**Rizika ICT a internetu**

Rizikové vlastnosti ICT a internetu

* propojení , přístupnost... (v čase i prostoru)
* anonymita
* virtuální realita (zdánlivá, možná, neskutečná)
* široký dosah, globálnost
* dospělí o krok za dětmi, učitelé za žáky

Riziková komunikace

* on-line chat
* e-mail
* videokomunikace, skype
* sociální sítě a virtuální komunity
* GSM sítě (sms, mms, hlasové služby)
* rychlý vývoj nových forem – složitost zjištění aktuální situace, nedostupnost dat
* zpravidla – vědomá spolupráce oběti
* snáze napadnutelné – znevýhodněné osoby
* nedostatečné znalosti hrozícího nebezpečí
* virtuální přátelení atraktivnější než reálné (kamarádi, členové domácnosti...)
* děti a mládež – umí používat, neumí se bránit
* internet jako úniková strategie, reakce
* útočník – často falešná identita

Kybergrooming

* manipulativní techniky a postupy
* cílem – vyvolání falešné důvěry a osobní schůzky
* důsledek – napadení, sexuální zneužití...
* využití sugestibility a nedostatku kritického myšlení dětí
* často motivace – peníze či jiná odměna (mp3 přehrávač, hry....mobil)
* vyhledání potenciální oběti
* snaha navázat přátelský vztah a vzbudit důvěru
* snaha o izolaci oběti od blízkých
* rozvíjení vztahu – dárky, uplácení, služby
* cílem – emoční závislost a následné setkání
* *Vrátný Pavel Hovorka přes služební internet* ***vyhledával mladistvé chlapce ze sociálně slabšího prostředí****,* ***zjišťoval*** *jejich zájmy a* ***sliboval*** *jim peníze nebo splnění jejich přání za to* ***požadoval*** *jejich nahé fotografie. Pomocí fotografií a prozrazením jejich sexuálního zaměření pak chlapce* ***vydíral*** *a* ***nutil*** *k orálnímu či análnímu sexu. Svou první oběť získal tak, že jí v červenci roku 2005* ***namluvil, že vyhrála soutěž*** *»Dítě VIP«Odměnou byl pobyt v Praze v jeho vrátnici, kde chlapce původem z dětského domova znásilnil. Hovorka využíval k seznamování* ***internetové servery****,* ***nejdříve chatoval, pak telefonoval, následovalo pozvání oběti k němu do práce****. Soud uznal Hovorku vinným celkem ze sedmi případů pohlavního zneužívání, třinácti případů vydírání. Navíc také ohrožování výchovy mládeže a ze svádění k pohlavnímu styku. Hovorka byl odsouzen na 8 let vězení.“(E-bezpečí, 2009)*

Kyberšikana

* druh šikany, který využívám ICT technologie k agresivnímu napadání oběti
* ne fyzické , nýbrž psychické napadání (vyhrožování, zastrašování, nadávání, ponižování, zesměšňování, vydírání, publikování ponižujících fotografií...
* agresor napadá oběť samoúčelně – s úmyslem ublížit
* využití mocenské převahy nad obětí
* často „technologická“ převaha – ovládá lépe než oběť, ta se nemůže bránit
* Cílem kyberšikany je
* někomu ublížit nebo
* zesměšnit
* za použití elektronických prostředků.
* úmyslné, nepřátelské chování, které se obvykle opakuje
* jednotlivec nebo skupina útočníků ubližuje takovým způsobem, že se oběť nemůže účinně bránit.

Kyberšikana je například:

* hanlivé a urážlivé zprávy prostřednictvím SMS, MMS nebo internetu
* zesměšňující nebo ponižující obrázky či videa posílané e-mailem nebo vyvěšené na webové stránce
* webové stránky, blogy s cílem zesměšnit někoho
* instant messageingem
* zesměšňování prostřednictvím komunitních sítích
* zneužití identity oběti rozesíláním obtěžujících a urážlivých zpráv pod jejím jménem

Kyberšikana není oprávněná kritika na internetu bez zlého úmyslu, bez nadávek a ponižování.

