EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
OP Praha – pól růstu ČR

Prevence kyberšikany

Metodika pro pedagogy

Fórum pro prožitkové vzdělávání, z.ú.

Vytvořeno v roce 2020 v rámci projektu
CZ.07.4.68/0.0/0.0/19_068/0001408
Prožitková pedagogika pro posilování
demokratické kultury a občanských
kompetencí žáků

OBSAH

„KAŽDÁ POKROČILÁ TECHNOLOGIE
JE K NEROZEZNÁNÍ OD MAGIE.“

ARTHUR CHARLES CLARKE

„ANI VŠECHNA TECHNIKA NA SVĚTĚ
NEODČINÍ NESCHOPNOST VŠÍMAT SI.“

ELLIOT ERRWIT

TEORETICKÁ ČÁST

KYBERŠIKANA JAKO NOVÁ HROZBA PRO DEMOKRACII

1. ZABEZPEČENÍ POČÍTAČE

Svůj počítač budete schopni sami dostatečným způsobem zabezpečit, porozumíte-li alespoň v základní míře bezpečnostním rizikům, která dnes v souvislosti s používáním počítačů hrozí. Zároveň je ale také vždy potřeba používat i při práci počítačem přirozenou ostražitost a zdravý rozum. Nutné rovněž je umět případným problémům nejen předcházet, ale zároveň vědět, jak je následně řešit. Dnes bohužel platí, že řada činností vykonávaných na počítači potenciálně rizikových z principu je. To platí především o používání hesel, pin kódů apod. či o stahování obsahu potenciálně infikovaného závadným softwarem. V takovém případě mluvíme o tvz. malwaru, jehož cílem je Váš počítač poškodit, získat Vaše důvěrné údaje, jako přístupová hesla do on-line bankovnictví apod.

V této metodice budete mít možnost seznámit se podrobněji se všemi základními typy takovéhoto škodlivého softwaru, tedy viry, červy, trojskými koňmi a spywarem. Je zde popsáno i to, jak je podle různých příznaků možné zjistit, že je Váš počítač napaden, a jak na tuto situaci správně reagovat. S tímto tématem pak souvisí i základní bezpečnostní pokyny pro prevenci nákazy Vašeho počítače. Jde zejména o práci na internetu vždy jen na počítačích chráněných aktualizovanou verzí antivirového programu a tzv. anti-spywaru. Neméně důležitá je pak i bezpečná práce s e-mailovými přílohami, obsahy flash disků či datových CD a DVD apod.

ZÁKLADNÍ NÁSTROJE A POSTUPY PRO BEZPEČNOU PRÁCI S POČÍTAČEM

Aktualizovaný antivirový program

V tomto případě máme na mysli nejen aktualizace tzv. virové databáze, tedy seznamu známých virů a dalších škodlivých kódů, ale také aktuálnost vlastního programu. Zastaralý antivirový program i přes průběžné aktualizování vlastní virové databáze může počítači poskytnout pouze omezenou ochranu.

Aktualizovaný operační systém a další klíčový software

Převážná většina útoků na osobní počítače je v současnosti vedena prostřednictvím známých softwarových chyb v operačním systému nebo v běžně dostupných aplikacích. Výrobci softwaru průběžně tyto bezpečnostní chyby odhalují a opravují prostřednictvím tzv. bezpečnostních záplat. Ty je zapotřebí průběžně do svého počítače instalovat, obvykle jsou tyto bezpečnostní aktualizace stahovány a následně instalovány do těchto programů automaticky.

Zapnutý firewall

Tzv. firewall představuje bránu mezi lokálním počítačem a vnějším světem. Jeho úkolem je blokovat potenciálně nebezpečné akce, například pokusy o průnik do Vašeho počítače z vnějšího prostředí.
Firewall lze také nakonfigurovat pro selektivní zákazy vybraných akcí a činností realizovaných prostřednictvím daného počítače na internetu.

Silná hesla a zodpovědně spravované uživatelské účty

Kvalitní hesla jsou základem klidné a bezpečné práce na počítači. Právě na prolomení bezpečnostních hesel je přitom založena řada bezpečnostních útoků. Jedná se zejména o tzv. slovníkový útok, kdy útočník vyzkouší všechna známa slova. Nepoužívejte proto jako své heslo běžně užívaná slova. Dále se pak útočníci mohou snažit Vaše heslo jednoduše odhadnout. Často není zase tak složité domyslet

si, jaké asi heslo bylo asi v daném případě použito. Nepoužívejte tedy proto jako hesla jména svých blízkých či názvy sportovních klubů apod. Riziková je také varianta, kdy používáte stejné heslo ve více aplikacích. V takovém případě může dojít k tomu, že útočník například odpozoruje heslo při jeho zadávání do jedné aplikace a může ho pak použít i pro přístup do všech dalších chráněných oblastí a aplikací. Doporučujeme tedy, aby každá aplikace měla své vlastní heslo. Existuje také tzv. útok hrubou silou, kdy útočník s pomocí automatického programu zkouší všechny kombinace písmen a číslic. Tomuto typu útoku neodolá žádné heslo, ale dostatečnou délkou a používaným různých znaků můžeme útočníkovi jeho záměry ztížit.

Ochrana proti spamu

Podle nejnovějších odhadů patří až 90 % e-mailů do kategorie tzv. spamu, tj. nevyžádaných e-mailů. Ty kromě toho, že sami o sobě obtěžují a zaplňují Vaši e-mailovou schránku, mohou představovat i významné bezpečnostní riziko pro dětské uživatele internetu. Pokud se na internetu zapojíte do diskusní skupiny, chatu, veřejného fóra, sociální sítě nebo vyplníte online dotazník a na příslušných stránkách zveřejníte svoji e-mailovou adresu, nevyhnutelně se stanete adresáty spamů. Speciální software dokáže z webu stahovat e-mailové adresy, sestavovat jejich seznamy a hromadně na ně takovéto spamy rozesílat. Společnosti zabývající se touto de facto nelegální činností navíc obvykle sídlí v zemích bez příslušné legislativy, která by zasílání nevyžádaných e-mailů postihovala. Spamy velice často nabízejí pornografické materiály, farmaceutické výrobky či podvodné finanční služby. Prostřednictvím spamů se navíc mohou šířit škodlivé programy. Ve většině případů jsou tyto e-maily rozesílány s úmyslem adresáta oklamat.

Mezi základní pokyny, jak rizika spojená se spamy omezit, patří používání spamových filtrů, kdy správce příslušného e-mailového účtu obvykle nabízí možnost aktivovat si protispamovou ochranu v e-mailové schránce. Většinou je tak k dispozici složka nevyžádané pošty, kam jsou tyto spamy automaticky ukládány. Pravidelně ale svoji složku nevyžádané pošty kontrolujte a přesvědčte se, že zde neskončily některé neškodné e-maily. Ani nejpreciznější spamové filtry totiž nemohou být zcela neomylné. Zároveň také naučte děti, aby neotvíraly e-maily od neznámých lidí. Spamy téměř vždy obsahují lákavé nabídky a přílohy.

Ukažte jim, jak si mohou přijímání e-mailů zaslaných z určitých adres zablokovat nebo je jednoduše naučte, aby podezřelé e-maily vždy smazaly.

