MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 7
KYBERGROOMING

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

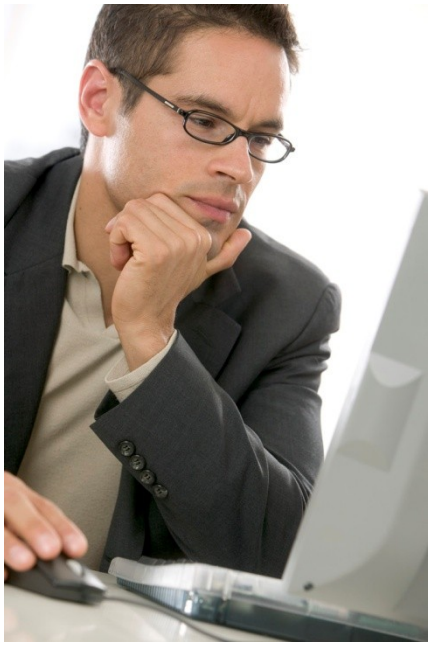
(reg. č.: CZ.1.01/2.2.00/15.0070)

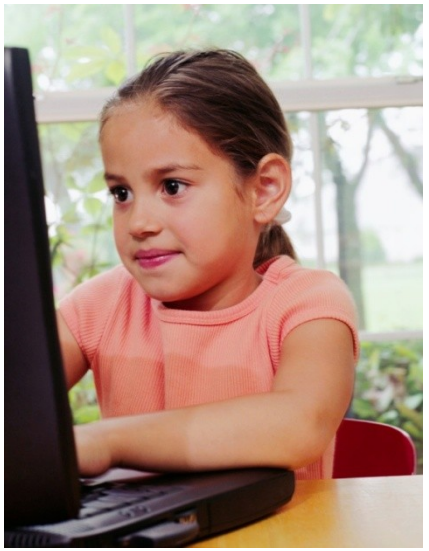
esf evropský sociální fond v ČR | EVROPSKÁ UNIE | MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY | OP Vzdělávání pro konkurenceschopnost | UNIVERZITA OBRANY

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

OBSAH

1. Vysvětlení pojmu kybergrooming
2. Charakteristické rysy kybergroomingu
3. Fáze/etapy kybergroomingu
4. Případy kybergroomingu
5. Právní rámec kybergroomingu
6. Ochrana před kybergroomingem





esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Literatura

Základní

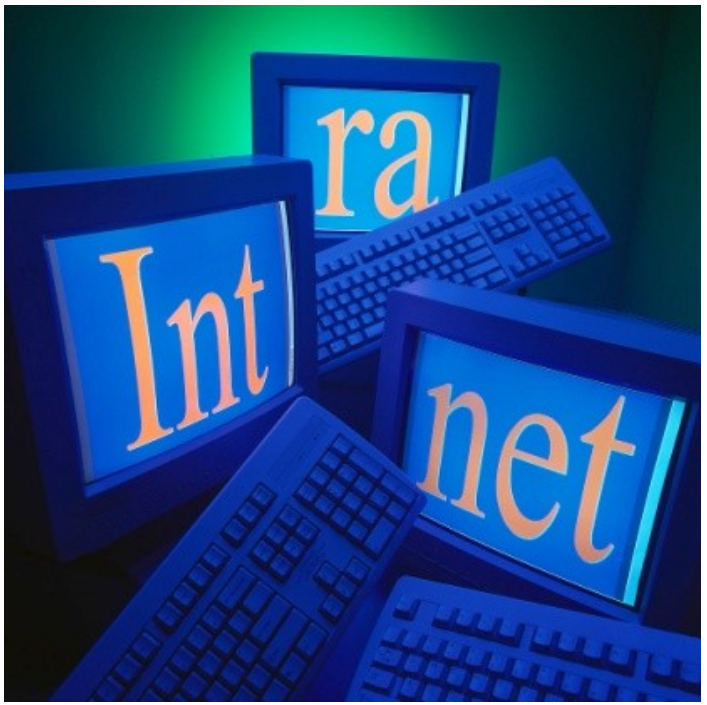
- OConnel, R. a kol. Cyber Stalking,Abusive Cyber sex and Online Grooming: A Programme of Education for Teenagers.University of Central Lancashire.

