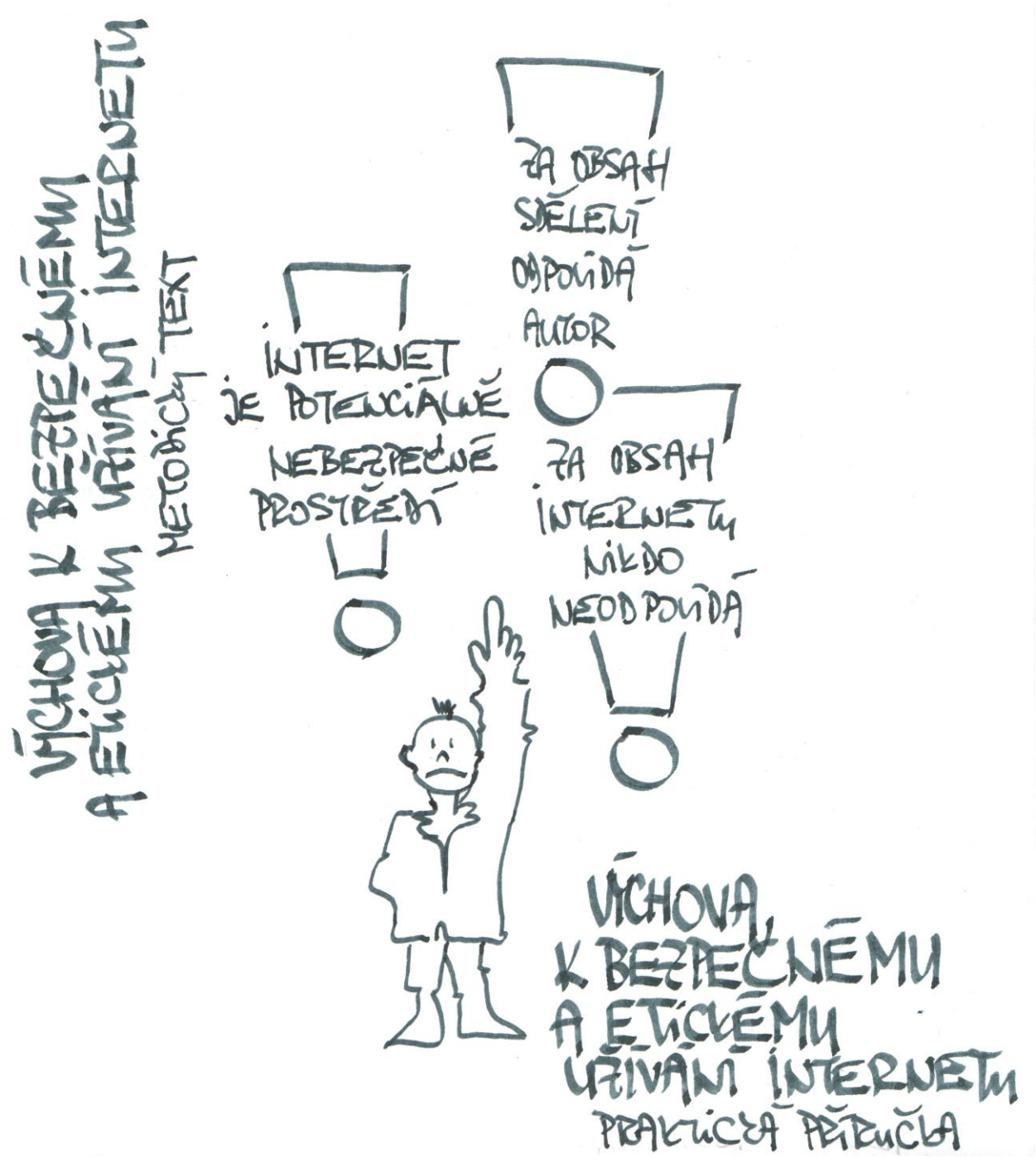
VÝCHOVA K BEZPEČNÉMU A ETICKÉMU UŽÍVÁNÍ INTERNETU

Metodický materiál pro pedagogické pracovníky

Národní centrum bezpečnějšího internetu

2012

užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.



Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

VÝCHOVA K BEZPEČNÉMU A ETICKÉMU UŽÍVÁNÍ INTERNETU NA ZÁKLADNÍCH A STŘEDNÍCH ŠKOLÁCH
Metodický materiál pro pedagogické pracovníky

1. Úvod

Svět i dění okolo nás se vyvíjejí stále dynamičtěji. Nové komunikační technologie přinášejí stále novější a kvalitnější možnosti informací, globálních propojení, kontaktů, konverzace, nákupů, her a cestování. Internet nám přináší svět až do našeho nejintimnějšího soukromí. Krom pozitiv má internet ale také svá negativa. Tím nejvýznamnějším je anonymita. Zatím nemá běžný uživatel možnost se stoprocentní jistotou zjistit, kdo se na druhém konci komunikačního kanálu nalézá. A není povinností, aby účastníci vzájemného kontaktu sdělili svou pravou identitu. Záleží jen a jen na každém z nich, zda v internetové komunikaci dodrží běžné mravní, sociální a zákonné normy.