BEZPEČNOST DĚTÍ V ON-LINE PROSTŘEDÍ

Internet může být velkým přínosem dokonce i pro velmi malé děti, ať už zde surfují pro zábavu nebo navštěvují vzdělávací webové stránky. Na druhou stranu zde narazí na množství stránek s obsahem, který pro uživatele jejich věku vhodný není. Pro nalezení informací k určitému tématu jsou velmi vhodné vyhledavače. Jelikož však hledání probíhá na základě zadaných klíčových slov, velmi snadno se dostaneme na stránky s nevhodným obsahem. Nevinně znějící klíčové slovo nás může navést na stránku, která již tak nevinně nevyhlíží, a přesto zde zadané slovo figuruje. Chcete-li, aby děti byly při surfování na internetu v bezpečí, máme pro vás několik rad:

- ➔ Ve většině běžných operačních systémů (např. Windows, Linux, Mac OS) existuje možnost vytvořit dítěti vlastní uživatelský účet, na kterém lze aktivovat funkci rodičovská kontrola.
- ➔ Malé uživatele internetu ve vaší péči seznamte s vyhledavači vytvořenými přímo pro děti, příkladem jsou stránky http://kids.yahoo.com nebo http://www.askforkids.com
- ➔ Adresy webových stránek, které vaše děti navštěvují nejčastěji, jim uložte ve složce „Oblíbené" (najdete ji v menu prohlížeče). Svá oblíbená místa na internetu budou tak moci navštěvovat opakovaně, aniž by musely znovu používat vyhledávač. Omezíte tak dále riziko jejich kontaktu s nevhodným internetovým obsahem.
- ➔ Kromě aktivace funkci rodičovské kontroly existuje také možnost využití přídavných filtrů, tj. softwaru, který chrání nezletilé uživatele před nevhodným obsahem některých webových stránek. Zároveň ale platí, že ani nejmodernější filtry nemohou plně nahradit dohled rodičů či pedagogů. Filtrační software může být naopak natolik omezující, že zablokuje i přístup na stránky s naprosto neškodným obsahem. Může se například stát, že se děti nedostanou k materiálům o druhé světové válce, protože půjde o stránky popisující násilí. Navíc pokud je možné nějaký filtr zapnout, dokáží ho chytré děti také vypnout a dokonale zahladit stopy po svých aktivitách. Tyto jejich praktiky odhalíte pouze tehdy, když se sami naučíte počítač a software používat.

Navštivte webové stránky SIP-Bench, kde jsou zveřejněny výsledky studie, kterou podpořila Evropská komise. Autoři studie testovali 30 nástrojů pro rodičovskou kontrolu a anti-spamovou ochranu a zjišťovali, nakolik účinně chrání děti ve věku 6–16 let při jejich nejrůznějších aktivitách na internetu před škodlivým obsahem. Sledovány byly tyto aktivity: prohledávání internetu, zasílání e-mailů, přenášení souborů, chatování a instant messaging.

Samotná ochrana před škodlivým obsahem nepostačí. Děti byste měli zejména naučit, aby nevěřily všemu, co na internetu vidí a čtou. Nejvhodnějším doporučením pro ně je, aby při vyhledávání určité informace navštívily nejméně tři různé webové stránky a uvedené informace porovnaly. Také by se měly již od útlého věku naučit respektovat princip, že kdykoli přebírají jakoukoli informaci například do nějaké školní práce, je účelné uvádět příslušné zdroje informací.

Pravidla pro ochranu dětí používajících internet

- ➔ V maximální možné míře využívejte nástrojů pro rodičovskou kontrolu, které vám poskytuje software vašeho operačního systému, a to v internetovém prohlížeči, vyhledavači a e-mailovém programu. Svým dětem vytvořte vlastní uživatelské účty. Ochranu soukromí zde nastavte na nejvyšší možnou úroveň (v menu svého prohlížeče vyberte „Možnosti").
- ➔ Zvažte, zda si nepořídit přídavný filtrační software.
- ➔ Pokud narazíte na internetu na stránky s nevhodným obsahem, oznamte jejich existenci na národní internetovou horkou linku (viz „Užitečné odkazy").
- ➔ Kdykoli vaše děti surfují na internetu a vy si k nim můžete přisednout, udělejte to. Je to skvělá příležitost, jak zahájit diskusi a posílit vzájemnou důvěru. Vezměte to jako výzvu a učte se společně s nimi.
- ➔ Nezapomínejte, že bezpečnostní pravidla se týkají jak dětí, tak vás samotných. Veďte děti k tomu, aby vás informovaly, kdykoli uvidí na internetu něco podivného.

Rekapitulace obecných bezpečnostních pokynů

- ➔ Svůj počítač si zabezpečte. Nainstalujte si firewall a také antivirový a anti-spyware software, které pravidelně aktualizujte. Věnujte pozornost veškerým upozorněním, které tyto programy vygenerují. Zjistěte si, zda váš poskytovatel internetových služeb (Internet Service Provider – ISP) nabízí antivirové a anti-spyware nástroje, které můžete využít.
- ➔ Ve svém e-mailovém programu používejte filtr spamů a svoji e-mailovou adresu uchovávejte pokud možno v tajnosti, neuvádějte ji na webu. Vyhýbejte se e-mailům od neznámých odesilatelů a přílohy před otevřením zkontrolujte antivirovým programem.
- ➔ Jakmile se Váš počítač začne chovat podivně, může to znamenat, že je zavirovaný. Kontaktujte ihned svého ISP (poskytovatele internetových služeb) nebo jiného odborníka. ISP by také měl být schopen poskytnout rady rodičům.

2. KOMUNIKACE V ON-LINE PROSTŘEDÍ

Vzpomínáte si, jak byl pro vás v době dospívání důležitý kontakt s kamarády? Internet nabízí uživatelům řadu nových příležitostí k setkávání s přáteli a umožňuje jim vyjadřovat se a komunikovat mnoha různými způsoby – mohou si zasílat e-maily, sdílet soubory, psát vlastní blogy nebo se stát členy různých komunit (např. v prostředí MySpace, Facebook, Hi5, Habbohotel atd.). V současné době teenageři využívají moderní technologie nejen proto, aby si vyzkoušeli nové věci, ale také aby navazovali kontakty v prostředí, které považují za soukromé a kde nejsou pod dohledem rodičů.

Kapitola věnovaná komunikaci seznamuje rodiče i děti se způsobem zveřejňování osobních údajů a s možnostmi ochrany soukromí. Dozvíte se, v čem je online komunikace přínosnáa jak se chovat v rizikových situacích, mezi které patří např. kontakt s neznámými lidmi. Problém ochrany soukromí na internetu je velice úzce spojen s vytvářením účtů & profilů. Prostřednictvím vlastního účtu máme přístup k online službám.

Na své legitimaci na autobus, permanentce do fitness klubu či jiném průkazu, který používáte v každodenním životě, máte zapsány některé osobní informace. Totéž platí také o online účtech a objednávkách určitých internetových služeb. Zřídit účet či objednat službu si můžete pouze za předpokladu, že uvedete konkrétní informace o své osobě, které se pak stanou součástí vašeho „uživatelského profilu". Skutečnost, že sami určujete, jaké informace o sobě zveřejníte a kdo k nim bude mít přístup, je velmi důležitá. Chcete-li si chránit své soukromí, neuvádějte lživé informace, ale zvažujte, co se o vás ostatní mají dozvědět. Mladí lidé jsou velmi nadšeni možností komunikovat se svými přáteli po internetu a vytvářet si vlastní online podobu. Ne vždy si však uvědomují, jaké následky může mít zveřejnění soukromých informací.

