Základní škola T.G. Masaryka Rajhrad, okres Brno-venkov, příspěvková organizace

Kyberšikana

1. 12. 2018

1. Co je to kyberšikana?

Kyberšikana (také cyberbulling, počítačová šikana, kybernetická šikana) je specifickou formou šikanujícího chování agresora vůči oběti. Specifik je v rámci procesu kyberšikanování, tedy šikanování pomocí elektronických prostředků – mobilních telefonů, e-mailů, internetu a digitálních technologii, mnoho.

1. 1 Jaké jsou nejčastější projevy/způsoby kyberšikanování?

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

1. 2 Jaká jsou specifika kyberšikany?

- větší **anonymita**, kterou poskytuje virtuální realita, umožňuje stupňovat agresi a dovolit si to, co by si agresor vůči oběti přímo nedovolil.
- **jednosměrná komunikace** znemožňuje agresorovi vnímat reakci oběti. Agresor se tak nemusí chovat empaticky a nemá příležitost si uvědomit důsledky svého konání. Oběť nemůže bezprostředně reagovat.
- **nezáleží na místě,** kde k šikanování dochází, **ani na době**, kdy útok oběť zastihne. Útoky kyberagresora mohou oběť dostihnout kdykoliv a kdekoliv. Velmi rychle tak oběť ztrácí pocit bezpečí i tam, kde doposud byl zcela samozřejmý.
- k šikanování pomocí komunikačních technologií není zapotřebí fyzické převahy agresora, ale technologická dovednost. Agresorem se může stát i jedinec, který by při klasické šikaně neuspěl. Rovněž obětí nemusí být jen outsideři. Kyberšikana neprobíhá jenom mezi vrstevníky, ale i napříč generacemi.
- kyberšikana probíhá dlouho skrytě, klasické znaky šikany u kyberšikany chybí, což **ztěžuje kontrolu** a umožňuje její **rychlejší šíření**.
- vzhledem k tomu, v jaké prostředí k šikanování dochází, je zaručeno **velké publikum.**

- kyberšikanování může být způsobeno i **neúmyslně.**
- kyberšikana se **nemusí odehrávat opakovaně.**[2]

2. Typy kyberšikanování

1. přímé útoky – útok agresora je zřejmý, útočí sám agresor – posílá výhružné zprávy, bloguje, pomlouvá, zveřejňuje choulostivé informace o oběti, krade hesla a zneužívá osvojeného účtu, na webových stránkách zveřejňuje lživé informace či obrázky, video s nahraným záznamem klasické šikany, rozesílá oběť dehonestující fotografie, videa, obrázky, na nichž je oběť zesměšňována, druhým lidem, iniciuje internetové hlasování: např. kdo je ve třídě nejvíce škaredý, šikanuje v rámci virtuálního prostoru interaktivní hry, posílá viry, pornografické či jiné obtěžující emaily a zprávy, vydává se za někoho jiného atd.
2. útoky v zastoupení – špinavou práci za agresora vykoná někdo druhý, často nevědomě se stává komplicem.

3. Kyberšikana a zákon

Kyberšikana může nabývat skutkovou podstatu trestných činů – omezování osobní svobody, krádeže, ublížení na zdraví, poškození cizí věci, vydírání, znásilnění atd. Soud může osobě mladší 15 let uložit opatření jako dohled probačního úředníka, zařazení do terapeutického, psychologického nebo jiného vhodného výchovného programu v rámci SVP, ochrannou výchovu.

Mladiství ve věku 15 – 18 let jsou posuzování soudem pro mládež s ohledem na jejich rozumovou a mravní vyspělost.

Osoby starší 18 let jsou plně trestně odpovědné za své skutky.

Nelegální činy, které se vážou na internet, jsou popsány v souboru zákonných norem trestního zákona – zákon č. 140/1961 Sb.

4. Prevence a postup v případě napadení

4. 1 Netiketa

[2] http://proti-sikane.saferinternet.cz/sikana-a-kybersikana

Obecným rámcem pojednávajícím o vhodném chování uživatele na internetu je netiketa. Jedná se o pomyslnou sbírku pravidel a zásad, která by se měla dodržovat v internetovém světě. Slovo *netiketa* je odvozeno z anglického *net* (= síť; častá zkratka pro internet) a slova *etiketa*.

Jedním z mýtů, kterému podléhají zejména děti, je přesvědčení, že internet je zcela anonymní. Internetového uživatele jde dobře vystopovat. Proto jakýmkoli nevhodným chováním – urážením, pomlouváním, znevažováním, zesměšňováním, poškozováním majetku druhé osoby atd. se dostávají do situace, kdy hrozí nebezpečí trestního stíhání. Z toho plyne obecné doporučení, aby se lidé chovali ve virtuálním světě stejně dobře jako ve světě reálném.

S pravidly netikety by měli být seznámeni nejen žáci škol, ale také by měla vejít do povědomí veřejnosti.

A o jaká pravidla se jedná?

