KAMIL KOPECKÝ, vedoucí projektu E-Bezpečí, zabývající se rizikovým chováním (nejen) dětí na síti:

S některou z forem kyberšikany se setkala polovina českých dětí

Moderní technologie nám v mnoha směrech usnadňují život, vítaným pomocníkem jsou také ve vzdělávání. V době, kdy jsou téměř všechny školy pokryty bezdrátovým internetem a většina dětí do školy nosí mobil či tablet, se však do on-line prostředí přesunula také mnohá riziková chování. Děti se snáze stanou oběti kyberšikany, která se navíc v internetovém prostředí dokáže šířit velice rychle. Jak s dětmi o nových hrozbách mluvit a co zvážit, než dítěti pořídíte telefon či vlastní počítač, jsme se ptali Kamila Kopeckého z Centra prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci

BARBORA HAVLOVÁ

Stál jste u zrodu portálu a organizace E-Bezpečí, která pomáhá bojovat s hrozbami elektronického světa. Kdy projekt vznikl a co bylo tím prvním impulsem k této aktivitě?

Projekt E-Bezpečí vznikl přibližně v roce 2007 v podstatě na zelené louce – v této době v ČR vlastně neexistovala funkční prevence rizikového chování dětí i dospělých, která by byla zaměřena na on-line prostředí, chyběla jakákoli relevantní data o tom, jaké formy rizikového chování existují, jak moc jsou rozšířeny a jak moc jsou pro děti i dospělé nebezpečné. Učitelé ani rodiče neměli téměř žádné relevantní informace. Prvním impulsem, který projekt E-Bezpečí nastartoval, byl projekt Grantové agentury ČR, Prevence nebezpečných komunikačních praktik spojených s elektronickou komunikací pro pedagogy a nepedagogy, jehož cílem bylo na jedné straně zajistit informace o výskytu rizikových fenoménů v českém prostředí a na straně druhé nastartovat vzdělávání a prevenci v této oblasti. A to se povedlo. V roce 2010 jsme pak projektu dali institucionální podobu a založili specializované univerzitní pracoviště Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci, orientované na prevenci, edukaci, výzkum a intervenci v oblasti internetové bezpečnosti.

Jsou dnešní děti ve světě chytrých telefonů a Facebooku ohroženější různými typy šikany a manipulace? Nebo se jen stejné chování přesunulo do jiného prostředí?

Je třeba říci, že šikana existovala i před příchodem internetu a moderních komunikačních technologií a pravděpodobně bude existovat i po jejich zániku. V zásadě tedy jde především o přenos psychické – lépe verbální šikany – do on-line prostředí, ve kterém mohu k útoku na jinou osobu využít podstatně více nástrojů, než mám k dispozici v případě běžné šikany. Někteří experti vnímají kyberšikanu vlastně jako variantu běžné přímé či nepřímé šikany, která se pouze přenesla do prostředí internetu a tím se změnila její charakteristika – v on-line prostředí může být útočník anonymní, může do šikanování zapojit velké množství lidí a může útok realizovat kdykoli a odkudkoli.

Kdy se v českém prostředí začala kyberšikana šířit?

První zdokumentované případy kyberšikany pochází zhruba z období let 2003 až 2004, jde tedy o velmi mladý fenomén, se kterým předcházející generace zkušenost neměly. Výskyt kyberšikany potvrzuje přibližně polovina českých základních a středních škol, podle našeho výzkumu některou z forem kyberšikany zažila přibližně polovina českých dětí.

Co tedy děti na síti ohrožuje nejvíce? Jaké případy řešíte nejčastěji v případě malých školáků a jaké u středoškoláků?

Děti se nejčastěji setkávají s různými formami verbální kyberšikany v kombinaci s fotografiemi a videi, jakmile dítě začne vstupovat do puberty, začnou se k útokům stále více využívat intimní materiály – fotografie zachycující částečně či zcela nahé dítě. V naší poradně (*www.napisnam.cz*) řešíme stále častěji tzv. sexting (*dobrovolné sdílení vlastních intimních materiálů s dalšími uživateli*) a z něj vycházející problémy – dehonestování, vyhrožování a vydírání. U menších dětí se také objevuje kyberšikana spojená s hraním on-line her, třeba oblíbeného Minecraftu.

Technologie by neměly nahrazovat aktivity, které dokáží dítě rozvíjet lépe.

Kyberšikanu mnoho lidí chápe jako problém týkající se dětí, tyto útoky však směřují také na učitele. Jak se kantor může těmto situacím bránit? Lze jim předcházet?

