

MANAGEMENT KYBERNETICKÉ BEZPEČNOSTI

TÉMA Č. 5
KYBERŠIKANA

pplk. Ing. Petr HRŮZA, Ph.D.

Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky

E-mail.: petr.hruza@unob.cz

Operační program Vzdělávání pro konkurenceschopnost

Projekt: ***Vzdělávání pro bezpečnostní systém státu***

(reg. č.: CZ.1.01/2.2.00/15.0070)



OBSAH

1. Vysvětlení pojmu kyberšikana.
2. Základní projevy.
3. Typy kyberšikanování.
4. Typologie kyberstalkerů.
5. Oběti kyberšikany.
6. Případy kyberšikany.
7. Ochrana před kyberšikanou.



Literatura

- Kopecký, K. [online]. 2011 [cit. 2011-12-08]. Jak na prevenci kyberšikany. Internetový portál E-Bezpečí. Centrum PRVoK PdF UP: Olomouc, 2011. Dostupné: <<http://www.e-bezpeci.cz/index.php/rodice-ucitele-zaci/361-prevence-kybersikany>>.
- ROTTOVÁ, Nina, a kol. *Kyberšikana a její prevence – příručka pro učitele*. První. Plzeň: DRAGON PRESS s.r.o., 2009. 108 s. ISBN 978-80-86961-78-1.
- *E-nebezpeci* [online]. 2010 [cit. 2011-12-10]. Materiály pro studium, studie atd - E-nebezpečí. Dostupné: <<http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd>>.
- *Poradenskecentrum* [online]. 2010 [cit. 2011-12-12]. Metodika k prevenci a řešení kyberšikany. Dostupné: <<http://www.poradenskecentrum.cz>>.

Základní pojmy

- **Kyberšikana** je úmyslné, opakující se a nepřátelské chování, jehož cílem je ublížit oběti za použití informačních a komunikačních technologií.
- Kyberšikana je druh šikany, který využívá elektronické prostředky jako jsou mobilní telefony, e-maily, pagery, internet, blogy a podobně.
- Zatímco klasická šikana se může projevovat jak fyzickými útoky tak útoky psychickými, kyberšikana se odehrává pouze v psychické rovině, je tedy druhem psychické šikany. Kyberšikana se projevuje především ponižováním, nadáváním, urážením, zastrašováním, vyhrožováním, vydíráním, obtěžováním a pronásledováním oběti - což jsou typické projevy psychické šikany.

Základní projevy kyberšikanování

- anonymita,
- jednosměrná komunikace,
- zasílání urážejících, útočných, zesměšňujících a zastrašujících či obět' zesměšňujících emailů a SMS zpráv, výhružné telefonáty, obtěžující chatování,
- tvorba webů a blogů, které různými způsoby (verbálně, graficky, zvukově) obět' urážejí a ponižují,
- fotografování a nahrávání oběti a posílání pořízených záběrů známým dotyčného nebo jejich vystavení na internetu.



Typy kyberšikanování

- **Přímé útoky** – zasílání SMS zpráv a emailů, kradení hesel, blogování, zveřejňování lživých informací a obrazových materiálů na webu, internetové hlasování, při interaktivním hraní, rozesílání virů, vydávání se za někoho jiného.
- **Kyberšikana v zastoupení** – agresor využívá k šikanování nevědomého komplice.
- **Kyberšikana v zastoupení je mnohem nebezpečnější.**

Přímé útoky

- Kradení hesel a následné zneužívání osvojeného účtu
- Blogování - zveřejňování intimních informací nebo pomlouvání prostřednictvím blogu.
- Zveřejňování choulostivých nebo lživých informací a obrazových materiálů na webových stránkách nebo jejich šíření telefonem, např. pornografické fotografie s tváří oběti.
- Posílání ponižujících obrázků přes email nebo mobilní telefony – nejčastěji posílání obrázků, fotografií a video nahrávek spolužáků nebo učitelů.
- Internetové hlasování - Kdo je super a kdo není? Kdo je největší kráva v šesté třídě? Tyto typy otázek nekontrolovatelně běží v různých internetových hlasováních a všechny jsou vytvořeny někým z blízkého okolí.

- Interaktivní hraní – při hraní na herních zařízeních typu X-Box Live a Sony Play Station 2 Network jsou děti v živém spojení přes chat nebo telefonování prostřednictvím Internetu s kýmkoli, na koho v online hře narazí. Někdy ostatní slovně napadají, uzamykají před někým hrací místnost, vypouštějí do éteru nepravdivé zvěsti, nebo nabourávají cizí účty.
- Rozesílání zákeřných kódů (viry, spyware, hackování).
- Zasílání pornografických nebo jiných obtěžujících emailů a zpráv – útočníci své oběti zapisují do různých hromadných seznamů a jim pak chodí tisíce nevyžádaných zpráv (v případě pornografie je pak například mohou rodiče podezírat z navštěvování erotických stránek).
- Vydávání se za jiného člověka – svoji oběť

Typologie kyberstalkerů

- Pro jednotlivé typy kyberagresorů jsou typické různé styly kyberšikanování. Liší se i způsoby, jak se skrývají nebo jak svoji činnost šíří.

„Pomstychtivý andílek“

- Pro tento typ je příznačné, že se jako agresor vůbec nevnímá. Vidí se jako „zlonapravující“, představuje si, že chrání sebe či ostatní před „zloduchem“, který díky jeho intervenci teď po právu trpí. Často sám (kyber)šikanu zažil a nyní oplácí stejnou mincí.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ



Bažící po moci

- Někteří kyberagresori chtějí dávat najevo svoji autoritu, ukazovat, že jsou dostatečně silní na to, aby ostatní dělali, co po nich chtějí. Snaží se ovládat druhé prostřednictvím strachu.