Děti a mladí lidé jsou v tomto ohledu nezkušení, důvěřiví a otevření. Vývoj možností bezprostřední online komunikace se světem se rozvíjejí v současné době rychleji než jejich psychická připravenost na setkání s možnými nebezpečími. Chybí jim vlastní zkušenost, zkušenost starších je nejen obtížně přenosná, ale také mnoha současným dospělým obdobná chybí zkrátka pro to, že s internetem a mobily nevyrůstali.

Vědomé a rozumné užívání internetu chrání před nebezpečími, které jeho prostřednictvím mohou přicházet z vnějšího světa. Míra možného ohrožení mladých s nástupem nových komunikačních technologií prudce vzrostla. V čím rannějším věku bude dítě seznámeno s možnými hrozbami ze strany internetu, tím účinněji mu bude možno vštípit nutné obrany a ochrany. Prevence by měla proto začít spolu s prvními krůčky dítěte v kyberprostoru.

To samé platí o etickém a ohleduplném užívání internetu. Hrubost, vulgarita, arogance, absence empatie a tolerance nepatří do internetové komunikace stejně jako do té "tváří v tvář". Vědomí anonymity často podporuje nezralé uživatele v jednání, na něž by si v otevřené komunikaci netroufl. Kdysi tuto možnost skýtal pouze anonymní dopis, nyní je těch možností mnohem více.

Účelem tohoto metodického materiálu je vybavit pedagogy informacemi, které jim pomohou poskytnout dětem a mladistvým základní vědomosti o bezpečnosti a etikou spojenou s užíváním internetu a moderních technologií. Na tento obecný metodický text navazují materiály, které představují soubor jednotně koncipovaných, tematicky zaměřených metodických textů. Osm různých metodických textů je propojeno společným jmenovatelem a tím je žákova dovednost a návyk bezpečně a eticky nakládat s internetem. V každém z textů najdete informace, které jsou

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

předkládány způsobem, jenž je umožňuje rychle a přesně použít v přímé pedagogické práci. Součástí každého jednotlivého metodického textu jsou pracovní listy, které se podle potřeb pedagoga dají používat i v jiných tematických celcích.

2. Bezpečné a etické užívání internetu a jeho začlenění do školního kurikula

Kurikulum je pojem vyššího řádu než osnovy výuky, plán výuky, obsah vzdělávání a učivo. Správné školní kurikulum pro oblast výchovy k bezpečnému a etickému užívání internetu by mělo v sobě zahrnovat veškerou zkušenost, kterou žáci mohou získat ve škole a činnostech ke škole se vztahujících. Zjednodušeně je celé kurikulum, tedy program, plán, průběh a obsah výchovy k bezpečnému a etickému užívání internetu vyjádřen v následujícím obrázku:

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Výchova k bezpečnému užívání moderních technologií a škola

Téma internetové bezpečnosti a etické online komunikace získalo v posledních letech do té doby nevídanou pozornost médií a postupně i veřejnosti. Zasloužily se o to především konkrétní případy, kdy se děti a dospívající staly obětí nejrůznějších forem elektronického násilí a trestných činů. Přes poměrně vysokou míru digitální gramotnosti českých dětí a související míru ohrožení zůstává oficiální vzdělávací systém zatím pozadu. Výchova k bezpečnému a etickému užívání internetu a online technologií není zařazena do školního kurikula, absentuje v Rámcovém vzdělávacím programu, problematika často není zařazena ani v minimálních školních programech prevence, chybí v profesní přípravě pedagogických pracovníků.

Přestože řada pedagogů absolvovala proškolení v některých z témat online bezpečnosti v rámci dílčích projektů, většina pracovníků škol není připravena na výuku tématu, preventivní aktivity či účinnou pomoc dětem ohroženým elektronickým násilím.

Řada škol řeší situaci tak, že prostředkuje žákům preventivní besedy, zpravidla monotematicky zaměřené na prevenci kyberšikany, pořádané policií či neziskovou organizací. Při užívání internetu dnes zdaleka nehrozí jen kyberšikana, jakkoli je významnou hrozbou. Stejně jako v „reálném životě“ si v tom virtuálním našly svůj prostor sociálně patologické jevy nejrůznějších forem.

Problematika online bezpečnosti zahrnuje širokou škálu témat:
Charakteristiku rizik, rizikových a společensky nebezpečných jevů spojených s užíváním internetu a online technologií,

- Etiku online komunikace a bezpečné chování uživatelů,
- Didaktiku online bezpečnosti a online etiky,
- Technické nástroje ochrany uživatelů a kontroly,
- Právní a trestně právní souvislosti,
- Nástroje intervence a pomoci obětem elektronického násilí a kriminality.

