru a čte ji často obrovské množství lidí. Tím se pocity ponížení u oběti násobí, oběť má často pocit, že už to četli všichni na světě a všichni si teď na ni/něj ukazují a už nemůže ani chodit ven. Toto je často pro oběť značně traumatizující a může to vést až k pokusům o sebevraždu.

Místo, odkud agresor útočí, nehraje žádnou roli. Stejně tak jako fyzická vzdálenost mezi obětí a agresorem. V kyberšikaně není podstatné, zda byl agresor velký a fyzicky zdatný, ale stačí pouze, aby byl dostatečně gramotný v oblasti využití informační a telekomunikační techniky.

Možná rizika: Oběť je vystavena nejen verbálním útokům ze strany útočníka, často je také vystavována veřejnému ponižování zveřejňováním intimních a choulostivých údajů a dat, oběť bývá zastrašována. Dítě se může stát obětí vydírání, poté i zneužití a znásilnění. Velmi často se útočníkovi podaří proniknout na sociální účet oběti. Je zde riziko zcizení fotografií a videí a následné šíření na internetu za účelem oběť ztrapnit nebo vydírat. Hrozí riziko ztráty virtuální identity, kdy se útočník vydává za oběť.

Možné způsoby ochrany: Nejdůležitějším způsobem ochrany je prevence, která spočívá v informovanosti všech zúčastněných osob. Prohlubujte vzájemnou důvěru mezi dětmi a rodiči, dětmi a pedagogy, protože je nutné, aby se dítě s problémem svěřilo. Teprve pak je

možné nastalý problém účinně řešit. Obejte na vhodné zabezpečení počítače a telefonu. Buďte všímaví ke svému okolí a ke svým blízkým. Mluvte se svým dítětem o tom, co kyberšikana je, snažte se, aby se Vaše dítě nejen nestalo obětí, ale aby se nestalo byť nevědomky agresorem v kyberprostoru. Mluvte s dítětem o netiketě (etiketě na internetu), prohlubujte empatii Vašeho dítěte, posilujte sebevědomí, učte je vycházet s ostatními a veďte je k úctě k ostatním lidem. Rodič a pedagog by měli být vzorem v chování, ale i v používání informační a telekomunikační techniky.

Kyberstalking - v překladu jde o pronásledování v kyberprostoru

Jedná se o obtěžování, které se stupňuje, opakuje a odehrává se v kyberprostoru. Má různou intenzitu a liší se i druhy projevu. Využívají se při ní prostředky komunikační techniky (např. Skype, SMS, chat, email, telefon, sociální sítě). Stalker je velmi často znám oběti, může jít o bývalého partnera, milence, kamaráda, zrazeného přítele nebo milovníka. Ten například není ochotný akceptovat ukončení vztahu nebo nezájem oběti, a tak se pokouší oběť v kyberprostoru obtěžovat a donutit ji k reakci či návratu. Toto obtěžování může mít rozličnou podobu od SMSek, emailů, po prozvánění a vyhrožování. Obtěžování se stupňuje a často se zvyšuje i jeho četnost. V některých případech může být stalker pro oběť neznámý, to proto, že si oběť útočník vyhlédl na internetu na základě tam dostupných informací. Stalker je většinou společensky příjemný člověk a ani jeho okolí nemá tušení, že se může jednat o útočníka. Proto je někdy těžké jej identifikovat nebo naopak uvěřit oběti. Z dostupných statistik vyplývá, že častěji se tohoto činu dopouští muži, ženy zase bývají vytrvalejší.

Možná rizika: Stalker dokáže svoji oběť velmi dlouho pronásledovat. Na první pohled se nemusí zdát, že se již jedná o patologické pronásledování a oběti to zprvu nemusí být nepříjemné. Z tohoto důvodu velmi často oběť poskytne dostatek informací a materiálu útočníkovi, které pak on využije. Hrozí naprostá ztráta soukromí, ztráta osobních údajů a ztráta pocitu bezpečí, která je z psychologického hlediska nejhorším faktorem, neboť pocit bezpečí patří do jedné ze základních lidských potřeb a u dítěte či mladistvého vede neuspokojení této potřeby k celkovému selhávání, nejistotě, strachu, dítě či mladistvý může přestat chodit do školy, může zažívat i školní neúspěšnost a celkově se zhoršovat ve všech výkonech, může i unikat do nemoci.

Možné způsoby ochrany: Je velmi těžké útočníka odradit od jeho činů. Pokud je to možné, co nejrychleji přímo a jednoznačně dejte stalkerovi na vědomí, že nemáte o jeho projevy zájem. Poté je nutné přestat s útočníkem jakkoli komunikovat. Neodpovídat mu na email, SMS, volání a v žádném případě se také nesetkávat osobně (pokud to jde). S tím je spojena potřeba například změnit své obvyklé trasy do školy, práce. Změnit dopravní prostředek. Ale v našem případě hlavně změnit svoji virtuální identitu (změnit telefonní číslo, vytvořit si jiný profil na sociální síti, založit si jiný email, apod.). S informacemi o nové virtuální identitě je potřeba zacházet velmi opatrně, sdělovat ji skutečně jen těm, kterým naprosto věřím a svým nejbližším. Jen tak je reálná šance přerušit kontakt s pronásledovatelem. Rozhodně je nutné uchovávat a nemazat veškerou komunikaci mezi obětí a pachatelem. V případě potřeby může pak posloužit jako důkazní materiál. Kontaktujte policii, neboť od 1. 1. 2010 je stalking trestný čin, pokud se cítíte být

ohroženi. Musí být splněny podmínky, že pronásledování je proti vůli oběti, že jde o intenzivní a dlouhodobé pronásledování. (§ 354 zákona č. 40/2009 Sb., trestní zákoník).

