Projekt prevence kriminality „Kraje pro bezpečný internet – Videospoty pro klienty NZDM“

Metodika k videospotům

PhDr. Mgr. Eva Burdová, MBA PhDr. Mgr. Jan Traxler

Autoři metodiky: PhDr. Mgr. Eva Burdová, MBA a PhDr. Mgr. Jan Traxler
Název: Projekt prevence kriminality „Kraje pro bezpečný internet – Videospoty pro klienty NZDM“- Metodika k videospotům
Autorka scénářů: Mgr. Nina Moravcová
Vydavatel: Vzdělávací institut Středočeského kraje
Kontaktní osoba: Mgr. Jiří Holý
e-mail: holy@visk.cz
počet stran: 55
Pořadí vydání: 1.
Měsíc a rok vydání: listopad 2017
ISBN:

OBSAH

Úvod

Vážení kolegové,

předkládáme Vám metodiku, která vznikla v rámci projektu prevence kriminality „Kraje pro bezpečný internet – Videospoty pro klienty NZDM“.

Cílovou skupinou jednotlivých videospotů je riziková skupina dětí ve věku 10 až 15 let, klienti NZDM, nicméně videospoty s odbornými komentáři může shlédnout jakákoli cílová skupina, pokud jí to bude adekvátně předáno a doplněno kvalitním výkladem uzpůsobeným věkovým a jiným zvláštnostem.

Cíle daného projektu jsou nastaveny takto:

- snižovat míru a závažnost kybernetické kriminality a elektronického násilí
- snižovat rizikové faktory vedoucí k rozvoji elektronického násilí a kybernetické kriminality, kterou je ohrožena tato cílová skupina
- zvýšit digitální gramotnost a povědomí o bezpečném a etickém užívání informačních technologií, mobilních zařízení a internetu u veřejnosti, zejména u uživatelů ve věku 10 až 15 let

Rádi bychom Vám touto metodikou zjednodušili práci s videospoty a pomohli s aplikací dané problematiky do praxe.

Metodická příručka k deseti videospotům si klade za úkol vysvětlit sociálním pracovníkům a dalším odpovědným osobám, které pracují s dětmi v nízkoprahových zařízeních pro děti a mládež, záměry a cíle videospotů.

Zároveň bychom chtěli, aby tato metodika pomohla sociálním pracovníkům a další odpovědným osobám pracujícím s dětmi v orientaci v dílčích tématech. Současně nabízíme rozšíření informací přímo na podrobných scénářích videí.

U sociálních pracovníků a dalších odpovědných osob pracujících s dětmi se však počítá i s kreativitou, schopnostmi přizpůsobit se dané cílové skupině a v neposlední řadě i se základními dovednostmi a znalostmi z oblasti virtuálních technologií a kyberprostoru.

Metodikou bychom rádi chtěli všem pracovníkům NZDM podat pomocnou ruku tam, kde mohou tápat, když klienti hovoří o počítačovém světě. Dále chceme nabídnout, jako vodítko po cestách v kyberprostoru, využití našich textů a postřehů či rad.

Metodická příručka obsahově odpovídá jednotlivým tematicky zaměřeným videospotům.

V rámci každé kapitoly naleznete následující sekce:

- ✓ Cíl tématu:
- ✓ Odborné ukotvení:
- ✓ Na co si dát pozor:
- ✓ Slovníček pojmů

Přejeme vám příjemně strávený čas v diskusích s klienty nad videospoty, metodickými doporučeními a předem připravenými pracovními listy, které budete moci okamžitě použít.

Eva a Honza

Didaktické pojetí přenosu informace

Didaktika je „… všeobecné umění, jak učiti všecky všemu.“

Komenský 1657

Pokud chceme děti zaujmout a chceme, aby si z odvysílaných videospotů odnesly nějakou dovednost pro život, je třeba abychom dodrželi základní didaktické postupy a aby se nejednalo jen o rychlé shlédnutí filmu, ale o opravdu smysluplnou aktivitu, která by napomohla ke zvýšení digitální gramotnosti a povědomí o bezpečném a etickém užívání informačních technologií, mobilních zařízení a internetu a to hlavně u dané cílové skupiny dětí ve věku ve věku 10 až 15 let.

Při jakémkoli předávání informací, které je komplexním vyučovacím počinem, bychom se měli zamyslet nad několika základními body.

Tyto body celkově ovlivňují schopnost jedince cílové skupiny informace dále nejen vstřebávat, ale i efektivně dokázat využívat:

Prvním specifickým bodem, o kterém musíme uvažovat, je **cíl** našeho konání – tedy proč se tím má daný jedinec zabývat.

Dále bychom měli přemýšlet o **kompetencích**, tedy hlavně jaké znalosti, vědomosti, dovednosti a návyky chceme v daném tématu cílové skupině předávat.

Obsahová náplň daného tématu je dána obsahem videospotu, s kterým by se měl dopředu každý sociální pracovník, či osoba odborně způsobilá, jež bude s dětmi na tématu pracovat, nejdříve dokonale seznámit a nastudovat k tématu i odborný text.

Při předávání odborných informací dětem z cílové skupiny bychom neměli zapomenout ani na didaktické zásady, které jsou součástí každého efektivního přenosu informací směrem k cílové skupině. Je to vlastně takové shrnutí, na co bychom neměli zapomenout, co bychom neměli opomenout.

Výběr z didaktických zásad

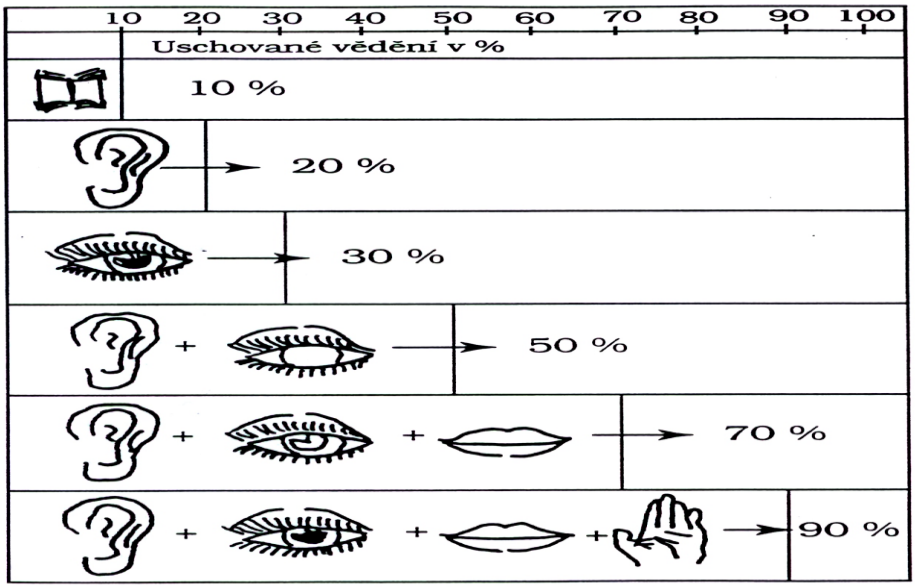
1/ Zásada **KOMPLEXNOSTI –** cílem je komplexní rozvoj osobností dětí, ke kterým budeme hovořit a kterým budeme pouštět videospoty. Komunikujeme s nimi a snažíme se o rozvíjení a včlenění problematiky do všech oblastí života dětí.

2/ Zásada **VĚDECKOSTI –** dětem máme říkat jen to, co odpovídá současným vědeckým poznatkům a ne všechno, co by nás napadlo, či co je zažité a tradované. Musíme to mít opravdu ověřené.

3/ Zásada **INDIVIDUÁLNÍHO PŘÍSTUPU –** myslete zvlášť na každé dítě, které je na Vaší přednášce, kde pouštíte videospoty. Děti k Vám chodí pravidelně, zkuste se u každého zaměřit na jeho individuální zvláštnosti a potřeby.

4/ Zásada **SPOJENÍ TEORIE A PRAXE** - snaha, aby teoretické znalosti byly spojeny s praktickou činností, aby učení mělo nějaký praktický důsledek pro život.

5/ Zásada **NÁZORNOSTI –** člověk je nastaven především na zrakové vjemy, k tomu slouží i natočené video. Ovšem myslete i na vysvětlování a diskusi. Celkové zapojení dětí je důležité, více si odnesou. K bližšímu pochopení Vám může sloužit následující obrázek.[1]



[2]

[1] Burdová, E.: *Základní orientace ve struktuře vzděl. programů, didaktické a výchovné činnosti*
[2] Obst, O.: *Obecná didaktika*

6/ Zásada **PŘIMĚŘENOSTI** – přemýšlejte také o tom, koho máte před sebou. Je důležité vědět, jaká věková skupina a jaké děti zrovna přišly. Nemusíme přeci říci úplně všechno. Vždy je potřeba zodpovědět otázky.
7/ Zásada **TRVALOSTI A OPERATIVNOSTI** – aby dětem v hlavě něco zůstalo, je třeba se k tomu občas vrátit. To už nemusí být nad videospotem, ale je dobré si o daných tématech občas popovídat naprosto nenásilně, jen tak. [3]

Nezapomínejte ani na sociální učení, které je u dané cílové skupiny velice důležité. Děti se s Vaší pomocí učí sociálním rolím, vzorcům chování a často jste pro ně autoritou i vzorem. Přebírají Vaše vzorce, tedy i to, jak Vy dokážete pracovat s virtuálními technologiemi a jak se v nich dokážete pohybovat a chovat. Nezapomínejte na to, že toto je často mnohem silnější než jakékoli sdělení.

Před každým pouštěním videospotu si v rychlosti zopakujte pár otázek a hned si na ně odpovězte.

- PROČ se do této aktivity pouštíme?
- KOHO tím oslovíme?
- K ČEMU to má být dobré?
- JAK budeme předávat informace, máme čas na celý videospot a diskusi?
- KDY začneme, až přijde kolik dětí, jak to rozvrhneme?
- ZA JAKÝCH PODMÍNEK to bude? Je dobré mít plán, nastavit i podmínky aktivity- dopředu sdělit, nastavit pravidla pro příchod a odchod apod.
- S JAKÝMI OČEKÁVANÝMI EFEKTY budeme počítat?

