Nebezpečí kyberprostoru

(kybergrooming a sexting)

Anotace

V posledních letech nastal velký rozvoj v oblasti informačních a komunikačních technologií, které vytváří tzv. kyberprostor. Tento kyberprostor přináší velké možnosti a výrazně ulehčuje život. Zároveň však s sebou přináší velké množství nástrah a rizik. Díky těmto vyspělým technologiím žijeme nejen skutečné životy, ale i ty virtuální, skryté za přezdívkami a příběhy. Můžeme mít přátele z různých zemí bez ohledu na národnost, věk či etnickou příslušnost. Na druhé straně takovéto anonymní prostředí představuje možné nebezpečí a může vést až k vážné újmě. Technologie se mohou stát mocnou zbraní, která nás může vážně ohrožovat. Samy o sobě nejsou ani dobré, ani špatné. Záleží jen na lidech, k čemu je použijí. Proto musíme být na tato četná rizika připraveni. Obzvláště děti, rodiče a pedagogové.
Cílem mého příspěvku je upozornit na nebezpečí spojená se zneužíváním kyberprostoru převážně se sexuálním podtextem a představit některé instituce, které se danou problematikou zabývají a nabízí pomoc.

KYBERPROSTOR VS. KYBERŠIKANA

Kyberprostor je označení pro virtuální svět vytvořený moderními technologickými prostředky. Nejčastěji využívané elektronické prostředky jsou mobilní telefony, videoportály, e-maily, chaty, instant messaging, blogy, webové stránky, sociální sítě a jiné internetové služby. Jedním z hlavních projevů zneužívání těchto prostředků je kybernetická šikana, tzv. kyberšikana. Kyberšikana se stává fenoménem dnešní doby. Téměř každý týden se v médiích objeví nová kauza a závažnost projevů kyberšikany narůstá. Málokteré sociálně patologické chování se šíří s takovou rychlostí a je tak variabilní, jako kyberšikana.

Aspekty, které napomáhají zneužití kyberprostoru:
Anonymita útočníka. Jeho anonymita je sice jen zdánlivá, ale vzbuzuje v něm odvahu a pocit, že je nepostižitelný. Pomocí specifických znalostí a s využitím potřebných technologií (např. sledováním IP adres, proxy serverů nebo paketů) lze totožnost útočníků ve většině případů odhalit. Každý účastník kyberprostoru po sobě zanechává množství „kyberotisků“, datových stop, které se dají vysledovat. Přesto bývá obecně velmi obtížné útočníka vystopovat.
Lehce dostupné nástroje. Informační a komunikační technologie, především mobilní telefony a internet, jsou velmi rozšířené a lehce dostupné (cenově i místně). Díky těmto nástrojům je velké množství vzájemně propojeno a nástroje vznikají rychleji než pravidla, ICT umožňují snadný přístup k oběti.
Riskantní chování lidí ve virtuálním světě. Ve virtuálním světě se někteří lidé chovají méně opatrně, než v reálném světě (jsou odvážnější v komunikaci, probírají citlivá témata, komunikují často bez zábran apod.). Zatímco v reálném životě jsme vychováváni před různými nástrahami k opatrnosti, informovanost o virtuálním nebezpečí je minimální. Mezi jednoznačně rizikové chování patří sdílení osobních údajů, fotografií a videozáznamů. Další velkou chybou je, že uživatelé nečtou smluvní podmínky služeb, které používají, a často ani netuší, co všechno správci služby umožnili.
Velké množství diváků a sekundárních útočníků. Používání ICT je pro mnohé nezbytnou součástí života. Potřebujeme je téměř denně. Útočník nemusí oběť napadat opakovaně, stačí, když citlivé zprávy nebo nahrávky publikuje na internetu a o jejich šíření se pak postarají ostatní. Tito lidé pak sehrávají jednak roli diváků, ale také sekundárních útočníků, protože úmyslně či neúmyslně rozesílají materiály dál. Tím se podílejí na zvyšování intenzity útoku na oběť.