Internetové zdroje:

- http://pomoc-online.saferinternet.cz/index.asp
- http://www.e-bezpeci.cz/index.php/temata/kybergrooming
- http://www.nebudobet.cz/?page=kybergrooming
- http://www.saferinternet.cz/pro-rodice/sexting-kybergrooming

ZÁKLADNÍ POJMY

- **Internet,**
- **sociální sítě,**
- **kybergrooming** (child grooming, grooming),
- **kyberútočník,**
- **kybergroomer,**
- **efekt zrcadlení (mirroring),**
- **sexting,**
- **vábení a uplácení oběti (luring),**
- **právní rámec.**



Termín **kybergrooming** (child grooming, grooming) 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 tedy druhem psychické manipulace realizované prostřednictvím internetu, mobilních telefonů a dalších souvisejících technologií.

Útočníci tedy bývají velmi často pedofilové.

Pojem **kybergrooming** překládáme jako kyberkrášlení a označujeme jím jednání osoby, která se snaží zmanipulovat vyhlédnutou oběť a donutit ji k osobní schůzce. Útočník s obětí komunikuje prostřednictvím **chatu, SMS zpráv, ICQ, Skypu a sociálních sítí**. Důvodem schůzky bývá nejčastěji **sexuální zneužití, fyzické napadení nebo donucení k terorismu**.

Kybergrooming je velice zákeřný způsob, jak zneužít dětské důvěřivosti, naivity, touhy po přátelství, intimitě i dobrodružství. Jedná se vlastně o typický příklad zneužití osobních údajů, které oběť agresorovi poskytuje, avšak její lstivost vězí především v uhoupání a ošálení dětské obezřetnosti v rozsáhlém časovém horizontu a získávání důvěry pozvolna. Nejedná se o krátkodobé a přímé manipulování!

Charakteristické rysy kybergroomingu

1. Kde se kybergrooming vyskytuje?
2. Jak dlouho manipulace dítěte probíhá?
3. Kdo jsou oběti?
4. Kdo jsou útočníci?

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Kde se kybergrooming vyskytuje?

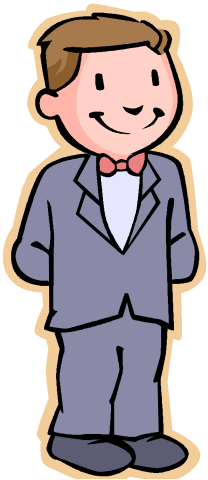
Kybergrooming je často vázán na synchronní i asynchronní komunikační platformy:

- nejčastěji veřejný chat,
- internetové seznamky,
- instant messengery a VoIP (např. ICQ, Skype),
- na sociální sítě (Facebook, Twitter, MySpace a další),
- inzertní portály,

Jak dlouho manipulace dítěte probíhá

Jak dlouho manipulace dítěte probíhá?

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. Existují případy, kdy predátor manipuloval dítě po dobu 2 let, než došlo k osobnímu setkání a sexuálnímu zneužití.



Kdo jsou oběti?

Oběťmi kybergroomingu jsou zpravidla děti a mládež nejčastěji **ve věku 11 – 17 let.** Častěji jsou oběťmi kybergroomingu **dívky** než chlapci. 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.).

Kdo jsou oběti?

Mezi nejčastější oběti patří:

a) děti s nízkou sebeúctou nebo nedostatkem sebedůvěry (lze je snadněji citově či fyzicky izolovat),

b) děti s emocionálními problémy, oběti v nouzi (často hledají náhradu za své rodiče a potřebují pomocnou ruku),

c) děti naivní a přehnaně důvěřivé (jsou ochotnější zapojit se do online konverzace s neznámými lidmi, obtížněji rozpoznávají rizikovou komunikaci),