Kybergrooming - manipulace v kyberprostoru

Útočník se snaží v kyberprostoru (chat, ICQ, sociální sítě, SMS...) vytipovat a najít vhodnou osobu, ve které vzbudí postupně důvěru a postupem času ji přinutí k osobní schůzce, kde oběť pak nějakým způsobem zneužije či využije.

Velmi zranitelné jsou nejen děti, ale všichni, kteří si často hledají kamarády v kyberprostoru a kteří nejsou dostatečným způsobem poučeni. Touha po dobrodružství, riziku, svěřování se, hledání nových kamarádů a zkoušení dalších nových věcí jen nahrává útočníkovi, který čeká na svou příležitost. V této oblasti jsou často nejvíce ohroženy děti, které jsou na informačních technologiích závislé, jsou to děti, které tráví velkou většinu času na internetu a se svým mobilem a většinu přátel a kamarádů mají pouze ve virtuálním světě a v realitě kamarády nemají, s nikým si nehrají, nikdo je nenavštěvuje.

Kybergrooming probíhá v několika krocích, které na sebe postupně navazují. V první fázi si útočník vyhlédne oběť a to právě na základě informací, které získá na internetu a osloví ji. Ne vždy použije svoji pravou identitu. Často se útočník vydává za úplně jinou osobu a to z důvodu, aby u oběti vzbudil pocit důvěry. Vydává se za osobu, která je oběti nějakým způsobem blízká (věkem, zájmy, problémy, vzhledem, potřebami apod.). Zároveň se pokouší oběť postupně izolovat od okolí. Jedině „on" dokáže oběti se vším poradit a vždy ji zcela chápe – druhá fáze. V této fázi může oběti nabídnout „svoji" fotografii či poslat nějaký vhodný dárek, např. dobít kredit u mobilního telefonu, aby vzbudil větší důvěru. Ve třetí fázi se pokouší útočník získat nějaký kompromitující materiál. Vhodným způsobem oběť motivuje, aby mu za-

slala např. fotografie, videa. A pokud fotografie či videa, tak nějaká, kde je oběť spoře oděná, či je dokonce nahá. V případě, že oběť zašle požadované materiály, útočník je systematicky sbírá a následně je použije proti oběti. Útočník ale také postupně sbírá veškeré osobní údaje a informace, které mu oběť během komunikace podá. V poslední fázi útočník žádá oběť o osobní schůzku. Ta může proběhnout zcela dobrovolně na základě oboustranné dohody, anebo pokud se oběť nechce nechat vylákat,

může ji útočník začít vydírat zveřejněním fotografií na internetu, ve škole apod. Tím oběť vydírá a s největší pravděpodobností dosáhne osobní schůzky. Na té pak může následovat to, proč vlastně útočník oběť kontaktoval (znásilnění, vydírání, napadení....)

Možná rizika: Každému z nás hrozí toto riziko. Zvýšené riziko pak těm, kteří o sobě mají na internetu zveřejněné osobní údaje. Děti jsou ovšem kategorií nejohroženější. Útočníky zajímají především fotografie, videa, jména, kontakty a zájmy. Na jejich základě si vytipují oběť a tu se pak pokouší kontaktovat s cílem ji zneužít. Také hrozí zneužití veškerých údajů, které útočníkovi oběť poskytne.

Možné způsoby ochrany: Za nejdůležitější považujeme vždy prevenci. Každý by měl být řádným a vhodným způsoben informován o možných rizicích a důsledcích. Dítě by mělo mít důvěru ve své rodiče a svěřovat se především jim. Rodič by měl vědět, s kým si dítě ve virtuálním světě vyměňuje informace. Pokud dítě tráví většinu času ve virtualitě a ne s reálnými kamarády, měl by rodič jistě zbystřit. Naučte své dítě, aby nikdy nevěřilo slibům, které dostává ve virtuálním světě, byť znějí sebelákavěji. Naučte dítě všímat si možných rozporů v komunikaci s útočníkem. Povídejte si s dítětem o tom, že není normální, že někdo chce vše uchovat v tajnosti a nechce se prozrazovat, že problematické je i to, pokud někdo píše, že by nikdo neměl o jejich „vztahu" nic vědět. Varujte dítě, aby se nikdy nescházelo s osobou, kterou zná jen z internetu. V případě, že již jde na schůzku, vždy je nutné informovat své blízké o této skutečnosti. Zde rodičům může velice výrazně pomoci film „Seznam se bezpečně", který doporučujeme zhlédnout rodičům, poté společně s dítětem a mluvit o něm. Pro starší děti společnost Seznam.cz připravila i „Seznam se bezpečně II", oba dostupné na www.seznamsebezpecne.cz.

Naučte dítě:

- *Nikdy nesdělovat žádné osobní informace.*
- *S tím je spojená i prevence, co již mám o své osobě na internetu uvedeno.*
- *Mám správně vyplněný profil?*
- *Kolik osobních informací obsahuje?*
- *Jak silná hesla používám?*

Flaming - v překladu hoření

Jde o nepřátelské chování útočníka vůči oběti, které se odehrává ve virtuálním světě. Nejčastěji v diskuzních fórech, chatu, sociálních sítích, ale i v emailu. Útočník urážlivým způsobem napadá oběť tím, že do kyberprostoru umisťuje vzkazy, ve kterých ho 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 svým přesvědčením. *Výzkumy ukazují, že „flaming" jako agresivní chování ve formě slovního napadání je v prostředí virtuální reality až čtyřikrát častější než v reálném životě.*[3]

Možná rizika: Oběť je neustále napadána verbálním způsobem, je urážena a může být i zastrašována. Hrozí ztráta společenského postavení, zvyšuje se riziko psychického neklidu.

