# Nebezpečí na internetu

# Přehled

- Útoky proti strojům:
- proti osobním počítačům, viry,
- útoky proti serverům, DoS, DDoS, hackeři.
- Útoky proti lidem:
- riziková komunikace.

# Aktuálně (9. 1. 2015)

- http://zena.centrum.cz/deti/zajimavosti/clanek.phtml?id=805742

VÝZKUM

# KYBERŠIKANA NA ZŠ

ZPRACOVAL PRO POTŘEBY ICTK PAVEL BROŽA

# Kyberšikana na českých školách – výsledky výzkumu

Výzkum byl realizován v rámci projektu Minimalizace šikany (MIŠ)[1].

Koncem roku 2009.

Cílem byl popsat tehdejší situaci v oblasti kyberšikany u českých dětí.

# Kyberšikana na českých školách – výsledky výzkumu

Znalost pojmu kyberšikana je mezi dětmi velmi nízká (39 % žáků).

Pojem vysvětlen ve škole jen v 18 % případů.

V posledním půlroce bylo obětí kyberšikany 10 % dětí.

Polovina žáků 8. a 9. ročníku ZŠ zhlédlo alespoň jednou video zesměšňující učitele.

# Kyberšikana na českých školách – výsledky výzkumu

Kyberšikana souvisí z 95 % s klimatem třídy.

Děti považují kyberšikanu za nebezpečnou, ale osobně se jí příliš nebojí.

Nejméně 78 % agresorů je ze stejné školy jako oběť.

V 80 % případů začala *jako sranda*.

***Dovednosti v používání digitálních technologií u žáků rostou, poroste i počet případů kyberšikany.***

# Nebezpečí elektronické komunikace – výsledky výzkumu

Centrum prevence rizikové virtuální komunikace Pedagogická fakulty Univerzity Palackého v Olomouci[2].

Dotazníkový systém portálu E-Bezpečí.

# Nebezpečí elektronické komunikace – výsledky výzkumu

V roce 2009 se setkalo s „kyberšikanou“ téměř 47 % dětí ve věku 11 až 17 let.

- Nepříliš relevantní, protože započítána i jediná zkušenost.

V roce 2012 se setkalo s „kyberšikanou“ téměř 57 % těchto dětí.

Zatím nejčastěji verbální útoky,

- 15,8 %, respektive 31,6 %.

Počet útoků využívající sociální sítě vzrostl na 40 %.

# Nebezpečí elektronické komunikace– výsledky výzkumu

**Kyberšikana učitelů**

- Roste počet případů kyberšikany učitelů.
- Již 11 % útočníků zkoušelo kyberneticky šikanovat učitele.
- Rostoucí trend.

- Podle výzkumu rizikového chování dětí v prostředí internetu, který realizoval projekt E-bezpečí a Seznam.cz v roce 2013, přiznalo 7,23 % dětí, že na internet umístilo svoji sexy fotografii nebo video, na kterých jsou částečně nebo úplně nazí.
- Přes 11 % dětí uvedlo, že to za ně udělal někdo cizí.
- Zároveň nám přes 21 000 respondentů uvedlo, že je v 7,33 % na internetu někdo vydíral.

# Riziková komunikace

- Seznam se bezpečně
- http://www.seznamsebezpecne.cz/

# Riziková komunikace

- kybergrooming,
- kyberšikana,
- kyberstalking,
- sexting, distribuce pornografie,
- happy slapping (náhodné napadení),
- e-maily, SMS zprávy (hoax, spam, SMS Spoofing),
- phishing a pharming.

# Informace

- Centrum prevence rizikové komunikace na facebooku http://www.fbportal.cz/bezpecnostni-rizika-facebooku/
- Příručka pro učitele a rodiče: Rizika virtuální komunikace www.e-nebezpeci.cz

- Příručka

# Kybergrooming

- Chování uživatelů internetu, které má vyvolat falešnou důvěru.
- Je druhem psychické manipulace realizované prostřednictvím elektronické komunikace

# Hovorkův případ

Muž, který pracoval jako ostraha v tiskárnách, sponzoroval dětské domovy. Jeho první oběť vyhrála jím vypsanou soutěž "dítě VIP", za což měla strávit dva týdny v Praze. Chlapec tak v červenci 2005 pobýval několik dnů u Hovorky na vrátnici, kde ho muž zneužil. Zhruba po dvou třetinách plánovaného pobytu však sociální pracovníci poslali kluka kvůli nevyhovujícím podmínkám zpět do domova.

Další oběti si již Hovorka vyhledával na seznamovacích serverech. Většinou si s nimi po nějaký čas dopisoval a telefonoval. Poté je pozval k sobě do práce, kde několik z nich 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.