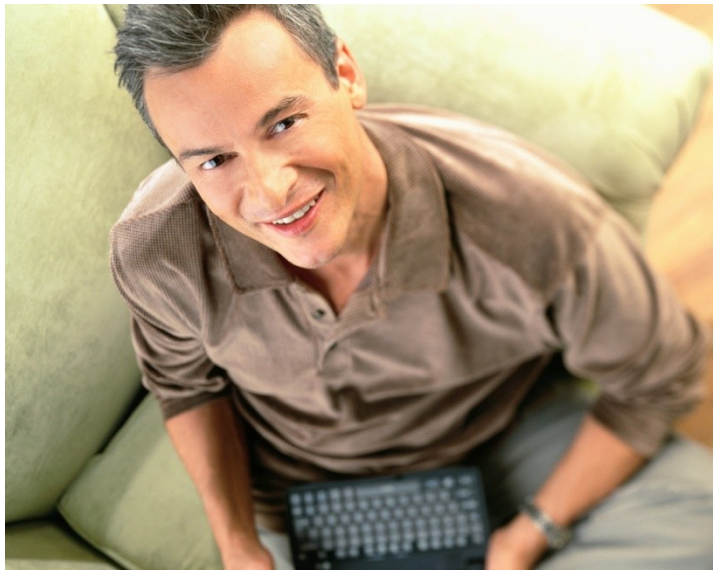
d) adolescenti/teenageři (zajímá je lidská sexualita, jsou ochotni o ní hovořit).

Kdo jsou útočníci?

Kyberútočníci (predátoři) tvoří heterogenní skupinu, ve které nalezneme jak uživatele s nízkým tak i vysokým sociálním statutem (právníky, učitele, policisty). V řadě případů oběť pachatele zná a je na něm závislá (v 85 - 95 % případů), 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.

Fáze/etapy kybergroomingu

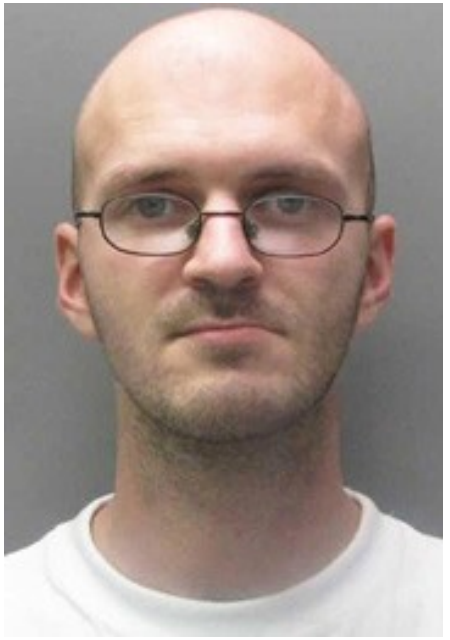
1. Příprava kontaktu.
2. Kontakt s obětí, navázání a prohlubování vztahu.
3. Příprava na osobní schůzku.
4. Osobní schůzka.

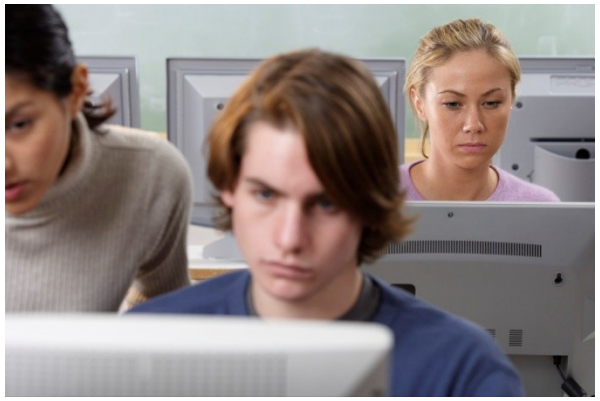


Příprava kontaktu

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. Útočníci jsou obvykle podstatně starší než vyhlédnuté oběti, proto si svůj věk dle potřeby upraví a doplní o odpovídající fotografii.





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:

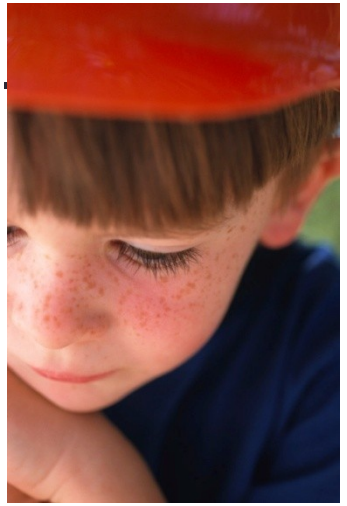
Ahoj kamarádi. Je vám méně než 15 let? Máte rádi počítače? Rádi brouzdáte internetem? Zapojte se do naší soutěže a vyhrajte atraktivní ceny. Stačí, když nám zašlete vaše jméno a příjmení, e-mailovou adresu a telefonní číslo a budete zařazeni do slosování. Těšit se můžete na rychlý počítač, mobilní telefony,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

Napište nám na: soutezvip@seznam.cz.

