

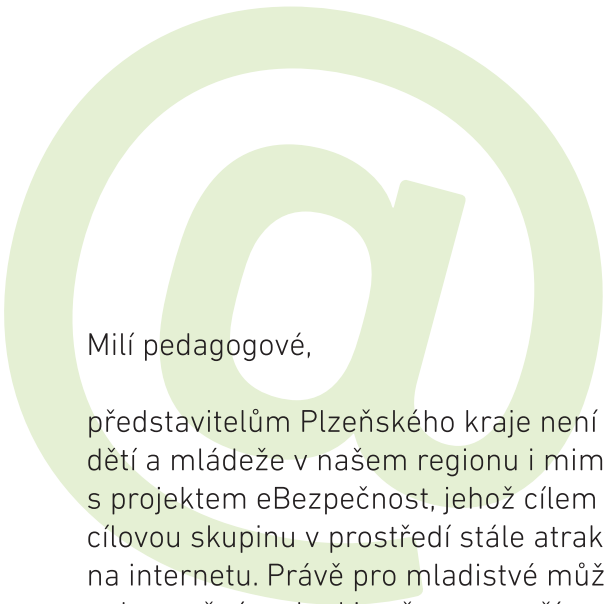
eBezpečnost

Kyberšikana

Manuál pro učitele

OBSAH BROŽURY:

- Charakteristika kyberšikany 4
- Typy kyberagresorů, typy kyberšikan 6
- Jak a kde nahlásit kyberšikanu přes internet 8
- Jevy související s kyberšikanou – kybergrooming, sexting 9
- Právní rámec 10
- Zajištění důkazů; jsem oběť? 13
- Prevence ve škole 14
- Zabavovat mobily při vyučování nebo ne? 15
- Příručka Kyberšikana a její prevence 16



Milí pedagogové,

představitelům Plzeňského kraje není lhostejná bezpečnost dětí a mládeže v našem regionu i mimo něj, a proto přichází s projektem eBezpečnost, jehož cílem je ochránit tuto citlivou cílovou skupinu v prostředí stále atraktivnějším a lákavějším – na internetu. Právě pro mladistvé může být internet hodně nebezpečný, pokud je včas nenaučíme několik zásadních pravidel při jeho užívání. Přál bych si, aby se nám podařilo díky projektu eBezpečnost „zaškolit“ co nejvíce z Vás, učitelů a profesorů, kteří pak budete formou preventivně-zábavních aktivit minimalizovat nebezpečí hrozící na internetu a v otevřené elektronické komunikaci.

Milan Chovanec, hejtman Plzeňského kraje

CO JE KYBERŠIKANA?

Předpona kyber- značí prostředí, ve kterém se šikana odehrává, tedy kybernetický svět počítačů, internetu a mobilních telefonů. Kyberšikana může samozřejmě probíhat i přes jiné technické komunikační prostředky, např. pagery, v české realitě jsou však v drtivé většině využívány právě výše zmíněné mobilní telefony a internet.

Stejně jako u šikany tváří v tvář se jedná o **úmyslné chování**, kdy je oběť **dlouhodobě** napadána útočníkem nebo útočníky, přičemž závažnost jednotlivých útoků se stále **stupňuje**.

KONKRÉTNÍ ZPŮSOBY KYBERŠIKANY

► přes mobil:

- SMS/MMS/video nevhodného obsahu (urážení, zastrašování...)
- volání, prozvánění
- natáčení a následné zveřejňování natočeného (rozesílání dalším lidem, umístění na YouTube apod.)
- focení bez svolení foceného a následné rozesílání třetím stranám

► přes Internet:

- zakládání falešných profilů nebo změna původního
- zakládání profilů proti nějaké osobě
- e-maily nevhodného obsahu
- krádež hesel a následné zneužití účtu
- obtěžování přes webkamery a IM (instant messaging, v ČR nejoblíbenější ICQ a Skype)

CHARAKTERISTICKÉ RYSY KYBERŠIKANY

- ▶ Anonymita – pouze domnělá. Útočníci si často myslí, že nemohou být nalezeni. Opak je ale v drtivé většině pravdou. Každý počítač má nějakou svoji IP adresu a poskytovatele internetového připojení. Tyto informace může policie během vyšetřování lehce zjistit, pokud jsou důkazní materiály stále k dispozici v mobilu nebo v počítači oběti.