[3] Burdová, E.: *Základní orientace ve struktuře vzděl. programů, didaktické a výchovné činnosti*

Příprava před videospotem

CO – které téma vyberu, připravím si předem, přečtu vše k tématu, terminologii, příprava faktů

PROČ – proč zrovna dnes volím toto téma? Souvisí to i s tím, co vlastně chceme, co jsou naše cíle

- stanovení si cílů
    - ✓ Čeho chci dosáhnout?
    - ✓ Jakých konkrétních cílů chci dosáhnout?
    - ✓ Co chci, aby posluchači věděli?
    - ✓ Co chci, aby posluchači udělali?
    - ✓ Jak chci, aby se posluchači cítili?

Základní pravidla komunikace s cílovou skupinou

Připomeňme si, jak být efektivní při práci a komunikaci s danou cílovou skupinou dětí v NZDM. Zde popisujeme několik důležitých pravidel, na které je třeba pamatovat.

- stručnost, jasnost a srozumitelnost
- názornost, přiměřenost
- udržení pozornosti
- komunikativnost, buďte konkrétní a dávejte příklady
- popište chování a jeho vliv

Faktory limitující naší komunikaci v NZDM

Všichni si uvědomujeme, že cílová skupina dětí v NZDM ve věku 10-15 let je z hlediska zaujetí pro přenos informací tou nejsložitější cílovou skupinou, jedná se o děti v období prepuberty a puberty. Toto období lidského života je samo o sobě složité, natož u dané cílové skupiny. Nesmíme zapomenout ani na již vyhrazenou názorovost a je třeba připravit základní podmínky. Nezapomeňme ani na to, že se děti mohou ztotožnit s problematikou videospotu, mohou si připomenout určitou situaci, kterou již zažili v reálném životě.

Může dojít i k tomu, že dítě zareaguje neadekvátním způsobem, např. bude nadšeně vyzdvihovat rizikové chování popisované ve videospotu. Může jít o obrannou reakci dítěte, které se ve videospotu pozná. Nebojme se v této situaci videospot přerušit a začněme diskutovat.

Také může nastat situace, že se dítě pozná v nějakém okamžiku videoprojekce a stáhne se do sebe, či může být smutné. Měli bychom během pouštění videospotu pozorovat reakce všech přítomných dětí a umět na ně reagovat. Předpokládáme, že videospoty s dětmi shlédnou erudovaní sociální pracovníci s dostatečnou praxí s dětmi dané cílové skupiny, a na takovéto situace, s kterými se v NZDM běžně setkávají, dokáží zareagovat.

Velice důležitá je, ze všech těchto důvodů, komplexní příprava před samotným videospotem. Ne nadarmo se říká: „Těžko na cvičišti, lehko na bojišti.“

Co by nás tedy mohlo limitovat, pokud bychom nebyli dokonale připraveni, si před přípravou každého videospotu si doplňte do pracovního listu přípravy:

Pracovní list Příprava před videospotem

- prostorové a časové omezení_____
- vymezení obsahu programu, rozsah_____

  _____
- vymezení pravidel chování_____

  _____

  _____

  _____
- vliv prostorového uspořádání_____

  _____
- vliv asymetrie sociálních rolí_____

  _____
- co vím o dětech, které pravděpodobně přijdou_____

  _____
- možný vliv jazykové bariéry_____

Práce s videospoty

Před každým videospotem je dobré se seznámit s cílem tématu, odborným ukotvením a tím, na co bychom si při práci s cílovou skupinou měli dát pozor. Každý videospot má samostatnou kapitolu věnovanou mu v této metodice a každá kapitola má nastavené členění, o kterém píšeme. V cíli tématu se vždy seznámíme s tím, o čem to bude a co bychom měli dětem předat a proč. Odborné ukotvení pomůže před diskusí získat širší pohled na danou problematiku. Odrážka na co si dát pozor nás může upozornit na možná úskalí při práci s cílovou skupinou. Ovšem nikdy není možné popsat vše, co může nastat. Předpokládáme schopnost daného sociálního pracovníka aktivně reagovat a řešit nastalé situace v celém širším kontextu.

Součástí každé samostatné tématiky je i slovníček základních pojmů z dané oblasti, který nám může pomoci blíže do problematiky proniknout.

Práce s pracovními listy

Ke každé oblasti je připraven pracovní list pro otevření diskuse, zopakování si a ukotvení dané problematiky jednotlivými dětmi. Jsou zde otázky k zamyšlení, ale např. i k vytvoření vlastních hesel, aktivity podněcující zpětnou vazbu a rozvoj hlubšího zamyšlení.

Jednotlivé pracovní listy si můžete volně nakopírovat dle počtu dětí v pracovní skupině.

Dle možností a schopností dětí volte práci jednotlivců nad daným materiálem, případně skupinovou práci, ale nikdy nezapomeňte na zpětnou vazbu a vzájemné sdílení. Vzájemné sdílení by nemělo být vynucené, ale každé dítě by mělo dostat prostor pro sdělení svých zážitků, informací či dotazů i z důvodu možné korekce sociálním pracovníkem. Na reflektivní rozhovor bychom si měli vyhradit dost času a nikdy by neměl být opomenut. Je často důležitější než samotné shlédnutí videospotu.

Vlastní videospoty

Jednotlivá témata

- *Bezpečná hesla*
- *Bezpečné chování online (zákeřný software, útoky na e-maily)*
- *Online nakupování, online platby (výhody a rizika, možnosti platby a rizika)*
- *Sociální sítě 1 (ochrana osobních údajů, rizika používání)*
- *Sociální sítě 2*
- *Mobilní telefony (zabezpečení mobilu, stahování aplikací)*
- *Mobilní telefony (riziko selfie, geolokace, …)*
- *Kybergrooming*
- *Kyberšikana a sexting*
- *PC hry a závislost*

Bezpečná hesla

Cíl tématu: Osvojit si, co je bezpečné heslo. Získat dostatečné a smysluplné informace, abych heslo uměl sám vytvořit a aplikovat všude tam, kde ho budu potřebovat. Uvědomit si důležitost měnění hesel a používání různých hesel u různých aplikací.

Odborné ukotvení:

Pro komunikaci s dětmi je nutné nastavit základní otázky, na které si budou umět odpovědět po zhlédnutí videa. Nad hesly je třeba přemýšlet. Pokud už dítě má několikátý profil na sociální síti či ve hře, případně kdekoli jinde, heslo by nemělo být stejné. Nutné je také dětem vysvětlovat, proč tomu tak má být**.** Kdyby náhodou jedno heslo někomu omylem prozradily, nebo někdo na něj přišel a rozluštil ho, tak ohrozí jen jeden profil nebo hru. Ale kdybychom měli všude stejné heslo, tak by to mohlo být značně problematické. To by ten někdo mohl používat všechny účty a profily daného jedince.

A jak si všechna ta hesla zapamatovat? Vymyslete s dětmi řadu různých pomůcek, které pomáhají. Vždy se pokoušejte společně vymyslet originální a nerozluštitelná hesla. Dobré heslo je dost dlouhé a má v sobě velká i malá písmena, číslice a znaky. A na zapamatování hesla je třeba s dětmi najít nějaký fígl, pomůcku. Někdy je to básnička, někdy jen zkratky oblíbených jídel a tak.

Také je třeba dětem sdělovat, že když se přihlásí do jakékoli aplikace, nesmí se zapomenout odhlásit. Je důležité nejen učit děti vytvářet chytrá hesla, ale naučit je i chytře tato hesla používat.

Pokud to tedy shrneme, podstatné je nemít jen jedno heslo ke všem aplikacím a hrám. Je mnohem lepší mít hesel několik a dobré je také heslo čas od času měnit. Říkejte dětem, že když se přihlašujeme do nějaké aplikace, neměli bychom heslo nikomu ukazovat ani prozrazovat. Kdokoli se pak klidně může přihlašovat i pod jejich jménem a pak třeba i jejich jménem páchat nějaké nepravosti.

Také je nutné hlídat si chytrý telefon a nepouštět na něj každého a nedovolovat všem spolužákům, aby měli přístup k čemukoli v jejich telefonu.

Vysvětlete dětem, že se to někdy stane z neopatrnosti i dospělým. Mohlo se to stát i tím, že se při odchodu z aplikace neodhlásili, nebo se přihlašovali někde z nezabezpečené wifi, nebo na nějakém počítači, který měl nastaveno a zobrazil možnost „zapamatovat si mě.“ Na to všechno je třeba děti upozornit a říci jim, že si musí dávat pozor. Každé dítě musí vědět, že u každé aplikace, kam se přihlašujeme, také vždy existuje tlačítko odhlásit se, na to nikdy nesmíme zapomenout.

Na co si dát pozor: Pozor na to, že děti ve skupině často nahlas sdílejí svá hesla, říkají je před ostatními a neuvědomují si, že mohou být zneužita. Vytahují své telefony, nechávají je bez dozoru apod.

Slovníček pojmů

Gesto: používá se často na mobilním telefonu nebo tabletu – jde o jakési pospojování určitého počtu bodů na displeji.

Heslo: posloupnost znaků (písmen, číslic, nestandardních znaků), která by měla být těžko zjistitelná nebo uhodnutelná, případně odvozená od osoby, která heslo používá. Slouží jako zabezpečení pro přístup k různým systémům nebo datům.

Místo hesla se dnes velmi často používá facebookový profil jedince.

Otisk prstu: dnes velmi oblíbený a rozšířený způsob ověřování se a přihlašování se do mobilního telefonu nebo i do počítače. Jde o sejmutí papilárních kreseb z článku prstu a tím dochází k ověření uživatele.

PIN: nejčastěji 4 místné číslo používající se u platebních karet, telefonů, tabletů a různých přístupových systémů.