Nedostatečná prevence. Nástroje ICT vznikají rychleji než obecně známá pravidla obdobná těm, jimiž se řídíme v běžném, nevirtuálním životě. Obecně platí, že děti se s novými technologiemi seznamuji rychleji než dospělí, tedy jejich rodiče a učitelé, Tato situace ztěžuje dospělým pozici v oblasti výchovy a prevence bezpečného používání kyberprostoru.
Na zneužívání kyberprostoru se také podílí nízká informovanost o rizicích ve společnosti a absence koncepce prevence.
Posun společenských hranic. Společenské hranice se výrazně posunuly k větší lhostejnosti, otevřenosti v sexualitě, toleranci k násilí a agresi. V této atmosféře je samozřejmě velmi obtížné stanovit etické normy kyberprostoru a vyžadovat jejich dodržování.

SPECIFICKÉ PROJEVY KYBERÚTOKŮ

- **Cyberbullying (kyberšikana)**

Tímto termínem je označován druh šikany, který zneužívá elektronické prostředky k poškození oběti. Vždy se jedná o psychickou újmu. Mezi její nejobvyklejší projevy patří zasílání obtěžujících, urážejících či útočných emailů a sms, vytváření stránek a blogů ponižujících jednotlivce či skupinu, popřípadě může kyberšikana sloužit k posilování klasických forem šikany, nejčastěji prostřednictvím nahrání scény na mobilní telefon a jejího následného rozeslání známým dotyčného, popřípadě vystavení na internetu.

- **Flaming (provokování)**

Jedná se o online útoky pomocí elektronických zpráv s urážlivým a vulgárním obsahem, které mají za úkol oběť provokovat a vtáhnout ji do podobného způsobu komunikace.

- **Harassment (obtěžování)**

Takto je označené opakované odesílání sprostých, drzých a urážlivých zpráv, opakované prozvánění nebo volání.
Příkklad: žákyně oznámila řediteli, že spolužák šikanuje jiného studenta. Během cesty ze školy domů jí přišlo velké množství výhružných zpráv z neznámého telefonního čísla.

- **Denigration (ponižování a pomlouvání)**

Jedná se o rozesílání pomluv nebo výmyslů o oběti v rámci sociálních sítí, blogů, nebo jiných webových stránek. Cílem útočníka je poškodit reputaci oběti a narušit její vztahy s přáteli. Čím dál tím víc toto chování postihuje dospělé osoby.

- **Impersonation (krádež identity)**

Je to označení pro zneužití cizí identity ke kyberšikaně nebo k jinému rizikovému chování (např. zcizení elektronického účtu).
Různé typy útoků na cizí účet nebo jeho zneužití

1. Manipulace s profily (zveřejňování nepravdivých/pomlouvačných informací o majiteli…).
2. Mazání kontaktů a zpráv.
3. Rozesílání zpráv s nevhodným obsahem jménem majitele účtu (např. urážky, záměrně chybně vypracované úkoly, zprávy s xenofobním nebo rasistickým obsahem, dětskou pornografií atd.).
4. Zneužití osobních údajů a kontaktních údajů k účtu – nejčastěji se jedná o přihlašování do různých služeb a aplikací (seznamky nebo pornoseznamky), objednávání zboží pomocí e-shopů, zneužití účtu k páchání trestné činnosti.

- **Fishing** (rybaření)

Je to jedna z metod krádeže identity. V tomto případě se jedná o získávání citlivých dat od uživatelů, která jsou následně zveřejněna bez uživatelova vědomí. Viz e-maily vypadající důvěryhodně např. od neznámých bank vyžadující si citlivé údaje od uživatele. S touto činností úzce souvisí **pharming,** kdy se jedná o podvodné stránky, které si žádají vaše osobní informace pro registraci. Tudíž je třeba doporučit všem, kteří se chtějí na podobných stránkách registrovat, aby byli velmi opatrní.

- **Outing (odhalování)**

Jedná se o online zveřejňování cizích tajemství, intimních nebo ztrapňujících informací nebo obrázků. Může se jednat např. o situaci, kdy chlapec natočí svým mobilním telefonem kamaráda při převlékání. Záznam pak přepošle ostatním kamarádům a během chvíle záznam obletí celou školu.