„Sprostý holky“

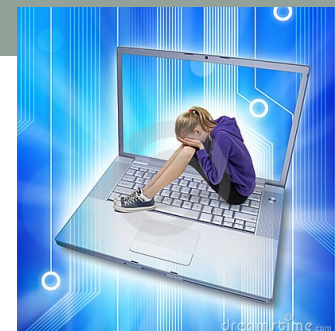
- Tento typ je znuděný nebo hledá zábavu. Typickými agresory jsou v tomto případě děvčata. Nejčastěji šikanují jiná děvčata, ale neuniknou jim ani chlapci.

Neúmyslný kyberagresor

- Tyto agresory vůbec nenapadne, že by agresory mohli být. Hrají na ostatní online uživatele, že jsou „tvrďáci“, mohou se vydávat za někoho jiného, nebo peprně odpovídat na nenávistné či provokativní zprávy, které obdrží například v chatovací místnosti.



Oběti kyberšikany



U 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. Zatímco oblíbený spolužák se stává obětí tradiční šikany jen zřídka, neboť má mnoho kamarádů, kteří jej chrání, ve virtuálním světě ho před útočníky neochrání nikdo – ani nejlepší kamarád nemůže zabránit tomu, aby mu agresor nevyhrožoval (např. pomocí e-mailů nebo prostřednictvím chatu).

Případ kyberšikany

- **Ghyslain Raza** (*1988) ztvárnil bojovou scénu z filmové ságy Hvězdné války.
- Nahrávka se dostala do rukou jeho spolužáků a ti ji zveřejnili na internet. Vznikla mutace nahrávky se zvukovými efekty a stal se z něj Star Wars Kid a jeho parodie se dostaly i do některých seriálů.
- Utrpěl těžký psychický otřes a musel jít na léčení.



Nejtragičtější případ kyberšikany.



Anna Halman z Polska (21. června 1992 – 21. října 2006)

- Vystavena před zraky svých spolužáků sexuální šikaně, vše bylo natočeno a zveřejněno na internetu.
- Další den Anna spáchala sebevraždu. Oběsila se na švihadle.
- Útočníci byli obviněni z účasti na skupinovém znásilnění, psychickém a fyzickém týrání a hrubém slovním napadání, kteréhož se měli vůči nezletilé dívce před celou třídou dopustit. Za to jim hrozí až dva roky odnětí svobody v nápravném zařízení.

Zdroj: http://cs.wikipedia.org/wiki/Anna_Halman

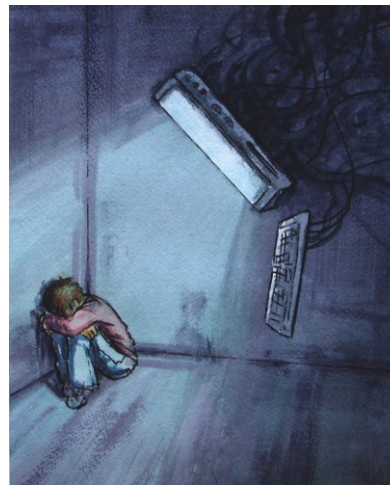
Ostrava - Poruba

- Jeden z žáků základní školy si nahrál pomocí mobilního telefonu, jak jeho kamarád z osmého ročníku bije tři starší žáky. Do každého ze spolužáků přitom uhodí tzv. boxerem, do jednoho dokonce i kopne. Tento záznam si pak žáci rozesílali mezi sebou.



Olomouc

- Student střední školy vytvořil na sociální síti Facebook stránku, ve které on i ostatní spolužáci ponižovali a uráželi neoblíbenou spolužačku. Nakonec dívky začali také vyhrožovat fyzickým ublížením a smrtí. V diskuzi např. řešili, jakým způsobem by se mohli zbavit jejího mrtvého těla, aby nemohla být identifikována (navrhovali, že by se mělo její tělo spálit, zuby rozřezat atd.).



Ochrana před kyberšikanou

Škola – kroky učitele

- Důkladně vyšetřete všechny incidenty.
- Zajistěte si podporu a pomoc externího pracovníka.
- Informujte rodiče kyberagresora.
- Poučte rodiče o tom, že mohou kontaktovat právníka.
- Ponechávejte si všechny důkazy kyberšikany.
- Poproste o radu ostatní školy.
- Používejte kreativní strategie neformálních řešení.
- Kontaktujte a spolupracujte s MySpace, Facebookem, nebo jakýmkoli jiným webovým prostředím, kde ke kyberšikaně došlo.

Rodina – kroky rodiče

- Ujistěte se, že se vaše dítě cítí (a je) v bezpečí.
- Důkladně vyšetřete situaci tak, abyste plně porozuměli tomu, co se stalo.
- Vyhněte se bezprostřednímu zákazu přístupu na ICQ, e-mail, sociální sítě, mobil, popř. Internet jako takový.
- Pokud to uznáte za vhodné, kontaktujte rodiče kyberagresora.
- V případě nutnosti kontaktujte a spolupracujte s poskytovatelem internetové služby.
- V některých případech je vhodné kontaktovat policii.
- Hovořte o kyberšikaně s ostatními rodiči a místními organizacemi.
- Detailně mluvte o problému se svým dítětem.

Dotazy?

pplk. Ing. Petr HRŮZA, Ph.D.

Univerzita obrany, Fakulta ekonomiky a managementu
Katedra vojenského managementu a taktiky

E-mail.: petr.hruza@unob.cz