Kyberšikana je projevem problému, který existuje přímo ve třídě – většina útočníků, kteří cílí kyberšikanu na učitele, jsou jejich vlastní žáci či žáci z okolních tříd. Kyberšikana a šikana jsou vlastně „onemocněními sociální skupiny“, ve které například nefunguje komunikace, důvěra, sociální interakce a podobně. Předcházet kyberšikaně lze tedy především nápravou školního klimatu, vzděláváním učitelů, v řadě případů se učitelé výrazně na vzniku šikany či kyberšikany podílejí, ale také prostřednictvím preventivních a intervenčních programů.

Platí to i pro šikanu mezi dospělými třeba v zaměstnání?

Ano, šikana či kyberšikana dospělých na pracovišti, tzv. mobbing či bossing, funguje podobně – dochází k poruše profesionálních vztahů mezi nadřízeným a podřízeným, což se projevuje různými formami vykořisťování a nátlaku.

Blokace závadných materiálů jako jsou fotografie, videa, chaty či diskusní skupiny pak samotný problém neřeší – dochází pouze k odstranění jeho projevů.

Co se týče kyberšikany učitelů, podle národního výzkumu kyberšikany učitelů, který jsme zrealizovali ve spolupráci s O2 a Seznam.cz v loňském roce, skutečnou kyberšikanu zažívá 3–5 procent učitelů ZŠ a SŠ, zkušenosti s on-line agresí má však přes 20 procent z nich.

Rodiče často trápí otázka, kdy pořídit dítěti telefon či tablet a jak ho dostatečně kontrolovat. Co byste jim poradil?

Samozřejmě neexistuje nějaká ideální hranice, kdy dítěti pořídit mobilní telefon, důležitá je hlavně příčina – rodiče dětem mobilní telefony pořizují zpravidla ve 2. až 3. třídě ZŠ, protože děti začnou chodit ze školy samy domů a rodiče s nimi potřebují komunikovat. Z pohledu dítěte je však mobilní telefon především zajímavá a také užitečná hračka, kterou využívají především ke hraní her, sledování YouTube a později ke komunikaci v prostředí sociálních sítí.

Při pořízení prvního mobilního telefonu malému dítěti je nutné dodržet několik základních principů – nastavit dítěti pravidla, jak bude mobilní telefon používat, zajistit technické zabezpečení mobilu, u menších dětí zabezpečit telefon systémem rodičovské kontroly, případně přepnout internetové vyhledávače do bezpečného režimu, který filtruje nežádoucí obsah. Každou restrikci však lze obejít.

Od jakého věku by měli rodiče s dítětem o bezpečném chování na síti mluvit? Co říct třeba takovému prvňákovi, který dostal první telefon a na domácím počítači hraje Minecraft s kamarády?

Prevence by měla začít co nejdříve, v podstatě již ve chvíli, kdy dítě začne s jakoukoli technologií pracovat. V úvodních etapách je třeba především omezovat čas, který dítě s technologií tráví, a nabízet mu dostatek dalších aktivit – mozek dítěte se nejvíce rozvíjí do šesti let věku, kdy snadno absorbuje velké množství informací. Technologie by pak měly být využívány smysluplně a cíleně, neměly by však nahrazovat aktivity, které dokáží dítě rozvíjet lépe – například hra s rodičem rozvíjí dítě podstatně více než hra na tabletu či mobilním telefonu.

Jakmile dítě již využívá mobilní telefon či internet, rodič s ním musí o těchto technologiích aktivně komunikovat – vysvětlit mu, jak si chránit své osobní údaje a proč, jak funguje komunikace s neznámými lidmi a na co může narazit. Celou problematiku podrobně osvětlujeme v naší příručce *Pravidla bezpečného používání internetu pro rodiče.*

A co výchova ve školách, je v rámci běžné výuky prostor pro vzdělávání týkající se právě rizikového chování na síti?

Rámcové vzdělávací programy pro základní vzdělávání s prostorem pro výuku v oblasti internetové bezpečnosti počítají, je ale otázkou, jak je v praxi výuka a navazující preventivní činnost realizována. V řadě škol chybí erudovaný informatik, stejně jako kvalitní školní metodik prevence. Školní metodici prevence navíc zajišťují prevenci ve všech oblastech – nikoli pouze v oblasti prevence rizikového chování v prostředí internetu – a k tomu musí provádět vlastní výukovou činnost. Proto školy aktivně využívají v procesu prevence služeb externí organizace, nejčastěji se obracejí na pedago-gicko-psychologické poradny a dále na orgány sociálně právní ochrany dětí, případně na policii a neziskové organizace.

