Uherské Hradiště
Srdce Slovácka

Kybergrooming

1. CO JE KYBERGROOMING?

Termín kybergrooming označuje chování uživatelů internetu (predátorů, kybergroomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce. Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod.

Kybergrooming je druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií. Často je vázán na synchronní i asynchronní komunikační platformy, nejčastěji veřejný chat, internetové seznamky, instant messengery a VoIP (např. ICQ, Skype) a v posledních letech také na sociální sítě (Facebook, Twitter, MySpace, Bebo a další). Internetoví predátoři využívají také inzertní portály, na kterých nabízející dětem různé možnosti výdělku či kariéry (např. v oblasti modelingu), často navštěvují portály zaměřené přímo na nezletilé uživatele internetu (dětské portály, portály zaměřené na volnočasové aktivity, herní portály a další internetové stránky).

2. KDO JSOU OBĚTI?

Oběťmi kybergroomingu jsou zpravidla děti nejčastěji ve věku 11-17 let. Častěji se jedná o dívky než o chlapce. Lze předpokládat, že oběti tvoří zejména ti uživatelé internetu, kteří tráví velké množství volného času v online komunikačních prostředích (chat, instant messengery, sociální sítě), kde také navazují virtuální kontakty s ostatními (hledají zde kamarády, přátele, životní partnery). V posledních letech se také objevuje stále více případů kybergroomingu, ke kterým došlo na některé ze sociálních sítí (Facebook, MySpace, Twitter apod.). Ty díky propracovanému systému virtuálních sociálních vazeb poskytují ideální podmínky pro realizaci kybergroomingu. Děti a mládež jsou k manipulaci náchylnější zejména proto, že dosud nemají plně rozvinuté sociální dovednosti a mají nedostatek životních zkušeností.

Nejčastější typy obětí

Děti s nízkou sebeúctou nebo nedostatkem sebedůvěry (lze je snadněji citově či fyzicky izolovat). Děti s emocionálními problémy, oběti v nouzi (často hledají náhradu za své rodiče a potřebují pomocnou ruku). Děti naivní a přehnaně důvěřivé (jsou ochotnější zapojit se do online konverzace s neznámými lidmi, obtížněji rozpoznávají rizikovou komunikaci). Adolescenti/teenageři (zajímá je lidská sexualita, jsou ochotni o ní hovořit).

3. KDO JSOU ÚTOČNÍCI?

Kyberútočníci (predátoři) tvoří heterogenní skupinu, ve které nalezneme uživatele s nízkým i vysokým sociálním statutem (právníci, učitelé, policisté). V řadě případů oběť pachatele zná a je na něm závislá, často bývá útočníkem také známý rodiny oběti. Mezi útočníky dle výzkumů převažují osoby, které dosud nebyly trestány. Kybergroomery se ale někdy stávají i ti, kteří již byli za sexuální útoky proti dětem a mladistvým odsouzeni a došlo u nich k recidivě. U většiny útočníků byl diagnostikován patologický zájem o děti. Chování útočníků - kybergroomerů - vysvětluje například model sociálních dovedností, podle něhož útočníci

navazují kontakty s dětmi, protože mají strach z navazování vztahů s dospělými. Vztahy s dětmi kybergroomeři vnímají jako méně ohrožující, cítí se bezpečněji než ve vztazích s dospělými. Kybergroomeři často vytvářejí sítě, ve kterých vzájemně spolupracují. Spolupodílejí se například na únosech dětí - dítě je manipulací donuceno k osobní schůzce, následně uneseno a převezeno na území jiného státu, kde je dále sexuálně zneužíváno, využíváno k výrobě dětské pornografie, fyzicky týráno apod. Sítě predátorů často shromažďují osobní profily obětí do databází, které pak využívají ostatní členové sítě.

4. ETAPY MANIPULACE DÍTĚTE

Psychická manipulace v rámci kybergroomingu probíhá obvykle delší dobu - od cca 3 měsíců po dobu několika let. Tato doba je přímo závislá na způsobu manipulace a na důvěřivosti oběti. Proces manipulace dítěte prochází čtyřmi základními etapami (příprava kontaktu - kontakt s obětí - příprava na osobní schůzku - osobní schůzka), během kterých může útočník využít velké množství technik a postupů.

Příprava kontaktu

V této etapě útočník připravuje podmínky pro realizaci manipulace oběti.

