

Příloha

Metodika bezpečného chování dětí na internetu

Tato metodika byla navržena k použití v rámci neformálního vzdělávání dětí ze sociálně znevýhodněného prostředí s cílem vybavit je **kompetencemi k předcházení a řešení rizikových situací na internetu**. Asi 90minutový workshop doporučuji realizovat v malých skupinách dětí prvního i druhého stupně základních škol, které již běžně přicházejí do styku s internetem a mají tak základní povědomí o moderních komunikačních kanálech, sociálních sítích apod.

Při práci s dětmi s poruchami koncentrace pozornosti případně kombinovanými se SPU je nezbytná individuální práce s dětmi ve skupině. Proto považuji za důležité, aby lektor vedoucí workshop s dětmi dlouhodobě pracoval a znal jejich **specifické potřeby** nebo úzce spolupracoval s takovým koordinátorem, který s danými dětmi dlouhodobě pracuje. U mladších dětí na prvním stupni základní školy vidím přínos i v zapojení současně několika asistentů, kteří by pomáhali dětem překonávat obtíže při práci s výpočetní technikou i případné jazykové bariéry.

Metodika vychází z principů zkušenostního učení a skládá se z **pěti simulací potenciálně rizikových situací**, se kterými se děti na internetu mohou setkat. Každá z aktivit má přibližně následující průběh:

1. lektor uvede děti do situace, představí problém k řešení a motivuje je k práci,
2. děti řeší předložený problém,
3. lektor sám nebo společně s dětmi dává zpětnou vazbu na navržená řešení formou nastínění možného vyústění reálné situace,
4. děti navrhují nové - lepší řešení problému.

Jako teoretický základ pro práci s touto metodikou slouží kapitola 2 *Bezpečnost na internetu* této diplomové práce a případně i další zdroje, na které text odkazuje.

1. Seznamte se: kybergroomer

- *cíl aktivity*: Simulace děti seznamuje s fenoménem anonymity internetu a ukazuje jim, jak snadno si lze vytvořit alternativní identitu a získat cizí důvěru. Děti se v praxi seznámí s jedním z modelů sociálního inženýrství a jeho možnými následky.
- *popis*: Lektor uvádí děti do situace, ve které internet hraje důležitou úlohu při socializaci, poznávání nových lidí i udržování a utužování stávajících kontaktů. Zapojuje děti do výčtu aktivit, které k tomu účelu slouží – aktivita na sociálních sítích, sdílení obrázků a videí, jejich vzájemné komentování, komunikace skrze chat a e-mail, a motivuje děti ke sdílení vlastních zkušeností s danými nástroji.

Lektor děti motivuje, aby si představily, jak vypadá jejich komunikace na chatu s někým, koho právě potkaly. Pak jim předloží počítač s otevřeným instant messengerem, na kterém již čeká přihlášený nový kamarád-pomocník v roli kybergroomera. Děti dostanou za úkol zkusit se s ním bavit stejně, jako kdyby seděly doma u svého počítače, jak jsou zvyklé. Lektor je pouze v roli technické podpory při práci s počítačem a nechává dětem volné ruce.

Pomocník přihlášený na chatu má za úkol vydávat se za vrstevníka dětí a vytvářet si v průběhu konverzace takovou identitu, aby působil atraktivně jako potenciální nový kamarád. Snaží se získat si důvěru dětí, vylákat z nich zneužitelné informace (osobní, kontaktní údaje, fotografie, informace o škole apod.) a vylákat je na osobní schůzku.

Ve vhodné chvíli lektor aktivitu ukončuje a ptá se dětí, s kým se seznámily, jaké informace se o novém kamarádovi dozvěděly. Vzápětí pomocník přichází do místnosti nebo se s ním spojuje pomocí webové kamery a odhalujeme jeho skutečnou identitu. Následuje krátká debata o tom, proč se vlastně vydává za někoho jiného, a co by se mohlo stát, kdyby někdo z dětí na schůzku s ním šel. Zhodnotíme i informace, které o sobě děti prozradily a k čemu je může kybergroomer zneužít. Lektor děti motivuje, aby se zamyslely nad tím, co by udělaly ve stejné situaci jinak.

Pokud dítě dodržuje zásady bezpečného používání internetu, nesmluví si s kybergroomerem osobní schůzku, nesdělí osobní ani kontaktní údaje.