Možné způsoby ochrany: S útočníkem nadále nekomunikovat a nesnažit se ho přesvědčit o své „pravdě". Nenechat se vyprovokovat dalšími otázkami k odpovědím. V krajním případě je možné změnit virtuální identitu (založit si jiný účet nebo profil).

Více informací najdete např. na:
http://www.bezpecny-net.estranky.cz/clanky/nebezpecne-komunikacni-praktiky/Flaming.html

Sexting - v překladu sextování. Složenina ze slov sex a posílání textů, obrázků a videí

Jde o využívání informačních a komunikačních prostředků k zasílání textů, fotografií a videí se sexuální tématikou. Tyto materiály často končí na internetu a můžou mít pro oběť fatální důsledky, neboť jsou často použity jako donucovací prostředek k vydírání. Některé případy pak končí až smrtí oběti.

Možná rizika: Zasláním erotické nebo porno fotografie či videa komukoli se vystavuji riziku, že v budoucnu může být tento materiál použit proti mně, např. k vydírání. Tato situace nemusí nastat bezprostředně po odeslání, ale v podstatě kdykoli, neboť útočník si tento materiál uchovává a použije jej kdykoli v budoucnu. Závažným rizikem se fakt, že ti, kdo šíří sexting, mohou být zároveň pachateli přestupku nebo trestné činnosti v oblasti šíření dětské pornografie nebo ohrožování výchovy dítěte apod. Dítě je v tomto případě osoba do 18 let.

Možné způsoby ochrany: Nejdůležitější je informovanost jednotlivých uživatelů. Nikomu za žádných okolností neposkytnout potencionálně nebezpečný materiál. To platí i v partnerských vztazích, neboť tento vztah může jednou skončit a jedna ze stran pak choulostivý materiál použije proti straně druhé ve snaze tento vztah udržet. To samé platí s umisťováním choulostivého materiálu na sociální profily. Ty nejsou ve skutečnosti přístupné jen vybraným jedincům. Fotografie či video se pak může nekontrolovatelně šířit po internetu. Obejte na zabezpečení sociálního profilu, emailové schránky a komunikačních prostředků silným heslem, neboť i zde může útočník zcizit Vaše choulostivé materiály.

Více informací najdete např. na:
http://www.sexting.cz/
http://www.e-bezpeci.cz/index.php/temata/sexting
http://www.nebudobet.cz/?cat=sexting

Phishing - v překladu rybaření.

Jedná se o podvodnou techniku na internetu, která má za cíl od uživatele vylákat jeho přihlašovací údaje a hesla, která můžou být následně útočníkem zneužita. Útočníci rozhazují „návnadu" a čekají, kdo se „chytne" – proto rybaření. Nejčastěji se potkáte s phishingem

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

ve Vaší emailové schránce, kde se email tváří jako skutečná a důležitá informace od legitimní společnosti (banka, Váš sociální profil, různé státní instituce nebo dokonce zpráva od IT technika). Otevřením této zprávy budete vyzváni ke spuštění odkazu a následně přesměrováni na podvodnou stránku, která je identická s oficiální stránkou, kterou imituje. Zde jste pak vyzváni k zadání osobních údajů např. (přihlašovací jméno, heslo, číslo kreditní karty, datum narození apod.) Jejich zadáním a odesláním je vlastně předáváte útočníkovi, který je může následně použít k libovolné činnosti. A nejen v emailové schránce na Vás čeká nebezpečí. Také si dávejte pozor při chatování, při používání mobilního telefonu a při navštěvování různých webových stránek. Zde se také můžete setkat s tímto druhem útoku.

Možná rizika: ztráta citlivých údajů – přihlašovací jména a hesla, která používáte k přístupu do zabezpečených aplikací. S tím je spojena možná ztráta virtuální identity. Útočník se pak může vydávat za Vás a z toho nějakým způsobem profitovat. V některých případech může i disponovat Vašimi finančními prostředky.

Možné způsoby ochrany: Pozorně sledujte stránky, na kterých se nalézáte. Phishing se vyznačuje tím, že jste přesměrováni na jinou URL adresu. Často jde jen o záměnu písmen v adrese domény, kam přistupujete. Využívá se také subdomén, kam jste přesměrováni, nebo zkrácených názvů domén. Pozorný uživatel si této skutečnosti může všimnout a tím odhalit, že je v ohrožení.

Důležité je neklikat na odkaz v emailu, který po Vás chce např. ověření přihlašovacích údajů do banky. Pamatujte si, že banka od Vás nikdy nebude vyžadovat sdělování a znovu ověřování přístupových údajů pomocí internetu. Obecně platí, nespouštět a neinstalovat programy, které mi jsou nabízeny emailem nebo ve vyskakovacím okně na internetu.

Vždy používejte aktualizovaný operační systém, aktualizovaný antivirový program a firewall bránu. Také nezapomínejte na aktualizace internetového prohlížeče a emailového klienta. Nikomu nesdělujte svá hesla a mějte na počítači každý svůj chráněný uživatelský profil.

„Většina phishingových útoků je na bankovní sektor nebo na služby s ním spojené. Často se také pojí se službami spojenými s penězi, např. Paypal, Paysec aj."[4]

Více informací najdete např. na:
http://hoax.cz/phishing/
http://www.bezpecnyinternet.cz/

Pharming - v překladu znamená farmaření

Pharming je obdobnou technikou jako phishing. Jde o způsob změny IP adresy a DNS serveru

[4] *[online]. [cit. 2014-08-01]. Dostupné z:* http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx

ze strany útočníka. K tomuto napadení může dojít jak na straně serveru, kam se připojujete, tak i na Vašem počítači. Tato změna Vás pak bez Vašeho vědomí skrytě přesměruje na falešné internetové stránky, které jsou k nerozeznání od původně požadovaných. Díky této skutečnosti například vyplníte přihlašovací údaje a heslo do zabezpečené aplikace a takto vyplněné údaje jsou pak známé útočníkovi, který je může libovolně zneužít. Pharming je svou podstatou nebezpečnější než phishing, protože nevyžaduje od uživatele otevření přílohy e-mailu nebo vědomou instalaci.