Předkládaný materiál samozřejmě nepostihne veškeré aspekty internetové bezpečnosti, snaží se o výčet aktuálně nejdůležitějších témat ve vztahu k dětem a jejich ochraně.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

DĚTI V KYBERPROSTORU

Domorodci versus přistěhovalci

Současná generace školních dětí je jednou z prvních generací, které se již narodily do světa, kde je internet naprostou samozřejmostí a neumí si svůj život bez něj představit. Vyrostla obklopená počítači, mobilními telefony, herními konzolemi, dnes i iPady a dalšími výdobytky moderního světa. Mezinárodně uznávaný odborník na digitální vzdělávání a programátor Mark Prensky pojmenoval tyto generace jako digitální domorodce (digital natives). Jazyk virtuální komunikace a kyberprostoru je pro ně „mateřským" jazykem. Naopak generace pedagogů a rodičů jsou převážně těmi, které vyrostly v předdigitálním věku a jazyk digitalizovaného světa se učí až v dospělém věku. Jsou tedy digitálními přistěhovalci (digital immigrants). Autor vychází z poznatku, že současní žáci zacházejí s informacemi a zpracovávají je zcela jinak než generace předchozí. Dochází tak k paradoxní situaci ve vzdělávání, kdy pedagogové - „přistěhovalci", kteří přemýšlí a hovoří „historickým jazykem" předdigitálního věku, zápasí s výukou žáků, kteří jsou v novém světě „rodilými mluvčími".

Jací jsou tedy Prenskyho noví žáci? Je prokázáno, že stimulace mozku má vliv na jeho fyzickou restrukturalizaci, a to po celý lidský život. Vědci dnes předpokládají, že z důvodu významně odlišné zkušenosti a podnětů v rozhodném vývojovém období mají dnešní žáci a studenti fyziologicky odlišný mozek. Zkrátka děti, které vyrostly s technologiemi, myslí zcela jinak, než my ostatní. Jsou zvyklí získat hledanou informaci velmi rychle, pracují zároveň s více úkoly, upřednostňují práci s obrazy a grafikou před prací s textem a hry před „skutečnou" prací, nejlépe pracují ve skupinách a neustále „propojené" a „připojené". Musí zpracovávat odlišné podněty a v jiných formách, než předchozí generace. Je možné, že přetrvávající metody výuky (já mluvím – ty posloucháš, lineární logika) ani obsah už ne zcela odpovídají potřebám. Dle Prenskyho jsme vstoupili do doby, kdy je nutné změnit jak formu, tak obsah vzdělávání.

Nebojte se digitálních domorodců

Moudří kantoři a vychovatelé přijímají fakt, že nerozumí novému digitálnímu světu, ve kterém se tak samozřejmě pohybují jejich žáci, a přijímají jejich pomoc a podporu. To neznamená, že by rezignovali na předávání toho, co považují za důležité, ale bude nutné zrychlit tempo, rozvíjet paralelně znalosti i dovednosti, zvýšit interaktivitu a okamžitou zpětnou vazbu, a využívat k tomu moderní technologie. Velkým trendem ve vzdělávání jsou nyní online video lekce – webináře či online edukační hry. Prensky sám vyvíjí mnoho vzdělávacích online her, je autorem didaktického přístupu „Digital Games-Based Learning". Za podpory hry se může velmi efektivně připravovat pilot dopravního letounu, voják – výsadkář, pracovník záchranné služby. V historicky orientovaných hrách se studenti mohou procházet Pompejemi, uzavírat důležité

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

politické dohody mezi středověkými státy či účastnit se stavby renesančních katedrál. Existují hry, které pomáhají dětem překonávat např. depresi.
Zdroj: Marc Prensky: „Digital Natives - Digital Immigrants", ©2001 Marc Prensky

Kyberprostor

Kyberprostor je pojem poprvé použitý v roce 1982 Williamem Gibsonem v jedné z povídek a v roce 1984 jako ústřední téma jeho románu Neuromancer. Věra Zelinková definuje kyberprostor zkráceně takto: „Kyberprostor je nehmotný svět informací, který vzniká vzájemným propojením informačních a komunikačních systémů. Toto prostředí umožňuje vytvářet, uchovávat, využívat a vzájemně si vyměňovat informace. Zahrnuje počítače a databáze propojené komunikačními systémy, jako například celosvětovou síť internet. Anglickým označením pro kyberprostor je slovo cyberspace". http://kisk.phil.muni.cz/wiki/Kyberprostor