- *pomůcky*: počítače pro děti, počítač pro asistenta/y, účty na instant messengeru pro děti i asistenta/y

2. Kde bydlíš?

- *cíl aktivity*: Simulace dětem nabízí zpětnou vazbu na rozsah a hloubku informací, které o sobě sdělují na svých veřejných profilech na sociálních sítích.
- *popis*: Lektor přednese téma sociálních sítí, ptá se dětí, které sociální sítě znají a na kterých mají svůj vlastní profil. Dále rozvíjí diskusi na téma soukromí na sociálních sítích a veřejně zobrazovaných informacích.

V rámci simulace se děti registrují do nové sociální sítě „Fejskuk“ a vyplňují si informace do svého profilu. Nejdříve děti navzájem a pak i lektor nebo vhodný nezávislý pozorovatel dává dětem zpětnou vazbu na vhodnost uvedených informací na profilu a uvádí příklady z praxe, jak je možné dané informace zneužít.

Na závěr lektor děti motivuje ke společnému návrhu, které z informací je vhodné mít na veřejném profilu. Odborníci doporučují, aby o sobě mladší děti na internetu nezveřejňovali žádné osobní údaje včetně fotografie obličeje, jména, věku, adresy, školy, telefonního čísla či jiného kontaktu. Např. ve veřejných chatovacích místnostech si dítě vystačí s přezdívkou. Jiná je situace tehdy, pokud dítě po internetu soukromě komunikuje s osobou známou i mimo prostředí internetu.

- *pomůcky*: předtištěné nebo elektronické registrační formuláře z následující strany

Registrace do Fejskuku

Pro registraci vyplňte údaje na veřejný profil:

Kontaktní údaje:

Jméno: Příjmení:

Datum narození: Škola:

Město: Ulice a č.p.:

E-mail: Skype:

Telefon: ICQ:

Co máte rád/a:

Koníčky:

TV pořady:

Muzika:

Nastavení soukromí:

Vaše fotografie si smí prohlížet: *všichni* */jen přátelé*

Vaše příspěvky a komentáře smí prohlížet: *všichni* */jen přátelé*

Zprávy vám mohou posílat: *všichni* */jen přátelé*

Děkujeme za registraci,

vítejte na Fejskuku!

3. Chceš si přivydělat?

- *cíl aktivity*: Simulace má vést děti ke kritické percepci informací na internetu a pomoci jim nahlédnout lež jako běžnou součást internetového obsahu. Na příkladu časté praktiky lákání fotografií a informací od dětí za úplatu mají děti zjistit, že nelze důvěřovat informacím z neznámých neověřených zdrojů.
- *popis*: Lektor dětem přednese téma internetu jako zdroje pracovních nabídek, brigád a přivýdělků. Ptá se dětí na zkušenosti jich samotných i jejich přátel a nejbližšího okolí s touto možností využívání internetu.

Samotnou náplň drobné aktivity tvoří návrh řešení situace, ve které děti dostanou z neznámé e-mailové adresy lákavou nabídku na přivýdělek. Jedná se o v praxi často využívanou formu manipulace dětí. Ústředním tématem jsou fotografie. Manipulátor z dětí láká jejich fotografie na ukázkou s příslibem brigády formou focení módních nebo jiných fotografií za lákavou finanční obměnu. V případě této simulace odesílatel od dětí navíc požaduje některé osobní údaje, jako je věk nebo navštěvovaná škola.

Děti navržené řešení lektor rozvede a nastíní možný vývoj takové situace. V případě odeslání fotografií a dalších osobních údajů v podobě jména, věku a navštěvované školy se děti stávají snadným cílem útoků i mimo prostředí internetu. Pokud by odesílatel z dětí vylákal dokonce citlivé fotografie, mohl by je snadno vydírat a požadovat další podobný materiál pod pohrůzkou zveřejnění fotografií. Jako ukázkou takového příběhu lektor může pustit úryvek z druhého filmu Seznam se bezpečně.

Vhodným řešením je rozhodnout se na zprávu neodpovídat a ideálně o ní říct i rodičům nebo učitelům. Naopak nevhodné řešení je na podobnou zprávu reagovat nebo dokonce poskytovat požadované osobní údaje včetně fotografií.

- *pomůcky*: text e-mailu v elektronické podobě nebo vytištěný (příklad e-mailu na následující straně), film Seznam se bezpečně, dostupný fotoaparát nebo webkamera, pokud by je děti chtěly využít

Dětský fotomodeling



Doručená pošta x



jaroslav.maly-foto@email.cz 21:58 (před 10 min) ☆

komu: mně ▾

Ahoj kamaráde,

chceš si snadno vydělat **2000 Kč**? Sháníme děti ve věku 6-13 let na **focení do módního časopisu**.

Pošli nám svou **fotografii, jméno, věk a název školy**, do které chodíš. Do konce listopadu vybereme 100 dětí, které pozveme na focení v ateliéru.