Problém nastává ve chvíli, kdy útočník páchá své činy z internetové kavárny, která nemá kamerový systém, nebo z nezabezpečené WiFi sítě, na kterou se může napojit kdokoli. Tyto informace však dětem z pochopitelných důvodů NESDĚLUJEME.

- ▶ Nezávislost na místě a čase – kyberšikana může probíhat 24 hodin denně, oběť o napadení leckdy ani nemusí dlouhou dobu vědět. Se vzrůstajícím počtem mobilních telefonů s připojením na internet může kyberšikana probíhat i při hodině matematiky.
- ▶ Proměna agresora i oběti – protože ve virtuálním světě nepotřebujete hrubou sílu k tomu, abyste ublížili, nebo se mohli bránit, mohou se leckdy uchylovat ke kyberšikaně ti jedinci, kteří jsou obětí šikany v realitě. Samozřejmě to neplatí paušálně, spíše je to vodítko pro pochopení toho, proč je internetovým útočníkem ten tichý, zamlklý žák.
- ▶ Pro pobavení kohokoli
- ▶ Obtížná kontrola
- ▶ Rychlé šíření

KYBERAGRESOŘI – typy řazeny od nejzávažnějšího po nejméně závažného. K typu kyberagresora by měl učitel přihlížet v momentě, kdy bude kyberšikanu řešit a udělovat tresty. Leckdy stačí domluva, stažení materiálu z internetu a omluva, u vážných případů se naopak nezdráhat udělit kázeňský trest, popř. udělit sníženou známku z chování.

Bažící po moci

- ▶ Obvykle potřebují pro svou činnost alespoň malé publikum.
- ▶ Často využívá kyberšikanu v zastoupení (viz dále).

„Sprostý holky“

- ▶ KŠ obvykle páchána ve skupině + z nudy.
- ▶ Vyžadují publikum.

Pomstychtivý andílek

- ▶ „Zlonapравující“ chce dát oběti lekci, vzít „právo“ do svých rukou.
- ▶ Cítí se být oprávněn ke svému jednání (např. někdo mi založí posměšný profil, založím mu ho tedy také, na oplátku).

Neúmyslný kyberagresor

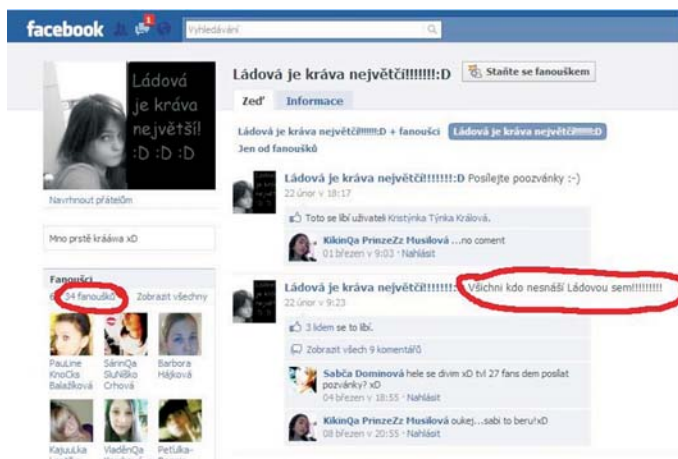
- ▶ Hra na „tvrďáka“ – ne záměr, ale obrana proti nenávisným či provokativním zprávám.
- ▶ Sklon vystupovat na Internetu jako někdo jiný.

Vtipálek

- ▶ Z legrace zakládají profily svým kamarádům a známým.
- ▶ Neuvědomují si, že jejich „legrace“ může někoho ranit.

TYPY KYBERŠIKAN

► Přímé útoky



Příklad přímého útoku na stránkách Facebooku.

Kromě zakládání falešných nebo hanlivých profilů sem můžeme počítat i jakýkoli jiný útok, který směřuje od útočníka přímo k oběti. Může jít mj. i o zasílání nevhodných SMS, e-mailů, komentářů, neustálé prozvánění, telefonování apod.