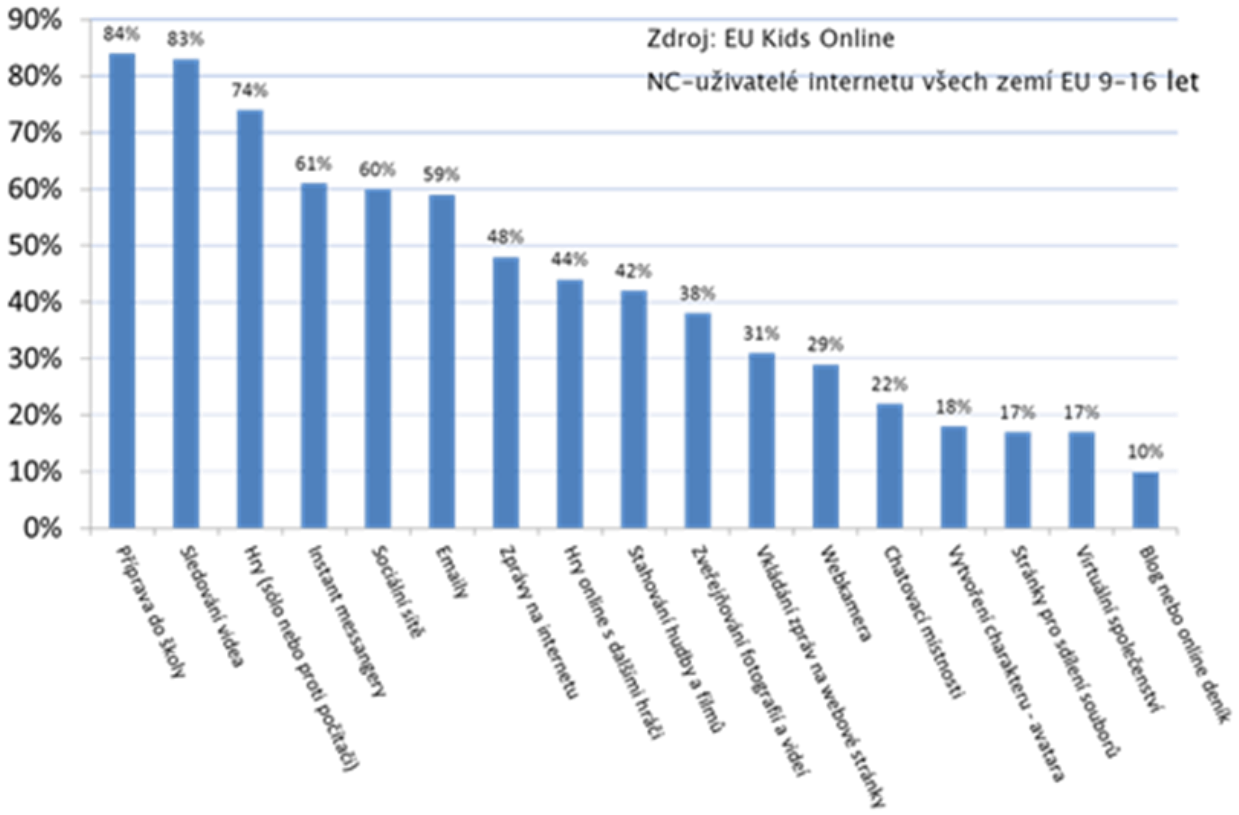
Děti a internet

Naprostá většina dnešních dětí má přístup na internet, ve škole i doma. Doma se k internetu většinou i připojují, a to prostřednictvím počítače, mobilního telefonu, tabletu či herní konzole. Podle celoevropského výzkumu EU Kids online (2011), který probíhal ve 25 evropských zemích včetně České republiky, stráví děti ve věku 9-16 let na internetu průměrně 88 minut denně. Nejvíce času tráví online děti v severských zemích, tradičně digitálně nejgramotnějších.

Pro preventivní, výukové i intervenční aktivity je důležité zamyslet se a porozumět tomu, k jakým účelům a jak děti moderní technologie a internet používají a jak se jejich zvyklosti liší od zvyklostí dospělých uživatelů.

Aktivity dětí na internetu napříč celou Evropou zmapoval mezinárodní výzkum EU Kids online, kterého se účastnila i Česká republika. K jakým účelům evropské děti v roce 2011 používaly internet, ukazuje následující obrázek:

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.



Obrázek: Livingstone, S.; Haddon, L., Görzig, A., and Olafson, K. (2011). Risks and safety on the internet: The perspective of European Children. Full Finding. LSE, London: EU Kids online

Možná se teď poučený pedagog diví a nevěří… na prvním místě studium a práce do školy? Můžeme se domnívat, že jsou výsledky trochu ovlivněny metodologií sběru dat – informace poskytovaly děti samotné. Na druhou stranu je pravdou, že v současnosti je internet (wikipedie) nejpoužívanějším zdrojem při přípravě do školy. Knihy, encyklopedie nezažívají nejlepší období. Výsledky se tedy mnoho neliší od skutečnosti.

Na aktivity dětí na internetu lze také pohlížet z hlediska jejich vývojových, psychologických a sociálních potřeb. A internet jim pomáhá mnoho z nich naplňovat či substituovat vhodnější naplnění.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Internet a dětské potřeby

Internet a online aplikace mohou rezonovat mnoho přirozených dětských potřeb. Je to jeden z jeho největších přínosů a jedno z největších rizik. K čemu současným dětem internet pomáhá?

Jedním z nejdůležitějších vývojových úkolů v období dospívání je budování vlastní identity. Identitu si mladý člověk vytváří kromě jiného na základě zpětné vazby okolí, především vrstevníků. Zpětnou vazbu potřebuje a vyhledává více než jindy. Sociální sítě a další komunikační nástroje umožňují nebývalým způsobem vlastní prezentaci a masivní zpětnou vazbu. Dospívající na internetu vyhledávají příležitosti ke komunikaci, vytvářejí si nové vztahy, experimentují se sebeobrazem a ochotně jej vysílají do světa. Na rozdíl od dnešních dospělých, nerozlišují komunikaci a vztahy na virtuální a skutečné. Komunikace a vztahy uskutečňované online jsou pro ně stejně reálné a důležité, jako ty tváří v tvář.