Možná rizika: ztráta citlivých údajů – přihlašovací jména a hesla, která používáte k přístupu do zabezpečených aplikací. S tím je spojena možná ztráta virtuální identity. Útočník se pak může vydávat za Vás a z toho nějakým způsobem profitovat.

Možné způsoby ochrany: Pozorně sledujte stránky, na kterých se nalézáte. V případě, že vidíte v internetovém prohlížeči zabezpečený přístup na dané stránky (řádek s URL adresou je zelený a začíná https://), můžete být klidnější. Zjištění pharmingu není jednoduché, ale pokud například v internetovém bankovnictví zadáte své přihlašovací údaje a následně chcete vstoupit do aplikace a v tu chvíli se nedostanete na svůj účet, zpozorněte! Příčin, proč nedošlo k úspěšnému přihlášení, může být několik. Od poruchy v internetovém připojení, přes chybně zadané přihlašovací údaje až po pharming. Pokud Váš internet a internetové bankovnictví funguje správně, zadali jste správné přihlašovací údaje, pak je namístě požádat banku a blokaci účtu, kterou je možné provést po telefonu, neboť jste se mohli stát obětí pharmingu.

Důležitou ochranou je právě Vaše informovanost, která často pomůže s řešením a minimalizací možných následků.

Více informací najdete např. na:
http://www.bezpecnyinternet.cz/

Sniffing - v překladu čichání, čmuchání

Jde o odposlech komunikace (dat) mezi dvěma a více počítači navzájem propojených v síti nebo s přístupem na internet. Toto monitorování elektronické komunikace může probíhat jak při klasickém metalickém připojení počítače do sítě (LAN), tak i při bezdrátovém připojení (WiFi). V praxi se tohoto používá například ke zjištění problémů v počítačové síti a nalezení problémového zařízení. Ke zjištění vytíženosti celé soustavy apod. Ale zároveň je možné toto monitorování zneužít.

Možná rizika: útočník může sledovat veškerou komunikaci a činnost, kterou na počítači provádíte. Může získat citlivá data, jako jsou přihlašovací údaje a hesla do různých aplikací a následně se pak vydávat za Vás. Tím může dojít ke zcizení virtuální identity a může být Vaším jménem páchána i trestná činnost. Zároveň může útočník získat přístup na Váš počítač a systematicky zcizovat data uložená na Vašem počítači.

Možné způsoby ochrany: Pokud žijeme v dnešní době, není asi reálné nemít internetové připojení a aktivně ho nevyužívat. Je tedy důležité naše přenášená data vhodným a účinným způsobem chránit. Použijte například šifrování dat pomocí certifikátu SSL, podepisujte Vaše emailové zprávy systémem dostupných certifikátů. Také je vhodné používat software

určený pro odhalování a následného zamezení tohoto monitoringu. Mezi nejznámější patří například program SpyBot Search & Destroy, který je zdarma – freeware. Pokud jste zkušenějším uživatelem, můžete se například podívat, kam a odkud Váš počítač odesílá a přijímá data. Vhodným programem může být například CommView nebo NMap. Dále je nutné vždy na svém počítači instalovat jen takové programy, o kterých víte, že jsou bezpečné. Mít správně zabezpečenou domácí síť pomocí silných hesel a šifrování. Také neumožnit přístup „nevhodným" lidem k mému počítači nebo do mé počítačové sítě. Další a neméně důležité je udržovat svůj počítačový systém aktuální a využívat všech jeho zabezpečovacích funkcí. A záleží i na používané technice. Některé modernější aktivní síťové prvky již mají základní systém ochrany zabudovaný v sobě.

Více informací najdete např. na:
http://www.itbiz.cz/
sniffing-odposlech-datove-komunikace

Hoax - v překladu jde o poplašnou zprávu, kanadský žertík, vtípek...

Jde o šíření emailových zpráv pomocí internetové sítě, které jsou nepravdivé, poplašné anebo třeba jen řetězové. Ty nejen, že člověka obtěžují, ale mohou v něm vyvolat i pocit strachu, viny anebo příjemce jinak mystifikovat. Nejčastěji se můžete setkat se zprávami, které Vás „varují" před nebezpečím, např. 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 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.

Možná rizika: Hoax Vás především obtěžuje. Zatěžuje Vaše internetové připojení a celou internetovou síť. Uvede Vás v omyl a Vy se pak řídíte nepravdivou informací. Touto pak můžete neúmyslně poškodit i jiné osoby. Můžete být pomocí poplašné zprávy vyzváni k navštívení webových stránek se závadným kódem (virem) a můžete si infikovat počítač. Značná část lidí také tento email-hoax skutečně přepošle svým známým a tím vlastně může šířit poplašnou zprávu a s největší pravděpodobností i osobní údaje (emailové 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.

Možné způsoby ochrany: Pokud máte podezření, že jste ve své emailové schránce nalezli hoax, neváhejte se o tom přesvědčit. Pomohou Vám například stránky věnované této problematice www.hoax.cz. Zde naleznete i podrobné informace o většině doposud šířených hoaxech a o aktuálním výskytu, včetně různých jazykových mutací. V případě, že jde o hoax, neváhejte a email rovnou smažte. Nepřeposílejte ho. Pokud znáte odesílatele, je možné ho vhodnou formou upozornit, že Vám poslal tento druh emailu.

Možným způsobem ochrany je využívání antispamového nastavení ve Vašem emailovém klientovi. Pokud už hoax pronikne do počítače, je na Vašich vědomostech, schopnostech a slušnosti, jak s ním naložíte.