Správce hesel: Software – program, kde si uživatel může uložit jednotlivá hesla, která používá. Celý správce hesel je pak zajištěn jedním univerzálním heslem, pod kterým pak uživatel může zjistit veškerá svá uložená hesla.

Šifrování: jde o proces, při kterém jsou nechráněná data převedena jistým tajným klíčem (šifrou) na zakódovaná, a tak téměř nezjistitelná, data. K opětovnému přístupu k těmto datům je bezpodmínečně nutné znát daný klíč – šifru.

Pracovní list Bezpečná hesla

Jak má vypadat bezpečné heslo- co obsahuje?

- _____
- _____
- _____
- _____
- **Jak dlouhé má být heslo? Kolik?_____znaků**

Co znamená heslo slovníkového typu?_____

_____

Jak si heslo nejlépe zapamatuješ?_____

_____

_____

Zde zkus sám vymyslet opravdu kvalitní heslo:

Bezpečné chování online

Cíl tématu: Seznámit děti se základními zásadami internetového bezpečí

Odborné ukotvení:

Na toto téma existuje již mnoho „desater“. Určitě jich spoustu najdete na internetu, hledat můžete i společně s dětmi a pokusit se společně i základní zásady s dětmi vytvářet např. na velké flipové papíry a rozvěsit si je po nízkoprahovém zařízení.

Nabízíme základní zásady pro inspiraci, utříděné a rozšířené:

- ✓ Využívej čas v kybersvětě efektivně a účelně
- ✓ Přemýšlej nad svými činy, abys někomu neublížil.
- ✓ Instaluj jen předem ověřené a známé programy.
- ✓ Neotevírej soubory, které neznáš nebo které Ti přišly v nevyžádané v mailové poště.
- ✓ Používej vhodné a moderní zabezpečení své veškeré IT techniky.
- ✓ Používej šifrování k ukládání dat i ke komunikaci.
- ✓ Měj nainstalované programy, které chrání tvé bezpečí.
- ✓ Nedůvěřuj všem informacím, které na internetu jsou.
- ✓ Nikdy nepřeposílej informace, které nejsou pravdivé.
- ✓ Udržuj svá hesla v naprosté tajnosti a nikdy je nikomu nesděluj.
- ✓ Komunikuj ve virtuálním světě jen s tím, koho znáš a ověříš si.
- ✓ Neboj se nevhodnou komunikaci ukončit a říci jasné NE.
- ✓ Nikdy nikomu nesděluj žádné osobní informace (jméno, příjmení, bydliště, školu, datum narození, rodné číslo, telefonní číslo, heslo, PIN, apod.).
- ✓ Nikdy nikomu neposílej svoji intimní fotografii nebo video.
- ✓ Nepoužívej webovou kameru s neznámou osobou. Tvé záběry si může někdo ukládat a následně je použít.
- ✓ Útočník je vždy o krok napřed před postupným zabezpečováním.

Na co si dát pozor: Pozor na informace o každém dítěti. Zde děti často sdělují, co mají na svých profilech. Jako sociální pracovníci, kterým děti důvěřují, můžeme nastavit korekci, použít např. techniku Life Stories- převyprávění příběhů ze života. Co se někomu stalo, když…..

Slovníček pojmů

Antivirový program: jde o program – software (placený nebo zdarma), který pomáhá chránit počítač, tablet, telefon před nežádoucími programy. Podmínkou funkčnosti je jeho instalace a častá aktualizace. V dnešní době je jeho používání nutností.

Flaming - v překladu hoření
Jde o nepřátelské chování útočníka vůči oběti, které se odehrává ve virtuálním světě. Nejčastěji v diskuzních fórech, chatu, sociálních sítích, ale i v emailu. Útočník urážlivým způsobem napadá oběť tím, že do kyberprostoru umisťuje vzkazy, ve kterých ho hrubým způsobem uráží a zesměšňuje. Své chování útočník postupně stupňuje. Častým motivem je, že útočník nesouhlasí s názory oběti a tu pak uráží a argumentuje svým přesvědčením.

Hacking – nabourávání se do cizího zabezpečeného sytému. Jde o techniku, při které se hacker (osoba hackující) snaží nestandardním způsobem proniknout do cizího nebo i vlastního zabezpečeného systému. Může jít o Váš počítač, Vaši počítačovou síť, WiFi nebo i zabezpečovací systém domu, email apod. Nemusí se vždy jednat o nelegální aktivitu.

Hoax - v překladu jde o poplašnou zprávu, kanadský žertík, vtípek… Jde o šíření emailových zpráv, pomocí internetové sítě, které jsou nepravdivé, poplašné anebo třeba jen řetězové. Ty nejen, že člověka obtěžují, ale mohou v něm vyvolat i pocit strachu, viny anebo příjemce jinak mystifikovat. Nejčastěji se můžete setkat se zprávami, které Vás „varují“ před nebezpečím, např. počítačového viru nebo jiné situace, která Vás může poškodit.

Kybergrooming - manipulace v kyberprostoru. Útočník se snaží v kyberprostoru (chat, ICQ, sociální sítě, SMS…) vytipovat a najít vhodnou osobu, ve které vzbudí postupně důvěru a postupem času ji přinutí k osobní schůzce, kde oběť pak nějakým způsobem zneužije či využije.

Kyberstalking - v překladu jde o pronásledování v kyberprostoru. Jedná se o obtěžování, které se stupňuje, opakuje a odehrává se v kyberprostoru. Má různou intenzitu a liší se i druhy projevu. Využívají se při ní prostředky komunikační techniky (např. Skype, SMS, chat, email, telefon, sociální sítě). Stalker je velmi často znám oběti, může jít o bývalého partnera, milence, kamaráda, zrazeného přítele nebo milovníka. Ten například není ochotný akceptovat ukončení vztahu nebo nezájem oběti, a tak se pokouší oběť v kyberprostoru obtěžovat a donutit ji k reakci či návratu. Toto obtěžování může mít rozličnou podobu od SMSek, emailů, po prozvánění a vyhrožování.

Kyberšikana - v překladu šikana, která se odehrává ve světě informační a telekomunikační techniky. Jde o takové jednání, které má oběť záměrně ohrozit nebo jí ublížit prostřednictvím prostředků informační a telekomunikační techniky. Nejčastěji se setkáte se zneužitím mobilního telefonu a internetu. Podle loňského výzkumu má každé druhé dítě na českém internetu zkušenosti s kyberšikanou.

Pharming - v překladu znamená farmaření. Pharming je obdobnou technikou jako phishing. Jde o způsob změny IP adresy a DNS serveru ze strany útočníka. K tomuto napadení může dojít jak na straně serveru, kam se připojujete, tak i na Vašem počítači. Tato změna Vás pak bez Vašeho vědomí skrytě přesměruje na falešné internetové stránky, které jsou k nerozeznání od původně požadovaných. Díky této skutečnosti například vyplníte přihlašovací údaje a heslo do zabezpečené aplikace a takto vyplněné údaje jsou pak známé útočníkovi, který je může libovolně zneužít. Pharming je svou podstatou nebezpečnější než phishing, protože nevyžaduje od uživatele otevření přílohy e-mailu nebo vědomou instalaci.

Phishing - v překladu rybaření. Jedná se o podvodnou techniku na internetu, která má za cíl od uživatele vylákat jeho přihlašovací údaje a hesla, která můžou být následně útočníkem zneužita. Útočníci rozhazují „návnadu“ a čekají, kdo se „chytne“ – proto rybaření. Nejčastěji se potkáte s phishingem ve Vaší emailové schránce, kde se email tváří jako skutečná a důležitá informace od legitimní společnosti (banka, Váš sociální profil, různé státní instituce nebo dokonce zpráva od IT technika). Otevřením této zprávy budete vyzváni ke spuštění odkazu a následně přesměrováni na podvodnou

stránku, která je identická s oficiální stránkou, kterou imituje. Zde jste pak vyzváni k zadání osobních údajů např. (přihlašovací jméno, heslo, číslo kreditní karty, datum narození apod.). Jejich zadáním a odesláním je vlastně předáváte útočníkovi, který je může následně použít k libovolné činnosti.

Ransomware: je to vyděračský program – software. Pokud je jím počítač či jiné zařízení napadeno, dochází k zašifrování dat pomocí uživateli neznámého šifrovacího klíče. Data jsou pak zcela nečitelná a nedostupná. Tvůrce ransomware následně požaduje „výkupné“ – nejčastěji v bitcoinech, kvůli nedohledatelnosti – za prozrazení šifrovacího klíče, který následně lze použit k rozšifrování dat na počítači.

Sexting - v překladu sextování. Složenina ze slov sex a posílání textů, obrázků a videí. Jde o využívání informačních a komunikačních prostředků k zasílání textů, fotografií a videí se sexuální tématikou. Tyto materiály často končí na internetu a můžou mít pro oběť fatální důsledky, neboť jsou často použity jako donucovací prostředek k vydírání. Některé případy pak končí až smrtí oběti.

Sniffing - v překladu čichání, čmuchání. Jde o odposlech komunikace (dat) mezi dvěma a více počítači navzájem propojených v síti nebo s přístupem na internet. Toto monitorování elektronické komunikace může probíhat jak při klasickém metalickém připojení počítače do sítě (LAN), tak i při bezdrátovém připojení (WiFi). V praxi se tohoto používá například ke zjištění problémů v počítačové síti a nalezení problémového zařízení. Ke zjištění vytíženosti celé soustavy apod. Ale zároveň je možné toto monitorování zneužít.

Spam – je nevyžádaná zpráva, email, SMS zpráva, která se masově šíří pomocí internetu. Rozesíláním spamu může za určitých okolností jedinec překračovat právní rámec.

Pracovní list Bezpečné chování online

Pracujte ve skupině a zkuste vymyslet vlastní desatero bezpečného chování na internetu:

1.

2.

3.

4.

5.

6.