Zjednodušeně se dá říci, že internet a jeho aplikace pomáhají naplňovat přirozené potřeby mladých uživatelů. Z titulu věku jsou však také zvýšeně ohrožení. Pozornost věnují situaci tady a teď, budoucí dopady svého jednání příliš neřeší. Ke komunikaci přistupují nenuceně a neohroženě, s důvěrou. Ochotně poskytují osobní údaje, soukromé informace, fotografie. Experimentují se sexualitou, ve zdánlivě anonymním prostředí internetu snadněji, než v kontaktu osobním. Jsou kritičtí, neváhají zveřejňovat nekonformní názory, mají tendenci k radikálnímu hodnocení a řešení. To vše v prostředí internetu.

Děti testují hranice… na internetu

Dětství a dospívání je obdobím vytváření a upevňování představ o světě a sobě. Tomu napomáhá testování a nastavování hranic.
V sociálním ohledu jde o hranice práv mých a práv ostatních, přijatelného a nepřijatelného, vlastních dovedností a dovedností těch druhých… zkrátka co, jak a kam až mohu….
Od hranic se odvíjí subjektivní vnímání vlastní pozice, kompetencí a možností ve vztahu k okolnímu světu. A internet je pro mnoho dětí vítaným a častým cvičištěm.
Děti testují na internetu své i cizí hranice

- hraním her (online hry, hraní rolí),
- hledáním obsahu, který není určen jejich věku,
- vytvářením a úpravami videí a fotografií,
- šířením provokativních názorů,
- experimentem s navazováním vztahů a sexualitou.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Děti se baví…na internetu

Hrát si a hrát…. Hlavní úkol dětství, kdekoli a kdykoli to jde. Jak si hrají a baví se děti na internetu?

- Hrají hry (rolové hry, online hry s ostatními, např. World of Warcraft i samy, např. na hraj.cz)
- Sledují videa na portálech pro sdílení videí (You Tube, Vimeo) nebo na sociálních sítích
- Sdílejí a poslouchají hudbu (You Tube, SoundCloud, MySpace).

Děti hledají identitu…. na internetu

Identitu si dítě vytváří především na základě zpětné vazby okolí. Internet poskytuje nebývalou možnost okamžité zpětné vazby obrovského publika. Internet umožňuje vytvářet a testovat nejrůznější varianty sebeprezentace a tím i identity. Dítě navíc v kybersvětě může vytvořit a otestovat identitu zcela fiktivní. Jak se prezentují děti a mladí lidé na internetu?

- Vytvářejí profily v sociálních sítích,
- sdílejí fotografie,
- zveřejňují videa,
- vytvářejí si své virtuální herní postavy,
- hrají hry, které jim umožňují zkoušet si různé role,
- komunikují anonymně,
- píší veřejně přístupné deníky a blogy.

Děti komunikují…. na internetu

Doba, ve které začínají děti aktivně, pravidelně a samostatně používat internet a mobilní technologie se překrývá s obdobím, kdy pro ně začínají být zásadně významné vztahy s vrstevníky a kdy se vytváří a upevňují sociální dovednosti ve vztahu k širší společnosti. Proto patří komunikátory k nejužívanějším aplikacím. Jak komunikují děti a mladiství na internetu?

- Posílají krátké zprávy prostřednictvím služeb instant messagingu např. Skype, ICQ, nebo přes sociální sítě (SNSs), např. Facebook, Lidé.cz, Spolužáci,
- Chatují, např. xchat, lidé.cz,

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- posílají adresné zprávy a e-maily,
- vkládají příspěvky na „zdi“ svých přátel,
- hrají hry na hrdiny (tzv. rolové hry),
- debatují na internetových fórech zabývajících se jejich zájmy nebo problémy.

Děti pátrají.... na internetu

Nikdy nebylo snazší dostat se k informacím prakticky o čemkoli. To je báječné pro hloubavé studenty stejně, jako pro lenochy. Jak loví děti informace?

- Přes internetové vyhledavače, např. Google, Yahoo,
- v prostředích tzv. walled garden, např. Alík.cz,
- prostřednictvím příspěvků přátel v sociálních sítích,
- v internetových platformách, které se zabývají jejich osobními zájmy nebo problémy.

Photos: © Klaus-Peter Adler, © Robert Kneschke, © Dream-Emotion, © caruso13, © Andreas Wolf – all Fotolia.com, vzdělávací program projektu SocialWeb – SocialWork, 2012.