Více informací najdete např. na:
www.hoax.cz

Hacking – nabourávání se do cizího zabezpečeného sytému

Jde o techniku, při které se hacker (osoba hackující) snaží nestandardním způsobem proniknout do cizího nebo i vlastního zabezpečeného systému. Může jít o Váš počítač, Vaši počítačovou síť, WiFi nebo i zabezpečovací systém domu, email apod. Nemusí se vždy jednat o nelegální aktivitu.

White hat – je hacker, který se snaží získat přístup do cizího zabezpečeného systému s cílem mu neuškodit. Může tak například testovat cizí systém s dovolením jeho tvůrce a upozornit ho na případné slabiny v jeho zabezpečení. V některých případech je dokonce tato činnost finančně ohodnocena.

Black hat – je hacker (někdy označován jako cracker), který se snaží nestandardním způsobem proniknout do cizího zabezpečeného systému s úmyslem poškodit druhého. Nejčastěji může tento útočník zcizit data a ty následně prodat třetí osobě nebo je využít sám k páchání jiné trestné činnosti. Může také data modifikovat – změnit a tím poškodit napadeného. Může získat plný přístup k napadenému systému a ten následně využívat do té doby, než je odhalen. Zatím k nějmasivnějšímu útoku došlo v srpnu 2014, kdy bylo zcizeno víc než 1,2 miliardy hesel.

Více informací najdete např. na:
http://cs.wikipedia.org/wiki/Hacker

Cracking – jde odstranění technologické ochrany programu

Cílem je modifikaci licenčního programu do té podoby, aby při následné instalaci již nevyžadoval zadávání licenčních kódů a byl přesto plně funkční. Je to odstranění technologické zábrany proti zneužití daného softwaru. Právě díky crackingu se pak na trhu setkáte s nabídkou programů za ceny velmi nízké (někdy až za ceny samotného CD nebo DVD nosiče). Tato aktivita porušuje autorská práva tvůrce programu a je postižitelná, což si řada uživatelů neuvědomuje. Měli bychom své děti tedy vést k tomu, aby cracking nepodporovali, i když je pro ně obvykle lákavé získat program za zlomek původní ceny. Je samozřejmé, že i my dospělí bychom jim v tomto ohledu měli jít příkladem.

Skiming – rizika spojená s platební kartou.

Jde o způsob jak získat data a přístup k vaší platební kartě. Většina z nás vlastní a aktivně využívá platební kartu. Lze ji používat i k platbám přes internet. Je to pohodlné a relativně bezpečné, pokud dodržíte bezpečnostní zásady.

V případě skimingu jde o podvodné jednání pachatele spočívající v získání dat (okopírování) z magnetického proužku platební karty. Nejčastěji pachatelé instalují kopírovací zařízení přímo do bankomatu. Toto zařízení není snadné odhalit. Zároveň potřebují získat PIN k Vaší platební kartě. Ten získávají instalací např. kamer, které snímají zadávání kódu na bankomatu a to i na značnou vzdálenost. Také jsou známy případy, kdy je na stávající klávesnici bankomatu připevněná druhá klávesnice, která zaznamenává zadávání PINu. Dalším způsobem je nepozorovaně si okopírovat data z platební karty, například při placení, kdy předáte platební kartu nepoctivému zaměstnanci firmy, kde platíte.

Dnes je také rozšířeným způsobem pouhé odpozorování údajů z platební karty, které v některých případech útočníkovi postačí k placení v obchodech na internetu. Stačí, pokud si zapamatuje, okopíruje nebo vyfotí číslo platební karty, jméno, na které je karta vedená, platnost karty a z druhé strany ještě třímístný číselný kód CVV2/CVC2. V případě, že nemáte blokované platby na internetu pomocí platební karty nebo nemáte zapnutou autorizaci těchto plateb pomocí SMS kódu, postačují tyto informace k čerpání finančních prostředků z Vaší karty. Stále ještě některé banky nemají tato bezpečnostní opatření automaticky nastavená.

Možná rizika: Ztráta finančních prostředků. Ztráta osobních údajů.

Možné způsoby ochrany: Zachovávat PIN v naprosté tajnosti. Při zadávání PINu na klávesnici je vhodné si druhou rukou krýt prsty, aby nebylo možné odpozorovat, jaký je PIN kód. Vždy mít přehled, kde je platební karta. Nedávat kartu obchodníkovi ani jinému člověku do ruky. Vždy požádat o možnost vsunout platební kartu do terminálu sám, vidět neustále na ni a zase si ji sám odebrat. Pravidelně kontrolovat stav svého bankovního účtu a v případě nesrovnalostí okamžitě kontaktovat banku.

Zdravotní rizika, psychické problémy, závislost

Dnes již víme, že dlouhé vysedávání u internetu může výrazně ovlivnit vývoj dítěte. A to nejen v oblasti tělesné, ale i z psychologického hlediska nám může přinést mnoho problémů včetně internetové závislosti nazývané netolismus a ztráty reálného vnímání okolního světa dítětem, jež je již příliš ovlivněno virtuální realitou. Tělesné i psychické zrání dítěte je velice úzce propojeno. Dítě potřebuje dostatek pohybu na čerstvém vzduchu. Již v předškolním věku se setkáváme s dětmi, jež se svým tabletem tráví i několik hodin denně. Bohužel tyto děti nemají dostatečně uvolněné celé tělo obyčejným pobíháním venku, lezením po prolézačkách, skluzavkách a houpačkách. Jen obyčejné zvedání rukou do výše, houpání se a poskakování uvolní ramenní kloub a značně ovlivní psychomotorický vývoj dětí. U tabletu či počítače dítě jen sedí, ruka má rozsah pohybu maximálně na délku úhlopříčky tabletu či klávesnice počítače. Při nástupu do školy najednou tyto děti mají obrovské problémy. Při psaní je potřeba vykonávat účelné pohyby, ruka musí být uvolněná už od ramene, lokte a pak není problém rotace zápěstí. Je zde nutná koordinace oka a ruky. Tyto děti také často hůře mluví, nepotřebují si s počítačem povídat a rozvíjet tak komunikační schémata jako při přímém kontaktu s ostatními dětmi venku. Nerozvinutá grafomotorika spolu s horší koordinací těla a často i s artikulačními problémy u těchto dětí vede k odkladu školní docházky a rodič se diví: „Vždyť naše dítě je tak šikovné, na počítači zvládá tolik věcí!“ Se vstupem do školy