- **Trickery (podvádění)**

Podvádění někoho ve snaze zjistit jeho tajemství nebo informace, které by ho mohly ztrapnit, a ty pak následně sdílet online.
Příklad: Dívka poslala své spolužačce zprávu, ve které předstírala, že chce být její kamarádkou. Vyptávala se jí na spoustu věcí. Ta odpovídala i na skutečně osobní otázky. Dívka pak jejich vzájemnou komunikaci přeposlala dalším lidem se svým vlastním komentářem, kde spolužačku označila za „ubožačku“.

- **Exclusion (vyloučení)**

Označení pro záměrné a hrubé vyloučení nějaké osoby z online skupiny.
Může se jednat např. o situaci, kdy se dívka snaží zapadnout do dívčí party ve škole. Následně je vyloučena vůdkyní party a všechny dívky z party si zablokují online kontakt s ní.

- **Cyberstalking (pronásledování, kybernetický lov)**

Takto je označováno opakované intenzívní obtěžování a ponižování spojené s vyhrožováním nebo zastrašováním.
Příklad: Je možno uvést situaci, kdy se dívka rozejde s chlapcem. Ten ji posílá mnoho zlostných, výhružných a prosebných zpráv. Rozšiřuje o ní a jejich přátelích nechutné výmysly. Zveřejňuje její sexuálně vyzývavé fotografie v sexuálně orientovaných diskuzních skupinách spolu s její emailovou adresou a telefonním číslem.

- **Vydírání**

Útočník využívá kyberšikanu k vydírání oběti, čímž se snaží dosáhnout svých záměrů.

- **Kybergrooming**

V tomto případě jde o chování uživatelů v kyberprostoru, které má v dítěti vyvolat falešnou důvěru a připravit ho na schůzku, jejímž cílem je zneužít dítě.

- **Ztrapňování pomocí falešných profilů.**

Jedná se o situaci, kdy se útočník vydává za někoho jiného, rozesílá jeho jménem nevhodné zprávy a jiné materiály ve snaze dostat ho do problémů nebo ho ohrozit či poškodit jeho pověst a vztahy.

- **Happy slapping (fackování pro zábavu)**

V tomto případě hovoříme o nečekaném fyzickém napadení (někdy i znásilnění) osoby spojené s nahráváním na mobilní telefon nebo kameru. Získané video je poté publikováno na internetu.
Jako příklad můžeme uvést situaci, kdy se skupina chlapců domluví a fyzicky napadnou jiného spolužáka nebo bezdomovce. Jeden z nich celou situaci natáčí na mobilní telefon a následně ji zveřejní na internetu.

- **Hoax**

Jde o falešnou zprávu, kterou útočník zveřejní na sítích, blogu apod. Nebo se může jednat o poplašnou zprávu, která má šířit paniku (upozornění na neexistující viry, zapíchnuté injekce v tramvaji apod.).

- **Sexting**

Využívání informačních technologií k rozesílání zpráv se sexuálním podmětem. Jedná se i o rozesílání lechtivých fotografií. Po rozchodu se může stát, že tyto fotografie jedna strana uveřejní. Sexting podporuje šíření mladistvé pornografie, a proto jej považuji za jednu z nejzávažnějších aktivit v kyberprostoru.

NEBEZPEČÍ KYBERGROOMINGU

Tímto termínem je označováno zneužívání moderních komunikačních technologií k psychické manipulaci s cílem získat důvěru oběti, vylákat ji na osobní schůzku a zpravidla sexuálně zneužít.

Přátelství online

Kybergroomingu výrazně nahrává snaha obětí získat na internetu přátele. Mnoho mladých lidí, ať už zletilých či nezletilých, hledá přátelství v online prostředí. Je to pro ně skvělá představa a často i výzva. Online přátelství má mnoho výhod. Na online přátele se nemusí čekat, člověk nemusí nikam chodit, stačí se připojit k internetu, vstoupit do chatovací místnosti a přidat se k ostatním. Velmi často se stává, že mladí lidé podlehnou iluzi, že potkali toho pravého kamaráda, přítele.Ve skutečnosti se jedná o dospělého člověka se sexuálními úmysly, který využívá uměle vytvořeného pocitu těchto mladých lidí že jsou milováni a že je má někdo rád k tomu, aby je vylákal na schůzku.