Formy kyberšikany

* prostřednictvím mobilního telefonu (lživá, hanlivá SMS zpráva) – 68 %
* chaty (ICQ, AOL,…) – 30 %
* e-maily – 29 %
* komunitní sítě (Facebook, Libimseti) - 14 % - vzhledem k prudkému rozvoji sociálních sítí se dá předpokládat, že se bude zvyšovat.
* Kyberšikana
* **OBĚTÍ KYBERŠIKANY JE 10% DĚTÍ**
* osobní zkušenosti s kyberšikanou v posledním půlroce na **základě přečtené definice** deklarovalo celkem **6 % dětí**
* při dotazování na jednotlivé způsoby obtěžování v posledním půlroce (e-mail, telefon, video, blogy apod.), celkový podíl dětí, které přišly do styku s některou z konkrétně jmenovaných forem kyberšikany (či obtěžování na Internetu), vzrostl na **10 %**
* Komu se děti svěřují a jak řeší

**Komu se děti svěřují**

* 40% kamarádům
* 37% nikomu – nechávají si to pro sebe, řeší si to sami
* 31% rodičům
* **pouze 8 % učiteli**

**Jak ji děti řeší**

* 37% obětí – ignorování agresora a odříznutí se od něj (výměna SIM karty, změna e-mailu…)
* 34% – kontakt s agresorem, snaha domluvit se
* 26% – zapojení rodičů
* 24% – útok na agresora (snaha kyberšikanu vrátit)
* **10%** – **případ řeší škola**
* Kyberšikana a klima třídy
* **Pro vznik šikany i kyberšikany - klíčové postavení dítěte ve třídě** (jak je ve třídě spokojeno a kolik má dobrých kamarádů)
* 39% českých dětí ve věku 8–15 let je ve svých třídách ***velice spokojeno***
* 53% dětí je se třídou ***celkem spokojeno***
* 9% českých dětí se cítí ***spíše nespokojeno nebo velmi nespokojeno*** (to představuje zhruba 78.000 dětí v ČR)
* 78% dětí má ve třídě více dobrých kamarádů
* zhruba 20% dětí deklaruje jednoho dobrého kamaráda
* 3% dětí **nemá** ve třídě kamaráda žádného (zhruba 23.000 dětí z ČR)

Kyberšikana učitelů

**Více než polovina dotázaných dětí již slyšela o případu kyberšikany učitele**

* 6 % dětí uvedlo, že se případ kyberšikany učitele odehrál u nich na škole
* 7 % dětí zná případ z jiné školy
* 32 % dětí zná nějaký případ z médií
* Vnímavost k případům kyberšikany učitelů roste s věkem dětí
* **Zhlédnutí videa zesměšňující učitele**
* 31 % dětí někdy zhlédlo zesměšňující video - chlapci výrazně více než děvčata (34% x 27%)
* Četnost sledování videí zesměšňujících učitele roste s věkem - **více než polovina žáků v 8. – 9. třídě ZŠ alespoň jednou zhlédla takové video**

Postoje dětí

* **děti považují kyberšikanu za nebezpečnou, ale osobně se jí příliš nebojí**
* 69% dětí považuje kyberšikanu za nebezpečnou
* 70% dětí, **které nebyly kyberšikanovány**, se domnívá, že se jim něco takového nemůže stát
* 14% dětí si myslí: necítil bych se strašně, pokud bych někoho zesměšňoval na internetu
* 22% dětí si myslí: natáčet učitele na video je velká zábava
* 17% dětí si myslí: oběti si za to mohou sami
* 15% dětí si myslí: kyberšikana je jen legrace
* 8% dětí si myslí: kyberšikana je vzrušující

Agresor bývá ze stejné školy

* **nejméně 78% agresorů je ze stejné školy jako oběť**
* **6% dětí přiznalo, že v posledním půlroce využilo některý z prostředků kyberšikany (někoho zesměšnily, ztrapnily, …)**
* Výskyt agresorů je závislý na věku
* použití některého z prostředků kyberšikany přiznalo 10% dětí z 8.-9. tříd, oproti 2% z 2. -3. tříd.
* 51% agresorů – přímo ze třídy
* 27% - ze školy
* 22% - agresor zůstal anonymní nebo pro oběť neznámý
* Zkušenosti dětí s ICT

**Počítačové dovednosti**

* To, že výskyt kyberšikany se s věkem zvyšuje, souvisí s tím, že s věkem roste i počítačová gramotnost dětí a také způsob využití jednotlivých médií.

**Mediální vybavenost**

* souvislost s věkem, ne však tak výraznou, protože i menší děti jsou velmi dobře počítačově vybaveny, ve věku 14. -15. let je vybavenost v podstatě univerzální.