OSOBNÍ PROFILY A ÚČTY V ON-LINE PROSTŘEDÍ

Prvním krokem při ochraně osobních informací je vytvoření bezpečného profilu. Je třeba pečlivě rozhodnout, jaké informace v něm uvedete a jaké bezpečnostní nastavení zvolíte. Pro různé online aktivity si vytvořte různé e-mailové účty. Pokud vaše dítě využívá internetové služby, jako je chatování,

instant messaging, psaní blogu apod., naučte ho při těchto aktivitách používat neutrální e-mailovou adresu a přezdívku. Chatující dítě tak v adrese nevyzrazuje celé své jméno.

Heslo k účtu vždy udržujte v tajnosti. Vysvětlete dětem, že informace o svých soukromých účtech nemají prozrazovat kamarádům, kteří by jejich důvěry mohli zneužít. Na druhou stranu možná budete chtít znát hesla svých dětí, abyste nad jejich účty měli kontrolu – promluvte si o tom s nimi.

Nezapomeňte si na svém profilu/účtu nastavit ochranu soukromí, tj. zadat, že se jedná o informace soukromé, nikoli veřejně přístupné. Pouze tak budete moci určovat, komu se vaše údaje zobrazují a s kým můžete komunikovat. Soukromý profil vám umožňuje sestavit si a měnit svůj seznam kontaktů (tj. seznam kontaktních adres). Naučte své děti, aby přijímaly zprávy pouze od osob, které již znají z prostředí mimo internet.

Pokud vaše děti využívají **chatovací místnosti**, podívejte se zda:

- ➔ na komunikaci dohlížejí moderátoři. Nepřítomnost moderátorů znamená nezabezpečené chatování;
- ➔ jsou zde nástroje, které umožňují ignorovat či zablokovat kontakt s osobami, se kterými děti chatovat nechtějí;
- ➔ jsou na webových stránkách k dispozici funkce „nápověda“ a „zpráva o chybě“, které lze použít, nastanou-li problémy;
- ➔ pravidla chatovací služby jsou jasně vymezena a zveřejněna na nepřehlédnutelném místě.

Fotografie a webkamery

Děti musí pochopit, že fotografie také patří mezi soukromé informace a že pohyb digitálních fotografií po internetu je téměř nemožné ovlivnit. Je velmi jednoduché poslat je do oběhu po síti a měnit jejich podobu (tj. manipulovat s nimi). Jakmile byly jednou z počítače či mobilního telefonu odeslány, velmi obtížně se odstraňují, mohou dokonce zůstat online navždy! S webovými kamerami je třeba zacházet s velkou opatrností a děti by neměly kamery používat bez dozoru. Chatovací služby s možností použití webových kamer mohou představovat riziko. Vy i vaše děti byste měli své fotografie zasílat pouze lidem, které znáte a kterým důvěřujete. Chcete-li zveřejnit fotografii jiné osoby, požádejte ji o souhlas. Své děti nenechávejte používat počítač s webovou kamerou, pokud jsou v místnosti samy.

Kontakt s neznámými lidmi

Lidé, které potkáte online, nejsou vždy těmi, za koho se vydávají. Naučte své děti chránit si vlastní soukromí na internetu stejným způsobem, jako to dělají v neinternetovém světě. Určitě jim říkáte, jak se mají chovat k neznámým lidem v běžném životě, proč by se tedy neměly řídit stejnými pravidly i na internetu?

Vaše děti si možná k přátelům z internetu vytvoří silný vztah. Není pro ně vůbec obtížné začít důvěřovat lidem, kteří je sice vůbec neznají, ale zajímají se o ně a mají pro ně pochopení. Velkým lákadlem pro děti je pak možnost se s novými přáteli sejít, aniž by vám cokoli řekly. Děti si často neuvědomují, jak nebezpečná mohou taková setkání být a nepovažují je za problematická. Stávají se velmi snadnou obětí

online groomingu (lákání na schůzky). Ze studií vyplývá, že mnoho dětí se na setkání s online „přáteli" vydává bez doprovodu a o svých schůzkách rodiče neinformují. Chcete-li mít jistotu, že vaše děti takto jednat nebudou, promluvte si s nimi o tomto jevu. Klíčem k řešení možného problému je dobrá komunikace.

Víte, jak se na chatu mluví?

Při online chatování používají mladí lidé specifický jazyk plný emotikonů a akronymů! Některé z nich si můžete prohlédnout v následující tabulce. Přehled základních akronymů používaných při chatování v angličtině, využívaných často i v prostředí českého internetu.

121	one to one	JJ	just joking
AFK	away from keyboard	K	all right /ok
A/S/L	age, sex, location	KFY/K4Y	kiss for you
BBB	bye bye baby	KISS	keep it simple, stupid
B4N	bye for now	KPC	keeping parents clueless
BBL	be back later	L8R	Later
BF	boyfriend or best friend	IRL	in real life
BFF	best friends forever	LMIRL	let's meet in real life
C	see?	LOL	laughing out loud, lots of love
Comp	computer	LY4E	love you forever
CU	see you	NE1	anyone
CUL	see you later	NP	no problem/ noisy parents
CYO	see you online	OIC	oh, I see

České akronymy se do elektronické komunikace dostaly jen v omezené míře. Mezi ty nejpoužívanější v současnosti patří:

JJ	jo jo	NN	ne ne
MMNT	moment – počkej chvilku	NJN	no jo no
O5	opět	Z5	Zpět
TTJ	tak to jo	TTPJ	tak to potom jo
PP	pápá	NZ	není zač

Emotikony si můžete vytvářet kombinováním interpunkčních znamének a písmen, podobně jako v následujících příkladech:

Smajlík (s nosem nebo bez)	:) nebo : -)	dvojtečka, (pomlčka), závorka
Smutný obličej (s nosem nebo bez)	:(nebo :-(	dvojtečka, (pomlčka), závorka
Mrkající obličej (s nosem nebo bez)	;) nebo ;-)	dvojtečka, pomlčka, závorka
Překvapený obličej (s nosem nebo bez)	: o nebo :-o	dvojtečka, (pomlčka), malé písmeno o
Široký úsměv (s nosem nebo bez)	:-D nebo : D	dvojtečka, (pomlčka), velké D
Vyplazený jazyk (s nosem nebo bez)	: p nebo :-p	dvojtečka, (pomlčka), malé p

PRAVIDLA PRO VÁS A DĚTI

Sledujte, jak vaše děti svůj čas na internetu tráví. Požádejte je, ať vám ukážou, jakým způsobem se svými kamarády komunikují.

Naučte je, jak si na internetu chránit svoji bezpečnost. Měly by vědět, že:

- ➔ si mají vytvářet bezpečné profily, na kterých je možné nastavit si ochranu soukromí;
- ➔ si mají chránit své heslo;
- ➔ mají reagovat pouze na zprávy od osob, které znají odjinud než z internetu a pouze tyto osoby také oslovovat;
- ➔ pokud chtějí vložit na internet svoji fotografii nebo fotografii své rodiny, domu nebo školy, musí vždy požádat o souhlas rodičů;
- ➔ soukromé informace, např. telefonní číslo, adresu, školu, sportovní klub apod., smějí sdělovat pouze lidem, které znají dobře z běžného života.

Rodinný počítač umístěte do obývacího pokoje, abyste měli aktivity svých dětí na internetu pod kontrolou.

Společně si vyzkoušejte, že:

- ➔ víte, jak odmítat nebo si zablokovat příjem zpráv od určité osoby ve svém seznamu kontaktů;
- ➔ na stránkách, které navštěvujete, si umíte zajistit bezpečnost a dokážete zde odeslat zprávu o případných problémech.

Budujte si se svými dětmi vztah založený na důvěře. Ujistěte je, že s vámi mohou mluvit i o svých chybách, protože jedině tak můžete společně hledat řešení! Chyby k učení patří.