Útočníci jsou tedy často pedofilové. Zpravidla se chovají velmi podobně. Nejprve si útočník vytvoří falešnou identitu, a to převážně dvojím způsobem: jednu tzv. statickou identitu, prostřednictvím které oslovuje vybrané oběti (například uživatelský profil na facebooku), nebo si svou identitu upravuje podle toho, s kým komunikuje, to je vytvoří tzv. dynamickou identitu. Převážně vystupuje pod několika přezdívkami/nicky/avatary. Účelově si upravuje osobní údaje, záliby, zájmy, případně i pohlaví tak, aby oslovil vybranou oběť co nejefektivněji. Často komunikuje s více oběťmi současně a musí si pamatovat, co komu sdělil. Této situace se dá využít k prevenci a ochraně. V případě, že si oběť všimne rozporů ve virtuální komunikaci (např. uživatel opakovaně uvede různý věk, jméno či jiné údaje), může se jednat o signály toho, že komunikuje s kybergroomerem.

Následně se útočník snaží v dítěti vzbudit důvěru, po určitém čase se snaží o uplácení různými dárky a dítě po čase svolí k setkání. V průběhu online konverzací může útočník požadovat po obětech, aby si sundaly oblečení, navádět je k účasti na sexuální činnosti, provozovat sexuální aktivity v jejich přítomnosti nebo je nutit ke sledování sexuálního aktu. Není vůbec jednoduché tyto lidi odhalit a vypátrat. Groomer s obětí často komunikuje přes internet i několik měsíců. Někdy stačí, aby dostatečně dlouho působil na svou oběť a zahrnoval ji svou pozorností tak, až si na něm vytvoří těžko odbouratelnou emocionální závislost. Převážně děti s nízkým sebevědomím, které nemají dostatek přátel, trpí absencí vztahů a sdílením intimity, jsou pro něj snadnou kořistí

V případě, že se mu nedaří oběť přesvědčit ke schůzce, začne používat nátlak ve formě vyhrožování zveřejněním choulostivých fotografií a videí. V tomto případě již mluvíme o kyberšikaně.

Typické chování kybergroomera

- Je neobyčejně trpělivý.
- Komunikuje se svou obětí i několik měsíců, někdy i přes rok, než se odhodlá zjednat si schůzku ve skutečném světě.
- Tváří se neobyčejně přátelsky.
- Výrazně se zajímá o rozvíjení vzájemného vztahu s obětí.
- Má zájem vztah udržet z větší části, pokud ne celý, v tajnosti.
- Bude hovořit o milujícím vztahu. Často se bude v konverzaci bavit o významu skutečné lásky.
- Bude hovořit o tom, že tento vztah bude pokračovat, jakmile se v reálném světě s obětí potká.
- Do konverzace vkládá i témata sexuální povahy.

- Často žádá o fotografie.
- Vyžaduje cybersex s použitím web kamery apod.

Etapy manipulace dítěte

1. Příprava kontaktu - falešná identita.
2. Kontakt s obětí, navázání a prohlubování vztahu .
3. Snaha získat co nejvíce osobních informací o oběti (fishing).
4. Vábení a uplácení oběti (luring).
5. Snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace.
6. Snahy o izolaci oběti od okolí.
7. Příprava na osobní schůzku.
8. Osobní schůzka.
9. Útok na oběť.

Desatero obrany

1. Přemýšlejte zda „online přátelství“ není až moc perfektní na to, aby to mohla být pravda.
2. Ukládejte si kopie vašich rozhovorů, abyste mohli rozpoznat jakékoli nesrovnalosti např. změnu svého věku nebo dalších údajů.
3. Zvažte, proč chce udržet vztah v tajnosti, proč se vás ptá na osobní a intimní údaje.
4. Sami si vytyčte své osobní hranice s ohledem na rozhovory o sexu a věřte svým rozhodnutím. Nebojte se odmítnout kybersex.
5. Nenechte se oklamat sliby naplňujícího, milujícího vztahu. Většinou tytéž věci zároveň slibují několika dalším mladým lidem.
6. Neposkytujte své osobní informace lidem, které jste zrovna potkali v online prostředí, na chatu, při užívání ICQ, skype apod.
7. Online přátelství jsou nejlepší, když zůstanou online, a je naprosto v pořádku odmítnout osobní setkání tváří v tvář.
8. Pokud se rozhodnete pro osobní setkání, řekněte to rodičům nebo aspoň kamarádům.
9. Schůzku si domlouvejte na veřejných prostranstvích, nesedejte do auta, nechoďte do soukromého bytu.
10. Do profilu na chat si dej nic neříkající fotku, neuváděj věk, budete tak nezajímaví a krytí.

