



Příručka Kyberšikana

Pojem kybernetická šikana můžeme definovat jako formu šikany využívající elektronických médií, jako jsou mobilní telefony, e-maily, pagery, internet, blogy a podobně, k odesílání obtěžujících, urážlivých nebo útočných zpráv, mailů a SMS, tvorbě webových stránek a blogů, které dehonestují konkrétní osoby nebo skupiny. Cílem kyberšikany je, stejně jako u klasické šikany, způsobit druhým jakýkoli druh újmy či bolesti. V případě kyberšikany se však jako prostředek za tímto účelem používají informační a komunikační technologie.

Různí autoři a odborníci definují kyberšikanu různě. Vycházejí ze základní definice klasické šikany, kde jde o agresivní, záměrné a opakované jednání vůči jednotlivci nebo skupině. Někteří uvádějí obtěžování, ponižování a ztrapňování založeném na nerovnováze sil mezi agresorem a obětí. Je klíčové rozlišit šikanu od agrese, která bývá jednorázovou záležitostí. Vzhledem k nejasnostem v definici je kyberšikana často zaměňována s online obtěžováním, což je jednorázový útok s menšími dopady na oběť, než jaké by mohla přivodit šikana.

Důležité je také odlišit šikanu od škádlení. Při kamarádských šprýmech nebo legraci jsou respektovány vzájemné hranice, role jsou vyvážené a výsledkem je pozitivní atmosféra. Je však náročné vždy jednoznačně určit hranici mezi šikanou a škádlením. Proto je důležité věci pojmenovat a vysvětlit dětem, že mají právo stanovit si vlastní hranice a dát najevo, když něco není v pořádku.

Z tohoto důvodu si dovolím zpochybnit úmysl jako charakteristiku kyberšikany. V online prostoru dochází k neúmyslnému ubližování častěji než jinde. Často jde o nedostatečně promyšlený vtip, který na internetu nabírá nečekané obrátky a stává se kyberšikanou. Typickým příkladem jsou četná zveřejnění zesměšňujících fotografií nebo videí, které se stanou virálními a nelze je již odstranit, ani kdyby autor chtěl. Kyberšikana v takovém případě probíhá ze strany tzv. sekundárních útočníků, kteří komentují, lajkují, sdílí a opětovně zveřejňují video. Identifikace těchto útočníků je obtížná a kdokoli se může stát sekundárním útočníkem.

Většina autorů se shoduje na tom, že "pravá" kyberšikana je opakovaná, dlouhodobá a má negativní dopad na oběť. V praxi je však určení toho, co je a co není kyberšikana, složité a individuální. Je důležité ptát se poškozeného, zda se považuje za oběť kyberšikany, a i tomu přizpůsobit úsudek. Osobně jsem se setkala s tímto přístupem u certifikovaných odborníků na intervenci. To však stále neznamená, že to, co neklasifikujeme jako kyberšikanu, by mělo být považováno za správné. Všechny formy kybernetické agrese mají negativní dopad a je možné je řešit.

Specifika kyberšikany

Neomezený čas a místo: U tradiční šikany má útočník ohraničený rámec, kde a kdy se setkává s obětí (např. během školní přestávky). Naopak, v případě kyberšikany tyto omezení mizí. Většina z nás nosí mobilní telefon s připojením k internetu neustále u sebe a je složité se odtrhnout od online činností, obzvláště pokud jste terčem pozornosti. To může vést k tomu, že některé děti budou kontrolovat svůj mobilní telefon mnohem častěji nebo budou trávit více času u počítače, pokud se stanou obětí kyberšikany. Existuje ale i opačná reakce, kdy některé děti ztratí zájem o internet a technologie.

Přesto však kyberšikana nezmizí, protože vypnutím zařízení internet nezmizí. Oběť nemá možnost se skrývat před útočníkem ani v případě, že změní školu nebo místo bydliště, protože se může připojit k internetu téměř odkudkoli a není tak možné se před útočníkem úplně ukrýt.