Mgr. Radek Novotný, VIP Child Centre, Prague

Klasický průběh budování závislosti probíhá přibližně takto:

1. Vzbuzení důvěry a snaha izolovat oběť od okolí.
2. Podplácení dárky, penězi, budování přátelského vztahu.
3. **Získání nebezpečných materiálů k vydírání.**
4. Příprava na osobní schůzku.
5. Osobní schůzka.
6. Zneužití, napadení, vydírání, sexuální obtěžování...



Vzbuzení důvěry a snaha izolovat oběť od okolí:

Groomer předstírá, že rozumí problémům dítěte a pomůže mu je vyřešit. Groomer získává pozici **dobrého kamaráda**.

Groomeři s dětmi řeší často citlivá témata (manželské problémy, lidská sexualita, často také dětem ukazují pornografické materiály, …).

Útočník **izoluje** oběť. Často v této etapě získá e-mail či telefonní číslo, případně fotografii, kterou využije k vydírání (viz. Případ Hovorka).

Vzbuzení důvěry a snaha izolovat oběť od okolí

Verbální projevy:

Rodiče ti nerozumí, já ano, mně se můžeš svěřit se svými problémy, …

Neříkej o tom ostatním dětem, žárlily by, …

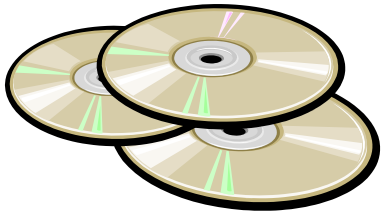
Neříkej o tom mamince … kdybys jí to řekl/a, nenáviděla by tě …

Efekt zrcadlení (mirroring)

Charakteristickým rysem chování kybergroomera je tzv. efekt **zrcadlení** (mirroring). Predátor napodobuje oběť ve snaze prolomit zábrany, chová se jako její zrcadlový odraz. 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 sounáležitost například **fiktivními společnými koníčky, názory na různá témata** apod.

Podplácení dárky, penězi, budování přátelského vztahu

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.



Příklad

Na začátku si dítě může například postěžovat na starý mobil, útočník, stále ještě v masce přítele, mu slíbí nový, avšak jako protislužbu bude žádat fotku v plavkách. Dítě si časem posteskne, že nemá dostatek kreditu, agresor opět nabídne pomoc. Dobití kreditu ovšem bude podmíněno další fotografií, tentokrát odhalenější. Dítě bere výměnu jako dobrý obchod, něco málo ukáže a dostane vytouženou věc. Možná už samo tuší, že není vše v pořádku a na druhém konci je někdo nenormální, ale na schůzku by se přece přemluvit nedalo! Avšak jakmile agresor získá nebezpečné materiály, je schopen jich využít proti dítěti. Začne oběti vyhrožovat, že pokud nepošle další fotky, video, tak vše zveřejní, pošle je rodičům, kamarádům, do školy učitelům. Pod takovým tlakem se může dítě zhroutit, ale také podlehnout a vyjít vstříc útočníkově vůli. O zneužití fotografií a videa se sexuálním obsahem pojednává SEXTING.

Získání nebezpečných materiálů k vydírání

Snaha získat co nejvíce osobních informací o oběti (fishing)
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 obětí
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 může zjistit, kde oběť tento údaj také použila, a postupně doplňovat další osobní údaje do profilu oběti. 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).

Získání nebezpečných materiálů k vydírání

Vábení a uplácení oběti (luring)

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.

Snižování zábran dětí a mládeže zaváděním sexuálního obsahu do konverzace

Cílem je snaha postupně snižovat zábrany dětí a mládeže v oblasti sexuality postupným zaváděním sexuálního obsahu do konverzace. Tím může být v prvé řadě diskuse o lidské sexualitě, sexuálním životě rodičů, může docházet také k tomu, že útočník dítěti nabídne různé erotické či pornografické materiály, například proto, aby vzbudil jejich zájem a snížil jejich stud. Útočník samozřejmě 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/nezletilého.

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 oběti

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.