SEXTING

Poměrně nový fenomén, který je spojen s využíváním informačních a komunikačních technologií mladistvými a dětmi, je tzv. **sexting** (česky sextování). Je jedním z nejrozšířenějších jevů v komunikaci mladých lidí. Termín sexting označuje rizikové odesílání sexuálně laděných zpráv, fotografií či videozáznamů, jehož cílem je nejčastěji navázání partnerského vztahu mezi odesilatelem a příjemcem nebo jeho zpestření. Lidé vlastně šíří své vlastní materiály, aniž si uvědomují rizika, kterým mohou být vystaveni.
Sexting podporuje šíření pornografie mladistvých a dětí, které je celosvětově zakázáno. Přestože stále přibývá případů, které upozorňují na nebezpečí této aktivity, zdá se, že to pořád nestačí.
Odborníci uvádějí, že největšími šiřiteli dětské pornografie jsou sami dospívající děti. Ve velké většině si to ale ani neuvědomují. V poslední době se pořizování intimních a vyzývavých fotografií stává součástí virtuální intimity mladých lidí. Dívky ve snaze zapůsobit na oblíbeného chlapce neváhají posílat erotické a choulostivé fotky či video. Náklonnost není většinou opětována a chlapec intimní materiály pošle dál svým kamarádům. Teenageři neváhají sdílet obscénní komentáře se svými vrstevníky na webu, fotí se nazí či ve spodním prádle . Fotografie následně dávají k dispozici na internetu. Odborníci v Česku vypozorovali

nový trend. Mladiství se na internetu sami nabízejí. Zveřejňují tu svoje intimní fotografie nebo se dobrovolně ukazují polonazí v choulostivých situacích na webových kamerách. „Dříve bylo víc útočníků, dnes je situace opačná. Je víc dětí, co se nabízejí, já říkám, že jsou největším výrobcem a distributorem pornografie, byť to neudělají úmyslně. My to máme odzkoušeno, získat pornografii od dětí trvá 5 minut, sehnat dítě na erotickou schůzku trvá 3 minuty," potvrdil manažer pro internetovou bezpečnost Seznam.cz Martin Kožíšek.*
* Online na: http://www.ceskatelevize.cz/ct24/domaci/215677-odbornici-varuji-teenageri-jsou-nejvetsimi-siriteli-detske-pornografie/ Cit. 26. 8. 2013

K takovému chování mimo jiné mladé lidi inspiruje dnešní svět reklamy a hudebních klipů, kde se k získání pozornosti využívá dráždivé předvádění ženského těla. Čím odvážnější, tím lepší, a hranice se stále posouvají.
Být provokativní je dnes zkrátka in. Je třeba si to přiznat a podle toho s mladými jednat. Nejde o moralizování, ale o upozornění na reálný stav. Jakmile se jednou intimní materiál objeví na internetu, velice obtížně se z něj odstraňuje.
Výzkum, zaměřený na rizikové chování ve virtuálních prostředích (zejména na internetu), který realizoval v průběhu loňského roku výzkumný tým Centra PRVoK PdF a projektu E-Bezpečí, se mimo jiné zaměřil také na fenomén sexting.
Z odpovědí vyplynulo, že 10,44 % českých dětí alespoň jednou odeslalo někomu dalšímu sexuálně laděnou fotografii nebo videozáznam. 9,15 % dětí má takové vyobrazení zveřejněno volně na internetu.
Výsledky šetření „Internet a české děti ve věku od 9 do 16 let„

- 29 % navštívilo pornografickou stánku
- 42 % se na internetu seznámilo s cizím člověkem
- 13 % z nich se s ním následně sešlo osobně

http://www.e-bezpeci.cz/index.php/temata/sexting/237-ceske-deti-o-sextingu71
Neopatrní bývají ale i rodiče. Lehkomyslně umísťují na internet fotografie svých nahých dětí z dovolených, rodinných oslav apod. Neuvědomují si, že snímky může někdo zneužít i za deset, dvacet let, kdy jejich potomek bude dospělý.