Když internet naplňuje potřeby více než blízcí lidé

Předchozí generace vyrůstaly v mnohem užším vzájemném kontaktu s vrstevníky, se stejnou generací - potkávaly se při společných hrách ve vesnickém prostředí nebo i v městských vnitroblocích, docházely do sportovních oddílů v místě bydliště, jezdily na tábory se spolužáky, na školních akcích se potkávaly na pokojích (výlety, lyžařské výcviky), vzájemná komunikace i komunikace s dospělými byla mnohem rozvinutější, bohatší, košatější.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Současná generace se tímto způsobem stýká méně, děti jsou častěji uzavřeny v bytech na sídlištích, rodinných domech v satelitních sídlištích, docházejí do kroužků nebo sportovních oddílů často velmi vzdálených nebo pouze individuálně zaměřených. Výlety, školy v přírodě, lyžařské výcviky jsou pro mnoho dětí z důvodu nedostatku financí nedostupné. Potřebu vzájemné komunikace a s ní spojené zpětné vazby ale mají stejnou jako předchozí generace. Tato separace a z toho plynoucí možná psychická deprivace je vedou k využívání dostupných komunikačních kanálů jako je internet, které jsou ale otevřené prakticky všem a není možno bezpečně určit, kdo se nalézá na druhé straně, čímž se samozřejmě zvyšuje míra možného ohrožení.

Psychické potřeby dítěte jsou bezpochyby nejvíce uspokojovány každodenním stykem s co nejširším a nejrůznorodějším sociálním prostředím. Když dítě nemá dostatek příležitostí k vlastní prezentaci a k přirozené interakci v osobním kontaktu, snaží se najít jiné dostupné prostředky k zajištění těchto potřeb. Často tak učiní třeba prostřednictvím internetu, aniž by si uvědomilo příslušná rizika, nebezpečí a možnosti snadného ohrožení či přímo napadení.

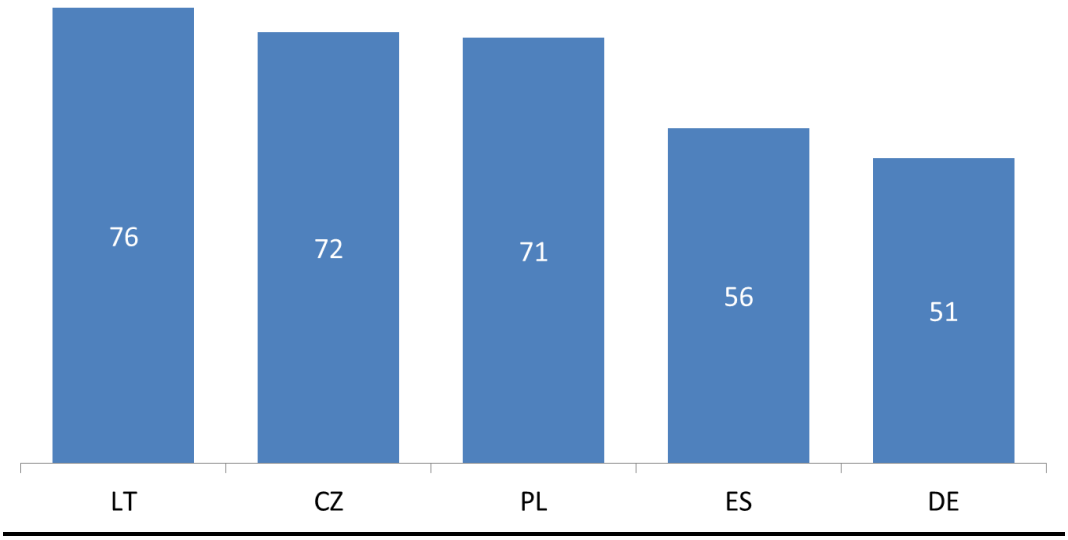
V extrémních případech internetové společenství a aktivity zcela nahradí přirozenou podporu rodiny a přátel. O takovém odcizení a útěku mladého člověka do virtuální komunity vypráví polský film Místnost sebevrahů režiséra Jana Komasy, 2011.

Sociální sítě pro pedagogy

Sociální sítí se nazývá internetová služba, která registrovaným členům umožňuje vytvářet si osobní (či firemní) veřejný či částečně veřejný profil, komunikovat s dalšími účastníky, sdílet informace, fotografie, videa, provozovat chat a další aktivity. Zásadní rozdíl mezi klasickým webem a sociálními sítěmi spočívá v tom, že u sociálních sítí uživatelé sami vytváří a sdílí obsah a komunikují o něm.

Děti, které mají profil na sociální síti napříč Evropou (z těch, co používají internet, 9-16 let):

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.



Livingstone, S.; Haddon, L., Görzig, A., and Olafson, K. (2011). Risks and safety on the internet: The perspective of European Children. Full Finding. LSE, London: EU Kids online

Zakázat dítěti mladšímu 13 let Facebook?

Užívání sociálních sítí je pro dnešní děti samozřejmostí a nehraje ani tak roli, zda je dítě začne používat ve dvanácti nebo ve čtrnácti letech, ale je-li dostatečně sociálně zralé a dostatečně informované.

Ve většině případů děti používají profil opravdu ke komunikaci a sdílení s vrstevníky, které znají. Nemají-li profil, vyčleňují se ze své sociální skupiny. S radikálním zákazem rodiče moc nepochodí - dítěti bude připadat Facebook o to více atraktivní a pořídí si profil tajně. Rodič se pak ocitne v horší situaci, než kdyby profil povolil, protože pokud se dítě dostane do problémů, nebude se mu chtít svěřit – žádný profil přece nemá.