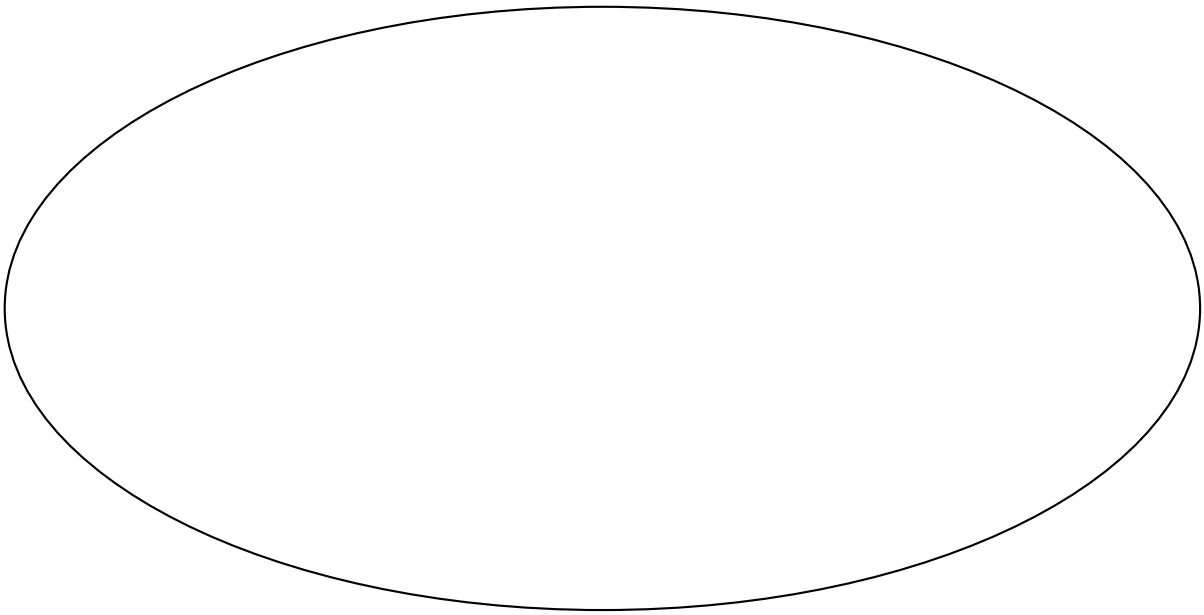
7.

8.

9.

10.

Zkus nakreslit, jak vypadá inteligentní serfař na netu, který se chová správně. Popiš, proč zrovna takto:



Online nakupování, online platby

Cíl tématu: Seznámit děti s riziky nakupování online a s riziky plateb online, hlavně např. při nákupu her apod. Naučit přemýšlet o možných rizicích a věnovat se tomu, na co si dát pozor.

Odborné ukotvení:

Jak nakupovat na e-shopu? Jak si ověřit důvěryhodnost? V dnešní době je moderní, rychlejší a často i levnější nakupovat zboží na internetu. Ale ani tato činnost se nemusí obejít bez problémů a rizik. Je dobré dát si pozor na několik věcí. Pokud jste již nalezli na internetu dané zboží, není vždy nejlepší kupovat jej v obchodě, kde je nejlevnější. Nejlevnější nákup s sebou může přinášet rizika. Také placení zakoupeného zboží předem může být rizikové. A to hlavně v případě, že s daným internetovým obchodem nemáte osobní zkušenost. Nebo alespoň někdo z vašich známých. Může se stát, že si vyberete a zaplatíte zboží, a to Vám pak nedorazí. Někdy se také stává, hlavně u neznámých obchodníků, že objednané zboží pošlou na dobírku, ale v balení se pak nenachází objednaná věc, ale jiná nebo třeba i kus cihly. I zde platí přísloví: „Nejsem tak bohatý, abych si kupoval nejlevnější věci.“ Než nakoupíte u daného obchodníka, doporučujeme si zjistit o daném internetovém obchodě co nejvíce informací. A to od známých, příbuzných nebo na internetových stránkách. Dobrým vodítkem Vám může být certifikace daného obchodu. Podívejte se např. na www.apek.cz, nebo na www.heureka.cz. Dalšími znaky dobrého obchodu by měly být dostupné veškeré údaje o obchodníkovi (název firmy nebo obchodníka, IČ, adresa, telefonní a jiné kontakty…). Dále pak reklamační řád, kompletní a přehledný ceník dopravy. Také pokud obchod používá reálné, vlastní fotografie prodávaného zboží, lze toto považovat za klad. Měli byste také vědět, že pokud nakoupíte zboží přes internet, máte nárok na odstoupení od kupní smlouvy, a to 14 dní. Toto platí v zemích EU. Mimo tyto země tato ochrana neplatí. Také zde často nastává problém v případě reklamace. Při nákupu ze zahraničí je nutné si dobře spočítat výslednou cenu, která se skládá nejenom z ceny zboží, dopravy, ale i případného DPH a cla. Při odstoupení od smlouvy je nutné toto odstoupení učinit písemně, např. e-mailem. Za lepší variantu považujeme doporučený dopis nebo dodejku. Následně nepoužité zboží, ideálně v neporušeném obalu (platí

např. pro CD a DVD), zaslat zpět prodejci. Ten Vám musí do 30 dní vrátit finanční plnění. Za zboží na internetu se dnes většinou platí pomocí platebních karet nebo speciálních aplikací. Zde je nutně znát a uvědomit si všechny výhody a nevýhody. Zvláště pak je nutné veškerá rizika s tím spojená vysvětlit neznalým, nebo málo znalým uživatelům. Naučte se používat elektronické peněženky nebo správně a bezpečně platit pomocí platebních karet a platebních bran. Seznamte se se zabezpečením a s podmínkami využívání těchto služeb.

Na co si dát pozor: Děti této věkové skupiny nakupují převážně hry a komponenty do her. Je třeba diskutovat i o tom, že nic není zadarmo. Vždy přemýšlet o tom, co za to. Měla by existovat kontrola toho, co si dítě na internetu kupuje a za co vydává peníze. Také je potřeba dát si pozor na automatické platby za služby, které dítě již nepoužívá.

Slovníček pojmů

Apek.cz: je to internetová stránka společnosti, která sdružuje podnikatele a firmy, které prodávají své zboží, služby i za pomocí elektronických služeb. Tato asociace podporuje a pomáhá elektronickému obchodování v ČR.

e-shop: je to elektronický obchod. Jde o možnost nabízet zboží, které obchodník má, pomocí webové aplikace na internetu. Je to jeden ze způsobů možného prodeje na internetu.

Elektronická peněženka: Většinou se jedná a speciálně vydávanou platební kartu (obsahuje čip), která je vhodná k placení drobných nákupů nebo placení menších hotovostních plateb. Tuto kartu je však nutné vždy „dobíjet“ – vkládat na ní finanční prostředky. Jde o relativně bezpečné řešení. Při jejím odcizení nebo zneužití hrozí ztráta „jen“ prostředků na kartě uložených.

Heureka.cz: Jde o internetový hodnotící a srovnávající systém. Jednotliví uživatelé,

kteří zakoupili zboží na internetu, získávají možnost podělit se o své kladné, ale i záporné zkušenosti všem dalším uživatelům internetu. Na těchto stránkách má možnost člověk najít informace nejen o daném zboží/produktu, ale také o prodejci nebo prodejně.

PayPal: jde o internetový platební systém, který umožňuje placení na internetu. Účet PayPalu je identifikován pomocí emailové adresy jednotlivých uživatelů. Je možné tento účet propojit i se svojí platební kartou. (Pozor na možnost zneužití při zadání platební karty). Systém PayPal dnes umožňuje platit i v CZK.

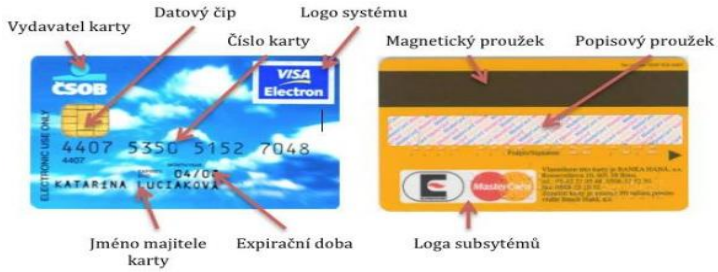
PaySec: Je to internetová aplikace-brána, která umožňuje obchodníkům přijímání okamžité platby od zákazníků při využití jejich bankovních účtů. Zatím nejsou podporovány všechny dostupné bankovní společnosti. Veškeré transakce probíhají v reálném čase.

Pracovní list Online nakupování, online platby

Na co si dát pozor při nákupu on-line?

Namaluj platební kartu z obou stran- označ, co by mělo být uchováno v tajnosti

Pomůcka pro sociální pracovníky, PL kopírovat při zakrytí této části



Sociální sítě

Cíl tématu: Seznámení se sociálními sítěmi, ochranou osobních údajů, riziky používání těchto sítí. Zaměření se na bezpečnost profilu. Tedy, co do profilu napsat a také jak profil zabezpečit.

Odborné ukotvení:

Děti samy vědí, že mnoho her, sociálních sítí i aplikací chce, aby si v nich vytvořily profil. Veďte děti k tomu, aby přemýšlely, zda je to nutné. Zda všichni musí znát jméno a příjmení? Nezapomeňte dětem říci, aby zbytečně nikdy nevyplňovaly to, co není povinné a i u povinných políček přemýšlely. Učte je zvolit si nějaký nick (přezdívku) a pod tou přezdívkou vystupovat. Vysvětlete jim, aby v žádném případě nedávaly svou adresu, nepsaly, kde bydlí, ani jaké mají telefonní číslo. To by opravdu mohlo být nebezpečné. Vysvětlete proč, uveďte příklady. Musí také vědět, aby nesdílely, a to ani na profil, kam chodí, co dělají, kde se pohybují. Většina profilů chce i fotku, dokonce některé aplikace neustále vyzývají, že jste fotku ještě stále nenahráli a po spuštění nejprve spustí výzvu k nahrání profilové fotografie. Profilový obrázek nemusí být za každou cenu fotka. Je lepší, když si dítě a ani dospělý svou vlastní fotku nikam nedává. Když už jedinec trvá na své fotce, měl by ji upravit, nebo být ve stínu, mít vlasy do obličeje, natočený z boku nebo něco podobného. Lepší je ale použít úplně jiný obrázek, fotku vlastního domácího mazlíčka, sportovního náčiní apod. Profilový obrázek by měl být hezký, příjemný a jedinečný. Nepříjemně působí profily, kde na nás koukají lebky, náhrobní kameny, hřbitovy…

Také pozor na autorská práva u obrázků, které dítě nevyfotilo. Určitě upozorněte i na tuto problematiku. Vysvětlete dětem, co to znamená.