Projekt E-Bezpečí ročně v prostředí škol zrealizuje přibližně 150–200 vzdělávacích akcí pro děti a učitele. Zde bych rád ocenil podporu Ministerstva školství, mládeže i tělovýchovy ČR, ale také soukromých firem – například společnosti O2 – díky kterým jsme schopni většinu našich aktivit realizovat zcela zdarma.

Kybergrooming, kyberstalking či sociotechnika jsou jen některé z poměrně neznámých pojmů označujících nebezpečné chování na internetu. Prozraďte nám, co znamenají.

Začal bych termínem sociotechnika (sociální inženýrství) v on-line prostředí – jde vlastně o manipulaci uživatelů jednotlivých internetových služeb s cílem oklamat je – třeba k tomu, aby nám prozradili své heslo, autorizovali platbu, přihlásili se na podvržené stránky internetového bankovnictví, poskytli nám své osobní údaje, nakazili si počítač virem apod. Terčem sociotechnického útoku může být v podstatě kdokoli – dítě, dospělý, v posledních letech pak také často senioři.

Kybergrooming je vlastně druhem sociálního inženýrství, které se zaměřuje na dětské uživatele internetu a jehož cílem je donutit dítě k osobní schůzce v reálném světě. V rámci kybergroomingu s dítětem komunikuje dospělá osoba, která může předstírat, že je dítětem, které si chce s vybranou obětí chatovat. Postupně však chatování přejde k podstatně nebezpečnějším aktivitám...

V poradně projektu E-Bezpečí jsme řešili řadu případů, kdy se například útočníkovi maskovanému za falešný profil dvanáctileté holčičky podařilo vylákat z dítěte intimní materiály, které pak byly využity k vydírání dítěte. Vystrašené dítě pak nakonec dorazilo na schůzku v reálném světě, na které došlo k jeho zneužití. Někdy se však pachatel omezí pouze na sběr intimních materiálů a na vydírání, aniž by dítě donutil přímo ke schůzce v reálném světě.

Případy, které jsou spojeny s touto formou útoků na dítě, automaticky předáváme k řešení Policii ČR. Stejně tak policie potvrzuje nárůst počtu případů, ve kterých figuruje sexting a vydírání dítěte i dospělých.

Termín kyberstalking je pak spojen především s dospívajícími či dospělými uživateli internetu – jde o pronásledování v on-line prostředí, ve kterém je vybraná oběť, často expartner či expartnerka, v on-line prostředí dlouhodobě obtěžována, dehonestována, očerňována, je poškozována její pověst apod.

V jednom z vašich výzkumů uvádíte, že každé šesté dítě sdílí své intimní fotografie a videa a nezdráhají se ani osobních schůzek. O jak staré děti se jednalo? Překvapila vás tato poměrně vysoká čísla?

Jedná se o data z výzkumu Sexting a rizikové seznamování českých dětí v kyberprostoru, který jsme s naším hlavním partnerem, společností O2 Czech Republic zrealizovali v loňském roce. Do výzkumu se zapojilo téměř 5000 dětí s průměrným věkem 14 let (8–17 let).

Své intimní materiály po internetu s cizími lidmi sdílí až 16 procent českých dětí, dominují především fotografie nad videem. Za pět let se toto číslo zvýšilo téměř o polovinu, což samozřejmě vede i k rostoucímu počtu případů úniků nebo zneužití takových materiálů.

Nárůst sextingu jsme v podstatě předpokládali – v českém vzdělávání téměř neexistuje prevence cílená na sexting, případně je realizována nesystémově a často na konci povinné školní docházky. Nárůst počtu případů sextingu a následného zneužití intimních materiálů potvrzují také naše spřátelené poradny: Linka bezpečí a poradna projektu Seznam se bezpečně!

Jak postupujete, obrátí-li se na vás rodič či dítě s tím, že se stali oběťmi kyberšikany? Jak dokážete pomoci?

Předně je třeba říci, že každý případ kyberšikany je jiný a žádá si jiné řešení. Klienta zpravidla nejprve uklidníme a následně mu nabídneme postup řešení jeho problému – může to být zablokování závadného obsahu, právní posudek (zda je možné věc řešit v trestněprávní rovině), policejní rozbor (zda jde o trestný čin či ne a co lze dělat), jsme schopni zajistit komunikaci s metodikem prevence příslušné školy, školním psychologem, v dané škole jsme pak schopni realizovat preventivní program a podobně. Ne vždy však oběti dokážeme pomoci – v některých případech oběti vyžadují odstranění jejich vlastního intimního materiálu z internetu, což však není možné, protože se materiál již stal virálním a šíří se v podstatě nekontrolovaně. Jak jsem již ale vysvětloval, příčinu kyberšikany je třeba hledat v sociální skupině, jejíž je dítě součástí – tu je třeba napravit a zajistit zdravé prostředí.