SCHÉMA ÚTOKU: ÚTOČNÍK > OBĚŤ

► Kyberšikana v zastoupení

Schéma útoku je oproti přímým útokům obohacena o třetí stranu. Platí zde tedy: **útočník > třetí osoba > oběť**.

Může se jednat např. o falešné hlášení závadného profilu, neoprávněného použití fotek apod. Třetí osobou je zde administrátor webových stránek, který může přístup k účtu nebo fotkám zablokovat, nebo účet úplně zrušit. Oběť je pak naštvaná na administrátora, nikoli na útočníka, který vše vymyslel a administrátorovi dal falešné podněty.

Administrátoři a správci webových stránek jsou si tohoto jevu vědomi, ne vždy se jim však podaří rozlišit falešné hlášení od oprávněného.

JAK A KDE NAHLÁSIT KYBERŠIKANU PŘES INTERNET

► Nahlášení profilů na Facebooku

1. V levém sloupci kliknout na Nahlásit/blokovat tuto osobu.
2. V rámečku vybrat jednu z možných variant:
 - Nevhodná profilová fotka
 - Falešný profil
 - Nevhodné informace v profilu
 - Nevyžádaný kontakt
3. Odeslat.
4. V dalším rámečku zatržením specifikujete vaši stížnost.
5. Opět zvolíte odeslat.

Facebook čas od času předělává tyto nahlašovací formuláře, je tedy možné, že v době vašeho hlášení budou otázky formulovány jinak.

► Nahlášení jakéhokoli závadného obsahu

1. Kontaktujte správce webu nebo poskytovatele internetových služeb.
2. Pokud selžou, obraťte se na:
 - <http://eporadna.bezpecnykraj.cz>
 - k dispozici on-line poradna
 - oblastního metodika prevence Vaší okresní pobočky Pedagogicko-psychologické poradny:
 - Plzeň-město: kovarova@kapezet.cz,
slivka@kapezet.cz
 - Plzeň-sever: zizka@kapezet.cz

- Plzeň-jih: skarda@kapezet.cz
- Rokycany: cikova@kapezet.cz
- Klatovy: moravcova@kapezet.cz
- Domažlice: hendrichova@kapezet.cz
- Tachov: suchardova@kapezet.cz

3. Možná další pomoc:

- www.bezpecnyinternet.cz/poradna
(provozuje Seznam.cz)
- www.horkalinka.cz (provozuje CZI v rámci projektu Národní centrum bezpečnějšího internetu ve spolupráci s Policií ČR)
- www.internethotline.cz
(provozuje Nadace Naše dítě ve spolupráci s PČR)

JEVY SOUVISEJÍCÍ S KYBERŠIKANOU – KYBERGROOMING, SEXTING

KYBERGROOMING

= druh psychické manipulace, kdy se útočník snaží přesvědčit svou oběť k osobní schůzce. Nejčastějšími oběťmi jsou děti a mládež ve věku 6–15 let.

Fáze:

- ▶ Vzbuzení důvěry a snaha izolovat oběť („Neříkej to rodičům, zlobili by se na tebe...”)
- ▶ Podplácení (dárky, služby; oblíbený trik – dobití kreditu v mobilu – zároveň získají tel. číslo)
- ▶ Závislost oběti na predátorovi („Jen ty mi rozumíš...”)
Osobní setkání
- ▶ Sexuální zneužití, točení, focení pornografických materiálů apod.

SEXTING = rozesílání textu, fotografií, audio- a videozáznamů se sexuálním obsahem

- ▶ Nejčastěji posílány svým (potenciálním) sexuálním partnerům, ale mohou se dostat i k ostatním + zneužití intimních fotografií po rozchodu partnerů.
- ▶ Zaznamenány sebevraždy v přímé souvislosti sextingu – dívky označeny za „kurvy“ nebo „coury“ (včetně ČR, viz video Seznam se bezpečně, www.seznamsebezpecne.cz).