Anonymita: Vzhledem k anonymitě, kterou kyberprostor poskytuje, může zůstat útočník neidentifikován. Může využívat falešný profil na sociálních sítích, prezentovat se pod pseudonymem, používat jiný e-mail nebo telefonní číslo a podobně. Pro oběť je tato situace velmi obtížná. Pro útočníka zase pocit anonymity posiluje odvahu pro větší krutost ve svých útocích. Nicméně ve skutečnosti není pro Policii ČR problém odhalit skutečnou identitu agresora. V případě vyšetřování kyberšikany ve školním prostředí může být také nápomocné, že agresor a oběť jsou často ze stejné třídy.

Profil agresora: Opět se setkáváme s různorodými představami o tom, jak vypadá nejtypičtější agresor kyberšikany. Někteří autoři i výzkumníci označují za typického agresora chlapce, někteří dívky a jiní nezohledňují pohlaví. Je však zřejmé, že virtuální prostředí stírá rozdíly mezi jednotlivci; v kyberprostoru nehrají věk, pohlaví, síla, společenské postavení, dovednosti, dosažené úspěchy a podobné odlišnosti roli. Agresorem se může stát za pomoci digitálních technologií kdokoli, bez ohledu na jakoukoli odlišnost. Přesto můžeme odlišovat několik různých typů agresorů kyberšikany, například na základě jejich motivace a dalších okolností. Jedním zajímavým typem je tzv. "Anděl pomsty", což je původní oběť šikany, která cítí křivdu a touží se pomstít původnímu útočníkovi. Sám sebe nevnímá jako útočníka, ale jako ochránce a správce.

Profil oběti: Velmi často dochází k tomu, že osoby postižené kyberšikanou tráví více času online, komunikují s ostatními v kyberprostoru, často budují vztahy prostřednictvím internetu a sdílí o sobě více osobních údajů. Avšak toto chování nemusí být pravidlem a není výjimkou, že kyberšikana postihne i jedince, kteří jsou jinak ve svém okolí oblíbení.

Publikum: Tradiční šikana může mít svědky, ale jejich počet je omezený (například v případě šikany ve třídě jsou to všichni spolužáci, eventuálně další žáci ze školy). V situaci veřejné kyberšikany je publikum, které sleduje situaci, mnohem větší a může obsahovat mnoho potenciálních sekundárních útočníků. Teoreticky to mohou být všichni uživatelé internetu. Primárnímu pachateli stačí jednou zveřejnit ponižující materiál a o další šíření se postarají ostatní uživatelé. Vzhledem k tomu, že se někteří uživatelé internetu chovají v digitálním světě méně opatrně a ohleduplně než v reálném životě, může být kyberšikana velmi drsná a téměř nezastavitelná.

Sílu internetového publika ilustruje příběh první mediálně známé kyberšikany. Chlapec Ghyslain Raza (Kanada, 2003), známý jako Star Wars Kid, natočil sám sebe na video, kde ztvárňoval bojovou scénu z filmu Hvězdné války. Jeho spolužáci získali toto video a zveřejnili ho na internetu, kde se velmi rychle začalo šířit. Během několika měsíců video viděly stovky milionů uživatelů a začaly vznikat posměšné koláže, vtipy a parodie. Chlapec prožil těžké trauma a musel absolvovat dlouhodobou léčbu.

Dopady nejsou na oběti vidět: V případě fyzické šikany jsou projevy týrání na oběti zřetelné fyzicky (modřiny, škrábance, poškozené oblečení, zničené nebo ztracené předměty atd.). V případě kyberšikany jsou důsledky převážně psychické a lze je rozpoznat pozorováním chování oběti nebo na základě její výpovědi. Nicméně oběti často nemluví o svých obtížích, buď kvůli obavám z nepochopení nebo z obavy, že by se situace ještě zhoršila. Důsledky kyberšikany mohou vypadat jako: negativní emocionální stavy zahrnující například hněv, smutek, strach, stres či úzkost, dále sem patří sebekritika, snížené sebevědomí, trauma, deprese, sociální fobie, izolaci, agresivní a impulzivní chování, duševní nestabilitu, poruchy spánku, bolesti hlavy, bolesti břicha, nevolnost a sníženou schopnost soustředit se, což vede k horším školním výsledkům.