- Nezapomínejte, že na druhém konci jsou lidé a ne počítač. To, co napíšete do počítače, byste možná dotyčnému nikdy neřekli do očí.
- Dodržujte obvyklá pravidla slušnosti normálního života. Co je nevhodné v obvyklém životě, je samozřejmě nevhodné i na internetu.
- Zjistěte si taktně, s kým mluvíte. Internet je přístupný lidem z celého světa, a v každé zemi platí jiná morálka. Co je dovolené na americkém chatu, nemusí být dovolené na arabském, a to platí o všech podobných skupinách. Politika, náboženství a podobné problémy by proto měly být diskutovány s maximálním taktem a v mezích slušnosti.
- Berte ohled na druhé. Ne každý má tak dobré internetové připojení jako vy. Někteří se připojují z domu přes vytáčené připojení a draze za to platí. Neposílejte proto zbytečně velké e-mailové zprávy a posíláte-li přílohy, komprimujte je. Při posílání velkých obrázků např. na diskusní server využívejte funkci náhledu obrázku.
- Je vhodné psát s diakritikou. Vyvarujete se tak nedorozumění. Nekomolíte rodnou řeč. Pokud jste z nějakého důvodu nuceni psát bez diakritiky, snažte se používat správný pravopis. Nebuďte grobián, nezveřejňujte nepravdivé, nebo i pravdivé, ale choulostivé informace.
- Pomáhejte v diskuzích. Pokud má někdo v diskuzi nějaký problém, odpovězte mu, pokud znáte odpověď. Někdo jiný zase pomůže vám. Platí zásada: „Napřed poslouchej, pak piš.“
- Respektujte soukromí jiných. Pokud vám omylem přišla zpráva, která vám nepatří, je vhodné ji smazat a taktně upozornit odesilatele na jeho chybu.

- Nezneužívejte svou moc či své vědomosti. Pokud jste správce serveru, máte sice přístup k poště ostatních, ale nemusíte ji neustále kontrolovat jenom tak z nudy, a pokud umíte hackovat, nemusíte to pořád zkoušet.
- Odpouštějte ostatním chyby. I vy je děláte. Nevysmívejte se jim a nenadávejte za ně.
- Nešiřte hoaxy. Zahlcují internet. Pokud vám přijde hoax, zdvořile upozorněte jeho odesilatele, že takové jednání je nevhodné. Nerozesílejte spam a reklamu.
- Neporušujte autorská práva. [4]
-

Návrh pravidel a doporučení pro bezpečné užívání Internetu ve škole

- **Respektuj ostatní uživatele. Nečiň druhým to, co nechceš, aby činili tobě.**
- **Nezapomeňte: opatrný internetový serfař je inteligentní serfař.**
- **Neposílejte nikomu, koho neznáte, svou fotografii a už vůbec ne intimní, nesdělujte mu svůj věk.**
- **Dobře si rozmyslete, co posíláte a komu.**
- **Udržujte hesla k emailu i jinam v tajnosti, nesdělujte je ani kamarádovi.**
- **Nedávejte nikomu své osobní údaje, adresu ani telefon. Nevíte, kdo se skrývá za monitorem.**
- **Nevěřte každé informaci, kterou na internetu získáte.**
- **Seznamte se s pravidly chatu či diskuse, ať víte, co je zakázáno dělat.**
- **Když se s někým nechcete bavit, nebavte se.**
- **Nikdy neodpovídejte ne neslušné, hrubé nebo vulgární emaily a vzkazy.**
- **Nedomlouvejte si schůzku po Internetu, aniž byste o tom řekli někomu jinému (nejlépe alespoň jednomu z rodičů).**
- **Pokud vás nějaký obrázek nebo e-mail šokuje, okamžitě opusťte webovou stránku.**
- **Svěřte se (nejlépe dospělému), pokud vás stránky vyděsí nebo přivedou do rozpaků.**
- **Nedejte šanci virům. Neotevírejte přílohu zprávy, která přišla z neznámé adresy.**
- **Seznamte se s riziky, která souvisí s elektronickou komunikací.[6]**

[4] http://cs.wikipedia.org/wiki/Netiketa

[6] http://www.bezpecnemesto.eu/prevence-kriminality/prevence-aktualne/kybersikana-a-jeji-prevence.aspx

4. 2. Jak se bránit při útocích – rady a doporučení žákům?

Jak postupovat ve chvíli, kdy už se staneme obětí kyberšikany? Následující kroky vám mohou pomoci odrazit případné další útoky či snížit intenzitu útoku a jeho dopad.

1. Ukončete komunikaci

Záměrem agresora je vyhlédnuté oběti ublížit, proto reakce na jeho útok, provokaci v něm posílí tendenci jeho chování opakovat. Uzavírá se tak začarovaný kruh, kdy agresor stupňuje své útoky a oběť se cítí více a více nejistá a ohrožená. Pokud nebude mít agresor odezvu ze strany oběti, zvyšuje se tím pravděpodobnost, že své chování změní, opustí. Nekomunikujte s útočníkem, nesnažte se ho žádným způsobem odradit od jeho počínání, nevyhrožujte, nemstěte se.