3. ZÁBAVA A STAHOVÁNÍ

Ve virtuálním prostředí na internetu probíhá celá řada aktivit, včetně aktivit komerčních. Jistě svým dětem nekupujete vše, na co vidí reklamu v televizi nebo co je zaujme v obchodě. Měli byste je tedy také naučit, že není třeba vlastnit každou věc nabízenou na internetu a nelze věřit všem internetovým reklamám. Ty nejčastější nabízejí hudební nahrávky, hry, vyzváněcí tóny, počítačové příslušenství či online služby.

Jestliže budete na internetu surfovat společně se svými dětmi, budete mít příležitost vysvětlit jim, že věci jako vyzváněcí tóny, tapety, mp3 nahrávky, avatary apod. jsou zdarma málokdy. Kdykoli narazíte na reklamu tvrdící opak, upozorněte děti na text psaný drobným písmem a ukažte jim, že ne všechna tvrzení na netu lze brát doslova.

Pokud si objednáváte jakoukoli službu (ať už zdarma či za poplatek), musíte vyplnit online formulář a uvést požadované osobní informace. Formuláře vyplňujte, pouze pokud je vám jasné, jakým způsobem budou vámi zadané informace použity. Děti by měly formuláře vyplňovat jedině ve vaší přítomnosti.

Vyskakovací okna se na internetu často používají pro propagaci výrobků. Ne vždy jsou však negativním jevem – záleží, nakolik důvěryhodné jsou samotné stránky, na kterých se objevují. Obecně lze říci, že pokud webovým stránkám důvěřujete, můžete věřit i informacím ve vyskakovacích oknech. V některých oknech se však objevují reklamy na podezřelé výrobky, jiná navádějí uživatele na online formuláře, které shromažďují osobní informace. Naučte své děti, aby podezřelá okna zavíraly kliknutím na červený křížek v pravém horním rohu.

STAHOVÁNÍ SOUBORŮ A PROGRAMŮ

Stahování z internetu je jednou z častých činností na počítači. Stažené soubory však mohou obsahovat nežádoucí kód, který infikuje vás počítač. Je proto nutné dodržovat několik zásad, jež sníží riziko nakaženi vašeho počítače nebo ho zcela vyloučí. Především je dobré vyvarovat se nelegálního software: statistiky nekompromisně uvádějí, že vice než padesát procent nelegálních kopii Windows na internetu je infikováno nějakou formou škodlivého kódu. Ovšem ani datové soubory (např. filmy) nejsou bezpečné. Častým trikem útočníků je to, že se při pokusu o spuštění filmu zobrazí hlášeni o chybějícím kodeku v počítači – a hned je nabídnutý odkaz na jeho stažení. Na dotyčné adrese ovšem není kodek, ale škodlivý kód, který si uživatel stáhne a sám nainstaluje do počítače.

Pamatujte si Stahujte soubory a programy jen z ověřených a důvěryhodných zdrojů a i tak je před spuštěním zkontrolujte antivirovým programem.

HRANÍ HER NA INTERNETU

Internetové hry vyžadují na rozdíl od starších digitálních her síťové připojení. Děti si hry mohou hrát z CD/DVD nosičů, na webových stránkách, herních konzolích, mobilních telefonech či jiných přenosných zařízeních.

Mezi online hry patří jak jednoduché, velmi rozšířené hry jako Pacman nebo Tetris, tak hry vycházející z virtuální reality, které hraje několik hráčů najednou online a společně vytvářejí jejich náplň a příběh postav. Okolo řady těchto víceuživatelských her vznikají celé virtuální hráčské komunity. Děti se při hrách tohoto typu dostávají na internetu do kontaktu s neznámými lidmi, což představuje určité riziko (viz kapitola „Komunikace“).

Hraní her hraje ve vývoji dětí významnou roli. Děti si při této činnosti rozvíjejí sociální dovednosti a strategické myšlení a to v prostředí vymezeném určitými pravidly. Mnohé z těchto interaktivních a velmi atraktivních her jsou využívány také pro vzdělávací účely.

Ne všechny digitální hry jsou však kvalitní. Vy sami musíte rozhodnout, jaké hry jsou pro vaše děti nejvhodnější. Zároveň musíte vymezit určitá pravidla a stanovit, jak dlouhou dobu mohou hraním online her strávit, aniž by utrpěly jejich ostatní aktivity.

Systém PEGI online je celoevropský systém třídění interaktivních her podle jejich obsahu a věku hráčů. Systém má podporu nejen řady výrobců konzolí jako PlayStation, Xbox, Nintendo, ale rovněž vývojových týmů a vydavatelů interaktivních her z celé Evropy. Zařazení do určité kategorie je vždy vyznačeno na obalu hry. Nezapomínejte však, že každé dvanáctileté dítě je jiné.

POUŽÍVÁNÍ VEŘEJNÝCH POČÍTAČŮ

Při prací s veřejnými počítači v knihovně, internetové kavárně, nebo třeba na letišti, je potřeba dbát zvýšené opatrnosti. Vždy se při prací s veřejnými počítači chovejte tak, jako by se vám někdo díval přes rameno. Neukládejte své přihlašovací údaje, prací s citlivými daty (např. internetové bankovnictví) omezte na minimum – či přímo vynechejte. Při odchodu od počítače odstraňte záznamy o své činnosti: navštívené webové stránky (mohou prozradit např. jaký využíváte e-mail nebo banku), stopy po otevřených dokumentech nebo uložené informace.

Také připojení k veřejné bezdrátové sítí je spojeno s bezpečnostními riziky: agresoři velmi často na veřejných místech (letiště, nádraží…) umisťuji vlastní přístupové body k internetu. A když se přes ně pokoušíte spojit, získávají vaše přihlašovací jména a hesla.

Pamatujte si Nikdy nevíte, kdo a s jakým úmyslem usedá k veřejnému počítači před vámi – a po vás!

Nejdůležitější pravidla

- ➔ Veďte svoje děti k tomu, aby navštěvovaly webové stránky, jejichž obsah neporušuje zákon. Vysvětlete jim také, že ne vše je ve skutečnosti takové, jak se na netu na první pohled jeví.
- ➔ Vysvětlete dětem, jaká rizika jim hrozí, pokud nebudou při stahování materiálů z internetu obezřetné.
- ➔ Přesvědčte se, že je váš počítač dobře zabezpečen. Vždy používejte aktualizovanou verzi antivirového programu.
- ➔ Učte své děti ukládat stažené soubory na harddisk tak, že daný soubor před otevřením prověří antivirovým programem.
- ➔ Ještě než si cokoli do počítače nainstalujete, přečtěte si text o ochraně soukromých údajů a prohlášení uživatele. Na internetu si ověřte spolehlivost softwaru, který si chcete stáhnout.
- ➔ Zavírejte podezřelá vyskakovací okna kliknutím na křížek v pravém horním rohu. Nikdy neklikejte dovnitř okna.

Děti & hry

- ➔ Stanovte, jak dlouhou dobu mohou děti hraním her trávit.
- ➔ Nechte je hrát na místech, kde nad nimi máte kontrolu.
- ➔ Sledujte hráčské návyky dětí. Hlídáte je na hřišti, proč byste tedy neměli dělat totéž při jejich aktivitách ve virtuálním prostředí?
- ➔ Povídejte si s nimi o obsahu hry. Které její prvky jsou podobné realitě a které ne? Co se jim na hře líbí?
- ➔ Předtím než dítěti hru zakoupíte, zkontrolujte si, zda je pro jeho věkovou kategorii vhodná (sledujte označení podle celoevropského systému PEGI nebo národního klasifikačního systému).