PRÁVNÍ RÁMEC

TRESTNÍ ZÁKONÍK

- Zákon č. 40/2009 Sb., volně ke stažení na internetu, stačí zadat do jakéhokoli vyhledávače.
- Definovány nové trestné činy, mj. vztahující se ke kyber-kriminalitě.
- Následující paragrafy se netýkají pouze kyberšikany, ale i další trestné činnosti, které se mohou lidé dopouštět např. na svých webových profilech.
- Redakční úpravy jsou psané kurzívou.

▶ **Trestné činy proti svobodě**

- § 175 Vydírání
- § 176 Omezování svobody vyznání

▶ **Trestné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství**

- § 182 Porušení tajemství dopravovaných zpráv
- § 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí
- § 184 Pomluva

▶ **Trestné činy proti lidské důstojnosti v sexuální oblasti (ad sexting)**

- § 191 Šíření pornografie
- § 192 Výroba a jiné nakládání s dětskou pornografií
- § 193 Zneužití dítěte k výrobě pornografie

► **Trestné činy proti rodině a dětem**

- § 202 Svádění k pohlavnímu styku

► **Trestné činy proti majetku**

- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

► **Trestné činy obecně ohrožující**

- § 287 Šíření toxikomanie

► **Trestné činy narušující soužití lidí**

- § 352 Násilí proti skupině obyvatelů a proti jednotlivci
- § 353 Nebezpečné vyhrožování
- § 354 Nebezpečné pronásledování (tzv. kyberstalking)
- § 355 Hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356 Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod

► **Jiná rušení veřejného pořádku**

- § 357 Šíření poplašné zprávy (pozor na HOAX!!!)
www.hoax.cz

► **Některé další formy trestné součinnosti**

- § 364 Podněcování k trestnému činu
- § 365 Schvalování trestného činu

!!! O trestný čin se jedná pouze v případě, že je **útok opakovaný** a trvá alespoň 3 týdny (případ od případu, může být i méně).

!!! Při podávání trestního oznámení chtějte sepsat **„Protokol o trestním oznámení“**, nikoli „Protokol o podání vysvětlení“ – na základě tohoto protokolu není zahájeno trestní řízení.

OBČANSKÝ ZÁKONÍK

- Zákon 40/1964 Sb.
- Redakční úpravy jsou značeny červeně a podtržením.

Ochrana osobnosti

- ▶ **§ 11** Fyzická osoba má právo na ochranu své osobnosti, zejména života a zdraví, občanské cti a lidské důstojnosti, jakož i soukromí, svého jména a projevů osobní povahy.
- ▶ **§ 12 (1)** Písemnosti osobní povahy, podobizny, obrazové snímky a obrazové a zvukové záznamy týkající se fyzické osoby nebo jejích projevů osobní povahy smějí být pořízeny nebo použity jen s jejím svolením.
(3) Podobizny, obrazové snímky a obrazové a zvukové záznamy se mohou bez svolení fyzické osoby pořídit nebo použít přiměřeným způsobem též pro vědecké a umělecké účely a pro tiskové, filmové, rozhlasové a televizní zpravodajství. Ani takové použití však nesmí být v rozporu s oprávněnými zájmy fyzické osoby.
= vztahuje se i na fotky dětí z akcí školy, pokud u dětí nejsou uvedena jejich jména

- ▶ **§ 19b, odst. 2 a 3** o neoprávněném použití názvu právnické osoby (např. školy)
- ▶ **§ 424** Odpovědnost za škodu způsobenou úmyslným jednáním proti dobrým mravům

ZÁKON O ELEKTRONICKÝCH KOMUNIKACÍCH

- Zákon 127/2005 Sb.
- ▶ **§ 67** Identifikace zlomyslných nebo obtěžujících volání
- ▶ **§ 93** Zneužití elektronické adresy odesílatele

ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ

- Zákon 101/2000 Sb.

► § 10

► § 44, odst. 2, písmeno c

► § 44a, odst. 3

ZAJIŠTĚNÍ DŮKAZŮ; JSEM OBĚŤ?

- Nemazat z mobilu SMS, MMS zprávy ani zvukové či videozáznamy.
- Nerušit své účty.
- Tisknout e-maily (zprávy z profilů, ICQ atd.) přímo z Internetu – neukládat předtím do Wordu!
- Fotit webové stránky prostřednictvím klávesy PrintScreen, následně zkopírovat do Wordu nebo Malování.