pak mohou vyvstat další problémy, které mohou značně ovlivnit školní úspěšnost dítěte, protože dítě najednou zažívá neúspěch nejen při psaní, ale i ve zvládání grafických znaků, ztrácí motivaci k další práci a tím i důvěru v sebe samo, což je z psychologického hlediska značně závažný problém do budoucnosti. Dítě pak stráví s počítačem či tabletem ve virtuálním světě mnohem více času, protože zde je úspěšné. Pocit úspěchu a ocenění potřebuje zažívat každý z nás.

Dalším rizikem ze zdravotního i psychologického hlediska se u dětí jeví omezenost smyslového vnímání a nižší schopnost „čtení" neverbální komunikace. Děti a často ani dospělí si při psaní a povídání na internetu často neuvědomují skutečnost, že se navzájem nevidí, neslyší ani necítí. Toto je při internetové komunikaci docela závažný rozdíl od reálného světa. Komunikace zde probíhá převážně ve verbální rovině. Naprosto chybí neverbalita, přitom neverbální projevy jsou naprosto nezpochybnitelnou součástí lidské komunikace. Psychologie popisuje, že při komunikaci tváří v tvář tvoří neverbální složka naší komunikace až 60% porozumění si navzájem. S tímto omezením komunikace vyvstává řada problémů, účastníkům internetové komunikace chybí důležité záchytné body jako např. sdělování

pohledy, řeč očí – vizika, sdělování výrazem obličeje, tváře – mimika, sdělování pohyby těla, hlavy, končetin – kinetika, sdělování postoji těla – posturologie, sdělování gesty - tj. mimoslovními projevy vázanými na určitou kulturu – gestika, sdělování dotekem, tělesným kontaktem – haptika, sdělování přibližováním nebo oddálením, tj. vzdáleností – proxemika, sdělováním úpravou zevnějšku (vzhledem) a prostředím – arteficiální faktory, paralingvistické faktory jako tempo, hlasitost, intonaci, zabarvení a tón hlasu, a vůbec všechny biologické a sociální znaky identity komunikujícího člověka (např. věk, pohlaví, upravenost člověka zevnějšku). V on-line komunikaci ochuzení o tuto složku komunikace může způsobit to, že si lidé navzájem nerozumí, nepochopí se, rozčilují se, nedokáží rozlišit, zda to, co člověk na druhém konci píše, myslí ironicky, či zda je to upřímné. Z dlouhodobého hlediska dochází k problematickému vnímání neverbální komunikace u jedinců komunikujících převážně on-line i v každodenním reálném životě. Je prokázáno, že současná generace mladistvých hůře „čte" neverbalitu a pocity ostatních i při komunikaci „face to face". Pouhým pozorováním můžeme srovnávat i psaní SMS zpráv u generace starší a současných mladých, kteří SMS zpráv napíší stovky denně. Starší generace se u čtení i psaní SMS usmívá, mračí, používá mimiku, to u mladší generace nevidíme, píší SMS bez zjevných emocí, bez mimiky, bez neverbality.

Vyšší agresivita v on-line komunikaci. Tento naprosto jasně prokazatelný faktor psychologové přisuzují nejen anonymitě prostředí internetu, ale i právě omezenosti smyslového vnímání a nižší schopnosti „čtení" neverbální komunikace. Tím, že se děti a často i dospělí při on-line komunikaci nevidí, neslyší ani necítí, jsou při agresivní komunikaci tvrdší. Všichni máme v sobě zakódováno empatické cítění, a pokud někomu říkáme něco velice nepříjemného, že se našemu protivníkovi v komunikaci chce např. brečet, jsme schopni okamžitě couvnout a komu-

nikaci zjemnit. Tvrdost jednání si dítě často vůbec neuvědomuje, protože nevidí a necítí, že to je někomu nepříjemné, že to druhého „bolí", že mu ubližuje. Na internetu si často lidé sdělí takové věci, které by tváří v tvář nikdy neřekli. Měli bychom dítě učit, aby se dokázalo vžít do pocitů ostatních a aby nikomu nečinilo to, co by jemu samotnému bylo nepříjemné. Také bychom dětem měli říci, že mám právo kdykoli nepříjemnou komunikaci ukončit a s člověkem, který mi ubližuje, komunikovat nemusím a ukončení komunikace není v těchto případech neslušné.

K dalším negativním faktorům dlouhodobého sžití se s počítačem, tabletem či mobilem patří zpravidla také pokles fyzické kondice, tyto děti mají mnohem méně pohybu než jejich vrstevníci, často zanedbávají hygienu, málo spí, trvale trpí spánkovým deficitem, jsou schopny si nastavit budík na telefonu, až rodiče usnou, aby trávily zbytek noci připojeny on-line. Objevit se mohou také zažívací potíže z důvodu zapomínání nebo odmítání jídla, jídlo zdržuje, zatím by člověk zvládl část hry. Výjimkou nejsou u dětí ani zhoršené funkce pohybového aparátu a stále se zhoršující zrak.