Pokud vaše děti hrají počítačové hry společně s dalšími hráči

- ➔ Vyberte jim stránky s přísnými pravidly, které sledují moderátoři.
- ➔ Důrazně je vyzvěte, aby své osobní údaje nesdělovaly ostatním hráčům.
- ➔ Dbejte na to, aby se s ostatními hráči mimo internet scházeli pokud možno pouze ve vašem doprovodu.
- ➔ Vyzvěte děti, aby vám oznamovaly jakékoli šikanování, vyhrožování, používání vulgárního jazyka, zveřejňování nepříjemného obsahu nebo výzvy k setkání v neinternetovém prostředí.
- ➔ Pokud vás hra nebo způsob, jakým se vyvíjí, znepokojuje, odhlaste dítě ze hry nebo změňte jeho virtuální identitu.

4. INTERNETOVÉ BANKOVNICTVÍ A NÁKUPY

Jednou z největších vymožeností internetu je on-line bankovnictví: kdykoliv a kdekoliv mate možnost kontrolovat stav svého účtu a provádět finanční transakce. S internetovými nákupy je to podobné: lze nakupovat kdykoliv, kdekoliv a odkudkoliv.

Ovšem i tyto výhody mají své hranice. Především bychom měli tyto finanční transakce realizovat pouze na chráněném počítači – tedy na počítači, nad kterým máme kontrolu a u něhož víme, co obsahuje za aplikace. Veřejný počítač v internetové kavárně to rozhodně není.

Zároveň si dejte pozor na phishing. Jedná se o způsob podvodu, kdy se vás útočník snaží přimět k návštěvě „své" stránky (která ovšem graficky vypadá velmi důvěryhodně). Obrana je jednoduchá: navštěvovat pouze oficiální stránky bank a obchodů. Tedy takové, které si sami vyberete (a mate je uvedené ve smlouvě). Ptejte se rovněž svých poskytovatelů služeb, zda používají bezpečnou doménu, kterou je obtížné přesměrovat.

5. ŠIKANA NA INTERNETU - KYBERŠIKANA

Kyberšikana ve stručnosti: jedná se o šikanování jiné osoby (ubližování, ztrapňování, obtěžování, ohrožování, zastrašování) s využitím internetu, mobilních telefonů či jiných informačních technologií.

ZNAKY KYBERŠIKANY

Anonymita útočníků Útočníci většinou vystupují ve virtuálním prostředí pod přezdívkou (nickem), používají pro oběť neznámou e-mailovou adresu, telefonní číslo atd., proto oběť jen zřídka přijde na to, kdo na ni útočí. Anonymita může být často zdánlivá, protože totožnost útočníků lze s využitím vhodné technologie odhalit.

Kde a kdy se s kyberšikanou setkáme Zatímco u tradiční šikany lze předpokládat, kdy a kde k útoku dojde (např. ve škole, na hřišti), s kyberšikanou se můžeme setkat kdykoliv a kdekoliv. Obětí kyberšikany se můžeme stát vždy, když budeme připojeni k internetu nebo když budeme mít u sebe svůj mobilní telefon. V takovém případě se před kyberútokem nemáme kam schovat. Útočník si nás může najít i v „bezpečí domova" a klidně to může být i o půlnoci.

Kdo jsou útočníci a oběti Ve virtuálním světě nezáleží na věku, pohlaví, síle, postavení v sociální skupině (partě) ani úspěšnosti útočníka nebo oběti ve společnosti. Původcem kyberšikany může být každý, kdo má potřebné znalosti informačních a komunikačních technologií, tedy i fyzicky slabý jedinec. Původce kyberšikany bývá někdy také sám její obětí. Obětí kyberútoku se často stávají děti, které tráví více času ve virtuálním světě a jsou na internetu nebo mobilním telefonu závislé. Na internetu také navazují vztahy, zatímco ve skutečném světě nemají příliš mnoho kamarádů.

Jak se chovají lidé ve virtuálním prostředí Ve virtuálním prostředí se lidé chovají jinak než v reálném světě. Mohou udávat jiný věk, jiné pohlaví, jiné povolání, a záměrně tak manipulovat s těmi, se kterými komunikují. Ve virtuálním světě se někteří lidé chovají méně opatrně než v reálném světě (jsou odvážnější v komunikaci, probírají citlivá témata, komunikují často bez zábran apod.). Někdy zkoušejí to, co by se v reálném světě báli udělat (např. útočit na jiné osoby, vyhrožovat jim nebo je vydírat), protože je menší šance na jejich odhalení, a nevidí, jaký dopad má jejich chování na oběti.

Při šíření kyberšikany pomáhá útočníkovi publikum Prostředky kyberšikany (zprávy a pořízené záznamy) se dají jednoduše rozesílat dál, proto může mít kyberšikana velmi početné „publikum". Útočník nemusí oběť napadat opakovaně, stačí, když citlivé zprávy nebo nahrávky publikuje na internetu a o jejich šíření se pak postarají jiní. Toto publikum zvyšuje intenzitu útoku, a tím zhoršuje jeho dopad na oběť.

Oběť kyberšikany není snadné rozpoznat Kyberšikana je většinou spojená s psychickým týráním obětí, které není snadné poznat (na rozdíl od modřin, jež mohou doprovázet fyzickou šikanu). Oběti kyberšikany jsou často uzavřené do sebe a nekomunikují o problémech s okolím (rodiči). Důvodů pro takové chování může být více (strach, stud, rodiče nerozumí počítačům, dítě nepozná, že jde o projevy psychického šikanování apod.).

Kyberšikana může být způsobena i neúmyslně Kyberšikana může být výsledkem toho, že špatně odhadneme situaci nebo reakci daného člověka (náš žert může způsobit bolest).

PROSTŘEDKY KYBERŠIKANY

Mobilní telefony Mobilní telefon je nejčastějším prostředkem šikanování. Většina školních dětí disponuje vlastním telefonem a ten je první zbraní po ruce. Mobilní telefon bývá zneužíván k zasílání výhružných a urážlivých SMS, opakovanému prozvánění, nepříjemným hovorům, fotografování a natáčení dehonestujících videí. Agresivní zprávy často přicházejí z neznámých telefonních čísel. U rozvinutějších šikan může dojít až k „zavalení" oběti zprávami a telefonáty z mnoha čísel. Zneužíván bývá i telefon oběti. Bývá uváděn jako kontakt v nejrůznějších falešných inzerátech, oběť je pak bombardována nechtěnými dotazy a kontakty (jako např. poskytovatel erotických služeb, výhodného prodeje, zájemce o seznámení).

Sociální sítě Mezi dospívajícími stále oblíbenější sociální sítě jsou ideálním místem pro nenápadnou i zcela otevřenou kyberšikanu: zveřejňování fotografií a vide bez vědomí oběti, jízlivé komentování profilu oběti a posílání nadávek, vytěsňování ze skupiny vrstevníků pomluvami a urážkami. Ke kyberšikaně může být také zneužit falešný profil oběti, vytvořený někým jiným, kde se oběť projevuje a vyjadřuje společensky nepřijatelným způsobem.

Videoportály Nejrůznější ponižující videa obvykle spatří světlo světa na některém z portálů pro sdílení videí, nejčastěji na YouTube, kde je oběť kyberšikany zachycená na videu vystavena veřejnému posměchu. Když se oběť o takovém videu dozví, má možnost požadovat jeho smazání, a to u autora videa nebo se může obrátit přímo na YouTube. Požádat o pomoc s odstraněním takového materiálu

může rovněž na Horké lince, intervenčním centru pro boj se škodlivým či nezákonným obsahem na internetu, www.horkalinka.cz.