Falešná identita

Jedním z velmi často pozorovaných postupů útočníka - kybergroomera je vytvoření falešné identity. Útočník o sobě uvádí nepravdivé osobní údaje, jako jsou jméno, příjmení, věk či fotografie obličeje. Manipulátoři jsou obvykle podstatně starší než vyhlédnuté oběti, proto si svůj věk dle potřeby upravují a doplňují o odpovídající fotografie. Identita útočníka může existovat v několika základních formách:

- **Statická identita** - útočník si vytvoří jednu falešnou identitu, prostřednictvím které oslovuje vybrané oběti (například uživatelský profil na Facebooku).
- **Dynamická identita** - Útočník si svou identitu upravuje dle potřeby, může tedy vystupovat pod několika přezdívkami/nicky/avatary. Účelově si dokáže přizpůsobovat věk, záliby a zájmy, případně i pohlaví a další osobní údaje tak, aby oslovil vybranou oběť co nejefektivněji. Útočník s dynamickou identitou často komunikuje s více oběťmi současně, musí si tedy pamatovat či evidovat, co komu sdělil. Udržet dynamickou identitu je pro útočníka podstatně náročnější než u identity statické, což se může projevit tím, že si útočník zamění oběť, se kterou právě komunikuje, za jinou. Pokud tedy oběť zaznamená ve virtuální komunikaci zjevné rozpory (např. uživatel opakovaně uvede různý věk, jméno či jiné údaje), může se jednat o signály toho, že komunikuje s kybergroomerem.
- **Falešná autorita** - Někdy útočníci nevystupují jako fyzické osoby, ale jako představitelé firem (jednatelé, ředitelé, manažeři), které vytipovaným obětem (dětem) přinesou nějaký užitek. Nalezneme případy, kdy útočník předstíral, že je jednatelem firmy zaměřující se na finanční pomoc sociálně slabým dětem. Jménem této firmy pak navazoval kontakty s potenciálními oběťmi pomocí internetových inzerátů. Autorita firmy (i když fiktivní) dodala informacím šířeným internetem na věrohodnosti.

Inzerát útočníka by mohl vypadat například takto:

Uherské Hradiště
Srdce Slovácka

Ahoj kamarádi. Je vám méně než 15 let? Máte rádi počítače? Rádi brouzdáte internetem? Zapojte se do naší soutěže a vyhrajte atraktivní ceny. Stačí, když nám zašlete vaše jméno a příjmení, emailovou adresu a telefonní číslo a budete zařazeni do slosování. Těšit se můžete na rychlý počítač,mobilní telefony, značkové oblečení a další dárky.

Napište nám na: soutezvip@seznam.cz. Mgr. Radek Černý, VIP Child Centre, Pratur

Kontakt s obětí, navázání a prohlubování vztahu

V druhé etapě manipulace útočník navazuje kontakt s obětí a dále pracuje na budování a prohlubování virtuálního vztahu.

Efekt zrcadlení

Charakteristickým rysem chování kybergroomera je tzv. efekt zrcadlení (mirroring). Predátor napodobuje oběť ve snaze prolomit její zábrany, chová se jako její zrcadlový odraz (viz dynamická identita). Pokud oběť útočníkovi sdělí, že se cítí například osamělá a má nějaké problémy a starosti, predátor odpoví, že má podobné problémy a plně ji chápe. Nabízí jí, že se mu může s důvěrou svěřit. Díky efektu zrcadlení útočník u oběti navozuje pocit přátelství či kamarádství, který oběti pomůže překonat strach z komunikace s neznámou osobou. Zrcadlení nemusí být spojeno pouze s emoční rovinou vztahu s obětí, může také navodit pocit sounáležitosti například fiktivními společnými koníčky, názory na různá témata apod.

Ukázka zrcadlení:

méďa_15: Ahoj myšičko, jak se máš? Myšička_13: Mám se fajn, nudím se. méďa_15: Můžu se nudit s tebou? Myšička_13: Třeba. méďa_15: Kolik je ti let? Myšička_13: 13, a tobě? méďa_15: 15, a co máš ráda? Myšička_14: mám ráda Hannah Montanu... méďa_15: Hannah Montanu úplně miluju!!! A děláš nějaký sport? Myšička_14: Jezdím na inlinech. méďa_15: Já si na inlinech občas taky vyjedu, je to skvělá zábava... Odkud jsi? Myšička_14: Z Prahy. A ty? méďa_15: Já jsem také z Prahy. Odkud přesně? Napovíš? Myšička_14: ... no, ze Smíchova.

Snaha získat co nejvíce osobních informací o oběti

Kromě osobních údajů (jméno, věk, fotografie) se predátor snaží zjistit další informace - např. jméno školy, kterou žák/žákyně navštěvuje, oblíbené celebrity, zájmy a záliby apod. Tyto údaje pak slouží útočníkovi k sestavení obecného profilu oběti.