Na druhou stranu má věková hranice 13-ti let pro uživatele Facebooku svůj význam.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Fatální rizika však spočívají nikoli ve Facebooku jako takovém, ale zejména v neinformovanosti dětských i dospělých uživatelů o jeho bezpečném používání a správném, tj. neveřejném nastavení profilu. Rodiče nestanovují pravidla a hranice, nesledují aktivity dětí na síti, neumí je varovat. Měli by se aktivně se zajímat o to, s kým se děti přátelí a jaké fotografie či videa na svůj profil dávají. Kromě standardních rizik s sebou profil na Facebooku nese zbytečně ranou konfrontaci dítěte s komerčním prostředím cílené reklamy, které je toto médium plné.

Rizika spojená s užíváním internetu

Na dítě číhá na internetu mnoho nástrah. Detailně je probíráme v tematicky zaměřených metodických materiálech. Zde si pro přehled uvedeme základní typy rizikových jevů a kriminality spojených s užíváním internetu a mobilních technologií. U každého z jevů shrneme přehled toho, co by žáci měli znát, jako opora pro začlenění tématu do výuky a preventivních snah.

Hrozby jsou spojené jednak se závadovým jednáním uživatelů, jednak se závadovým obsahem umisťovaným na internet. Dětského uživatele mohou ohrožovat především tyto jevy:

- Nevhodný a nezákonný obsah
- Happy slapping
- Kybergrooming
- Sexting
- Kyberšikana
- Kyberstalking
- Online hraní a závislosti.

Nezákonný obsah na internetu

Nezákonný obsah na internetu je obsah ohrožující mravní výchovu mládeže, svádějící k zahálčivému nebo nemravnému životu, navádějící k morálnímu úpadku nebo páchání trestné činnosti. Je jím především:

- dětská a tvrdá pornografie
- zobrazování násilí (týrání osob, zvířat)
- extremismus, podněcování k nenávisti vůči jiným osobám
- schvalování trestného činu aj. (vč. ohrožování výchovy dítěte).

Nevhodný obsah na internetu

Nevhodný obsah je obsah sice legální, ale z hlediska psychologického a pedagogického pro děti a mládež nevhodný. Může se jednat např. o

- pornografii – zejména deviantní,
- zobrazení násilí (přímé zobrazení napadení nebo ponižování jiné osoby, extrémní akční filmy, některé typy her),

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- online sázkové hry,
- nenávistné a netolerantní projevy,
- pro-Ana weby, proMia, sebepoškozování a propagující sebevraždu.

Co by měli Vaši žáci vědět?

- ✓ Ne všechno, co najdeme na internetu, je hodnotné.
- ✓ Na internetu se objevuje i materiál (texty, fotografie, videa), který je zákonem zakázaný.
- ✓ Na internet může kdokoliv vkládat cokoliv.
- ✓ Podobně jako v novinách nebo v televizi není dovolené ani na internetu šířit nezákonný obsah.
- ✓ Na internetu nesmí být zveřejněny, zprostředkovány, nabídnuty, uvedeny do oběhu ani jinak zpřístupněny žádné materiály zobrazující děti do 18ti let odhalené, v erotických situacích.
- ✓ Na internetu nesmí být propagováno hnutí a názory, které směřují k potlačení práv a svobod člověka, nebo hlásají rasovou, etnickou, národnostní, náboženskou či třídní zášť nebo zášť vůči jiné skupině osob.
- ✓ Na internetu je nezákonné zobrazování násilí (týrání osob).
- ✓ Nesmí být veřejně (tedy např. na internetu) surovým nebo trýznivým způsobem týráno zvíře.
- ✓ Na internetu je nezákonné schvalování trestného činu.
- ✓ Nelegální je obchodování, nabídka drog a zakázaných látek.

Když dítě obsah na internetu vyděsí, mělo by vědět, že…

- ✓ Nemusí být vystaveno obsahu, který je pro něj děsivý, odporný či nepochopitelný.
- ✓ Může zaklapnout notebook, vypnout obrazovku.
- ✓ Má-li pocit, že narazilo na něco, co je zákonem zakázáno nebo je nebezpečné, je nejlepší svěřit se dospělému, kterému důvěřuje, a to i v případě, že v něm obsah vyvolává pocity studu.
- ✓ Závadný a nezákonný obsah lze ohlásit několika cestami.

Prostřednictvím formuláře či e-mailu lze závadný a nezákonný obsah lze nahlásit např. Horké lince. Hlášení je anonymní.

www.horkalinka.cz

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Happy slapping

Jako happy slapping je označováno natáčení reálného fyzického napadení oběti a jeho umístění na internet. Může být začátkem nebo extrémním projevem kyberšikany, ale rozdíl bývá v motivaci pachatele. U happy slappingu může jít o snahu získat co „nejexkluzivnější“, šokující, brutální materiál. Proto natáčení takovýchto videí bývá iniciačním rituálem pro přijetí do různých mladistvých gangů. Oběť je často náhodná, zpravidla bez předchozího vztahu s pachatelem. Ve Francii je Happy Slapping trestným činem od roku 2007, v Anglii byl první rozsudek za happy slappingový útok vynesen v roce 2008.