**Vybavenost mobilním telefonem**

* 84% dětí z 3. až 9. tříd má mobil
* 66% – ve věku 8 – 10 let
* 96 % dětí 14 – 15 let

**DOPORUČENÍ – co může dělat rodič**

* přijměte fakt, že život ve virtuálním světě k vašim dětem patří
* pokud se v něm naučíte pohybovat, pomůže vám to pochopit vaše dítě
* vysvětlete dětem, že ve virtuálním světě je čekají i rizika
* naučte své dítě chránit svou identitu
* pokud zjistíte, že agresor je ze školy dítěte, kontaktujte zástupce školy
* uložte nebo vytiskněte maily, SMS… - může posloužit jako důkazní materiál

**DOPORUČENÍ – co může dělat škola**

* vzdělávejte učitele, jak v této oblasti postupovat – naučte ho vyhledat pro šikanované dítě pomoc
* zapojte ICT pracovníka do preventivního programu

**Nepodceňujte klima ve třídě, je pro rozvoj šikany i kyberšikany určující**

* sledujte spokojenost dětí ve třídě
* mluvte o vztazích
* seznamte děti s pojmem kyberšikana

**Jděte dětem naproti**

* pokud si na některé ze sociálních sítí založíte svůj profil, může to být prostředek pomocí něhož budete komunikovat s dětmi
* naučte děti využívat všechny softwarové blokace a ochrany technického rázu
* mluvte s dětmi o tom, jak chránit svou identitu

Jak to může vypadat - příklady

* *„Moji rodiče jsou rozvedeni a žiji s matkou a sourozenci a otce nezajímám, tak se mi každý směje a rozebírají to na Internetu a přes SMS. Řekla mi to sestra jednoho z deváťáků má spolužačka. Trvá to občas i dnes a nikdo to neřeší“*
* *„Nadávali mi do SMS, že jsem hnusná, škaredá potvora.“*
* *„Někdy kluci i holky mi píšou urážlivý SMS a taky mě natočili na tel. A dali to na Internet-jak se svlékám a nebo jsem na WC“*
* *„Na internetovém portálu byla založena skupina „Nesnášíme Annu V.“ kam ostatní přidávají posměšné komentáře“*
* *„Spolužáci asi tak před dvěma lety mi psali hanlivé SMS a maily, jako že jsem „špína, zavšivená, atp.“, ve škole do mne strkali, plivali na mne až se to dověděla učitelka a řešila to“*
* *„Pořád mě pronásledovali na chatu, když jsem si povídala s ostatními uživateli Internetu a ztrapňovali mě a nadávali na moji rodinu a když jsem se odhlásila a přihlásila na jiný chat, tak mě našli a zase nadávali.“*
* *„Do třídy přišla nová spolužačka, občas jsme se spolu hádaly a kvůli jedné z hádek napsala na svůj blog dlouhý článek se všemi možnými nadávkami“*

Kyberstalking

* spíše subkategorie kyberšikany
* pronásledování oběti
* trestní zákoník : dlouhodobé pronásledování tím, že je oběť vytrvale kontaktována prostřednictvím prostředků elektronických komunikací, písemně nebo jinak (sociální sítě...)

Sexting

* aktivní distribuce digitální pornografie
* rozesílání sms, obrázků či videozáznamů
* distribuce dětem (ohrožování výchovy dítěte)
* výroba a přechovávání, případně zneužití dítěte k výrobě

Happy slapping

* *veselé fackování*
* náhodné nebo nečekané napadení oběti, její natočení na video a následná publikace na vhodném úložišti v internetu (youtube.com...)
* zobrazení brutálního napadení oběti... reakce učitele po cílené provokaci...

Zprávy a e-maily

* *spoofing* – zasílání sms s falešnou identitou
* *hoaxy* – poplašné zprávy
* *spam*

phishing a pharming

* *phishing* – podvodné techniky zaměřené zejména na získání osobních údajů, hesel...
* *pharming* – phishing s využitím backdoorových virů, které okopírují citlivé údaje a odešlou na specifickou adresu

**Prevence rizikové komunikace, poučení o rizicích a hrozbách**

* PRVOK (Centrum prevence rizikové virtuální komunikace)
* http://cms.e-bezpeci.cz/
* http://www.prvok.upol.cz/
* http://www.e-nebezpeci.cz/
* http://www.saferinternet.cz/ – Národní centrum bezpečnějšího internetu
* rodičovské zámky a filtry
* http://www.seznamsebezpecne.cz/

Klíčové zdroje a odkazy

* Pešat, Pavel. Rizikové jevy související s využíváním informačních a komunikačních technologií ve vzdělávání na základní škole (sborník z konference)
* www.minimalizacesikany.cz
* http://www.msmt.cz/pro-novinare/metodicky-pokyn-k-prevenci-a-reseni-sikanovani-mezi-zaky