Podoby kyberšikany

Publikování ponižujících záznamů nebo fotografií: Mezi nejčastější formy kyberšikany patří situace, kdy jsou oběti zesměšňovány či uráženy prostřednictvím fotografií a videí. Tyto záběry získá útočník buď tím, že mu je oběť sama poskytne buď dobrovolně nebo pod nátlakem výhrůzek, nebo také tím, že je ukradne nebo vytvoří sám (natočí, upraví, zfalšuje atd.). Následně útočník tyto média publikuje online nebo je rozesílá pomocí zpráv. Občas se v těchto případech může spojit s klasickou šikanou, kdy útočník a jeho spolupachatelé naplánují fyzický útok na oběť. Tento útok pak někdo z nich natočí a později zveřejní online pro pobavení ostatních a zesměšnění oběti. Tento fenomén se označuje jako "Happy Slapping", což je anglický výraz pro "veselé fackování". Někdy tyto incidenty vedly až k závažným trestným činům, které mohly vést až ke smrti oběti.

Ponižování, pomlouvání, urážení: Tato forma kyberšikany zahrnuje odesílání zpráv (SMS, online chat, e-mail), vytváření falšovaných příspěvků, webových stránek a šíření nepravdivých informací atd. Jejím účelem je poškodit oběť, zranit ji, pošramotit její pověst a narušit její vztahy s okolím.

Vydírání a zastrašování: Oběť je vydírána prostřednictvím zpráv (SMS, online chat, e-mail). Útočník se snaží dostat se do výhody a získat z oběti ponižující materiál, vyžaduje od ní změnu chování, nutí ji k plnění různorodých úkolů nebo si vynucuje materiály. Pokud jde o intimní fotografie a videa, vydírání je často spojeno se sextingem, fenoménem revenge porn nebo dětskou pornografií obecně.

Falšování identity: Útočník vytváří falešný profil oběti na sociálních médiích a publikuje tam nepravdivé, urážlivé nebo degradující informace, fotografie a videa. Útočník si může vybrat platformu, kterou oběť nevyužívá a může se stát, že se oběť o tomto nežádoucím profilu dlouho vůbec nedoví.

Ukradení identity: Jde o podobný scénář jako při falšování identity oběti, s tím rozdílem, že útočník nevytvoří falešný profil, ale napadne skutečný profil oběti tím, že prolomí její heslo. Za použití této identity může zveřejňovat ponižující informace, degradující fotografie a videa a kontaktovat rodinu, přátele a známé oběti, kterým pak může posílat nevhodné zprávy, odkazy nebo šířit malware. Dále může z účtu oběti odstranit zprávy, dokumenty, fotografie apod. Pokud najde citlivé informace, může je zveřejnit nebo využít k vydírání oběti. Osobní data pak může využít k přihlášení do dalších účtů oběti nebo k online nákupům.

Odhalování cizích tajemství: Útočník získá důvěrné informace nebo osobní citlivé materiály (nejčastěji intimní fotografie a videa), které může zveřejnit online nebo rozeslat kontaktům oběti. Tyto údaje a materiály může získat agresor prostřednictvím manipulativních postupů, snažíc se přesvědčit oběť, aby mu věřila a sama je poskytla. V tomto smyslu se jedná o podobném jevu jako u kybergroomingu a sextingu. Držení osobních informací je často spojeno s vydíráním oběti.