# Kyberšikana

- Nejčastější projevy kyberšikany:
  - Publikování ponižujících záznamů
  - Ponižování a pomlouvání
  - Krádež identity
  - Ztrapňování pomocí falešných profilů
  - Provokování a napadání v online komunikaci
  - Zveřejňování cizích tajemství
  - Vyloučení z virtuální komunity
  - Obtěžování

# Kyberšikana
# Bullycide

Oběť (kyber)šikany je dohnána k sebevraždě.

# Kyberstalking

- Pronásledování v kyberprostoru.
- Oběť je opakovaně kontaktována a obtěžována prostřednictvím prostředků elektronických komunikací, nyní zejména: SMS, e-mail,  v sociálních sítích (Facebook, Spolužáci, Lidé, komunity na Skype či ICQ aj.).
- Trestní zákon 40/2009 Sb. § 354 (pro trestně zodpovědné).

Typické projevy:

- opakované a dlouhodobé pokusy kontaktovat oběť,
- demonstrace moci a síly stalkera (výhružky, které v oběti budí oprávněný strach a obavy),
- destrukce věcí (majetku) oběti (poškrábané auto, zaslání viru e-mailem, rozbité okno, zabití domácího zvířete),
- očernění oběti (šíření nepravdivých zpráv o oběti práce, rodina, přátelé, sousedé).

# Sexting, distribuce pornografie

- Zprostředkování digitálního obsahu s explicitní sexuální tématikou.
- Dětská pornografie (reálná i „animovaná“)
- Trestní zákon 40/2009 Sb. § 192, 193 (pro trestně zodpovědné).

# Happy slapping (kyberšikana)

- Náhodné či nečekané napadení oběti, její natočení na video a následné publikování videozáznamu na úložišti v Internetu.

# Phishing

- druh internetového podvodu, kterým se podvodníci snaží z uživatelů internetového bankovnictví vylákat přístupové údaje k účtům a zneužít je pro svoje obohacení.
- K získání těchto důvěrných informací využívají podvodné e-maily, které na první pohled vypadají, že jsou odeslány přímo z banky a snaží se přesvědčit uživatele, aby kliknul na odkaz.

# Hoax

- je šíření poplašných, nebezpečných a zbytečných řetězových zpráv.
- **Informace o tom, které podvodné emaily jsou nejrozšířenější najdete na Serveru HOAX.cz: http://hoax.cz/cze/**

# Loterie

- lidem jsou rozeslány e-maily s oznámením o výhře vysoké částky obvykle v eurech nebo dolarech.
- V případě, že oslovený výherce kontaktuje provozovatele loterie, je mu sděleno, že výhra bude vyplacena, jakmile zaplatí manipulační poplatek ve výši v přepočtu až několika desítek tisíc korun, který samozřejmě není možné odečíst ze slíbené výhry.

# Malware

- je všeobecné označení pro škodlivý kód.
- Nejčastěji to může být počítačový vir, červ nebo stále častěji Trojský kůň.
- Dříve docházelo k šíření přímo e-mailem, ale v dnešní době se stále více využívá situace, kdy v textu e-mailu je pouze odkaz na tento škodlivý kód pod záminkou, že odkaz směřuje na zajímavý obrázek, video nebo e-pohlednici.

# Řetězové emaily

- Mnoho řetězových zpráv však neobsahuje úplné nebo přesné informace nebo postupným šířením dochází občas i k jejich úpravám.
- Existují také zprávy, týkající se pouze určité skupiny uživatelů, přesto jsou často rozesílány na veškeré e-mailové adresy, které jsou v adresáři.
- Takové chování není přímo v souladu s Netiketou.
- Některé z nich jsou původně napsány a rozeslány s dobrým úmyslem.

# Sociální sítě jako prostředí pro nebezpečnou virtuální komunikaci

Problémy:

- Sociální sítě slouží jako úložiště osobních údajů.
- Uživatelé sociálních sítí se chovají v kyberprostoru jinak než v běžném životě.
- Sociální sítě jsou prostorem pro existenci sociálně-patologických jevů,

odkaz

# Kdo je kdo aneb identita účastníka Internetové komunikace

- skutečná (+nickname = přezdívka)

– existující osoba, kterou lze snadno identifikovat (jméno, e-mail, adresa, foto, IP-adresa,

- zfalšovaná (zcizená) (+nick)

– účastník se vydává za jinou, skutečně existující osobu, kterou lze snadno identifikovat (jméno, e-mail, adresa, foto, IP-adresa), identita samotného útočníka skryta.

# Identita

Zveřejňování osobních údajů: Co, kdy a jak zveřejnit?