Jaroslav Malý

FOTOateliér Jaro
Nepilova 12
Praha 9

jaroslav.maly-foto@email.cz

...

Odeslat | | | | Uloženo | | ▾

4. Vyrábíme neprůstřelné heslo

- *cíl aktivity*: Drobná aktivita učí děti, že heslo je soukromý údaj, který pomáhá chránit naše soukromí a identitu na internetu. Proto nepatří do ruky nikomu cizímu ani těm, ke komu máme důvěru. Aniž by o tom dítě vědělo, může heslo poskytnout agresorovi, který zneužije přístup do jeho účtu např. ke kyberšikaně. Navíc se děti dozví zásady pro tvorbu bezpečného hesla.
- *popis*: Na úvod lektor dětem přednese téma hesla jako bezpečnostního klíče k osobním účtům a informacím. Ptá se dětí, kolik takových hesel mají, jak si svá hesla vybírají a jestli si myslí, že jsou skutečně bezpečná a proč by vlastně měla být. Následně lektor dětem představí, z čeho se skládá bezpečné heslo a co by se v něm nemělo objevit:
 - nepoužívat snadno dostupné údaje (jméno, přezdívka, datum narození)
 - heslo musí mít minimálně 8 znaků
 - je vhodné použít kombinaci znaků (čísla, malá a velká písmena, další znaky ?!@#)
 - pomůcka – „Měla babka 4 jabka a dědoušek jen 2“ = Mb4jadj2

Na základě předchozí debaty lektor vyzve děti, aby si na místě vymyslely nové bezpečné heslo pro svůj účet na sociální síti nebo e-mailu. Každé z dětí si heslo napíše na vlastní podepsaný papír.

Poté lektor vyzve děti, aby svá hesla ukázaly a zkontrolovaly si tak, že jsou opravdu bezpečná. Ptá se, kde chtějí heslo použít, zkusí si ho od dětí opsat nebo je s ním vyfotit. Lektor volně naváže diskusi o tom, jestli je v pořádku, že si hesla vzájemně ukazujeme, opisujeme a fotíme, a co by se mohlo stát, kdyby se heslo dostalo do ruky někomu cizímu.

Pokud se děti se svým heslem svěří (např. i kamarádům), měly by následně reflektovat nevhodnost dalšího využívání takového hesla. Pokud by se dostalo do ruky někomu cizímu, ten by mohl zneužít přístup do účtu, zjistit osobní údaje dítěte nebo se prostřednictvím účtu vydávat za ono dítě za účelem ho poškodit (kyberšikana).

- *potřeby*: papíry a psací potřeby pro děti, fotoaparát

5. Přišel ti e-mail

- *cíl aktivity*: Tato aktivita dětem představí typické projevy kyberšikany a umožní jim vyzkoušet si kybernetického agresora zastavit. Na závěr se seznámí s odborníky doporučovaným a funkčním modelem obrany proti kyberšikaně.
- *popis*: Lektor nadnese téma šikany a kyberšikany – společně s dětmi vyjmenovává její projevy, charakterizuje osobu útočníka a oběti a motivuje děti, aby sdílely své zkušenosti s tímto jevem ze svého okolí, ze školy nebo od přátel.

Pro uvedení do aktivity lektor dětem představí smyšlenou postavu 10leté žačky Hany, která se stala obětí kyberšikany. Ukazuje dětem sérii zpráv, e-mailů a komentářů ze sociálních sítí, které Hana od útočníků pravidelně dostávala. Jedná se o verbální útoky, nenávistné projevy i výhrůžky. Lektor děti vyzývá, aby našly řešení, jak může Hana útoky zastavit.

Během plnění úkolu jsou děti zahrnovány stále novými zprávami. Jde o simulaci časové neohraničenosti útoků v případě kyberšikany. Ve vhodné chvíli lektor aktivitu ukončí a přistoupí ke zpětné vazbě navržených řešení. Sérií otázek se snaží děti navést na vhodné řešení situace.

Jako ideální postup pro řešení šikany odborníci radí svěřit se rodičům nebo učitelům, zablokovat účty agresora, uchovat zprávy jako důkaz kyberšikany a v závažnějších případech kontaktovat Policii ČR. Vhodným postupem je i kontaktování některé z horkých linek (Linka bezpečí). Naopak nevhodným řešením je odpovídání na šikanózní zprávy.

- *pomůcky*: počítače a založený e-mailový účet a mobilní telefon pro čtení zpráv, připravené texty a ukázky šikanózních projevů (příp. i v tištěné podobě)