Profilování oběti

Pachatelé si velmi často vytvářejí profily obětí. Při sestavování profilů vychází jak z údajů, které mu sdělily oběti, tak ze záznamů, které nalezl na internetu v rámci vyhledávání. Uživatelé různých internetových portálů z obavy o svou bezpečnost zveřejňují vždy jen některé osobní údaje, proto útočník zpravidla nenajde všechny osobní údaje na jedné stránce. Pokud ale potenciální oběti zveřejní například e-mailovou adresu či jiný údaj, který jednoznačně směřuje k jejich osobě (číslo ICQ, číslo mobilního telefonu aj.), může je díky tomuto údaji

útočník vystopovat. Pomocí internetových vyhledávačů (Google apod.) může zjistit, kde oběť tento údaj také použila, a postupně doplňovat další osobní údaje do jejího profilu. Například telefonní číslo, které oběť uvedla v inzerci, adresu školy z profilu oběti na sociální síti atd. Stejným způsobem může útočník ověřovat údaje, které mu o sobě oběť sdělila (věk, pohlaví dítěte, bydliště a další osobní údaje).

Vábení a uplácení oběti

K tomu, aby útočník navázal s obětí co nejužší vztah, často využívá různé formy úplatků a "dárečků", mezi které patří peníze, kredit do mobilního telefonu, moderní technika (mp3 přehrávače, mobilní telefony), počítačové hry, značkové oblečení apod. Tyto úplatky mohou pomoci ověřit osobní údaj, který útočník od oběti získal (např. telefonní číslo či adresu oběti, na kterou zašle úplatek), a také zvýšit důvěryhodnost kybergroomera. Úplatek útočníkovi může sloužit také k získání nejcitlivějšího údaje, kterým je fotografie obličeje dítěte.

Z úplatku se může stát mocná zbraň. To dokládají případy obětí, které se k útočníkovi pro úplatky několikrát vracely a nechaly se opakovaně zneužívat. V tomto kontextu již můžeme hovořit o dětské prostituci.

Snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace

Cílem tohoto popsaného jednání je snaha postupně snižovat zábrany dětí a mládeže v oblasti sexuality postupným zaváděním sexuálního obsahu do konverzace. Tím může být v prvé řadě diskuze o lidské sexualitě, sexuálním životě rodičů, může docházet také k tomu, že útočník dítěti nabídne různé erotické či pornografické materiály, například proto, aby vzbudil jeho zájem a snížil jeho stud. Útočník usiluje o získání fotografií či videozáznamů obnažené oběti (například snaží se přimět oběť k tomu, aby se mu ukázala na webkameru nebo aby mu zaslala své nahé fotografie). Pokud predátor získá tyto vysoce citlivé materiály, může je využít k vydírání dítěte.

Snahy o izolaci oběti od okolí

Ochota svěřit se neznámému člověku na internetu je díky 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 informacemi využívá ve svůj prospěch. Postupně se pro dítě stává nezastupitelným kamarádem, jediným, komu se dítě svěřuje se svými problémy, a stává se pro dítě "exkluzivním přítelem".

Pomocí citového vydírání a zastrašování dítěti například zakazuje sdělit určitou informaci rodičům nebo jiným lidem z okolí dítěte (Neříkej to mamince, nenáviděla by tě. Nikomu to neříkej, ostatní by to nepochopili.). Čím více důvěrných informací predátor zná, tím více je na něj oběť fixovaná a závislá. Zpočátku útočníka vyhledává dobrovolně, později z donucení. Pokud by totiž oběť chtěla tento vztah ukončit, mohl by jí predátor vyhrožovat a vydírat zveřejněním sdělených tajemství (Jestli se mi neozveš, napíšu tvému otci, co jsi mi tu navykládala). Dítě má pak strach z důsledků, které by toto zveřejnění mohlo mít v reálném životě (např. zákaz počítače), a raději ve virtuálním vztahu s útočníkem zůstane.

Příprava na osobní schůzku

Útočník již disponuje diskriminujícími informacemi a osobními údaji oběti a plánuje osobní schůzku. I v této etapě využívá techniky cílené manipulace.

Technika překonávání věkového rozdílu mezi útočníkem a obětí

V rámci kazuistiky nalezneme řadu případů, kdy kyberútočník využil specifické techniky zaměřené na překonání věkového rozdílu mezi ním a obětí. Tato technika funguje zhruba takto: Útočník komunikoval s obětí několik týdnů pod falešnou identitou, v rámci které o sobě tvrdil, že je nezletilý. Po čase však oběti oznámil, že mu jeho otec zakázal přístup k internetu, ale jeho dospělý 30letý bratr (další identita téhož útočníka) by chtěl v komunikaci pokračovat. Na základě této komunikace pak oběť postupně přijala skutečnost, že komunikuje s člověkem, který je již dospělý - tedy podstatně starší.