Jak se bránit?
Obrana je velmi obtížná. Na prvním místě je prevence, hlavně rodiče by se měli zajímat, co jejich dítě na internetu dělá, promluvit si s ním a poučit ho o nebezpečí, která mu hrozí. Dalším opatřením je dostatečná softwarová ochrana počítače před útoky hackerů. Pokud dojde k zneužití intimního materiálu, je nutné jej co nejdříve zablokovat/smazat. Více na online: http://www.e-bezpeci.cz/index.php/rodice-ucitele-zaci/546-prvnipomoc
Další doporučení:

- Neposílat nikomu, koho neznáme, svou fotografii zvlášť ne intimní.
- Udržovat hesla k e-mailu i jinam v tajnosti, nesdělovat je ani blízkému kamarádovi.
- Neodpovídat na neslušné, hrubé nebo vulgární maily a vzkazy.
- Informovat rodiče, nebo jinou dospělou osobu, pokud se objeví vaše nevhodné snímky na internetu.

KDE HLEDAT POMOC

Linka bezpečí ONLINE (Internet Helpline)
Je to asistenční služba zřízená Sdružením Linka bezpečí a je součástí projektu mezinárodního projektu Safer Internet Plus. Jde o první obdobně specializovanou linku krizové intervence v ČR.

Kontakty: www.pomoconline.cz e-mail: pomoc@linkabezpeci.cz, telefon: +420 116 111, +420 800 155 155
Online na: http://www.pomoc-online.cz/teprve-se-rozhlizim/hledas-pomoc Cit. 26. 8. 2013

Projekt E-Bezpečí
Projekt E-Bezpečí Pedagogické fakulty Univerzity Palackého v Olomouci se zabývá problematikou nebezpečných komunikačních jevů spojených s používáním ICT
Kontakty: www.e-bezpeci.cz**,** www.napisnam.cz e-mail: info@e-bezpeci.cz
Online na: http://www.e-bezpeci.cz/index.php/kontakt Cit. 26. 8. 2013

Národní centrum bezpečnějšího internetu (Safer Internet)
Zahrnuje moduly:
Safer Internet Awarenod/Helpline (Osvětové a asistenční centrum bezpečnějšího internetu) provádí osvětu s cílem zvýšit povědomí o bezpečnějším užívání internetu a zároveň poskytuje dětem podporu ve formě psychologické a sociální pomoci v osvojování si zásad bezpečné práce, získávání informací, chatování, brouzdání a pomoci cítit se na internetu bezpečně.
Safer Internet Hotline (internetová horká linka) bojuje proti ilegálnímu obsahu, umožňuje občanům České republiky hlásit nelegální obsah, především dětskou pornografii a další formy komerčního a sexuálního zneužívání dětí a předávat oznámení příslušným činným orgánům
Kontakty: www.saferinternet.cz
Online na: http://www.e-bezpeci.cz/index.php/kontakt Cit. 26. 8. 2013

Poradenská linka pro pedagogy
Tato linka je určena primárně pedagogickým pracovníkům v rámci celé České republiky, kterým je nápomocna výlučně při řešení problémových výchovných situací týkajících se školního prostředí. Telefonická linka je zcela anonymní. Je k dispozici v pracovních dnech od 8:00 do 16:00.
Kontakty: http://www.msmt.cz/ministerstvo/poradenska-linka-pro-pedagogy,
telefon: +420 841 220 220, +420 777 711 439
Online na: http://www.msmt.cz/ministerstvo/poradenska-linka-pro-pedagogy Cit. 26. 8. 2013

Úřad na ochranu osobních údajů
Úřad na ochranu osobních údajů je nezávislým orgánem, který provádí dozor nad dodržováním zákonem stanovených povinností při zpracování osobních údajů, vede registr povolených zpracování osobních údajů, přijímá podněty a stížnosti občanů na porušení zákona a poskytuje konzultace v oblasti ochrany osobních údajů.
Kontakty: www.uoou.cz**,** e-mail: posta@uoou.cz, telefon: +420 234 665 212
Poradenská linka pro pedagogy.
Online na: http://www.uoou.cz/uoou.aspx?menu=321 Cit. 26. 8. 2013