Vyloučení z virtuální komunity: Vyloučení jednotlivce z on-line komunity nebo skupinových konverzací, kam má právo být zařazen (např. chatová komunikace, kde jsou všichni členové třídy), může být v některých případech také považováno za kyberšikanu. Problémové bývají skupiny a skupinové konverzace přátel, kde není jasné, kdo má nárok na účast a kdo ne. Další výjimkou jsou situace, kdy je vyloučení člena komunity opodstatněné, například kvůli porušování pravidel komunity a zásad slušného chování (spamy, urážení ostatních členů apod.).

Obtěžování: Nepřetržité obtěžování prostřednictvím posílání zpráv, volání a opakovaného prozvánění, často v nepříhodných časech, může eskalovat do jevu známého jako kyberstalking. Tento termín popisuje opakované, dlouhodobé a systematické pronásledování a obtěžování oběti prostřednictvím informačních a komunikačních technologií.



Kyberšikana spojená s online hrami: Kyberšikana se často vyskytuje také v prostředí videoher. Projevuje se opakovaným a dlouhodobým napadáním, ponižováním, nadáváním nebo vyhrožováním hráčům ve společném chatu během týmové hry nebo na jiných komunikačních platformách využívaných hráči během hry. Toto chování zahrnuje i záměrné znevýhodňování hráčů, kažení hry či skóre danému hráči, ničení vytvořených prvků, cílené zabíjení, odcizování virtuálních postav a předmětů, krádež či zničení herního účtu a další podobné činy.

Použité zdroje

KOHOUT, Roman a KARCHŇÁK, Radek. Bezpečnost v online prostředí. Online. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9. Dostupné z: <https://www.internetembepecne.cz/wp-content/uploads/2017/03/Roman-KohoutBezpecnost-v-online-prostredi.pdf>

SZOTKOWSKI, René; KOPECKÝ, Kamil a KREJČÍ, Veronika. Nebezpečí internetové komunikace IV. Online. Olomouc: Univerzita Palackého v Olomouci, 2013. ISBN 978-80-244-3911-2. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/vyzkumne-zpravy/58-nebezpeci-internetove-komunikace-iv-2012-2013/file>

KOSOVÁ, Lucie a MARTINEK, Petr. Bezpečně v kyber!. Online. Národní úřad pro kybernetickou a informační bezpečnost. 2020. Dostupné z: https://www.nukib.cz/download/publikace/vzdelavani/Brozura%20bezpecne%20v%20cyber_A5.pdf.

KOPECKÝ, Kamil; SZOTKOWSKI, René a KREJČÍ, Veronika. Rizikové formy chování českých a slovenských dětí v prostředí internetu. Online. Křížkovského 8, 771 47 Olomouc: Univerzita Palackého v Olomouci, 2015. ISBN 978-80-244-4861-9. Dostupné z: <https://doi.org/10.5507/pdf.15.24448619>.

KAMIL, Kopecký. KYBERŠIKANA A JEJÍ SPECIFIKA V PROSTŘEDÍ SYSTÉMU PRIMÁRNÍ PREVENCE RIZIKOVÉHO CHOVÁNÍ. Online, HABILITAČNÍ PRÁCE. Olomouc: Univerzita Palackého v Olomouci, 2016. Dostupné z: <https://e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/105-kybersikana-a-jeji-specifika-v-prostredi-systemu-primarni-prevence-rizikoveho-chovani/file>.

Prevence kyberšikany - Metodika pro pedagogy. Online. Fórum pro prožitkové vzdělávání. 2020. Dostupné z: https://www.forumppv.cz/wp-content/uploads/2020/09/Metodika_Prevence-kyber%C5%A1ikany.pdf.

Licence

Toto dílo – Příručka Kyberšikana je licencován pod licencí Creative Commons Uveďte původ-Zachovejte licenci 4.0. Autorem je Lukáš Havelka.

Licenční podmínky navštivte na adrese <https://creativecommons.org/licenses/by-sa/4.0/legalcode.cs>.