Seznamte se také s jednotlivými sociálními sítěmi, či nechte děti, ať Vám je ukážou. Mnohé tak o jejich chování zjistíte. Uvidíte i to, kde se a jak často pohybují. To jsou pro Vás cenné informace. Zároveň je veďte k tomu, aby opravdu podrobně četly smluvní podmínky při zakládání profilu. Sami se seznamte se smluvními podmínkami alespoň facebooku, abyste věděli, o čem s dětmi mluvíte.

Na co si dát pozor: Nevěnujme se jen facebooku, děti mají profily na mnoha jiných sociálních sítích. Nebuďme šokovaní, když sdělují: Face mám proto, aby měla máma co kontrolovat, jinak jsem na Instagramu, Snapchatu, …….. Většinou v tomto věku mají profil na 3 a více sociálních sítích a žijí více on-line než v realitě. Na sociálních sítích sdílejí úplně vše. Fotí si nové oblečení, nové boty, jídlo, co zrovna snědly, naprosto vše a také nebezpečně o sobě naprosto vše a všem sdělují.

Slovníček pojmů Sociální sítě:

Facebook: v dnešní době asi nejrozšířenější internetový systém, který slouží ke komunikaci mezi jednotlivými uživateli, sdílení fotografií, videí a textových informací.

Fake Profil: jde o falešný, podvodný profil. Uživatel zde záměrně uvádí nepravdivé informace.

Instagram: je aplikace – program, který slouží k zasílání a sdílení fotografií a videí. Opět je možné je různě filtrovat, třídit a ukládat.

Messenger – internetová aplikace pro jednoduché a rychlé odesílání zpráv mezi uživateli.

Netiketa: jsou to pravidla slušného chování v internetové síti, která by se měla dodržovat.

Profil: jde o účet, registraci k jednotlivé službě. Uživatel zde o sobě uvádí různé informace. Tyto informace mohou a nemusí být pravdivé. Také rozsah zveřejněných informací se často liší dle toho, co uživatel je ochoten o sobě sdělovat.

Snapchat: je aplikace-program, který slouží především k posílání různých fotek mezi jednotlivými uživateli. Fotografie si lze ukládat a třídit do různých alb.

Sociální síť: je to služba na internetové síti, která umožňuje registrovaným členům využívat své služby. Jde především o vytváření profilů, komunikaci a sdílení různých informací. Komunikace na těchto sítích může probíhat mezi dvěma nebo i více uživateli najednou a v reálném čase.

YouTube: v současnosti největší internetový systém pro sdílení videosouborů. Tento systém umožňuje uživatelům nahrávat jednotlivá videa do systému, prohlížet si videonahrávky jiných uživatelů a ty následně i hodnotit a komentovat.

Pracovní list Sociální sítě

1. **Nakresli loga jmenovaných sociálních sítí:**

Facebook

Snapchat

Instagram

Twitter

další dle vlastního uvážení

_____

_____

_____

2. **Co se stane s fotografiemi, které vyvěsíš na facebook?**

_____

_____

3. **Komu tyto fotografie patří?**

_____

Co vše napsat do profilu? Vytvoř svůj profil na fiktivní síti

Mobilní telefony

Cíl tématu: Vysvětlit rizika spojená s mobilním telefonem, mobilními aplikacemi a připojeními. Cílem je opět rozšíření znalostí z hlediska bezpečí při práci s virtuálními technologiemi, tedy i s chytrým telefonem, a naučit děti některé potřebné návyky i v této oblasti.

Odborné ukotvení:

Proberte s dětmi, jak vypadá jejich mobil, co vše umí a jak vypadá stavový řádek u chytrých telefonů. Upozorněte je na to, že zde si mohou rychle zkontrolovat, co mají v mobilním telefonu zapnuté.

Co je tedy vhodné mít zapnuté v mobilu? V mobilním telefonu, zvláště pak v tom chytrém, je mnoho možností co si nastavit a zapnout. Často ani nevíme, co to může dále znamenat. Potřebnou pozornost je třeba věnovat i instalacím aplikací a her. Velice často tyto aplikace chtějí přístupy, které nejsou adekvátní. Povolit hrám přístup třeba ke kontaktům nebo poloze, kde se nacházíme, je naprosto zbytečné. Vysvětlujte dětem, proč to ta hra vlastně chce? Vše je obchodovatelné a data v současné době nejvíce. Všem je jasné, že tedy žádná hra asi není úplně „zdarma“. Potom se divíme, že nás neustále někdo obtěžuje reklamami a nevyžádaným voláním.

Ptejte se dětí, zda chtějí, aby cizí lidé věděli, kde jsou, co tam dělají a jak dlouho telefony používají. Určitě řeknou, že ne. Veďte je v tomto kontextu k zamyšlení nad tím, aby příště při stahování her či zapínání funkcí telefonu více přemýšlely. Je nutné si při stahování jakékoli aplikace rozmyslet, zda dovolíme hrám a ostatním aplikacím, aby nás takto sledovaly. Učte děti pravidelně kontrolovat stavový řádek a vypínat vše, co není nutné. Tedy i geolokaci.

Jak je to s připojeními. Připojovat se přes free wifi nebo raději data v mobilu?

Dnes téměř každá aktivita na počítači a mobilu chce, abychom byli on-line. Abychom měli přístup na internet. To dnes není problém. Ve škole i jinde na kroužcích a klubech mají děti wifi připojení. Free wifi jsou zadarmo a nechtějí ani žádné heslo. Ovšem připojování se do veřejných wifi sítí bez hesla a ověření, může být

problematické a nebezpečné. Často se pak stává, že někdo může připojený mobil a tablet „napíchnout“, sledovat a vidět, co na něm kdo dělá, s kým si píše apod. Dokonce může i vidět, jak se přihlašujeme do mailu a vidět naše hesla. Je tedy z hlediska bezpečnosti mnohem lepší se připojovat přes mobilní data v mobilu. Ovšem u mobilních dat musí děti přemýšlet, zda jsou součástí tarifu a nebo zda je mají placená. To musí zjistit od svých rodičů. Pozor na to, že se může jednat opravdu o drahou záležitost, pokud jsou data účtována samostatně. Velice drahé také může být připojení v zahraničí.

Na co si dát pozor: Děti mají mobily většinou stále u sebe, budou si je ukazovat. Pozor na krádeže. Pokud má nízkoprahový klub nastavená vlastní pravidla pro užívání mobilních telefonů při vstupu do nízkoprahu, je dobré si je v tuto chvíli zopakovat a s dětmi dostatečně ukotvit. Dále je vhodné si společně zkontrolovat, zda mají všichni antivirový program. Pozor na posílení postavení jedinců ve skupině, pokud mají starý tlačítkový telefon. (Lze jednoduše- oni jediní jsou v bezpečí, nikdo jim nemůže vysát data).

Slovníček pojmů

Antivirový program: jde o program – software (placený nebo zdarma), který pomáhá chránit počítač, tablet, telefon před nežádoucími programy. Podmínkou funkčnosti je jeho instalace a častá aktualizace. V dnešní době je jeho používání nutností.

Datové připojení: Jde o možnost se připojit k síti internet za využití datového spojení s daným telefonním operátorem (nejčastěji toto připojení využívají mobilní telefony, pokud nejsou v dosahu nějaké veřejné WiFi sítě).

FireaWall – je zařízení nebo program v počítači, telefonu, který slouží jako ochrana síťové komunikace mezi zařízením a internetem. Je to jakási kontrola toho, co přichází a odchází do internetu.

Geolokace: metoda, při které se za použití mnoha způsobů dá určit poloha dané osoby nebo předmětu na Zemi. Nejčastěji se používá GPS nebo lokalizace pomoci GSM signálu nebo IP adresy zařízení, pomocí kterého jste připojeni na internet.

GPS: - Global Positioning Systém - česky globální polohovací systém. Tento systém slouží k určení geografické polohy na světě, a to s přesností na několik metrů. Využívá se v navigačních systémech dopravních prostředků, ale i třeba při použití SOS tlačítka na Vašem telefonu. Sledování polohy daného zařízení lze samozřejmě i zneužít. Pokud máte GPS zapnuté, může se stát, že Vás někdo pomocí tohoto lokátoru může za určitých okolností sledovat. Může pak vědět, zda jste nebo nejste doma, nebo kde se nacházíte.

Instagram: je aplikace – program, který slouží k zasílání a sdílení fotografií a videí. Opět je možné je různě filtrovat, třídit a ukládat.

PIN: nejčastěji 4 místné číslo používající se u platebních karet, telefonů, tabletů a různých přístupových systémů.

Selfie: autoportrét. Jde o techniku fotografování mobilním telefonem nebo fotoaparátem sebe sama, a to nejčastěji za pomocí vlastní ruky nebo selfie tyče.

SIM: je karta účastníka mobilního telefonního operátora. Malá plastiková kartička s pozlacenými kontakty. Na ní je v současné době uložena identifikace volajícího.