Nebuď oběť
Občanské sdružení Rizika internetu a komunikačních technologií (alias Nebuď oběť!) se zaměřuje na preventivní osvětu žáků základních škol, pedagogů a rodičů v problematice nebezpečného užívání Internetu a komunikačních technologií. Varuje před možným zneužitím osobních údajů a seznamuje s novými fenomény kyberprostoru, jakými jsou například sexting, grooming, phishing, happy slapping. Věnujeme se natáčení videoklipů, tvorbě komixů a vzdělávacích programů, realizaci přednášek a mezinárodně kooperačních projektů.
Kontakty: http://www.nebudobet.cz, e-mail: nebudobet@email. cz,
telefon +420 774 242 507.
Online na: http://www.nebudobet.cz/?page=editorial Cit. 24. 8. 2013

Policie ČR
Kontakty: www.policie.cz **,** telefon +420 158
Online na: http://www.policie.cz/imapa.aspx Cit. 26. 8. 2013
Den bezpečnějšího internetu
Den bezpečnějšího internetu každoročně vyhlašuje evropská síť Insafe. Ta sdružuje organizace, které propagují bezpečné užívání sítě a mobilů. V Česku je to Národní centrum bezpečnějšího internetu.

Projekt IN(ternet) Generation
První ucelený projekt nabídne rodičům, učitelům i dětem nástroje pro zvýšení internetové gramotnosti Spuštěním webové stránky www.in-generation.cz začíná projekt IN(ternet) Generation, který připravil a realizuje institut ELAI (European Leadership & Academic Institute), www.elai.cz, ve spolupráci s českým Googlem a pod záštitou Ministerstva školství, mládeže a tělovýchovy. Hlavním cílem projektu je přinést dětem ve věku 9-15 let vzdělávání v oblastech etického, efektivního, pokročilého a bezpečného užívání internetu, který by měl sloužit jako pilot pro širší užití v zemích EU.*
* Online na: http://www.e-bezpeci.cz/index.php/component/content/article/693-prav-startuje-projekt-internet-generation Cit. 26. 8. 2013

DŮLEŽITÉ ONLINE ZDROJE A KONTAKTY:
www.saferinternet.cz
www.bezpecne-online.cz
www.horkalinka.cz
www.pomoconline.cz
www.sikana.org
www.nebudobet.cz
http://www.csicr.cz
http://www.csicr.cz/cz/Rodice/Na-co-se-casto-ptate/Sikana
www.e-bezpeci.cz
http://aplikace.policie.cz/hotline
http://www.nasedite.cz/
http://www.nasedite.cz/cs/projekty/internet_hotline
http://www.internethelpline.cz/
http://www.ovce.sk/projekt.phtml/
http://www.lupa.cz/
http://www.chovani.eu/
http://www.bkb.cz/
http://www.minimalizacesikany.cz/pribehy-ostatnich-zaku/
http://www.internethotline.cz/
http://www.saftonline.org/
http://www.minimalizacesikany.cz/
http://www.sikana.org
http://www.seznamsebezpecne.cz/

Metodický pokyn k prevenci a řešení šikanování mezi žáky. MŠMT. Online na: http://www.msmt.cz/vzdelavani/socialni-programy/metodicky-pokyn-k-sikanovani
Projekt Minimalizace šikany. Online na: http://www.minimalizacesikany.cz/

Beránek, J. Nová móda: Násilníci si točí své oběti mobilem. Idnes.cz, 2006. Online na: http://mobil.idnes.cz/nova-moda-nasilnici-si-toci-sve-obeti-mobilem-f3x-/mob_tech.aspx?c=A060815_155555_mob_tech_brz

Další odkazy a zdroje

Padesátka zemí bojuje proti zneužívání dětí na internetu
Pedofil se vydával za školačku, dívky mu pak posílaly erotické fotky
Evropský zátah proti dětské pornografii - stovky podezřelých
Na internetu přibývá případů obtěžování dětí
Odborníci varují: Teenageři jsou největšími šiřiteli dětské pornografie
http://www.sexting.cz/
http://www.prvok.upol.cz/
http://www.e-bezpeci.cz/
http://clanky.rvp.cz/clanek/o/z/9673/STRUCNY-UVOD-DO-PROBLEMATIKY-BEZPECNEHO-INTERNETU.html
http://www.bezpecne-online.cz/surfuj-bezpecne/komunikace-se-svetem/sexting
http://aktualne.centrum.cz/zpravy/krimi/clanek.phtml?id=632277
http://www.rightcelebrity.com/?p=5477
http://www.mahalo.com/jesse-logan