Možné způsoby ochrany: Co s tím? Je to jednoduché. Doba strávená dítětem na počítači či tabletu musí být rodičem kontrolovatelná. Je nutné domluvit s dítětem pár pravidel, ta dodržovat a vyžadovat, nabízet dětem alternativy trávení volného času. Jako i v jiných oblastech života i zde musíme dítěti nastavit hranice, čím je dítě menší, tím je jednodušší učit je vhodným návykům. Rodič by měl mít kontrolu nad časem stráveným s tabletem či počítačem, do postýlky či kočárku by dítěti neměl být tablet vkládán, aby se dítě zabavilo. U dětských tabletů můžeme nastavit časové omezení a tablet se po nastaveném času dítěti prostě vypne. U menších dětí je vhodné tento návyk vytvořit např. tím, že na internetu jsou společně s rodičem, tablet i počítač se používá jen v jedné místnosti, např. v obývacím pokoji, kde se všichni sejdou. Rodič by měl jít příkladem a nebýt připojen ke svému tabletu v jednom kuse, už vůbec by si ho neměl nosit s sebou do postele. Mluvte s dětmi o internetu, ptejte se, co tam dělají, proč je to tak zajímá, vyprávějte jim, co děláte Vy, bavte se i o tom, co dělají přátelé Vašeho dítěte i mimo internet. Povídejte si i o skvělých a zajímavých věcech, co se dají zažít i mimo internet, naučte dítě internet využívat, např. i k tomu, že si společně najdete, kam jet na skvělý výlet. Mluvte s dětmi i o potížích, které může internet přinést, nic jim nezastírejte a nic nepředstírejte. Vyprávějte dětem, co se stalo ostatním, a tak pomocí techniky life stories (životních příběhů) naučte děti, co dělat v určitých situacích. Mluvte s dětmi o tom, co by měly dělat, kdykoli se při používání internetu nebudou cítit dobře.

Netolismus – počítačová závislost

Když pomineme zdravotní rizika předeslaná v předchozí kapitole, která přímo souvisí s dobou strávenou na internetu, vyvstávají další rizika a poměrně závažné problémy ovlivňující i duševní zdraví a psychiku nevyzrálých jedinců. Dalším poměrně závažným problémem se jeví počítačová závislost nazývaná netolismus.

Netolismus jako pojem vznikl původně ze slova net, tedy ve své původní podobě byl považován za závislost člověka na internetu. Dnes je specifikován jako závislost na moderních komunikačních a počítačových technologiích, v nejčastější podobě je to u dětí mobil, tablet, počítač, kdy dnes je většina těchto technických prostředků již s trvalým připojením na internet - tedy nepřetržitě on-line.

Lynne Robertsová odhalila faktory nadměrného užívání internetu, pro pochopení závislosti na internetu, je to určitě zajímavý materiál i pro rodiče:

- *Vytváří se určitý podmíněný reflex (zvýšený tep a tlak) při připojování k internetu.*
- *Při pobytu v menší skupině na internetu (chat) se člověk dostane do jiného stavu mysli podobnému tranzu či meditaci (totální koncentrace na obrazovku monitoru).*
- *Při rychlém posunování textu se vytvářejí obrazové halucinace podobné snům.*
- *Vyvíjí se extrémní rozrušenost, když připojeného uživatele vyruší něco z vnějšího světa.*[5]

Jak tedy rozeznat závislost od běžného užívání informačních technologií? Informační technologie do dnešního života prostě patří, již většina lidí potřebuje ke své práci počítač. Doba strávená na internetu a počítači úzce souvisí s typem vykonávané práce. Jak rozeznat závislost u dětí? Kde je ta hranice? Jedná se o psychickou závislost, o to těžší je tuto závislost rozeznat. Děti začnou postupně ztrácet své kontakty a přátele v reálném světě, raději komunikují ve virtuálním světě. Vstávají i v noci, jsou schopny si nařizovat budík, aby mohly na počítač, až rodiče usnou. Ve škole se zhoršuje prospěch, jsou unavené, lžou o době strávené na počítači, mají jen on-line přátele, ztrácí pojem o reálném čase, zapomínají na dřívější koníčky, nechtějí nikam chodit, odmítají odjet na víkend, kde není signál. Později v rozvinuté závislosti zapomínají na stravu, přestávají jíst a pít, v této době se také často začne objevovat záškoláctví. To je již pokročilá forma závislosti. Závislost se rozvíjí pomalu, nenápadně a plíživě, dítě tráví na počítači čím dál více času, pak už musí být on-line téměř trvale. Největší riziko vzniku závislosti v souvislosti s internetem je přisuzováno intenzivnímu rozvoji počítačových her, které jsou programovány tak, že je hraje neuvěřitelné množství lidí, dítě zde sdílí kyberprostor s tisícovkami hráčů na celém světě, se svou figurkou plně patří do virtuálního světa dané hry, sžívá se se svou postavou, chce, aby jeho postava žila a plnila úkoly, jedinec má postupně potřebu raději se vůbec neodpojovat, aby jeho postava, tedy vlastně ono samo, o něco nepřišlo a stále žilo a plnilo všechny úkoly. Tyto hry patří mezi tzv. MMORPG – Massive Multiplayer Online Role Playing Game. Nejznámější MMORPG je World of Warcraft (zkráceně WoW). Tuto hru hraje podle společnosti Blizzard Entertainment, jež hru vyvinula, celkem 11 milionů hráčů. Odhaduje se, že na celém světě MMORPG hraje kolem 16 mil. lidí. Záludností těchto her je, že hráče úplně pohltí, hra nikdy nekončí, hráč potřebuje nakupovat čím dál lepší výbavu, potřebuje další propriety a pomůcky do hry. Hra je neustále nově naprogramovávána, žije sama svým životem, pokud chce hráč dosáhnout úspěchu, musí spolupracovat, neodpojovat se, rozvíjet vztahy s ostatními, domlouvat se, sdružovat se s ostatními hráči, vytvářet sociální síť. Snaha o dosažení výsledku, úspěchu vede hráče k neustálému vylepšování postavy, jejího vybavení a hromadění prostředků. To vše vede k patologickému trávení velkého množství času na internetu a k rozvoji závislosti. Někteří jsou schopni tyto hry hrát i deset hodin bez přestávky.

