Kyberšikana

Úvod do problematiky

Termínem kyberšikana označujeme nebezpečné komunikační jevy realizované prostřednictvím informačních a komunikačních technologií (např. pomocí mobilních telefonů nebo služeb v rámci internetu), jež mají za následek ublížení nebo jiné poškození oběti.

Toto ublížení či poškození může být jak záměrem útočníka, tak důsledkem např. nevhodného vtipu, nedorozumění mezi obětí a útočníkem, nedomyšlením důsledků jednání ze strany útočníka atd. Oběť je poškozována opakovaně, ať už původním útočníkem či osobami, které se do kyberšikany zapojí později.

Kyberšikana je druhem psychické šikany realizovaná v rámci služeb internetu nebo GSM sítí (mobilní telefony).

1. 1. ROZDÍL MEZI TRADIČNÍ ŠIKANOU A KYBERŠIKANOU

Kyberšikana se odehrává ve virtuálním světě. Tak, jako se liší virtuální svět od světa reálného, liší se i kyberšikana od klasické šikany. Místo a čas útoku Zatímco u tradiční šikany lze předpokládat, kdy a kde k útoku dojde (např. ve škole, na hřišti), s kyberšikanou se můžeme setkat kdykoliv a kdekoliv. Obětí útoku se můžeme stát vždy, když budeme připojeni k internetu nebo mobilní síti (GSM). V takovém případě se před kyberútokem nemáme kam schovat. Útočník si nás může najít třeba i o půlnoci v „bezpečí domova“. Útočník Pachatel kyberšikany je ve většině případů anonymní, skrytý za přezdívkou nebo jiným neurčitým identifikátorem. Z této skutečnosti vyplývá většina rozdílů mezi pachateli kyberšikany a tradiční šikany. Anonymita virtuálního prostředí smazává rozdíly mezi lidmi – ať už jde o věk, pohlaví, sociální postavení, fyzické dispozice, početní převahu či například odvahu zaútočit. Virtuální prostředí umožňuje provést útok i těm, kteří těmito možnostmi v dostatečné míře nedisponují. Původcem kyberšikany se může stát kdokoli, kdo má potřebné znalosti informačních a komunikačních technologií. Útočníci tráví podle výzkumů více času na internetu, a to bez dohledu rodičů, kteří se navíc příliš nezajímají o to, k čemu jejich děti internet používají.

KYBERŠIKANA Sekundární útočníci (diváci a šiřitelé) Množství diváků kyberšikany může být nepoměrně větší než počet přihlížejících u klasické šikany. V případě kyberšikany může být přihlížejícím v podstatě každý, kdo má přístup k internetu – tedy miliony lidí z celého světa. Kromě diváků se do kyberšikany zapojují i tzv. šiřitelé kyberšikany. Jsou to lidé, kteří dále rozesílají informace o kyberšikaně (např. posílají dalším lidem odkaz na stránky, kde se kyberšikana objevila), a tak se vědomě či nevědomě do kyberšikany sami zapojují. Obě tyto skupiny lidí mohou zmnohonásobit dopad útoku na oběť. Tím vlastně poškozují oběť mnohem více než primární útočník - z tohoto pohledu se tedy stávají sekundárními útočníky. Oběť stejně jako je tomu u původců kyberšikany ani u jejich obětí nezáleží na věku, pohlaví, fyzické síle, postavení v sociální skupině či úspěšnosti ve společnosti. V elektronické komunikaci jsou výše zmíněné aspekty potlačeny a nemají takový význam, jako při komunikaci tváří v tvář. Z výzkumů vyplývá, že oběti tradiční šikany se často stávají také oběťmi kyberšikany, která je v této souvislosti posunem šikany o krok dál. Výzkumy také uvádějí, že oběti kyberšikany tráví více času na internetu, bývají obvykle málo obeznámeny s riziky spojenými se zneužitím ICT, proto se na internetu chovají méně opatrně. Útok a jeho dopad na oběť Během kyberútoku nedochází k osobnímu kontaktu útočníka s obětí (útočník svou oběť dokonce nemusí znát, může si ji vytipovat např. podle přezdívky nebo podle věku). Nedostatek zpětné vazby z reakce oběti umožňuje rozvíjet agresivní a impulsivní chování bez zábran. Dopad vlivu informace zveřejněné např. na internetu trvá mnohem déle než nadávka či pomluva v reálném světě, která „prošumí davem“, ale dá se na ni poměrně rychle

zapomenout. Ve virtuálním prostředí zůstávají uložené diskriminující materiály, které mohou kyberšikanu znovu a znovu rozvířovat. Ponižující informace jsou navíc dostupné komukoliv, kdykoliv a odkudkoliv. Dopad útoku či útoků na oběť výrazně prohlubuje pocit beznaděje, který je vyvolaný minimálními možnostmi obrany proti anonymnímu útočníkovi. Diagnostika Vyhledávání obětí kyberšikany je stejně složité jako určování obětí jakékoliv jiné psychické šikany - psychické týrání na oběti nezanechává žádné zjevné stopy, na rozdíl od modřin a šrámů, jež mohou doprovázet fyzickou šikanu.