2. Blokujte útočníka

Zabraňte agresorovi v přístupu k vašemu emailu nebo telefonnímu číslu zablokováním přijímání agresorových zpráv, hovorů, změňte svou virtuální identitu. Kontaktujte poskytovatele služby za účelem zablokování přístupu k nástroji či službě, pomocí které své útoky realizuje. Vzhledem k tomu, že i útočník si může změnit identitu, nejedná se o definitivní řešení, jak zamezit agresorovi další útoky. Nicméně tak výrazně znesnadníme jeho počínání.

3. Oznamte útok, poraďte se s někým blízkým, kdo vám může pomoci

Útoky kyberagresorů nás zraňují, ponižují a není divu, že v nás mohou vznikat pocity méněcennosti a pochyby o nás samotných. I počáteční „nesmělé útoky“ je třeba řešit a svěřit se s nimi. Ve vašem okolí je mnoho lidí, kterým na vás záleží a není jim lhostejné, jak se cítíte. K vašemu problému budou přistupovat s odstupem a nadhledem, pomohou vám najít způsob řešení vašeho problému. Dítě by mělo informovat dospělého – nejlépe rodiče nebo učitele. Dospělí mají mnohem více zkušeností s řešením problémů obecně, proto mohou nabídnout účinnější rady než kamarádi. Dospělí jsou schopni lépe posoudit, kdy je problém natolik závažný, že je pro řešení potřeba zapojit specializované instituce (policii, intervenční služby specializující se na řešení kyberšikany, psychology apod.). Děti mohou samy využít linku bezpečí – www.internethelpline.cz.

4. Uchovejte důkazy

Pro oběť je velmi důležité, aby si uchovávala důkazy kyberšikany (SMS zprávy, e-mailové zprávy, zprávy z chatu, odkazy na webové stránky s problematickým obsahem apod.). Na základě těchto důkazů může být proti útočníkovi či útočníkům zahájeno vyšetřování.

5. Vyhledejte pomoc psychologa, zaměřte se na trénink asertivity

6. Nebuďte nevšímaví (pro svědky a okolí)

Pasivní přístup, ať už souhlasíme nebo nesouhlasíme s počínáním útočníka, z nás dělá spolupachatele. Navíc početnost publika, které je svědkem kyberšikany, pomáhá zvyšovat tlak na oběť a prohlubuje tak její trápení. Je třeba dát jasný signál, že kyberšikana je špatná, je potřeba se jí postavit a zastavit útočníka. Pomůžeme tak nejen člověku, jehož kyberšikanování jsme svědkem, ale také budoucím obětem. Mějme na paměti, že obětí kyberšikany se může stát každý z nás.

7. Podpořte oběti (pro svědky a okolí)

Poraďte jim, co mají dělat a na koho se obrátit. Pomozte jim kyberšikanu nahlásit. Pokud je člověk vystaven útoku jakéhokoli druhu (nejen kyberšikany), znamená to zásah do jeho sebedůvěry. Snažte se vcítit do situace obětí a přemýšlejte, jak byste se cítili, kdyby za vámi nikdo nestál.

5. Důležité kontakty a odkazy

3. oddělení OOK – UO SKPV MR PCR Brno - vyšetřování kyberšikany
Příční 31, 602 00 Brno
npor. Mgr. Radoslav Novák, vedoucí oddělení
telefon: 974 625 325

por. JUDr. Michaela Kučerová
telefon: 974 625 861
po – pá 06.30 – 14.30
www.policie.cz

Policie ČR
kpt. Mgr. Zdeňka Procházková
koordinátorka prevence
Krajské ředitelství policie Jihomoravského kraje
tel.. 974 622 458, 602161766
mail: prevencejm@mvcr.cz

kpt. Mgr. Borek Novický
telefon: 974 625 222

---

telefon: 548 526 802
e-mail: sladkova@pppbrno.cz
po – pá 8.00 – 16.30
www.poradenskecentrum.cz

Projekt E-bezpečí
doc. Kamil Kopecký, Ph.D.
Telefon: +420 777 146 808
E-mail: info@e-bezpeci.cz

Management vzdělávacích akcí:
Mgr. Klára Hrubá
Telefon: +420 776 322 357
E-mail: vzdelavani@e-bezpeci.cz

Adresa:
Projekt E-Bezpečí - Centrum prevence rizikové virtuální komunikace
Pedagogická fakulta UP V Olomouci, Žižkovo nám. 5, Olomouc 77140
http://cms.e-bezpeci.cz/
(velmi užitečný portál poskytující informace o kyberšikaně pedagogům, žákům i rodičům)

Facebook:
www.facebook.com/e-bezpeci

Poradna:
www.napisnam.cz

Bezpečně v kyberprostoru
Projekt JMK pro pedagogy, rodiče, děti
www.bezpecnevkyberprostoru.cz
https://www.kr-jihomoravsky.cz/kyber/

Nový výchovně vzdělávací server
mediapodlupou.cz › e-learning
www.bezpecne-online.cz
www.horkalinka.cz - kontaktní centrum, které přijímá hlášení týkajícího se nezákonného obsahu na internetu (např. dětská pornografie, rasismus…..)
www.pomoconline.cz - telefonické krizové intervence (když se děti cítí být ohroženi na internetu)
www.linkabezpeci.cz