Příprava na osobní schůzku

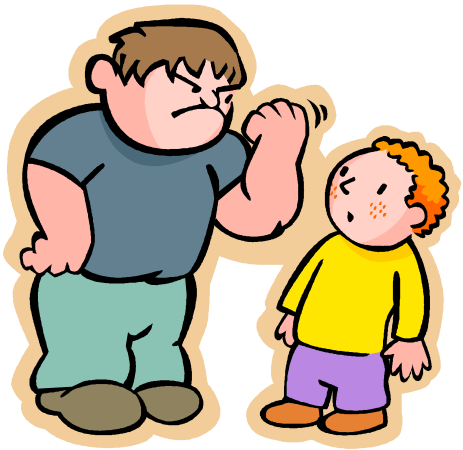
Vyhrožování a vydírání oběti

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 zveřejnění 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.

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 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.

Případy kybergroomingu

Jiří Kadrnožka (28)

MF DNES už před časem odhalila muže, který na internetu lákal dítě k sexu. Na osmadvacetiletého Jiřího Kadrnožku narazili redaktoři MF DNES na dětských diskusních stránkách, kde pod přezdívkou Jirzin napsal: *"Najde se tady holka, která mi ho vy...?"* (Následoval vulgární výraz pro uspokojení muže rukou.) Redaktoři si s ním pak psali pod identitou jedenáctileté Terezy. Kadrnožka se zajímal o to, jak vyspělé už je její tělo. S domnělou dívkou vystupující jako **Terezička44** si nakonec smluvil schůzku, na kterou posléze přišel. Když zjistil, že ve skutečnosti má schůzku s redaktory, utekl. Policie ho později dostihla na základě fotografie zveřejněné v novinách – poznala ho jeho bývalá kolegyně. Původně za svůj prohřešek dostal Kadrnožka podmínku na dva roky, kterou mu soud později snížil na rok díky tomu, že dobrovolně chodil do sexuologické ordinace a léčil se. Kadrnožka u soudů opakovaně tvrdil, že se považuje za nevinného, a jeho obhájce usiloval o naprosté zproštění viny. *"Neměl jsem žádné postranní úmysly. Přihlásil jsem se na chat ze zvědavosti. Jednání lituji,"* prohlašoval Kadrnožka.

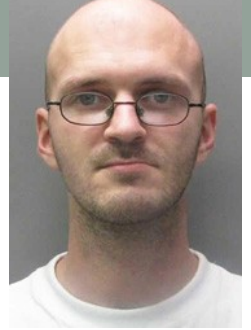
Zdroj: http://www.nebudobet.cz/?page=kybergrooming

Pavel Hovorka (36)

Hovorka, který pracoval jako ostraha v tiskárnách, sponzoroval dětské domovy. Jeho údajně první oběť vyhrála jím vypsanou soutěž "dítě VIP", za což měla strávit dva týdny v Praze. Chlapec tak v červenci 2005 strávil několik dnů s obžalovaným na vrátnici, kde ho muž podle žalobců zneužil. Další oběti si prý vyhledával na seznamovacích serverech. Poté je pozval k sobě do práce, kde několik z nich údajně donutil k pohlavnímu styku. Nabízel jim za něj peníze, některé také vydíral. Hrozil, že vyzradí jejich homosexuální orientaci a zveřejní jejich nahé fotografie, které mu za úplatu poslali. Někteří se bránili, a tak je podle obžaloby znásilnil. Pavel Hovorka se zodpovídal z trestných činů pohlavního zneužívání, vydírání, ohrožování výchovy, svádění k pohlavnímu styku a znásilnění. Soud mu kromě vězení uložil také sexuologickou léčbu. Trestné činy se týkaly 20 nezletilých chlapců, 8 z nich muž opravdu k sexuálnímu styku donutil. Byl odsouzen na 6,5 roku odnětí svobody (původní trest 8 let mu byl zmírněn u odvolacího soudu).