Oběti kyberšikany jsou často uzavřené do sebe a nekomunikují o problémech s okolím. Důvodů pro takové chování může být více (strach, stud, rodiče neovládají práci na počítači, dítě nepozná, že jde o projevy psychického šikanování, bojí se, že mu rodiče zakáží používat internet atd.).

Oběti kyberšikany na řešení svých problémů často zůstávají samy, což může vést k tomu, že situaci nezvládnou.

1.2. **Nejčastější projevy kyberšikany:**

Ztrapňování, urážení, nadávání, pomlouvání, v rámci sociálních sítí, blogů či jiných webových stránek, v diskuzích, chatech, e-mailech, SMS zprávách…

Zastrašování, vydírání, vyhrožování…

Zveřejňování ponižujících fotografií, videozáznamů či audiozáznamů na internetu.

Krádež identity obětí – vytváření falešných účtů, krádeže cizích účtů a manipulace s nimi s cílem dostat oběť do potíží.

Obtěžování a pronásledování např. psaním zpráv, voláním, prozváněním…

Vyloučením z on-line komunity jako forma šikany.

1.3. **Jak se chránit před kyberšikanou?**

Respektovat ostatní, nevyvolávat zbytečné konflikty ve skutečném ani virtuálním světě.

Nesdělovat citlivé informace, které by mohly být zneužity: nezveřejňovat osobní údaje, osobní fotografie, hesla k elektronickým účtům, nesvěřovat se se svými problémy, neřešit svou sexualitu atd. Umístěním na internet nad těmito materiály ztrácíme kontrolu.

Nebýt přehnaně důvěřivý (výzkumy ukazují, že většina lidí ve virtuální komunikaci lže).

Seznámit se s pravidly služeb internetu a GSM sítí.

Seznámit se s riziky, která souvisí s elektronickou komunikací.

1.4. **Jak se bránit kyberútokům ?**

UKONČIT – přestat komunikovat s útočníkem, nemstít se.

BLOKOVAT – zamezit útočníkovi přístup k oběti i k dané službě (kontaktovat poskytovatele služby, zablokovat si přijímání útočníkových zpráv nebo hovorů změnit svou virtuální identitu).

OZNÁMIT – oznámit útok dospělým, schovat si důkazy pro vyšetřování (např. zprávy videozáznamy, odkazy na weby, blogy).

ODHALIT PACHATELE – pokud je to možné (např. podle profilu)

2. 1. JAK SE CHRÁNIT PŘED KYBERGROOMINGEM? Kromě technických možností je nejúčinnější obranou před kybergroomingem prevence.

Ta spočívá zejména v dobré informovaností 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

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.

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 (např. v obývacím pokoji), které můžete namátkou kontrolovat.

3. Vysvětlete dětem, jaká rizika může internet představovat.

4. 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!

Společná strategie proti kyberšikaně na škole:

Vhodně informovat žáky, pedagogy a rodiče o hrozbách kyberšikany.

Zapojit téma kyberšikany do výuky.

Připravit seminář na téma kyberšikany do minimálního preventivního programu na aktuální školní rok. Pokračování semináře Šikana II. Od VISK.

Možnost seznámit se s danou problematikou na nástěnce a uvedení kontaktů na pomoc na viditelném místě (preventivní nástěnka v budově školy). Možnost obrátit se na metodika prevence, výchovného poradce a vedení školy.

2. 2. **KDO PORADÍ, CO DĚLAT?**

Pomoc online (Internet Helpline) www.pomoconline.cz +420 116 111, +420 800 155 155 pomoc@linkabezpeci.cz xchat.centrum.cz/lb/

Národní centrum bezpečnějšího internetu (Safer Internet) www.saferinternet.cz Bílý kruh bezpečí www.bkb.cz +420 257 317 110

E-Bezpečí www.e-bezpeci.cz www.napisnam.cz info@e-bezpeci.cz

Úřad na ochranu osobních údajů www.uoou.cz +420 234 665 212 posta@uoou.cz

Policie ČR 158 www.policie.cz

Projekt E-Nebezpečí pro učitele (www.e-nebezpeci.cz)

Projekt E-Bezpečí (www.e-bezpeci.cz)

Centrum prevence rizikové virtuální komunikace PdF UP (PRVoK) (www.prvok.upol.cz)

Online poradna Centra prevence rizikové virtuální komunikace PdF UP (www.napisnam.cz)

Pomoc online – linka bezpečí online (www.pomoconline.cz) Poradenská linka pro pedagogy (www.rspp.cz)

Kybergrooming (www.kybergrooming.cz)

Kyberstalking (www.kyberstalking.cz)

Sexting (www.sexting.cz) Policie ČR (www.policie.cz)

Úřad pro ochranu osobních údajů (www.uoou.cz)

Bílý kruh bezpečí (www.bkb.cz)

Konference E-Bezpečí (konference.e-bezpeci.cz)

Národní centrum bezpečnějšího internetu (www.saferinternet.cz)