Existují také případy, kdy kybergroomer oběti tvrdil, že ji na osobní schůzce vyzvedne starší osoba, třeba tatínek či sourozenec útočníka. Touto osobou však byl právě onen útočník, který oběť odvezl na "bezpečné místo" a tam ji sexuálně zneužil.

Vyhrožování a vydírání oběti

Ve chvíli, kdy má predátor o oběti dostatek informací a citlivých materiálů, může se ji pokusit pozvat na osobní schůzku. Pokud oběť odmítne na schůzku dorazit, útočník ji začne vydírat. Vyhrožuje, že o ní zveřejní kompromitující materiály - například zašle nahé fotografie jejím kamarádům, přátelům a rodičům, případně tyto materiály vytiskne a vyvěsí v okolí bydliště a školy oběti. Může také tvrdit, že zveřejní diskriminující fotografie na internetu s hanlivým označením oběti (např. Honza Novák je gay! Toto je jeho telefonní číslo XXX-XXX, zavolejte mu! Jana Nováková je špinavá prostitutka! Pište jí na e-mail XXX-XXX.apod.). Mnoho dětí těmto výhrůžkám nedokáže vzdorovat a raději se na schůzku dostaví, než aby byly vystaveny ponížení ze strany okolí. Ne vždy je však nutný nátlak ze strany útočníka, protože řada obětí je ochotna jít na schůzku i bez předchozího vydírání.

Osobní schůzka

Osobní schůzka je ústředním cílem snah kybergroomera a logickým zakončením předcházejících etap.

Pokračující manipulace

První schůzka útočníka s obětí může být úplně nevinná, nemusí ještě dojít k sexuálnímu či jinému zneužití oběti. Útočník si může na schůzce pouze ověřit, zda je oběť skutečně nezletilá, zda se nejedná o nasazeného agenta (v některých státech jsou tito agenti běžnými nástroji v boji proti zneužívání nezletilých). Na schůzce rovněž může útočník prohloubit navázaný vztah s obětí dalším dárkem (úplatkem). Oběť tak nabude dojmu, že je útočník neškodný a že je skutečně tím "exkluzivním kamarádem", za kterého se na internetu vydával. K útoku může dojít až po několika osobních schůzkách.

Útok na oběť

Útok (sexuální útok, fyzický útok apod.) má pro oběť nedozírné následky. Jak v oblasti fyzické, tak zejména v oblasti psychické. Pokud má kybergroomer dostatek účinných nástrojů pro manipulaci, může oběť donutit k opakovaným schůzkám, na kterých útoky pokračují.

5. JAK SE CHRÁNIT PŘED KYBERGROOMINGEM?

Kromě technických možností je nejúčinnější obranou před kybergroomingem prevence. Ta spočívá zejména v dobré informovanosti učitelů i žáků o nebezpečích této internetové manipulace. Velmi důležitým preventivním nástrojem je také fungující komunikace mezi dítětem a rodičem. Významné je rovněž integrování témat internetové komunikace s neznámými uživateli (a logicky také témat spojených s rizikovou virtuální komunikací) do systému vzdělávání (například prostřednictvím rámcových vzdělávacích programů).

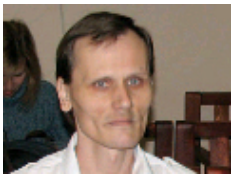
Pravidla pro děti a mládež

- 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.
- Vytyčte si své osobní hranice s ohledem na sex. Nepřijímejte ani neodesílejte jiným uživatelům materiály sexuální povahy.
- Ve virtuálním prostředí nikomu nesdělujte své osobní údaje (zejména své fotografie).
- Nikdy nechoďte na osobní schůzku, aniž by o ní věděli rodiče. Uvědomte si, co všechno se vám na schůzce může stát a jak může být schůzka riskantní.
- 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.

Pravidla pro rodiče

- Komunikujte se svými dětmi o tom, co dělají na internetu. Uvědomte si, že i když je vaše dítě v bezpečí domova a sedí u počítače, nemusí to znamenat, že je v bezpečí!
- Počítač dítěte nechejte na veřejně dostupném místě (např. v obývacím pokoji), které můžete namátkou kontrolovat.
- Vysvětlete dětem, jaká rizika může internet představovat.
- Uvědomte si, že když doma dítěti zakážete používat počítač a internet, najde si jinou cestu, jak se k těmto nástrojům dostat (u kamaráda, ve škole, prostřednictvím mobilního telefonu atd.). V případě, že se vaše dítě dostane do problémů spojených s kybergroomingem, kyberšikanou či dalšími nebezpečnými komunikačními jevy, nepoužívejte nefunkční metodu zákazu práce s počítačem a internetem!