Zdroj: http://www.nebudobet.cz/?page=kybergrooming

Případy kybergroomingu



Ashleigh Hallová (17) Velká Británie

Ashleigh, studentka ošetřovatelství, byla společenská a měla hodně přátel. Aktivně také využívala sociální síť Facebook, na které se seznámila s 16letým chlapcem. S tím si po delší komunikaci domluvila osobní schůzku. V neděli 25. října 2009 večer oznámila matce, že jde ke kamarádce, u které přespí. V pondělí již Ashleigh nedorazila k obědu. K zabití dívky se přiznal 32 letý bezdomovec Peter Chapman, který byl již v minulosti trestaný za sexuální delikty a jeho jméno figuruje na rejstříku sexuálních útočníků. Muž byl náhodně zadržen policií za řízení vozidla bez zákonného pojištění. Poté, co byl převezen na policejní stanici, se přiznal k tomu, že Ashleigh zabil. Dle jeho výpovědi pak také policie našla tělo oběti v příkopu u nedaleké farmy. Muž zmanipuloval dívku právě díky sociální síti Facebook, kde pod falešným profilem předstíral, že je 16-letý chlapec. Asleigh pak důvěřovala informacím, které od útočníka získala prostřednictvím chatu, a souhlasila s osobní schůzkou. **Peter Chapman (32) byl v březnu 2010 odsouzen k trestu doživotí.** Měl falešný profil (udal jméno Peter Cartwright a věk 16 let).

Matka Ashleigh, devětatřicetiletá Andrea Hallová, vystoupila s varováním před všemi komunitními sociálními weby: *"Řekněte svým dětem, ať jsou na internetu mnohem opatrnější*. *Nikomu nevěřte, a nepouštějte své děti na Facebook a jemu podobné stránky, dokud nebudou plnoletí.“*

Zdroj: http://www.nebudobet.cz/?page=kybergrooming

Případy kybergroomingu

Případ z USA

Čtrnáctiletá žákyně dostala od svých rodičů dárek – nový počítač. Po dvou měsících používání internetu se seznámila s dospělým mužem, se kterým chatovala a udržovala e-mailovou korespondenci. Když se o tom její rodiče dozvěděli, učinili řadu kroků, aby tomuto kontaktu zabránili – odstranili od počítače klávesnici, monitorovali poštu a telefonní hovory, navštívili s dcerou poradnu. Bohužel, kontakt žákyně s dospělým mužem pokračoval prostřednictvím mobilního telefonu, který žákyni útočník poslal. Po několika měsících dívka zmizela z domova. Když policie prohledala její počítač, objevila řadu e-mailů, které je přivedly až k síti pedofilů, komunikujících mezi Evropou a USA. Pedofilní uživatel z Řecka si díky této síti „objednal“ nezletilou dívku z USA, zabezpečil falešný pas a poskytl finance na transport dívky z USA do Evropy – do Řecka. Po pěti měsících bylo dítě navráceno rodičům. Nejprve dívka tvrdila, že pedofilního groomera miluje a zbožňuje, avšak po rozsáhlé terapeutické léčbě si začala vzpomínat na detaily sexuálního a fyzického mučení, začala mít sebevražedné sklony a bylo nutné ji hospitalizovat na psychiatrické klinice. Dívka se postupně zotavovala, ale její zkušenosti a trauma ji budou provázet po zbytek života.

Zdroj: http://www.nebudobet.cz/?page=kybergrooming

Muž vydíral dívky fotkami, které mu samy poslaly

Kriminalisté v těchto dnech obvinili 41letého muže z Pardubic z vydírání a několika dalších trestných činů. Muž vydíral mladé dívky po internetu. Poté, co z nich vylákal jejich pornografické fotografie, po nich požadoval další. Nyní mu hrozí až šestiletý pobyt za mřížemi.

10. 3. 2011 ve 14:48 - Pardubice – www.novinky.cz

Muž byl obviněn ze svádění k pohlavnímu styku, výroby a jiné nakládání s dětskou pornografií, zneužití dítěte k výrobě pornografie a vydírání. Stíhán je na svobodě, vyšetřovatel u něj nařídil znalecké vyšetření duševního stavu.

V letech 2008 a 2009 na internetu ze svého bydliště komunikoval s dívkami, kterým bylo v té době mezi 13 a 18 lety. Požadoval po nich zaslání pornografických fotografií nebo videí, kde měly dívky osobně vystupovat. Za to jim nabízel finanční odměnu. Obviněn je zatím za 24 skutků a celkem je 14 poškozených dívek.

Informace a kontakty na dívky získával prostřednictvím sociálních sítí. Všem nabízel za zaslání fotografií finanční odměnu.