Emaily a chaty Posílání výhružných emailů a zpráv, nevyžádaných obrázků (např. pornografických), spamování, krádež hesla k emailu a jeho následné zneužití – tak je možné zneužít email nebo chat k šikanování. Emailová komunikace obvykle probíhá mezi dvěma lidmi a kyberšikana tak je zcela soukromá. Chaty umožňují komunikaci i skupiny lidí, před kterou může agresor oběť ponižovat, urážet nebo ji vytěsňovat ze skupiny diskutujících.

Webové stránky Webovou stránku může vytvořit kdokoliv, tedy i člověk, který chce stránku zneužít k útoku na někoho jiného. Veřejnosti tak zpřístupní např. stránku s ponižujícími fotkami a videi oběti, doplní je o pikantní komentáře a dá prostor i ostatním uživatelům, aby se k materiálům dle libosti vyjádřili.

PROJEVY KYBERŠIKANY S PŘÍKLADY

Kyberšikana se může projevovat různým způsobem. Kyberútoky mohou být realizovány dlouhodobě i krátkodobě, s rozdílnou intenzitou a s využitím velkého množství nástrojů. Útočník při napadání ostatních velmi často kombinuje více typů útoků.

Fyzické napadení oběti spojené s natáčením videozáznamu U uvedeného typu útoku dojde k fyzickému násilí na oběti, které si původci kyberšikany pro své pobavení zaznamenají pomocí mobilního telefonu a nahrávku dále šíří (např. prostřednictvím serveru YouTube, pomocí MMS zpráv apod.). Jde tedy o spojení kyberšikany s tradiční šikanou. Toto jednání patří mezi nejtypičtější formy kyberšikany. Variantu tohoto jevu představuje nečekané fyzické napadení osob spojené s nahráváním na mobilní telefon nebo kameru. Jedná se o tzv. happy slapping. Útočník se baví reakcí oběti (překvapení, strach, údiv, zděšení). Získané video poté publikuje na internetu. Happy slapping může končit i smrtí oběti.

Dvojice mladíků si vyhlédla hocha čekajícího na autobusové zastávce. Jeden z nich k němu přiběhl a „vrazil" mu facku. Druhý mladík celou situaci, včetně překvapené reakce hocha, nahrával na svůj mobilní telefon. Nahrávku poté zveřejnili na stránkách YouTube.

Pomlouvání s využitím internetu a mobilních telefonů Útočník se snaží poškodit pověst oběti a narušit její vztahy s přáteli/rodiči tím, že o ní zveřejňuje nepravdivé informace (pomluvy).

Robert vytvořil internetové stránky s názvem „Nesnášíme Tomáše Černého". Na stránky umisťoval jeho karikatury, pomluvy, výmysly a vtipy o Tomášovi. Na existenci stránek upozornil většinu svých kamarádů.

Vyvedení oběti z rovnováhy spojené s natáčením videozáznamu. Útočník se snaží vyprovokovat oběť k reakci, kterou pak nahraje. Nahrávku může zneužít např. k vydírání oběti nebo ji pro pobavení sebe a svého okolí může umístit na internet. Oběťmi podobných útoků jsou často učitelé.

Dva žáci 9. třídy Marek a Libor se snažili během hodiny vyprovokovat učitelku češtiny Marii K. (pokřikovali na ni, narušovali hodinu, nadávali jí apod.). Když učitelka situaci nezvládla, tajně ji natočili mobilním telefonem a záznam umístili na YouTube. Nahrávku zhlédlo přes 70 tis. uživatelů. Učitelka se o její existenci dozvěděla, až když se na ni přišli zeptat rozčílení rodiče.

Odhalování cizích tajemství Útočník zná intimní či ztrapňující informace o oběti (intimní fotografie, důvěrné informace apod.), které může zveřejnit prostřednictvím internetu nebo mobilního telefonu. Odhalování může být spojeno s vydíráním oběti. Útočník také může svou oběť zmanipulovat, pod záminkou z ní vylákat její tajemství a ta potom zveřejnit.

Jana a Honza se spolu rozešli. V době, kdy spolu chodili, poslala Jana Honzovi na mobil svou intimní fotografii. Po rozchodu se Honza chtěl Janě pomstít, a proto zveřejnil její intimní fotografii na internetu.

Provokování a napadání uživatelů v diskusních fórech Jedná se o tzv. flaming a trolling. Jsou to online útoky pomocí elektronických zpráv s urážlivým a vulgárním obsahem, které mají za úkol oběť provokovat a vtáhnout ji do podobného způsobu komunikace, nebo ji z komunikace vyštvat. Někteří uživatelé (trollové) také tzv. „tapetují" diskusní fóra (donekonečna vkládají do diskuze stejný text).

Petr se nudil a brouzdal internetem, až narazil na diskuzi zaměřenou na počítačové hry. Pro pobavení začal do diskusního fóra psát urážlivé zprávy o ostatních diskutujících, popichoval je proti sobě, útočil na ně. Nezajímalo ho téma diskuze, chtěl se jen pobavit na úkor ostatních, proto zaplavil diskusní fórum nesmysly a nadávkami.

Vydírání s pomocí informačních a komunikačních technologií Útočník využívá mobilní telefon nebo počítač s připojením k internetu k vydírání oběti, čímž se snaží dosáhnout svých záměrů (např. v rámci SMS, diskusních fór, chatu, pomocí e-mailu).

Zbyněk chodil s Katkou. Danovi se ale Katka také líbila, a tak začal Zbyňkovi posílat výhružné SMSky a e-maily. Hrozil, že pokud se s Katkou nerozejde, vyřídí si to s ním ručně.

Obtěžování a pronásledování oběti spojené s kyberšikanou Jedná se o tzv. kyberstalking. Kyberstalking spojuje více praktik kyberšikany, jako jsou intenzívní obtěžování (volání, prozvánění, psaní zpráv) a ponižování, vyhrožování nebo zastrašování oběti. Může vést i k fyzické šikaně a v krajních případech může být zakončeno i smrtí oběti. Útočník se chová jako lovec a oběť je pro něj kořist.

Gábina chodila s Petrem. Když se s ním rozešla, Petr se s rozchodem nemohl smířit a začal ji doslova bombardovat různými zprávami. Prosil, ať se k němu vrátí, vyhrožoval jí, urážel ji, pomlouval před jejími známými, vyhrožoval, že sobě i jí fyzicky ublíží, obtěžoval i její rodiče a známé. Často také Gábině telefonoval.

Krádež identity, zneužití cizí identity ke kyberšikaně Útočník získá přístup k cizímu účtu (e-mailu, chatu apod.). Pod cizím jménem rozesílá nevhodné zprávy nebo jiné materiály. Snaží se tím dostat majitele účtu do problémů, ohrozit ho nebo poškodit jeho pověst a vztahy. Útočník může také manipulovat s účtem uživatele (mazat zprávy, měnit osobní informace o majiteli účtu, mazat a měnit kontakty, fotografii majitele účtu apod.). Informace, které z účtu získá, se může snažit dále zneužít.

Tereza tajně pozorovala Kláru, když se přihlašovala ke svému e-mailovému účtu. Viděla její heslo. Pak se přihlásila na Klářin účet a začala z něj posílat hrubé zprávy jejím známým. Kláře pak dalo velkou práci vysvětlit známým, že zprávy nepsala ona.