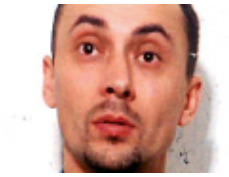
6. PŘÍPADY KYBERGROOMINGU (SKUTEČNÉ KAUZY)



Pavel Hovorka (ČR, 2005-2007)

Usvědčený deviant Pavel Hovorka (vrátný v tiskárnách) využíval k seznamování se s oběťmi např. diskuzní fóra, chat či inzeráty. Předstíral, že vybírá děti z dětských domovů do soutěže Dítě VIP apod. Osobní informace a fotografie, které od dětí získal, pak použil k vydírání. Kombinací vydírání a uplácení přiměl některé děti k osobní schůzce.

Důsledky: Znásilňování a zneužívání 20 chlapců. Byl odsouzen na 8 let odnětí svobody.



Michael Wheeler(VB, 2003)

Pedofil Michael Wheeler (35, elektroinženýr) používal k seznamování se s dívkami veřejný chat. S jednou ze zneužitých dívek se seznámil, když jí bylo 11 let. Postupně jí manipuloval, až se na něm stala citově závislá. Krátce po jejích 13. narozeninách ji začal sexuálně obtěžovat. Kontaktoval a obtěžoval také její kamarádky.

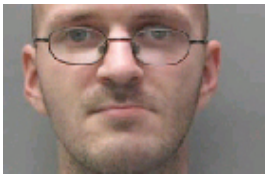
Důsledky: 11 sexuálních útoků, zneužití 2 dívek (13 let). Byl uvězněn na 3 roky.

Uherské Hradiště
Srdce Slovácka

Douglas Lindsell (VB, 2003)

Bývalý pošťák Douglas Lindsell (64) na internetu vystupoval pod falešnou identitou 15letého chlapce. Sympatie dívek získával např. tvrzením, že má rakovinu. Vedl si databázi dívek, se kterými se seznámil online, plánoval si s nimi osobní setkání a znásilnění, některým posílal své nahé fotografie nebo je nutil např. k obnažování. Dvě dívky (13 a 14 let) dokonce přiměl k osobní schůzce. Jednu z nich se snažil nalákat do svého auta a znásilnit.

Důsledky: Sexuální obtěžování několika dívek, pokus o znásilnění. Byl uvězněn na 5 let.



Peter Chapman (VB, 2009)

Již dříve trestaný sexuální deviant Peter Chapman (33 let) se seznámil se 17letou Ashleigh Hall na sociální síti Facebook. Pod falešnou identitou (předstíral, že je mu 19 let) ji vylákal na osobní schůzku, kde ji znásilnil a následně zavraždil. Po zveřejnění případu se začaly ozývat další ženy, se kterými Chapman také plánoval osobní setkání. Ve svém profilu na síti Facebook měl přes 3 000 virtuálních přátel (žen ve věku 13-31 let). Pomocí různých dotazníků od nich získával osobní informace. Od některých vylákal také citlivé fotografie.

Důsledky: Za znásilnění a vraždu byl uvězněn na doživotí.

Zdroj článku : RIZIKA VIRTUÁLNÍ KOMUNIKACE, autoři Mgr. Kamil Kopecký, Ph.D. , Mgr. Veronika Krejčí , NET UNIVERSITY, Olomouc, 2010, ISBN 978-80-254-7866-O,

http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=10:brozura

KDO PORADÍ, CO DĚLAT?

Pomoc online (Internet Helpline)	www.pomoconline.cz Tel.: +420 116 111 +420 800 115 155 email: pomoc@linkabezpeci.cz

	http://xchat.centrum.cz/lb/
E-Bezpečí	www.e-bezpeci.cz www.napisnam.cz email: info@e-bezpeci.cz
Národní centrum bezpečnějšího internetu (Safer Internet)	www.saferinternet.cz
Bílý kruh bezpečí	www.bkb.cz Tel.: +420 257 317 110
Úřad na ochranu osobních údajů	www.uoou.cz Tel. : +420 234 665 212 email : posta@uoou.cz
Policie ČR	www.policie.cz , tel.: 158

Zveřejněno 17. březen 2017, aktualizováno 28. březen 2017, vytištěno 20. srpen 2019