„*Jedna z dívek se dokonce s mužem sešla a za vzájemné sexuální hrátky obdržela finanční obnos v řádu několika tisíc korun. Některé z dívek se finanční odměny za fotografie nedočkaly, ale dočkaly se vyhrožování typu, jestli mi nepošleš další fotografie, ty tvé rozešlu tvým kamarádům a podobně*,“ uvedla mluvčí policie Markéta Janovská.

http://www.novinky.cz/krimi/227460-muz-vydiral-divky-fotkami-ktere-mu-samy-poslaly.html

Právní rámec kybergroomingu:

Termín kybergrooming (child grooming) trestní zákon (Zákon č. 40/2009 Sb23.) nezná, není tedy vymezen jako trestný čin. Nicméně pod toto jednání mohou být zahrnuty například následující trestné činy:

1. Obchodování s lidmi (168) – v 1. odstavci trest odnětí svobody ve výši 2 - 10 let.
2. Omezování osobní svobody (171) – v 1. odstavci trest odnětí svobody ve výši 2 roky.
3. Vydírání (175) – v 1. odstavci trest odnětí svobody 6 měsíců až 4 roky.
4. Pohlavní zneužití (187) – v 1. odstavci trest odnětí svobody 1 až 8 let.
5. Výroba a jiné nakládání s dětskou pornografií (192) – v 1. odstavci trest odnětí svobody až 2 roky.
6. Zneužití dítěte k výrobě pornografie (193) – v 1. odstavci trest odnětí svobody 1 – 5 let.
7. Ohrožování výchovy dítěte (201) – v 1. odstavci trest odnětí svobody až 2 roky.
8. Podvod (209) – v 1. odstavci trest odnětí svobody až 2 roky.
9. Nebezpečné vyhrožování (353) – v 1. odstavci trest odnětí svobody až 1 rok.
10. Nebezpečné pronásledování (354) - v 1. odstavci trest odnětí svobody až 1 rok.

Ochrana před kybergroomingem

Kromě technických možností je nejúčinnější obranou před kybergroomingem prevence. Ta spočívá zejména v dobré informovaností rodičů a dětí 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). Zde hraje velkou roli informovanost učitelů.

Nejlepší ochranou je prevence!!!!
Existuje několik základních pravidel, jak se před kybergroomingem chránit.

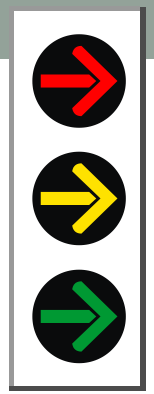
Ochrana před kybergroomingem

Základní pravidla pro děti a mládež

1. 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!
2. Všímejte si nesrovnalostí v komunikaci s kyberútočníky (útočník například udává různý věk, mění informace, které vám o sobě sdělil dříve apod.).
3. Uvědomte si, proč by někdo chtěl za každou cenu udržet internetový vztah nebo obsah komunikace v tajnosti.
4. Vytyčte si své osobní hranice s ohledem na sex. Nepřijímejte ani neodesílejte jiným uživatelům materiály sexuální povahy.
5. Ve virtuálním prostředí nikomu nesdělujte své osobní údaje (zejména své fotografie).
6. 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.
7. 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.

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Ochrana před kybergroomingem



Pravidla pro rodiče

1. 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!

2. Počítač dítěte nechejte na veřejně dostupném místě, například v obývacím pokoji, které můžete namátkou kontrolovat.

3. Vysvětlete dětem, jaká rizika může internet představovat.

4. 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! Uvědomte si, že když dítěti doma zakážete počítač a internet, najde si jinou cestu, jak se k těmto nástrojům dostat (u kamaráda, ve škole, prostřednictvím mobilního telefonu atd.).

ZÁVĚR

S kybergroomingem se můžete potkat v podstatě kdykoliv. Kybergroomer se s největší pravděpodobností pokusí naplánovat kontakt se svou obětí získáním jejího/jeho telefonního čísla, použitím e-mailu a následně se bude chtít domluvit na schůzce mezi čtyřma očima.

Ochrana před kybergroomingem - nejlepší ochranou je prevence!!!!

Existuje však několik základních pravidel, jak se před kybergroomingem chránit.

Dotazy?

pplk. Ing. Petr HRŮZA, Ph.D.
Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky
E-mail.: petr.hruza@unob.cz

esf evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
UNIVERZITA OBRANY
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