- služby vyžadující skutečnou či dohledatelnou identitu (e-learning, školní síť, on-line banking),
- služby nevyžadující skutečnou či dohledatelnou identitu (sociální sítě, chaty, seznamky…),

“schizofrenní“ matení dětí ve věku do 9–10 let vychovávaných k poctivosti a pravdomluvnosti,

které se musí učit skrývat v Internetu (1/4 by zveřejnila své osobní údaje).

# Digitální komunikace dětí a mládeže

- Vnímání digitálního světa očima dětí (digitální generace) podstatně odlišné od našeho.
- My si dovedeme představit svět bez počítačů, děti už ne.
- Děti žijí více přítomností, méně budoucností – jiná stupnice hodnot.
- Digitální technologie a sociální sítě – únik od sociální izolace doma a ve škole.

# Riziková komunikace a kyberšikana ve vzdělávání

- Prevence v RVP ZV - Problematika prevence se obecně prolíná celým výchovně-vzdělávacím procesem. Koncepčně je zapracována do ŠVP a
- Minimálního preventivního programu školy.(VÚP Praha)
  - VO: Člověk a jeho svět (1. stupeň),
  - Člověk a zdraví (2. stupeň).
  - Průřezová témata Osobnostní a sociální výchova a Mediální výchova

# Co dělat proti on-line NEBEZPEČÍ

- Opatření preventivní, průběžná i následná:
  - technická (poskytovatelé připojení, filtry, červené tlačítko),
  - legislativní (nelze vůči dětem a zahraničí),
  - represivní (policie, rodiče, škola),

- výchovná (rodina, škola, příznivé
- školní/rodinné klima, NGO, „dobré mravy“),
- vzdělávací (škola, rodina, NGO, E-bezpečí).
- ICT vzdělání učitelů a rodičů!

Žádné opatření nemá 100% účinnost,

při aplikaci jednotlivých opatření je nezbytná promyšlená koordinace

# Co dělat proti on-line NEBEZPEČÍ

- Chladná hlava, poučený postup.
- Prevence a informování dětí, mládeže,
- rodičů, učitelů.
- PRVOK – Centrum rizikové virtuální
- komunikace UPOL, weby e-bezpečí a e-nebezpečí.
- Národní centrum bezpečnějšího internetu Safer Internet.

# Úloha školy

- Osvěta probíhá od 1. třídy.
- Pravidla používání digitálních technologií (ICT) ve škole zakotvena ve školním řádu.
- Minimální preventivní program.
- Řád školní sítě a počítačových učeben.

- Pedagog orientující se v problematice!

# Pravidla chování v síti

- http://www.hoax.cz/hoax/netiketa
- http://www.jabber.cz/wiki/Netiketa

# Netiketa

- http://www.lupa.cz/clanky/netiketa/
- Pojmem netiketa bývá označována sada doporučení pro slušné chování v síti, čili jakýsi Guth-Jarkovský moderní doby. Přestože její kořeny sahají až do velmi raných dob Internetu, neztrácí na významu. Při pohledu na některé výdobytky elektronické komunikace se člověk leckdy neubrání úvahám, že by snad měla být zařazena do povinného vzdělání.

# http://wiki.siliconhill.cz/Netiquette

**Desatero slušného chování - základní pravidla netiquette**

- Neměl bys používat počítač k tomu, abys škodil ostatním lidem.
- Neměl bys bránit ostatním lidem pracovat na počítači.
- Neměl bys čmuchat v cizích souborech.
- Neměl bys pomocí počítače krást.
- Neměl bys pomocí počítače šířit fámy.
- Neměl bys používat ani kopírovat program, za který si nezaplatil.
- Neměl bys používat prostředky na cizím počítači bez svolení.
- Neměl bys upírat ostatním lidem užívat svůj intelekt.
- Měl bys myslet na společenské souvislosti programu, který píšeš.
- Měl bys používat počítač s respektem a uvážením.
- Měl bys znát aspoň základy češtiny, popřípadě jazyka který hodláš používat.

# Zdroje materiálů

1. Bullycide in America [online]. [citováno 18. 11. 2014]. <http://www.bullycide.org/>.

E-bezpečí. Internetový portál [online]. c2009 [citováno 18. 05. 2014].

http://www.e-bezpeci.cz/

2. E-nebezpečí. Internetový portál [online]. c2010 [citováno 18. 11. 2014]. http://www.e-nebezpeci.cz/

3. Krejčí, V., Kopecký, K. Nebezpečí elektronické komunikace [on-line]. c2010-02-02. [cit 2014-05-10].

<http://prvok.upol.cz/index.php/component/docman/doc_download/5-nebezpei-internetove-komunikace-e-bezpei-prvok-2009-2010>.

4. Pešat, P. Komplexní přístup v boji proti nebezpečí z kyberprostoru aneb není jednoduché cesty... [on-line]. c2010-04-08. [cit 18.11.2014]