Možná rizika: Nadměrné trávení času na internetu, ztráta ostatních zájmů, ztráta přátel a sociálních vazeb v reálném světě, propadnutí virtualitě, úplné sžití s virtuální postavou, zkreslené vnímání okolní reality, vytvoření patologických vzorců cho-

[5] *[online]. [cit. 2014-08-06]. Dostupné z: http://www.lupa.cz/clanky/zavislost-na-internetu-bluf-ci-realita/*

vání, využívání herních schémat a problémů k řešení běžných životních situací, zvyšující se agresivita, přenos asociálních vzorců chování do reálného života. Výzkumy zveřejněné Michiganskou univerzitou uvádí, že při dlouhodobém hraní agresivních her může dojít u dětí a jedinců psychicky nedozrálých dokonce až ke snižování prahu bolesti, v horším případě dojde k takovým změnám psychického stavu jedince, že může být naprosto ovlivněno sociální cítění hrajícího dítěte v reálném životě. Ve své konečné podobě se pak z takového člověka stane dospělý jedinec, který je necitlivý k problémům a nesnázím ostatních lidí, objevuje se zvýšená neochota pomoci jinému člověku nebo nepřirozená agresivita při řešení malých konfliktů či sporů mezi vrstevníky nebo i agresivní chování vůči rodičům, sourozencům a blízkým osobám.

Možné způsoby ochrany: Včas ovlivňujte čas dítěte strávený na internetu, kontrolujte, zda dítě netráví na počítači příliš dlouhou dobu, nabízejte dítěti jiné zajímavé aktivity v reálném životě, podporujte jeho zájmy a aktivity, dopřejte mu kamarády a přátele. Snažte se trávit volný čas se svými dětmi, učte je smysluplnému trávení volného času, sami buďte příkladem.

Základní pravidla bezpečného používání a chování se na internetu:

Na toto téma existuje již mnoho „desater", přesto se je pokusíme utřídit a rozšířit

- Vždy používej IT techniku k předem stanovenému cíli.
- Nevěnuj virtuálnímu světu nadbytek svého volného času, využij čas efektivně.
- Chovej se tak, abys svými činy neubližoval jinému a zároveň se sám chraň před možným nebezpečím.
- Používej techniku, které rozumíš a nesnaž se zbytečně jen „zkoušet", zda se ti něco podaří.
- Instaluj jen předem ověřené a známe programy. Neotevírej soubory, které neznáš nebo které Ti přišly v nevyžádané v mailové poště.
- Používej kvalitně zabezpečený počítač, notebook, telefon.
- Pamatuj, že silné heslo by mělo obsahovat velké písmeno, malé písmeno, číslici a nestandardní znak. Délka by měla být alespoň 8 znaků.
- Měj na paměti, že heslo není jediný způsob zabezpečení dat. Používej šifrování k ukládání dat i ke komunikaci, používej certifikaci.
- Nezapomínej na veškeré aktualizace operačního systému, který používáš.
- Měj nainstalované vhodné programy, které chrání tvé bezpečí a chrání tvé zařízení před útočníkem.
- Nedůvěřuj všem informacím, které na internetu nalezneš – nejsou vždy pravdivé.
- Nešiř informace, které nejsou pravdivé, a jejich pravdivost nemáš dostatečně ověřenou.
- Udržuj svá hesla v naprosté tajnosti a nikdy je nikomu nesděluj.
- Komunikuj ve virtuálním světě jen s tím, s kým chceš Ty sám. Neodpovídej na nezačatou komunikaci s člověkem, kterého bezpečně neznáš.
- Neboj se nevhodnou komunikaci ukončit a říci jasné NE.
- Za žádných okolností nikomu nesděluj žádné osobní informace (jméno, příjmení, bydliště, školu, datum narození, rodné číslo, telefonní číslo, heslo, PIN, apod.).
- Nikdy nikomu neposílej svoji intimní fotografii nebo video.
- Nepoužívej webovou kameru s neznámou osobou. Tvé záběry si může někdo ukládat a následně je použít.

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

Kde např. hledat pomoc:

☎ 840 111 234 – rodičovská linka

☎ 116 111 – linka bezpečí

http://chat.linkabezpeci.cz

pomoc@linkabezpeci.cz

www.napisnam.cz

☎ 158 – Policie ČR

http://aplikace.policie.cz/hotline/

www.horkalinka.cz – hlášení nevhodného či nezákonného obsahu na internetu

Seznam literatury:

DIVÍNOVÁ, Radana. *Cybersex : forma internetové komunikace*. Praha: Triton, 2005. 167 s. ISBN 80 -7254-636-8.

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

[online]. [cit. 2014-07-15]. Dostupné z: http://www.novinky.cz/internet-a-pc/327263-netolismus-a-dalsi-stinne-stranky-internetu.html

[online]. [cit. 2014-07-20]. Dostupné z: http://www.e-bezpeci.cz/index.php/tiskove-zpravy/884-ahoj-potkame-se-osobne-40-deti-na-internetu-by-souhlasilo

[online]. [cit. 2014-08-06]. Dostupné z: http://www.lupa.cz/clanky/zavislost-na-internetu-bluf-ci-realita/

[online]. [cit. 2014-08-15]. Dostupné z: http://www.slunecnice.cz/special/bezpecnost-deti/pro-deti-nevhodny-obsah-a-jeho-filtrovani/

[online]. [cit. 2014-08-01]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/e-mail/phishing.aspx

Poznámky: