

# **E-bezpečí**

**Barbora Šomodíková**

# Kyberšikana

- Šikana, která je uskutečněna pomocí komunikačních technologií (mobil, internet)
- Bývá nejčastěji spojována se školním prostředím; oběťmi takové šikany bývají především žáci
- Moderní technologie jsou schopny agresorovi zajistit anonymitu (neznámý e-mail, přezdívka)
- Pro agresora je anonymita výhodou – nemusí se osobně setkat s obětí
- Oběťmi kyberšikany mohou být také učitelé (1/5 anglických učitelů zažila kyberšikanu)
- U dětí je kyberšikana realizována především „z žertu“, u dospělých je situace opačná (účel ublížit)

# Kyberšikana a prevence ve škole

- Určení osoby, která bude „garantem“ prevence kyberšikany
- **1. Pochopení podstaty kyberšikany**
  - Co lze zahrnout do termínu kyberšikana, vědomí nebezpečí, odlišení od ostatních forem šikany, odpovědnost při používání ICT
- **2. Aktualizace existujících postupů a praktik týkajících se patologického chování**
  - Úprava Vnitřního řádu školy a předpisů, týkajících se počítačových učeben, úschova nahrávek případů souvisejících s kyberšikanou, kontrola žáků, k čemu používají internet

# Kyberšikana a prevence ve škole

- **3. Usnadnit obětem postup nahlášení kyberšikany**
  - Jak a komu oznámit kyberšikanu
- **4. Podpora pozitivního využívání technologií**
  - Poutavé a efektivní učení
- **5. Hodnocení vlivu prevence a její účinnosti v boji proti kyberšikaně**
  - Kontroly, průzkumy (žáci, rodiče)
- **6. Vytvoření podmínek k řešení šikany ve škole**
  - Preventivní program, krizový plán

# Kyberšikana a prevence ve škole

- **7. Zajištění vzdělávání členů pedagogického sboru**
  - Psychologie, právo, osobnostně-sociální výcvik, IT kompetence
- **8. Zajištění podpory vedení školy k řešení situace**
- **9. Okamžité řešení kázeňských problémů**
  - Přiměřený trest za každý prohřešek
- **10. Realizace preventivních programů pro žáky**

# Řešení kyberšikany

- Podpora oběti – vyhledání odborníka (preventista, výchovný poradce), obeznámení rodičů
- Doporučení dalšího postupu – schování důkazů, zabránění opakování kyberšikany
- Vyšetření všech případů šikany
- Vyřešení problému, zabránění šíření – použití kázeňských pravomocí
- Práce s problémem, potrestání viníků – snaha, aby se podobná věc neopakovala, důraz na prevenci



# Mobilní telefony a kyberšikana

## • Volání

- Zneužití: nemravné telefonáty, vyhrožování, zastrašování, obtěžování, „prozvánění“
- Prevence: nesdělovat své číslo cizím lidem
- Řešení: zablokování daného tel. čísla, pomoc školy, u závažných případů nahlásit policii

## • SMS

- Zneužití: textové zprávy se sexuální podtextem, výhrůžky, zastrašování, obtěžování
- Prevence: nesdělovat své číslo cizím lidem
- Řešení: zablokování daného tel. čísla, pomoc školy, nahlášení policii – uchovat SMS jako důkaz

# Mobilní telefony a kyberšikana

- **Fotografování, posílání obrázkových zpráv (MMS), videa**
  - Zneužití: pořizování a sdílení ponižujících vyobrazení
  - Prevence: lze těžko zabránit
  - Řešení: zablokování daného tel. čísla, kontakt policie – doložit důkazy



# Internet a kyberšikana

- **Instant messengery (ICQ, Skype)**

- Příklady zneužití: zasílání zpráv se sexuálním podtextem, výhrůžky, zastrašování, obtěžování; kopírování a sdílení textů, zneužití hesla
- Prevence: nesdělovat heslo, opatrnost při psaní
- Řešení: blokace přijímání zpráv

- **Chatovací místnosti (Xchat), diskusní nástěnky, fóra**

- Příklady zneužití: jiná identita násilníka, vytváření přátelství pod falešnými záminkami (získání osobních informací, jejich zneužití, rozšiřování)

# Internet a kyberšikana

- Prevence: při podezření ukončení komunikace, nesdělovat osobní údaje
- Řešení: blokace zpráv, informování správce o nevhodném chování jiného uživatele

## • E-mailly

- Příklady zneužití: zasílání nemravných zpráv, videí, obrázků, vyhrožování, zastrašování, obtěžování, viry, získání hesla
- Prevence: nesdělovat heslo
- Řešení: filtrace příchozí pošty, vytvoření nového účtu

# Internet a kyberšikana

- **Videorozhovor, videokonference, videozáznamy nebo obrázky pořízené webovými kamerami (Skype)**
  - Příklady zneužití: nahrávání a zneužívání záznamů
  - Prevence: mít se na pozoru, s kým realizujeme videorozhovor
  - Řešení: kontakt provozovatele služby
- Další příklady: on-line dotazování (ankety – např. „výzkum“, který posuzuje náš vzhled), webové stránky (web o nás – zesměšňování, ponižování), blogy (nevhodné komentáře na autora, nevhodné obrázky, vytváření falešných profilů), stránky s hostitelskými videi (YouTube; umístění zesměšňujícího videa)

# Happy slapping

- Nový druh šikany; jedná se o nečekané fyzické napadnutí mladistvého nebo dospělého člověka
- Celý čin je nahráván na kameru nebo na mobil komplicem agresora
- Video je vloženo na internet (např. YouTube) a je určeno pro pobavení
- Oběť může být kdokoliv

# Kyberšikana zaměřená na učitele

- Kyberšikana je spojena se sociálními sítěmi, bloggy, běžnými internetovými službami
- V současnosti útočníci začínají využívat služeb serveru [www.ask.fm](http://www.ask.fm)
- [www.ask.fm](http://www.ask.fm) - vytvoření profilu, uživatelé nám mohou klást otázky, my odpovídáme
- Založení falešného profilu učitele žákem → kladení otázek → fiktivní odpovědi
- Server je přeložen do češtiny, je snadno přístupný

# Kyberšikana zaměřená na učitele

## Jak se bránit?

- Motiv – ublížení jiné osobě, diskreditace, zničení jejího osobního a profesního života
- Školní řád – zákaz používání mobilních telefonů při výuce
- Domácí vězení žáků – vyloučení ze školy na několik dní, využíváno v zahraničí
- Školní psycholog – ve spolupráci s učitelem může efektivně zastavit projevy kyberšikany
- Ředitel – zastání se učitele x podlézání rodičům, od ledna 2009 může ředitel oficiálně zakázat užívání telefonů ve výuce



# Kyberšikana zaměřená na učitele

## Jak se bránit?

- Pedagogové by měli žáky učit respektovat pravidla a vytyčené hranice
- Záleží na schopnosti učitele řešit tento problém
- Důležité: důslednost v dodržování pravidel, netolerance překročení vytyčených hranic
- Toto chování pramení zvláště ze špatné domácí výchovy, dítě by mělo respektovat učitele jako autoritu

# Kyberšikana zaměřená na učitele

## Jak se bránit?

- Více než 50 % případů není učiteli hlášena
- Agresi vnímají jako vlastní selhání
- Přesvědčení, že problém sám zmizí a odezní (špatný vzorec jednání – klidně ubližujte ostatním, nic se vám nestane)
- Pasivita vedení školy – žádné řešení situace, žádný trest viníkům
- Nejistota, zda vedení instituce podpoří učitele
- Nežádoucí publicita
- Prank = vtip; vytočení oběti + zachycení situace na mobilní telefon + zveřejnění na internetu

# Dopad kyberšikany na učitele

- V rovině emocionální, fyziologické, behaviorální
- Změny v jednorázových afektech, v dlouhodobějších náladách
- Poruchy spánku, bolest hlavy, břicha, špatná koncentrace, snížená imunita
- Růst konfliktů s okolím (rodina, kolegové, žáci)

# Dopad kyberšikany na děti a mládež

- Negativní emoce – frustrace, rozčílení, rozpaky
- Vyhybavost, sociální izolace oběti
- Ovlivnění chování a účasti ve škole
- Pocit ohrožení vlastního bezpečí
- Zástupné aktivity – např. konzumace sladkostí, zlehčování, opilství
- Vyčerpání organismu, změna váhy, nechutenství, nevolnost, oslabená imunita, sebepoškozování, pokus o sebevraždu

# Kyberšikana a tradiční šikana

- Cíl je stejný – někomu ublížit či ubližovat (fyzicky, psychicky)
- Kyberšikana někdy začíná jako klasická šikana
- Původcem kyberšikany může být kdokoliv (i fyzicky slabý jedinec), stačí mu mít dostatečné znalosti ICT
- Kyberšikanu obvykle provádějí jedinci, kteří jsou původci tradiční šikany
- Původci kyberšikany mohou být sami oběťmi
- Lidé se ve virtuálním světě chovají jinak než ve skutečnosti
- Útočníkovi při šíření kyberšikany pomáhá „publikum“
- Kyberšikana není na první pohled vidět

## KYBERŠIKANA

- Svědci šikany: stovky, tisíce, miliony lidí
- Sdílení na internetu, propagace videa, „vylepšování“ nahrávek ostatními
- Nemožnost zbavit se zveřejněných materiálů

- Kyberšikana je podle výzkumu stejně škodlivá jako fyzická šikana
- Stejná náchylnost k záškoláctví, přemýšlení o sebevraždě
- Příznaky šikany: změny nálady, smutek, špatné školní výsledky, sociální odloučení atd.

## KLASICKÁ ŠIKANA

- Svědci šikany: desítky lidí
- Čin „uzavřen“ ve skupině



# Ochrana před kyberšikanou

- Respektovat ostatní uživatele („Nečiň druhým to, co nechceš, aby činili tobě.“)
- Rozmyslet si, co komu posíláme
- Chránit svá hesla
- Nездělovat své osobní údaje cizím lidem
- Seznámit se s pravidly chatu či diskuze
- Seznámit se s riziky souvisejícími s el. komunikací
- Jak se bránit: ukončení komunikace s útočníkem, blokace útočníka, oznámení útoku (rodičům, učitelům, kamarádům), uchování důkazů!
- Podpora obětí, nebýt lhostejný
- Dopad kyberšikany na oběť je podceňován

- Doporučení rodičům
  - Sledovat varovné příznaky (viz dříve)
  - Kontroly online aktivit dětí
  - Sledování mobilu dítěte
  - Vzdělávat děti v oblasti nebezpečí kyberšikany
  - Mluvit s dítětem o jeho zkušenostech

Kyberšikana v ČR není trestným činem, avšak její projevy mohou být trestnými činy (pomluvy, nebezpečné vyhorožování).

K šíření přispívají zejm. média – touha po senzaci, zvyšování návštěvnosti svých stránek – sekundární útočníci (šířitelé kyberšikany)

# Kybergrooming

- Chování internetových uživatelů, kdy v dítěti vyvolávají falešnou důvěru a připravují ho na schůzku
- Cílem schůzky je pohlavně zneužít nezletilou/zletilou oběť
- Kybergrooming má několik fází:
  - 1. Vzbuzení důvěry a snaha oběť izolovat
  - 2. Podplácení dárky, službami, vznik kamarádského vztahu
  - 3. Vyvolání emoční závislosti oběti na útočnickovi
  - 4. Osobní setkání
  - 5. Sexuální obtěžování, zneužití dítěte
- Nejlepší obrana – prevence (komunikace rodičů s dětmi)

# Kybersex

- Komunikace prostřednictvím internetu, jejímž účelem je sexuální vzrušení; posílání zpráv sexuálního charakteru
- Škodlivý je v tom případě, když jednomu z komunikačních partnerů je nepříjemný
- Objevuje se v chatovacích místnostech (veřejné, soukromé, poté SMS) a v době, kdy jsou mladí lidé nejvíce online
- Motivací je sexuální uspokojení; jakmile je ho dosaženo, dochází k přerušení kontaktu mezi útočníkem a obětí

# Kybersex - obrana

- Neúčastnit se tohoto typu konverzací
- Zdrženlivost při prvním rozhovoru, snaha poznat toho druhého
- Uložení kopie online rozhovoru, ukončení komunikace, oznámit vše moderátorovi chatovací místnosti či fóra, případně kontaktovat policii
- Nebát se říct NE kybersexu
- Neposkytovat osobní informace
- Nesetkávat se osobně

# Sexting

- Rozesílání zpráv, fotografií a videí se sexuálním obsahem prostřednictvím internetu
- Nejčastěji je cílem navázání partnerského vztahu, nebo jeho zpestření
- Tyto materiály pak mohou být zveřejněny na internetu
- Podporuje šíření pornografie mladistvých a dětí (zakázáno)
- V ČR se každý případ posuzuje individuálně (přestupek, trestný čin)
- Sexting provozuje 7 – 9 % dětí ve věku 11 – 17 let a 12 – 23 % dívek ve věku 20 – 25 let



# Rizika sextingu

- Ztráta kontroly nad intimním materiálem
- Materiály mohou internetem kolovat několik desítek let
- Útoky na zobrazenou osobu
- Poškození dobré pověsti či ztráta dobré pověsti zobrazované osoby
- Ztráta zaměstnání, omezení možnosti získat práci

# Proč děti realizují sexting?

- Sexting jako součást romantických vztahů
  - Úvodní části partnerských vztahů – upoutání pozornosti partnera, flirtování, vzrušení
  - Navázaný vztah – znak lásky, intimity, vzájemné důvěry; fyzické odloučení partnerů
- Sexting jako nástroj pro zahnání nudy
- Sexting jako produkt sociálního tlaku
  - Tlak spolužáků, partnera
- Sexting jako produkt konzumní společnosti, sebeprezentace
  - Média prezentují, že odhalovat se a sdílet intimitu je „normální“ - nevhodný model chování pro děti
- Sexting jako nástroj pomsty
  - Vydírání, pomsta ex-partnerům

# Prevence sextingu

- Nepořizovat materiály, na kterých je zobrazeno vaše částečné či úplné obnaení
- Nepořizovat tyto materiály ani pro partnera
- Pokud se materiál již objevil:
  - Kontaktovat administrátory služeb, kde se materiály objevily
  - Využití dostupných blokačních tlačítek
  - Oznámit vše specializovaným poradnám či policii ČR

# Dětská prostituce

- Dítě je použito pro sexuální účely výměnou za peníze nebo odměnu v naturáliích
- Dobrovolná dětská prostituce
  - Vyskytuje se častěji v komunitách, kde lidé žijí spíše „na ulici“
  - Potřeba dítěte přežít ve zmiňovaném prostředí (zvyšující se nároky na vzhled, nutnost finančních prostředků)
  - Vidina rychlého zbohatnutí

# Závislost na kybersexu

- Může pramenit i z jiné závislosti, např. ze závislosti na sexu
- Projevy závislosti
  - Pravidelné trávení času v chatových místnostech, vysílání soukromých vzkazů se záměrem najít kybersex
  - Pravidelné používání anonymní komunikace k zapojení se do neobvyklých sex. fantazií
  - Očekávání sexuálního vzrušení či uspokojení při další on-line akci
  - Přejít z kybersexu k sexu po telefonu

- Ukrývání konverzací před blízkými osobami
- Pocit viny nebo studu kvůli používání internetu
- Nejdříve náhodné vzrušení kybersexem, nyní jeho aktivní vyhledávání
- Masturbování při erotickém chatu
- Snížení zájmu o sexuálního partnera v reálném životě, preference kybersexu jako primární formy sexuálního uspokojení
- Lidé s nízkým sebevědomím, zkreslením své tělesné představy, neléčenými sex. dysfunkcemi apod., jsou náchylnější k rozvoji závislosti na kybersexu



# Stalking a cyberstalking

- Stalking = opakované a stupňované obtěžování, může mít různé formy a intenzitu (SMS, e-maily, telefonáty, dárky)
- Cyberstalking = pokud ke stalkingu útočník užívá ICT (zprávy z messengerů, chatu atd.)
- Systematické obtěžování oběti nevyžádanou a nechtěnou pozorností
- Nejčastější oběti: celebrity, ex-partneři, politici atd.
- Cyberstalker svou oběť nemusí znát, může si ji vybrat za cíl jen proto, že mu připadá zranitelná
- Snaha získat moc nad obětí pomocí strachu
- Od 1. 1. 2010 - trestný čin nebezpečného pronásledování

# Projevy stalkingu

- 1. Opakované a dlouhodobé pokusy o kontakt s obětí (dopisy, e-maily, SMS, telefonáty, dárky, vzkazy na ICQ, Skype apod.)
  - Vyhrožování, vydírání, vyvolávání pocitu viny atd.
- 2. Demonstrace moci a síly stalkera
  - Fyzické pronásledování oběti, výhrůžky násilí, zabitím
- 3. Ničení věcí oběti
  - Poškrábané auto, likvidace domácího zvířete atd.
- 4. Stalker se vydává za oběť
- 5. Snaha o poškození reputace oběti stalkerem
  - Šíření nepravdivých informací o oběti

# Obrana při cyberstalkingu

- Opatrnost při komunikaci
- Rozmyšlení příslibu nového a úžasného vztahu
- Zvážit, zda nehledáme lásku na špatném místě
- Vytyčení hranic a jejich dodržení
- Ignorovat posměchy a hrozby
- Upozornit na hrozby a posměchy moderátora chatu
- Nerozdávat osobní kontakty
- Ignorace, blokace obtěžujících uživatelů

# Profily stalkerů

- Bývalý partner – neschopnost přijmout konec vztahu (partnerský, pracovní, obchodní)
- Uctívač – touha po vztahu s osobou, která stalkera zaujala (pronásledovatelé celebrit)
- Neobratný nápadník – sociální neobratnost, nízká schopnost seznámit se
- Ublížený pronásledovatel – pronásledování oběti kvůli skutečnému nebo domnělému zranění
- Sexuální útočník – útočné až sexuálně agresivní chování
- Poblouzněný milovník – stalker věří, že ho oběť miluje
- Kyberstalkeři – využití ICT

# Sociální inženýrství

- Založeno na ovlivňování a přesvědčování lidí, cílem je oklamat je tak, aby uvěřili, že sociální inženýr (sociotechnik) je člověk s identitou, kterou předstírá a kterou si vytvořil pro potřeby manipulace a ovlivňování lidí
- Sociotechnik může zneužít osoby, se kterými mluví nebo telefronuje, aby získal hledané informace pro další útok
- Způsob získávání důležitých informací od uživatelů bez vědomí, že tak činí

# Manipulativní komunikace

- Etapy:
  - Izolace oběti od okolí
  - Získávání základních informací o manipulovaném
  - Přímá manipulace (vydírání)
  - Manipulace na bázi hoaxu (zfalšovaná zpráva)
- Řešení: být připraven na manipulativní komunikační jevy, informace o jejich nebezpečnosti



# Rizika sociálních sítí

- Sociální sítě – projekty, které jsou zaměřeny na sdílení informací o jednotlivých uživateli, umožňují navazovat sociální vztahy s okolními uživateli, prostor pro interaktivní zábavu
- Rizika:
  - Slouží jako úložiště osobních údajů
  - Uživatelé se chovají v kyberprostoru jinak než v běžném životě
  - Prostor pro existenci sociálně-patologických jevů – kyberšikana, kybergrooming, sexting atd.

# HOAX

- Poplašná zpráva, která varuje před neexistujícím nebezpečím
- Většinou obsahuje výzvu žádající další rozesílání hoaxu mezi přátele, někdy se označuje jako řetězový mail
- Rady:
  - Nevěřit všem informacím, které nám z neznámého zdroje přijdou na e-mail
  - Nesdělovat neznámým osobám naše osobní informace
  - Nedůvěřovat zprávám, které nám naše bankovní instituce posílá e-mailem
  - Vždy si vše ověřovat

- Čím hoaxy škodí příjemcům:
  - Obtěžování
  - Nebezpečné rady
  - Nadbytečné zatěžování linek a serverů
  - Ztráta důvěryhodnosti šířitele
  - Prozrazení důvěrných informací
  - Přetěžování cílové e-mailové schránky
  - Poškození konkrétní instituce
  - Nekritický příjem informace a její další šíření
- Typické hoaxy – falešný poplach, zábavné, prosby

# Další rizikové jevy

- Flaming – nepřátelské chování uživatelů na internetu (urážky, nadávky, vyhrožování) např. v diskusních fórech
- Phishing – praktika, která je zaměřena na krádež citlivých osobních údajů (PIN, hesla k bankovním účtu); realizace zejm. spamem
- SMS spoofing – rozesílání falešných SMS
- Google bombing – zneužití vlastností Googlu
- Troll – uživatel internetu, který narušuje diskusi (chat) vkládáním nevhodného obsahu – provokace ostatních, rozpoutání ohlasů

- Chatroullete – po připojení webkamery se uživatel může vidět s náhodně vybanou osobou
- Planking – položení těla jako prkno tváří dolů na neobvyklém místě (ruce u těla, napjaté tělo), pořízení záznamu, zveřejnění
- Netolismus – závislost na tzv. virtuálních drogách (PC hry, sociální sítě, internetové služby)
- Virální video – nahrávka, která se rychle šíří díky dostupným komunikačním nástrojům – šíří se rychle a nekontrolovaně jako virus; vyvolávají u člověk buzz (rozdruh) – snaha podělit se o toto video s ostatními

- ASMR – reakce organismu, kdy dochází k mrazení nebo mavenčení v oblasti hlavy, horní části těla a podél míchy (spouštěčem je většinou video); relaxační, uspávací účinek, terapeutický efekt
- Nomofobie – strach, že nemůžeme používat mobilní telefon
- Webcam trolling – podvržené videozáznamy, účelem je pobavit se na úkor předem vyhlášeného chatujícího, který pak plní rozkazy či příkazy, které jsou mu zadávány



# Děti a závadný obsah na internetu

- Děti se na internetu mohou setkat s následujícím konfrontovaným obsahem:
  - 1. Dětská pornografie a nelegální sexuální praktiky
  - 2. Obsah spojený s extremismem
  - 3. Nelegální obchodování, nelegální nabídka drog a zakázaných látek
  - 4. Obsah, který porušuje autorská práva
  - 5. Další nelegální obsah
  - 6. Pornografie (předládána dítěti)

# Zdroje

<https://www.e-bezpeci.cz/index.php/home>