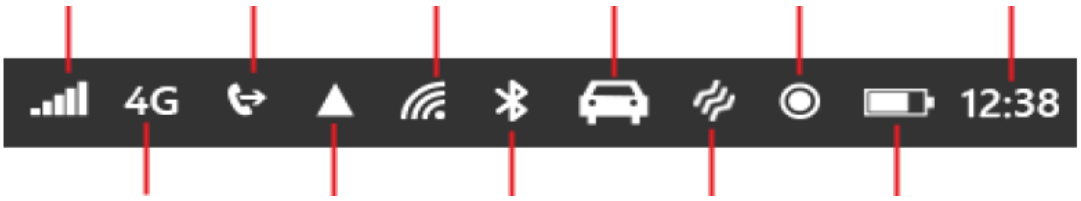
Smatrphone: neboli chytrý telefon. Je to mobilní telefon s různým operačním systémem, který umožnuje nejenom telefonovat a zasílat SMS (krátké textové zprávy). Je to vlastně malý počítač.

Snapchat: je aplikace-program, který slouží především k posílání různých fotek mezi jednotlivými uživateli. Fotografie si lze ukládat a třídit do různých alb.

WiFi: jde o bezdrátovou komunikaci v počítačových sítích. Většina dnešních mobilních telefonů, notebooků je připojena bezdrátově k WiFi vysílači a tím je připojena k internetové počítačové síti.

Pracovní list Mobilní telefony

- **popiš, co znamenají jednotlivé ikony stavové lišty mobilního telefonu**



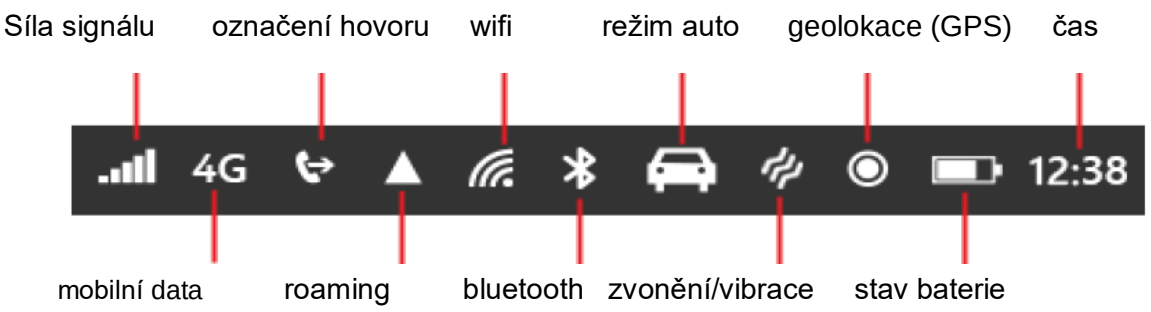
Které ikony a proč budeš mít zapnuté?

- _____
- _____
- _____
- _____

Které je nutné vypínat a jaká jsou rizika při jejich stálém zapnutí.

- _____
- _____
- _____
- _____

Pomůcka k pracovnímu listu pro sociální pracovníky



Kybergrooming

Cíl tématu: Upozornit děti na rizika komunikace s cizí osobou, seznámit se strategií kybergroomingu a hledat cesty, jak mu předcházet. Jak se nestat obětí.

Odborné ukotvení:

Útočník se snaží v kyberprostoru (chat, ICQ, sociální sítě, SMS…) vytipovat a najít vhodnou osobu, ve které vzbudí postupně důvěru a postupem času ji přinutí k osobní schůzce, kde oběť pak nějakým způsobem zneužije či využije. Velmi zranitelné jsou nejen děti, ale všichni, kteří si často hledají kamarády v kyberprostoru a kteří nejsou dostatečným způsobem poučeni. Touha po dobrodružství, riziku, svěřování se, hledání nových kamarádů a zkoušení dalších nových věcí jen nahrává útočníkovi, který čeká na svou příležitost. V této oblasti jsou často nejvíce ohroženy děti, které jsou na informačních technologiích závislé. Jsou to děti, které tráví velkou většinu času na internetu a se svým mobilem a většinu přátel a kamarádů mají pouze ve virtuálním světě. V realitě kamarády nemají, s nikým si nehrají, nikdo je nenavštěvuje. Kybergrooming probíhá v několika krocích, které na sebe postupně navazují.

V první fázi si útočník vyhlédne oběť, a to právě na základě informací, které získá na internetu a osloví ji. Ne vždy použije svoji pravou identitu. Často se útočník vydává za úplně jinou osobu, a to z důvodu, aby u oběti vzbudil pocit důvěry. Vydává se za osobu, která je oběti nějakým způsobem blízká (věkem, zájmy, problémy, vzhledem, potřebami apod.). Zároveň se pokouší oběť postupně izolovat od okolí. Jedině „on“ dokáže oběti se vším poradit a vždy ji zcela chápe – druhá fáze. V této fázi může oběti nabídnout „svoji“ fotografii či poslat nějaký vhodný dárek, např. dobít kredit u mobilního telefonu, aby vzbudil větší důvěru. Ve třetí fázi se pokouší útočník získat nějaký kompromitující materiál. Vhodným způsobem oběť motivuje, aby mu zaslala např. fotografie, videa. A pokud fotografie či videa, tak nějaká, kde je oběť spoře oděná, či je dokonce nahá. V případě, že oběť zašle požadované materiály, útočník je systematicky sbírá a následně je použije proti oběti. Útočník ale také postupně sbírá veškeré osobní údaje a informace, které mu oběť během komunikace
podá. V poslední fázi útočník žádá oběť o osobní schůzku. Ta může proběhnout zcela dobrovolně na základě oboustranné dohody, anebo pokud se oběť nechce nechat

vylákat, může ji útočník začít vydírat zveřejněním fotografií na internetu, ve škole apod. Tím oběť vydírá a s největší pravděpodobností dosáhne osobní schůzky. Na té pak může následovat to, proč vlastně útočník oběť kontaktoval (znásilnění, vydírání, napadení….). Za nejdůležitější považujeme vždy prevenci. Každý by měl být řádným a vhodným způsoben informován o možných rizicích a důsledcích. [4]

Pro bližší seznámení s danou problematikou a rozšíření si informací doporučujeme sociálním pracovníkům i filmy „Seznam se bezpečně“. První film je technikou již zastaralý, nepouštěli bychom ho dětem, ale pro sociální pracovníky z hlediska obsahu a podstaty tématiky je velice vhodný pro ukotvení daných zásad a seznámení se s případy, které se opravdu staly. Dále společnost Seznam.cz připravila i „Seznam se bezpečně II“, Seznam se bezpečně III, všechny dostupné na www.seznamsebezpecne.cz.

Na co si dát pozor: Děti často nepovažují schůzku s cizí osobou za problém. Mnohým z nich to přijde normální, přestože již o daném problému slyšely. Ze zkušenosti z práce s třídními kolektivy víme, že všechna rizika děti znají, přesto je často podceňují a nemají problém s tím, aby se setkali s cizím člověkem z internetu. Mnoho se jich dokonce v tomto věku takto seznamuje. Upozorněte na daná rizika. Zopakujte. Varujte.

Slovníček pojmů

Flaming – hoření. Jde o nepřátelské chování útočníka vůči oběti, které se odehrává ve virtuálním světě. Nejčastěji v diskuzních fórech, chatu, sociálních sítích, ale i v emailu. Útočník urážlivým způsobem napadá oběť tím, že do kyberprostoru umisťuje vzkazy, ve kterých ho hrubým způsobem uráží a zesměšňuje. Své chování útočník postupně stupňuje. Častým motivem je, že útočník nesouhlasí s názory oběti a tu pak uráží a argumentuje svým přesvědčením.

[4] BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*.

Intimní materiál: ze něj lze považovat fotografii, video i text na základě které pak následně může být člověk identifikován a vydírán kvůli nevhodnému obsahu.

Kybergrooming - manipulace v kyberprostoru. Útočník se snaží v kyberprostoru (chat, ICQ, sociální sítě, SMS…) vytipovat a najít vhodnou osobu, ve které vzbudí postupně důvěru a postupem času ji přinutí k osobní schůzce, kde oběť pak nějakým způsobem zneužije či využije.

Online hra: počítačová hra, která se hraje na internetu a na sociálních sítí. Může ji hrát jeden hráč (single-player) nebo více hráčů (multi-player).

Trolling: jde o takové jednání na internetu, které má za úkol ostatní lidi rozzlobit a vyvolat u nich nějakou rekci. Příkladem může být to, že jeden uživatel říká úplné nesmysly a pozoruje při tom reakce druhého uživatele.

Další možné náměty k tématu Kybergrooming k využití pro práci s cílovou skupinou:

- Napiš, jak si ověříš identitu člověka, kterého znáš jen z internetu?

- Jaké zásady platí pro komunikaci s neznámou osobou?

- Za jakých okolností se sejdeš s osobou známou jen z internetu?

- Co bys doporučil kamarádům, když je někdo osloví na internetu a chce od nich fotky?

- Vyjmenuj alespoň 5 osobních údajů.

Kyberšikana a sexting

Cíl tématu: Seznámit se s formami kyberšikany. Informovat o tom, jak se nestat obětí, ale i jak se nestat agresorem. Upozornit na úskalí dané problematiky a věnovat se i problematice sextingu u dětí a mladistvých.

Odborné ukotvení:

Kyberšikana je takové jednání, které má oběť záměrně ohrozit nebo jí ublížit prostřednictvím prostředků informační a telekomunikační techniky. Nejčastěji se setkáte se zneužitím mobilního telefonu a internetu. Podle loňského výzkumu má každé druhé dítě na českém internetu zkušenosti s kyberšikanou. Rozsáhlý výzkum[5] ukázal, že mezi nejčastější druhy kyberšikany patří verbální útoky (33%), obtěžování za pomoci prozvánění (24%) a vyhrožování či zastrašování (17%). Děti se navíc přiznaly k tomu, že v nezanedbatelné míře jsou samy autory kyberšikany vůči svým vrstevníkům. Kyberšikana má svá specifika oproti „klasické“ šikaně. Rozdíly jsou především ve velké anonymitě. Pachatel se cítí bezpečně, neboť si myslí, že se o něm nikdo nedozví. Některé děti- agresoři ani nevědí, že páchají kyberšikanu. Berou to za jakousi formu uvolnění svých vlastních tenzí a nespokojeností. Někteří potřebují demonstrovat svou sílu, vyvolat strach, někdy samy v reálném světě strachem trpí, či jsou oběťmi klasické šikany. Častým spouštěcím faktorem takovéhoto jednání může být pouhá nuda, hádka s kamarády, konflikty se spolužáky, pomsta. Většina obětí se nedozví, kdo je agresorem kyberšikany, což je velice nepříjemné a pocit strachu se tím zvyšuje i v reálném světě. Dalším rozdílem je doba trvání.