Detail klávesy „Print Screen“

► „VYGOOGLUJTE SE“

- Jméno a příjmení
- Přezdívka/nick
- E-mail
- Telefonní číslo
- Adresa domů
- Jakákoli další hesla, která by mohla vést k Vaší osobě

DOPORUČENÉ KROKY

- Monitoring mezi žáky/studenty (rozhovory, dotazníky...).
- Kyberšikana během vyučování = disciplinární řízení ve škole.
- Jasná pravidla pro používání IT ve škole.
- Využívat vrstevnického prvku.
- Krizový plán školy ještě před incidentem.
- Pojem „kyberšikana“ do školního řádu a prev. programu.
- Blokovací software do školních počítačů.
- Pozitivní školní klima.
- Besedy nejen pro studenty, ale i pg sbor, rodiče, komunitu.
- Školní „specialista“ na kyberšikanu.

SOFTWARE

- Možné programy:
 - Vision 6.7 (dříve MasterEye):
 - aktivní monitorování studentských počítačů
 - dohlížení na práci studentů na internetu
 - sdílení obrazovek, projekce
 - dálkové řízení počítačů v učebně
 - blokace obrazovek, zamykání klávesnic, myší
 - zapínání a vypínání počítačů z učitelského PC
 - distribuce souborů, jejich rozesílání a sběr
 - spouštění programů a otevírání www stránek na dálku
 - PC Control:
 - Podobné jako u Vision
 - <http://www.pachner.cz/html/tipy/pc-control.htm>
 - Demoverze ke stažení
 - Kompletně český program
 - Dostupný ve 3 verzích (edice Start, Standard, Zlatá)

ZABAVOVAT MOBILY PŘI VYUČOVÁNÍ NEBO NE?

Ať už se rozhodnete jakkoli, je třeba mít na paměti, že žádné řešení není samospásné a fungovat bude pouze spolu s dalšími opatřeními, jako je vysvětlování nebezpečí na internetu, preventivní programy ve třídách, diskuze s rodiči atd.

JAK HOVOŘÍ ŠKOLSKÝ ZÁKON Č. 561/2004 SB. O ŠKOLNÍM ŘÁDU:

- **§ 22**, odst. 1, písm. **b** a **c**: (1) Žáci a studenti jsou povinni
 - b) dodržovat školní a vnitřní řád a předpisy a pokyny školy a školského zařízení k ochraně zdraví a bezpečnosti, s nimiž byli seznámeni,
 - c) plnit pokyny pedagogických pracovníků škol a školských zařízení vydané v souladu s právními předpisy a školním nebo vnitřním řádem.
- **§ 29**, (1) Školy a školská zařízení jsou při vzdělávání a s ním přímo souvisejících činnostech a při poskytování školských služeb povinny přihlížet k základním fyziologickým potřebám dětí, žáků a studentů a vytvářet podmínky pro jejich zdravý vývoj a pro předcházení vzniku sociálně patologických jevů.
- **§ 30**, (1) Ředitel školy vydá školní řád; ředitel školského zařízení vnitřní řád. Školní řád a vnitřní řád upravuje
 - c) podmínky zajištění bezpečnosti a ochrany zdraví dětí, žáků nebo studentů a jejich ochrany před sociálně patologickými jevy a před projevy diskriminace, nepřátelství nebo násilí.

DOPORUČENÉ KROKY PŘI ZABAVOVÁNÍ MOBILU

- trezor
- přítomnost dvou svědků
- předávací protokol (typ telefonu, míra opotřebení apod.)
- telefon přebírat vypnutý, popř. bez SIM karty
- vydání do rukou zákonného zástupce, u zletilých studentů do jejich rukou po skončení vyučování

OBSAH:

- základní informace
- kazuistiky
- prevence, diagnostika, intervence
- metodické listy, plány lekcí
- užitečné materiály
- slovníček pojmů
- odkazy na další zdroje informací a materiály

Volně ke stažení na: www.kapezet.cz > metodické materiály > kyberšikana