Sexting Slovo sexting je složeninou slov sex a textování. Sexting je elektronické rozesílání textových zpráv, fotografií nebo videa se sexuálním obsahem. Tyto záznamy poté mohou být zveřejněny na internetu, zejména dojde-li k ukončení vztahu mezi dotyčnými osobami. Mohou být také použity k vydírání apod.

Doporučení pro komunikaci s dětmi

- ➔ Mezi dospělým a dítětem či náctiletým na internetu je jeden zásadní rozdíl. Dítě má zpravidla technické znalosti, dospělý životní zkušenosti. Dítě se neostýchá používat moderní technologie, ale zároveň se velmi snadno může stát oběti podvodníků – třeba dospělých, kteří se vydávají za vrstevníky apod. Naopak dospělý často nemá tak hluboké technické znalosti, ale díky nabytým životním zkušenostem (nejen v počítačovém světě) je přece jen ostražitější.
- ➔ Problémy se snažte řešit společně, každý pohled (znalost vs. zkušenost) vzájemně obohacuje.
- ➔ Jděte při používaní počítačů příkladem – dítě dobře pozná, kdy něco myslíte vážně a kdy „kážete vodu, ale pijete víno".
- ➔ Počítač mějte ve společných prostorách (chodba, obývací pokoj…), nikoliv v dětském pokoji.
- ➔ Stanovte pravidla pro používání počítačů a internetu.
- ➔ Proberte s dětmi modelové situace.

Co dělat, když se „něco“ děje

- ➔ Drtivé většině problémů ve vazbě „děti a informační bezpečnost“ se dalo dopředu zabránit. Stačilo mít oči i uši otevřené a byt ostražitý vůči některým „varovným příznakům“.
- ➔ Dítě se začne chovat „jinak“ (= divně). Co dříve bez problémů akceptovalo nebo vyhledávalo (např. vaši pomoc u počítače) je mu najednou na obtíž a je to nežádoucí.
- ➔ Dítě v určeném čase náhlé bez zjevné příčiny MUSI byt u počítače.
- ➔ Dítě začne používat neobvykle programy a odmítá vás seznámit s jejich účelem.
- ➔ Dítě za sebou znenadání začne „zametat stopy“ a mazat třeba historii navštívených www stránek, má evidentně důvod nebo potřebu něco skrývat.
- ➔ Dítě se zdráhá povídat si o tom, co na počítači děla a s kým komunikuje. Na počítači chce najednou trávit veškery volny čas.

Pamatujte si Internet nejsou jen domácí počítače. Zákazy nic neřeší, protože dítě se k internetu dostane u kamaráda, ve škole, v knihovně, v mobilu…

Jak se chránit?

- ➔ Vždy respektujte ostatní uživatele.
- ➔ Dobře si rozmyslete, co odesíláte a komu.
- ➔ Nakládejte se svým heslem jako s vlastním životem.
- ➔ Nikdy nikomu neznámému nesdělujte své osobní údaje (vystupujte pod obecnou přezdívkou, nikde neuvádějte své jméno a příjmení, adresu atd.), podle nichž by vás mohl útočník vystopovat.
- ➔ Nikomu nedávejte své fotografie nebo fotografie své rodiny.
- ➔ Seznamte se s pravidly dané služby, ať víte, co je zakázáno.

Desatero bezpečného internetu

1. Nedávej nikomu adresu ani telefon. Nevíš, kdo se skrývá za monitorem.
2. Neposílej nikomu, koho neznáš, svou fotografii i a už vůbec ne intimní (ostatně, tu neposílej ani tomu, koho znáš – nikdy už ji nevezmeš zpět).
3. Udržuj hesla k e-mailu i jinam v tajnosti, nesděluj je ani blízkému kamarádovi.
4. Nikdy jakkoliv nereaguj na neslušné, hrubé nebo vulgární e-maily a vzkazy.
5. Nedomlouvej si schůzku na internetu. Pokud už je to nutné, informuj dospělou osobu a setkávej se jen na frekventovaném místě.
6. Pokud narazíš na obrázek, video nebo e-mail, který tě šokuje, opusť webovou stránku.
7. Svěř se dospělému, pokud tě někdo nebo něco uvede do rozpaků nebo vyděsí.
8. Nedej šanci virům. Neotvírej přílohu zprávy, u které si nejsi jistý původem – raději si u odesílatele ověř, zdali ji opravdu poslal
9. Nevěř každé informaci, kterou na internetu získáš.
10. Když s někým nechceš komunikovat, nekomunikuj. Máš na to právo.

Kam se obrátit v případě problémů?

- ➔ **Nevhodný marketing** Rada pro reklamu sleduje etické principy marketingu a provádí regulaci marketingu. Nevhodný marketing, nepoctivé podmínky a další problémy můžete oznámit Radě pro reklamu. www.rpr.cz
- ➔ **Podvody, stránky hlásající nenávist a další nezákonné činnosti** Podvodné stránky, stránky hlásající nenávist, pokusy o podvod pomoci e-mailu nebo jiné nezákonné činnosti můžete hlásit Policii ČR. www.policie.cz
- ➔ **Zneužití osobních údajů** Úřad pro ochranu osobních údajů poskytuje rady a dohlíží na zpracovávání osobních údajů. Elektronická adresa podatelny: posta@uoou.cz
- ➔ **Dětská pornografie** Nadace Internet Watch Foundation provozuje on-line službu pro hlášení webů, u kterých existuje podezření na to, že obsahují materiály se zneužívaným děti a jiné nezákonné materiály (www.iwf.org.uk). Obdobně lze využít web: www.virtualglobaltaskforce.com či lze v závažnějších případech problém nahlásit přímo na Policii ČR.
- ➔ **Jiný urážlivý nebo nevhodný materiál** V ostatních případech se obraťte na vlastního poskytovatele internetových služeb nebo správce příslušného webu.
- ➔ **Nedostatky internetových obchodů** Internetové obchody musí řádně plnit informační povinnosti, zejména musí mít uveřejněny obchodní podmínky a konečně ceny zboží. Nedostatky můžete nahlásit České obchodní inspekci. www.coi.cz
- ➔ **Phishing** Podvodné pokusy o získání přístupových dat k vašemu účtu ohlaste Policii ČR a vaší bance.

Kde dále lze hledat pomoc?

- ➔ **Linka bezpečí** Rodičovská linka poskytuje telefonickou krizovou intervenci a poradenství především rodičům, prarodičům a ostatním členům rodiny z cele České republiky. Nabízí jim pomoc v krizové situaci, která se tyká děti, dospívajících a mladých dospělých. www.linkabezpeci.cz
- ➔ **E-bezpečí** www.e-bezpeci.cz
- ➔ **Seznam se bezpečně** www.seznamsebezpecne.cz

PRAKTICKÁ ČÁST

KYBERŠIKANA JAKO NOVÁ HROZBA PRO DEMOKRACII

HRY NA ROZEHŘÁTÍ

ČLOVĚK K ČLOVĚKU

Rozdělíme se do dvojic. Pedagog dává instrukce v podobě jednotlivých částí těla, které musí partneři ve dvojici propojit. Například „hlava k hlavě" – partneři ve dvojici spojí hlavy k sobě, nebo „chodidlo k lokti" - chodidlo jednoho z dvojice se musí dotknout lokte druhého (a současně naopak, pokud je to možné). Hráči nesmí toto spojení přerušit až do okamžiku, kdy dostanou nové instrukce. Účastníci mohou kontakt vymyslet jakýmkoliv způsobem. Mohou u toho sedět, ležet, stát. Po čtyřech až pěti různých instrukcích, kdy děti došly až na hranice svých možností, pedagog zadá novou instrukci „člověk k člověku". Dvojice se rozdělí a každý si najde nového partnera a začíná nová hra. Instrukce také mohou dávat samotní účastníci.