Ke kyberšikaně může docházet kdykoli (365 dní v roce/24 hodin denně). Ale může také proběhnout pouze jednou a následky mohou trvat po zbytek života oběti. K SMS se můžeme kdykoli vrátit a neustále ji číst dokola, jakákoli zpráva pomocí ICT technologií „visí“ v kyberprostoru a čte ji často obrovské množství lidí. Tím se pocity ponížení u oběti násobí. Oběť má často pocit, že už to četli všichni na světě a všichni si teď na ni/něj ukazují a už nemůže ani chodit ven. Toto je často pro oběť značně traumatizující a může to vést až k pokusům o sebevraždu. Místo, odkud agresor útočí,

[5] KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*.

nehraje žádnou roli. Stejně tak jako fyzická vzdálenost mezi obětí a agresorem. V kyberšikaně není podstatné, zda byl agresor velký a fyzicky zdatný, ale stačí pouze, aby byl dostatečně gramotný v oblasti využití informační a telekomunikační techniky. Nejdůležitějším způsobem ochrany je prevence, která spočívá v informovanosti všech zúčastněných osob.[6]

Sexting

Jde o využívání informačních a komunikačních prostředků k zasílání textů, fotografií a videí se sexuální tématikou. Tyto materiály často končí na internetu a můžou mít pro oběť fatální důsledky, neboť jsou často použity jako donucovací prostředek k vydírání. Některé případy pak končí až smrtí oběti. Zasláním erotické fotky nebo pornofotografie či videa komukoli se vystavujeme riziku, že v budoucnu může být tento materiál použit proti nám, např. k vydírání. Tato situace nemusí nastat bezprostředně po odeslání, ale v podstatě kdykoli, neboť útočník si tento materiál uchovává a použije jej kdykoli v budoucnu. Závažným rizikem je fakt, že ti, kdo šíří sexting, mohou být zároveň pachateli přestupku nebo trestné činnosti v oblasti šíření dětské pornografie nebo ohrožování výchovy dítěte apod. Dítě je v tomto případě osoba do 18 let.

Nejdůležitější je informovanost jednotlivých uživatelů. Nikomu za žádných okolností neposkytnout potencionálně nebezpečný materiál. To platí i v partnerských vztazích, neboť tento vztah může jednou skončit a jedna ze stran pak choulostivý materiál použije proti straně druhé ve snaze tento vztah udržet. To samé platí s umisťováním choulostivého materiálu na sociální profily. Ty nejsou ve skutečnosti přístupné jen vybraným jedincům. Fotografie či video se pak může nekontrolovatelně šířit po internetu.[7]

Na co si dát pozor:

Mluvte s dětmi o tom, co kyberšikana je. Snažte se, aby se děti nejen nestaly obětí, ale aby se nestaly, byť někdy nevědomky, agresorem v kyberprostoru. Velice

[6] BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*
[7] BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*

často o aktivitách mluví a říkají, že je to jen sranda. Pozor na to. Mluvte s dětmi i o netiketě (etiketě na internetu).

Slovníček pojmů

Facebook - jedna z největších společenských sítí na internetu. Slouží ke komunikaci mezi jednotlivými uživateli. Můžete si psát, posílat obrázky a videa. Zároveň tyto soubory můžete sdílet s jinými uživateli nebo i skupinami uživatelů. V dnešní době je možné se pomocí facebookového profilu přihlašovat i k různým aplikacím a hrám. Riziko je v množství a citlivosti údajů, informací, fotek a videí, které tam uživatelé vkládají a ostatním je tímto zpřístupní.

Kyberšikana - v překladu šikana, která se odehrává ve světě informační a telekomunikační techniky. Jde o takové jednání, které má oběť záměrně ohrozit nebo jí ublížit prostřednictvím prostředků informační a telekomunikační techniky. Nejčastěji se setkáte se zneužitím mobilního telefonu a internetu. Podle loňského výzkumu má každé druhé dítě na českém internetu zkušenosti s kyberšikanou.

Kybergrooming - manipulace v kyberprostoru. Útočník se snaží v kyberprostoru (chat, ICQ, sociální sítě, SMS…) vytipovat a najít vhodnou osobu, ve které vzbudí postupně důvěru a postupem času ji přinutí k osobní schůzce, kde oběť pak nějakým způsobem zneužije či využije.

Kyberstalking - v překladu jde o pronásledování v kyberprostoru. Jedná se o obtěžování, které se stupňuje, opakuje a odehrává se v kyberprostoru. Má různou intenzitu a liší se i druhy projevu. Využívají se při ní prostředky komunikační techniky (např. Skype, SMS, chat, email, telefon, sociální sítě). Stalker je velmi často znám oběti, může jít o bývalého partnera, milence, kamaráda, zrazeného přítele nebo milovníka. Ten například není ochotný akceptovat ukončení vztahu nebo nezájem oběti, a tak se pokouší oběť v kyberprostoru obtěžovat a donutit ji k reakci či návratu. Toto obtěžování může mít rozličnou podobu od SMSek, emailů, po prozvánění a vyhrožování.

Sexting - sextování. Složenina ze slov sex a posílání textů, obrázků a videí. Jde o využívání informačních a komunikačních prostředků k zasílání textů, fotografií a videí se sexuální tématikou. Tyto materiály často končí na internetu a můžou mít pro oběť fatální důsledky, neboť jsou často použity jako donucovací prostředek k vydírání. Některé případy pak končí až smrtí oběti.

Další možné náměty k tématu Kyberšikana a sexting k využití pro práci s cílovou skupinou:

- Napiš, co vše považuješ za kyberšikanu.

- Na koho se obrátíš, pokud Ti někdo vyhrožuje nebo Tě vydírá?

- Napiš číslo Linky bezpečí.

- Napiš alespoň 5 důvodů, proč je nebezpečné posílat svojí erotickou fotografii nebo video.

- Vysvětli, proč bys nikdy neměl mazat SMS, emaily a důkazy o tom, že Ti někdo ubližuje.

PC hry a závislost

Cíl tématu: Seznámení s tím, jak MMORPG (Massive Multiplayer Online Role Playing Game) mohou zapříčinit rozvoj závislosti. Co je netolismus a jak daným problémům se závislostí předcházet.

Odborné ukotvení:

Netolismus – počítačová závislost

Netolismus je popisován jako závislost na virtuálních technologiích, původně se jednalo o složeninu slova net (jako internet) a –ismus jako označení závislosti. V prvopočátcích se o ní hovořilo jako o čisté závislosti na internetu. Dnes je již tato závislost vnímána v širším kontextu, je specifikována jako závislost na moderních komunikačních a počítačových technologiích. V nejčastější podobě je to u dětí mobil, tablet, počítač, kdy dnes je většina těchto technických prostředků již s trvalým připojením na internet - tedy nepřetržitě on-line. V této souvislosti popisujeme veškeré závislostní chování na počítačových hrách, všech možných internetových službách, na různých sociálních sítích, chatech, virálních videích, mobilních telefonech apod.

Když pomineme zdravotní rizika v oblasti pohybového aparátu a vizuálního systému, která přímo souvisí s dobou strávenou na internetu, vyvstávají další rizika a poměrně závažné problémy ovlivňující i duševní zdraví a psychiku nevyzrálých jedinců. V oblasti zdravotních rizik je dalším charakteristickým jevem i problematika RSI (Repetition Strain Injury), což je skupina postižení, kterou vyvolávají drobné opakované pohyby při práci s počítačem. Společným znakem pro všechny druhy těchto postižení je značná bolestivost. Patří sem i zánět šlach, zánět nekloubního výčnělku a syndrom karpálního tunelu.

V oblasti psychiky dětí pozorujeme značně změněné chování. Děti začnou postupně ztrácet své kontakty a přátele v reálném světě, raději komunikují ve virtuálním světě. Vstávají i v noci, jsou schopny si nařizovat budík, aby mohly na počítač, až rodiče usnou. Ve škole se zhoršuje prospěch, jsou unavené, lžou o době strávené na počítači, mají jen on-line přátele, ztrácí pojem o reálném čase, zapomínají