Videa

Odborníci varují: Teenageři jsou největšími šiřiteli dětské pornografie
Seznam se bezpečně (1, 2)
NET-Story video o příběhy o nebezpečí v kyberprostoru
http://www.youtube.com/watch?v=DtdaEggUDPI
http://www.youtube.com/watch?v=rZTgyFmTVdc
http://www.youtube.com/watch?v=D6HE-fihpjU
Jít či nejít ke stažení (http://www.e-bezpeci.cz/index.php/ke-stazeni/cat_view/43-e-bezpei-dvd)
http://www.nebudobet.cz/?page=videa

Doporučená literatura:

Kolář, M.: Nová cesta k léčbě šikany. Portál, Praha, 2011
Hulanová, L.: Internetová kriminalita páchaná na dětech, psychologie internetové oběti pachatele a kriminality. Triton, Praha, 2012
Vágnerová, M.: Psychopatologie pro pomáhající profese. Portál, Praha, 2004
Šámal, P. a kol.: Trestní zákoník. C. H. Beck, 2009
Nešpor K.: Návykové chování a závislost. Portál, Praha, 2011
Rogers V.: Kyberšikana: Pracovní materiály pro učitele a žáky i studenty. Portál, Praha, 2011
Kol. aut.: Jak zvládnout kyberšikanu, metodický materiál. NCBI, 2010

POUŽITÉ ZDROJE:

Encyklopedie Vševěd
Online: http://encyklopedie.vseved.cz/sextov%C3%A1n%C3%AD
Čermák, M. Dětská pornografie je fakt hnusná. Ale jakou jinou mají dělat děti?
Online: http://extra.cz/blog/2009/04/detska-pornografie-je-fakt-hnusna-ale.html
http://cs.wikipedia.org/wiki/Cyber_grooming
http://cms.e-bezpeci.cz/content/view/70/63/lang,czech/
K. Kopecký - Moderní trendy v elektronické komunikaci E-Bezpečí. O projektu. Online na: http://cms.e-bezpeci.cz/content/view/15/60/lang,czech/

1Safer Internet. O projektu. Online na: http://www.saferinternet.cz/o-projektu/80-3
www.saferinternet.cz www.ncbi.cz www.bezpecne-online.cz
Mašková A., Lukášová K., Pacák, R. a Brandejsová, J.: Kyberšikana ve školním prostředí. Online na: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy
Mašková A., Lukášová K., Pacák, R. a Brandejsová, J.: Kybergrooming s kyberstalking. Online na: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy

http://www.e-bezpeci.cz/index.php/temata/kybergrooming/125-42
http://www.e-bezpeci.cz/index.php/temata/kyberikana/17-cojekybersikana
http://www.e-bezpeci.cz/index.php/temata/sexting/137-154
http://www.e-bezpeci.cz/index.php/temata/socialni-sit
http://www.nebudobet.cz/?page=kybergrooming
http://www.nebudobet.cz/?page=sexting
http://www.nebudobet.cz/?page=vyzkum
http://www.ceskatelevize.cz/vysilani/31.08.2008/208411058250831-21:45-1-168-hodin-pedofil-lovil-na-internetovych-strankach-25-zneuzitych-deti.html?streamtype=RH
http://tn.nova.cz/zpravy/krimi/davejte-pozor-na-deti-na-webu-lovi-pedofilove.html

Použitá literatura

Bendl, S,: Prevence a řešení šikany ve škole. Praha : ISV, 2003
Kolář, M.: Bolest šikanování. Praha, Portál, 2001
Říčan, P.: Agresivita a šikana mezi dětmi: jak dát dětem ve škole pocit bezpečí. Praha, Portál, 1995
Krejčí, V.: Kyberšikana. Kyberbetická šikana. Olomouc, 2010
Kopecký, K.: Kybergrooming nebezpečí kyberprostoru.Olomouc, 2010