Masáž pomocí zad Dvojice se postaví k sobě zády a vzájemně se pomocí zad masírují, jako když se kůň snaží podrbat
o strom.

Přilepeni v bahně Dva z hráčů honí ostatní. V okamžiku, kdy někoho chytí, zůstanou stát rozkročení na místě. Mohou být vysvobozeni pouze v případě, že někdo další podleze mezi jejich nohama. Hra končí buď vyčerpáním účastníků, nebo tehdy, kdy jsou všichni hráči přilepeni v bahně.

NASTARTOVÁNÍ TÉMATU KYBERŠIKANY

JÁ A MÉ TECHNOLOGIE - PAVOUK

Instrukce Při této aktivitě si děti uvědomí, s jakými technologiemi nejvíce pracují a s kým přes ně nejvíce komunikují. Budeme potřebovat papíry A3, kreslicí a psací potřeby. Poté, co dětem představíme základní online technologie, zadáme dětem úkol, aby nakreslily, jaké technologie nejvíce využívají oni. Ke každému obrázku napíší, jakým způsobem přes tuto technologii komunikují. Například u kresby počítače bude napsáno mail, chat, hovor na skypu, apod. Vedle těchto obrázků děti napíšou, s kým nejvíce prostřednictvím těchto technologií komunikují. (Rodiče, sourozenci, kamarádi, příbuzní, apod.)

Následuje vzájemná prezentace pavouků. Při tom diskutujeme s dětmi o tom, jak ovlivňují tyto technologie náš život a jak jej mohou ohrožovat.

ČTYŘI ROHY

Instrukce Toto cvičení se dá použít (podobně jako Ano, ne, možná či Horké křeslo) pro naladění se na jakékoliv téma. Věnujte ale velkou pozornost výběru otázek. Učitel vysloví tři otázky/postoje. Každý z postojů má svůj roh, do kterého se přesunou ti žáci, kteří s ním souhlasí. Čtvrtý roh zůstává otevřený pro všechny ostatní názory.

Vytvořené skupinky pak mezi sebou diskutují. Pokud je v některém rohu skupina příliš početná, můžeme je rozdělit na menší skupinky a naopak pokud je v některém z rohů někdo osamocen, dáme jej do diskuse se zastánci jiného „rohu“. Příklady otázek:

Kyberšikanu:

- ➔ Znám jen jako teoretický pojem. Nikdy jsem ji nezažil ani neznám nikoho, koho by se mohla týkat.
- ➔ Znám dobře několik konkrétních příkladů kyberšikany ze svého okolí.
- ➔ Vůbec nerozumím pojmu a nevím, co to je.
- ➔ Jiná odpověď

Ten, kdo šikanuje ostatní, to dělá nejčastěji protože:

- ➔ má strach, aby sám nebyl šikanován.
- ➔ ho to prostě baví.
- ➔ protože to od něj okolí očekává.
- ➔ z jiného důvodu.

V případě, že bych byl/a svědkem kyberšikany:

- ➔ Okamžitě bych to řekl někomu dospělému
- ➔ Neřekl bych to nikomu, měl bych strach, že budu sám obětí
- ➔ Zkusil bych si s tím, na koho je šikana namířená promluvit a pomoct mu.
- ➔ Jiné řešení.

O kyberšikaně si myslím:

- ➔ Že je mnohem závažnější než klasické šikanování ve škole.
- ➔ Kyberšikana, může být do jisté míry zábavná, ale nesmí se překročit určitá mez.
- ➔ Oběti kyberšikany může být jen někdo, kdo je hloupí. Je přece snadné se bránit
- ➔ Jiná odpověď

Během tohoto cvičení se snažíme rozproudit se žáky debatu o tématu kyberšikany. Ptáme se dětí, z jakého důvodu si vybrali ten který roh. Opět jde o velmi citlivé téma, takže dáváme pozor, abychom nenutili odpovídat děti, které se nechtějí vyjadřovat. V případě, že by nechtěl mluvit nikdo, zkuste příklad, který znáte a ptejte se dětí, jak se asi účastníci vybrané situace cítí a jaká je jejich motivace k takovému chování.

TVOŘÍME PŘÍBĚH

Rozdělíme účastníky na menší skupinky asi po šesti až deseti dětech. S přihlédnutím k jejich věku a zkušenostem s divadlem fórum jim zadáme úkol: Vymyslete situaci, ve které je váš vrstevník obětí kyberšikany. Tuto situaci vyjádřete sousoším. Situace může být inspirovaná předešlým cvičením. Pokud je skupina nezkušená, pracujeme s dětmi společně a pomáháme jim příběh vytvořit. V okamžiku, kdy jsou sousoší hotová, prezentujeme je před zbytkem skupiny. Postupně k sousoší přidáváme věty, které postavy mohou říkat, dále přidáme pohyb. Diskutujeme s diváky, zda je sousoší srozumitelné a situace čitelná.

Příběh můžete také použít jako základ pro strukturování dramatické práce s dětmi. Více tipů, jak dále v práci s dětmi postupovat najdete v metodikách zaměřených na divadlo fórum a na strukturované drama.

SEZNAM DOPORUČENÉ LITERATURY

1. KOPECKÝ K., E – bezpečí, II. Sestava - brožurka
2. ROUBAL, P., Informatika a výpočetní technika pro střední školy – teoretická učebnice, Computer Press, a.s., BRNO 2011. ISBN 978-80-251-3228-9
3. KALHOUS, Z., OBST, O.: Školní didaktika, UP PdF, OLOMOUC 2011. ISBN 80-7067-920-4
4. PRŮCHA, J.: Učitel – současné poznatky o profesi, Portál, s.r.o., PRAHA 2002. ISBN 80-7178-621-7
5. PETTY, G.: Moderní vyučování, Portál, s.r.o., PRAHA 2002. ISBN 80-7178-681-0
6. PASCH, M., GARDNER, T. G., LANGEROVÁ, G. M., STARKOVÁ, A. J., MOODYOVÁ, CH. D.: Od vzdělávacího programu k vyučovací hodině, Portál, s.r.o., PRAHA 2005. ISBN 80-7367-054-2
7. BELZ, H., SIEGRIST, M.: Klíčové kompetence a jejich rozvíjení, Portál, s.r.o., PRAHA 2001. ISBN 80-7178-479-6
8. VÁGNEROVÁ, M.: Školní poradenská psychologie pro pedagogy, KAROLINUM, PRAHA 2005. ISBN 80-246-1074-4
9. JURÁŠKOVÁ, J.: Základy pedagogiky nadaných, Institut pedagogicko-psychologického poradenství ČR. ISBN 80-86856-19-4
10. ZELINKOVÁ, O.: Poruchy učení, Portál, s.r.o., PRAHA 2003. ISBN 80-7178-800-7
11. HRABAL, V., PAVELKOVÁ, I.: Jaký jsem učitel, Portál, s.r.o., PRAHA 2010. ISBN 978-80-7367-755-8
12. TYŠER, J.: Školní metodik prevence – soubor materiálů, Nakladatelství Hněvín, MOST 2006. ISBN 80-86654-17-6
13. BOAL, AGUSTO. Games for actor and non-actors. London, New York, Routledge. ISBN 0-203-99481-7 Master e-book ISBN