na dřívější koníčky, nechtějí nikam chodit, odmítají odjet na víkend, kde není signál. Později v rozvinuté závislosti zapomínají na stravu, přestávají jíst a pít, v této době se také často začne objevovat záškoláctví. To je již pokročilá forma závislosti. Závislost se rozvíjí pomalu, nenápadně a plíživě, dítě tráví na počítači čím dál více času, pak už musí být on-line téměř trvale. Největší riziko vzniku závislosti v souvislosti s internetem je přisuzováno intenzivnímu rozvoji počítačových her, které jsou programovány tak, že je hraje neuvěřitelné množství lidí. Dítě zde sdílí kyberprostor s tisícovkami hráčů na celém světě, se svou figurkou plně patří do virtuálního světa dané hry. Specifikum těchto her je to, že se účastník věnuje rozvoji vlastní herní figurky, která je součástí světa, jenž má vlastní vývoj, a zároveň je také součástí komunity spoluhráčů v reálném světě. Dítě se sžívá se svou postavou, chce, aby jeho postava žila a plnila úkoly, jedinec má postupně potřebu raději se vůbec neodpojovat, aby jeho postava, tedy vlastně ono samo, o něco nepřišlo a stále žilo a plnilo všechny úkoly. Tyto hry patří mezi tzv. MMORPG – Massive Multiplayer Online Role Playing Game. Nejznámější MMORPG je World of Warcraft (zkráceně WoW). Tuto hru hraje podle společnosti Blizzard Entertainment, jež hru vyvinula, celkem 11 milionů hráčů. Odhaduje se, že na celém světě MMORPG hraje kolem 16 mil. lidí. Záludností těchto her je, že hráče úplně pohltí, hra nikdy nekončí, hráč potřebuje nakupovat čím dál lepší výbavu, potřebuje další propriety a pomůcky do hry. RPG, tedy Role-playing games, jsou epické, dlouhodobé skupinové hry odehrávající se ve fiktivním („fantasy“) světě. Hra je neustále nově naprogramovávána, žije sama svým životem. Pokud chce hráč dosáhnout úspěchu, musí spolupracovat, neodpojovat se, rozvíjet vztahy s ostatními, domlouvat se, sdružovat se s ostatními. Hráči soustředění v jedné hře vytvářejí vlastní komunitu, vlastní sociální síť. Snaha o dosažení úspěchu nutí každého hráče k neustálému vylepšování postavy, jejího vybavení a hromadění prostředků. To vše vede k patologickému trávení velkého množství času na internetu a k rozvoji závislosti. Někteří jsou schopni tyto hry hrát i spoustu hodin bez přestávky za neustálého povzbuzování ostatních členů RPG komunity, kteří často dítě nutí, aby vydrželo a „nezkazilo“ hru. Někdy dokonce vyhrožují, že ho z komunity vyhodí a ve hře zabijí, tím ho vyloučí apod. Děti tedy v komunitě zůstávají a ztrácí zájem o reálný svět a jeho aktivity. Své potřeby začnou uspokojovat ve virtuálním světě a reálný svět jim začne připadat nudný a nezajímavý. Jako velké riziko je pak vnímáno naprosté odtržení dítěte

od reality a často velmi intenzivní identifikace s virtuální postavou a celou RPG komunitou.

Na co si dát pozor: Jak děti mluví o hrách, které hrají, s kým je hrají, pozor, upozorňujme na dobré příklady a na vzory chování a sociální role ve skupině. Vnímáme případné ztotožnění s postavou či hrou. Komunikujeme, vyhledáváme zajímavé činnosti v realitě. Využíváme pozitivní sociální tlak skupiny v reálném životě.

Slovníček pojmů

Facebook - jedna z největších společenských sítí na internetu. Slouží ke komunikaci mezi jednotlivými uživateli. Můžete si psát, posílat obrázky a videa. Zároveň tyto soubory můžete sdílet s jinými uživateli nebo i skupinami uživatelů. V dnešní době je možné se pomocí facebookového profilu přihlašovat i k různým aplikacím a hrám. Riziko je v množství a citlivosti údajů, informací, fotek a videí, které tam uživatelé vkládají a ostatním je tímto zpřístupní.

Multi-player hra: v této hře hraje zároveň několik hráčů současně. Jednotliví hráči nemusí být v daném čase na jednom místě. Stačí mít internetové spojení a jednotliví hráči se připojují z různých míst.

Netolismus: počítačová závislost. Netolismus jako pojem vznikl původně ze slova net, tedy ve své původní podobě byl považován za závislost člověka na internetu. Dnes je specifikován jako závislost na moderních komunikačních a počítačových technologiích. V nejčastější podobě je to u dětí mobil, tablet, počítač, kdy dnes je většina těchto technických prostředků již s trvalým připojením na internet - tedy nepřetržitě on-line.

PC hra: je program, který umožňuje uživateli na počítači, tabletu, telefonu hrát elektronickou verzi hry. PC hry mají mnoho podmnožin a kategorií.

RPG hra: hra, kde se hráč vydává za hrdinu nebo hrdiny. Jedná v této hře v roli hrdiny, kladného nebo záporného. Může se jednat o PC hru nebo i stolní hru. Tyto hry bývají velmi často výpravné, zábavné a interaktivní. Často tyto hry také mívají dost složitá a obsáhlá pravidla.

Single-player hra: je hra, která je určena pro hraní jednoho hráče v dané hře. Veškeré ostatní pohyby a děje ve hře řídí pouze počítač.

Virtuální kamarád: je zdánlivý kamarád. Nejcharakterističtějším znakem je, že tito kamarádi se osobně neznají a komunikuji spolu výhradně pomocí elektronických médií. Ve skutečnosti asi neví, kdo je jeho „kamarád“. Zde se každý může vydávat za kohokoli. Může hrát nějakou roli.

Virtuální komunita: je to jistá skupina lidí, kteří se neznají osobně a komunikují mezi sebou elektronickou cestou. Nejčastějším komunikačním prostředkem jsou sociální sítě.

Pracovní list Závislost- netolismus

Zakroužkuj, co může být znakem závislosti na virtuálních technologiích (netolismu)

silná touha zapnout počítač **neustálá kontrola SMS**

kontrolovat statuty na sociální síti **neschopnost vymezit si začátek a konec aktivit na internetu**

postupně zanedbávat další aktivity kvůli počítači **stálá kontrola mobilu**

nezvladatelná chuť hrát **chtít být trvale on-line**

Vypiš, co Tě ještě napadá jako další znak závislosti- netolismu:

- _____
- _____
- _____
- _____
- _____
- _____

Zkontrolujte ve skupině s kamarády a vyberte na flip opakující se body a diskutujte o nich.

Pracovní list Počítačové hry a závislost

1. **Na co dát pozor při stahování PC her?**

- _____
- _____
- _____

2. **Co napsat do profilu hry?**

3. **Jak se bránit na chatu v RPG, když Ti zakazují jít spát, abys nezkazil hru?**

Nejprve napište nápady, poté dejte hlavy dohromady a zahrajte scénku ve skupině

4. **Máš nějakou oblíbenou PC hru? Co bys o ní řekl ostatním?**

5. **Hraješ ji sám, či s jinými lidmi? Je ta hra on-line?**

Další možné náměty k tématu Počítačové hry a závislost k využití pro práci s cílovou skupinou:

- Napiš názvy her, které rád hraješ a podtrhni ty, ve kterých jsi kladný hrdina.

- Kde a jak zjistíš, že hra je pro Tebe vhodná?

- Dokážeš si ráno přivstat, aby sis mohl zahrát hru sám nebo se svým kamarádem?

- Už jsi někdy vynechal třeba večeři, aby sis mohl déle hrát?

- Jak se chráníš, aby ses nestal závislým?

. . . a nezapomínejte,

že i Vy byste měli být

vzorem v chování,

ale i v používání

informační

a telekomunikační techniky

a virtuálních technologií.

Seznam literatury, zdrojů a možnosti rozšíření informací

BURDOVÁ, Eva a Jan TRAXLER. *Bezpečně na internetu*. Vyd. 1. Praha: Středočeský kraj ve spolupráci se Vzdělávacím institutem Středočeského kraje (VISK), 2014, 43 s. ISBN 978-80-904864-9-2.

BURDOVÁ, Eva. *Základní orientace ve struktuře vzděl. programů, didaktické a výchovné činnosti: metodický materiál*. 3. vyd. Praha: VISK, 2013.

JANIŠ, Kamil a Irena LOUDOVÁ. *Obecná didaktika: (vybraná témata)*. Ústí nad Orlicí: Oftis, 2016. ISBN 978-80-7405-407-5.

KALHOUS, Zdeněk a Otto OBST. *Školní didaktika*. Vyd. 2. Praha: Portál, 2009. ISBN 978-80-7367-571-4.

OBST, Otto. *Obecná didaktika*. 2. vydání. Olomouc: Univerzita Palackého v Olomouci, 2017. ISBN 978-80-244-5141-1.

Získání podnětů ke komunikaci nad videospoty:

BARTOŠÍKOVÁ, Ivana a VOŘÍŠEK. *Příručka pro nízkoprahové terapeuty*. Boskovice: Albert, 1998. ISBN 80-858-3457-X.

BURDOVÁ, Eva, SIXTA, Jiří, TRAXLER, Jan. *Zdravé klima, aneb, Prevencí rizikového chování si vytvoříme "domeček", kde nám bude dobře: studijní text ke stejnojmennému kurzu.* Vyd. 1. Příbram: Elrond, 2012, 28 s. ISBN 9788026023326

BURDOVÁ, Eva. *Komunikace mezi učitelem a jeho žáky*. 1. vyd. Písek: Arkáda sociálně psychologické centrum, 2014.

BURDOVÁ, Eva, SIXTA, Jiří a ŠPERER, Josef et kol*. Didaktické metody a techniky. Konkrétní problémy*. Příbram: Elrond o.p.s., 2014,132 s.

BURDOVÁ, Eva, TRAXLEROVÁ, Jaroslava a SIXTA, Jiří. *Sociální klima školy a zdravá komunikace.* 1. vyd. Příbram: Elrond o.p.s., 2014

BURDOVÁ, Eva a SIXTA, Jiří. *Projektové vyučování, využívání projektových metod.* Příbram: Elrond o.s., 2012, 24 s.

ELICHOVÁ, Markéta. *Sociální práce: aktuální otázky*. Praha: Grada, 2017. ISBN 978-80-271-0080-4.

GINOTT, Haim G. *Umění komunikace s dětmi: láska a selský rozum nestačí*. Praha: Portál, 2015. ISBN 978-80-262-0926-3.

KOPECKÝ, Kamil. *Rizikové formy chování českých a slovenských dětí v prostředí internetu*. Olomouc: Univerzita Palackého v Olomouci, 2015. ISBN 978-80-244-4861-9.

Slovo a obraz v komunikaci s dětmi: komunikace s dětmi v multikulturním světě : sborník příspěvků z odborného semináře pořádaného katedrou českého jazyka a literatury s didaktikou PdF OU a Kabinetem literatury pro mládež, jazykové a literární komunikace KCD PdF OU.. Ostrava: Pedagogická fakulta Ostravské univerzity, 1997.

Doporučené internetové zdroje:

https://www.apek.cz/dokumenty-a-videa
http://www.bezpecnyinternet.cz/
https://www.heureka.cz/
http://www.kyberšikana.eu
http://www.overenozakazniky.cz/
https://www.seznamsebezpecne.cz/ke-stazeni