Co by měli Vaši žáci vědět?

V ČR není happy slappingové jednání samostatným trestným činem, není ale ani beztrestné. Může být kvalifikováno a postihováno například jako těžké ublížení na zdraví (při ochrnutí aj. podobném dopadu), nepřekažení trestného činu a neoznámení trestného činu (ze strany komplice), následně neposkytnutí první pomoci.

Kybergrooming

Kybergrooming je psychická manipulace dítětem prostřednictvím moderních komunikačních technologií s cílem využít dítě k uspokojení vlastních zájmů, zpravidla sexuálních. Zbraní groomera je postupné budování důvěry a citové vazby. Tito internetoví lovci se snaží vylákat dítě na osobní schůzku, která může skončit sexuálním nátlakem, pohlavním zneužitím, znásilněním, zneužitím dítěte k výrobě pornografie, přinucením k prostituci, zavlečením mimo území ČR (obchod s „bílým masem“). Postižitelnost pachatelů je problematická. Obětí může být v podstatě kterékoli dítě používající internet a mobilní technologie. Zvýšeně ohrožené mohou být osamělé děti, které strádají nedostatkem lásky a pozornosti, mají sníženou sebeúctu a trpí nedostatkem sebedůvěry.

Kybergoomer bývá vytrvalý manipulátor, jde si za svým cílem plánovitě a bezohledně, s obětí nemá soucit, neváhá ji vydírat, zastrašovat. Používá rafinované manipulační techniky: zrcadlí, slibuje dítěti věčné přátelství a lásku, posílá dárky a uplácí, láká soukromé a intimní věci, vyžaduje lechtivé a erotické fotografie a komunikaci, žádá, aby dítě komunikaci utajil/a, hanobí rodiče a vyhrožuje, pokud dítě něco odmítá.

Co by měli Vaši žáci vědět?

- ✓ Na internetu jsou lidé, kteří se snaží zneužívat děti a mladé lidi pro své vlastní záměry.
- ✓ Často skrývají svou pravou identitu.
- ✓ Použijí cizí fotografie, založí si falešný profil, vystupují jako vrstevníci.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- ✓ Na chatech jsou zpočátku velmi přátelští, ale mají zlé úmysly.
- ✓ Kybergroomer je internetový útočník, který zneužívá internet a online komunikaci k manipulaci s dětskými uživateli.
- ✓ Snaží se vylákat dítě/mladého člověka na osobní schůzku a tam mu ublížit (sexuálně, fyzicky).
- ✓ Bývá zdatným psychologem a jeho záměry je zpravidla těžké od počátku odhalit.
- ✓ S obětí nemá soucit, neváhá ji vydírat, zastrašovat.
- ✓ Kybergroomer brouzdá po Facebooku, Lidé.cz, Badoo.com a dalších sociálních sítích.
- ✓ Otevřené a veřejné profily jsou pro něj snadnou kořistí.
- ✓ Vstupuje do chatovacích místností, a zvláště těch, které jsou určeny mladým lidem
- ✓ Nevyhýbá se ani výhradně dětským webům.
- ✓ Čím více osobních informací má internetový útočník k dispozici, tím snazší je pro něj oběť oslovit a najít ji v reálném prostředí.
- ✓ Osobní a citlivé a soukromé informace jsou pro útočníka silnou zbraní.
- ✓ Může Tě kontaktovat na internetu, telefonu, vyhledat osobně, vydírat.
- ✓ Při komunikaci na internetu nikdy nikomu cizímu nesděluj nic, na základě čeho by tě mohl vystopovat.
- ✓ Své profily v sociálních sítích si pečlivě zabezpeč tak, aby cizí lidé neměli přístup k tvým kontaktním údajům, fotografiím a dalším informacím o tvém soukromí.
- ✓ Pamatuj, že ani dobře nastavené profily nezaručí 100% ochranu Tvých údajů a soukromí.
- ✓ Buď opatrný/á, než někomu dáš své telefonní číslo.

Co by dítě mělo vědět, když neví, kdo mu píše…

- ✓ Ověř si identitu
- ✓ Požádej kamaráda z internetu, aby ti zaslal svoji aktuální fotografii, kde splní nějaké tvé pokyny (např. pozici, vzkaz se Tvým jménem a určeným datem).
- ✓ Komunikaci s cizími lidmi na internetu neutajuj!
- ✓ Pokud Tě někdo na internetu žádá, abys o Vaší komunikaci nikomu neříkal/a, svědčí to o nedobrých úmyslech. Nikdy takovou komunikaci před svými rodiči netaj, nemohli by třeba včas pomoci.
- ✓ Neposílej intimní a erotické fotografie a videa!
- ✓ Mohou být zneužity k vydírání, umístěny na pornografických webech, zveřejněny.
- ✓ Nevydávej se na schůzku s neznámými lidmi z internetu! A už vůbec ne sám/sama.
- ✓ I v ČR jsou případy, které skončily znásilněním či vraždou.

Co by dítě mělo vědět, když se bojí toho, kdo mu píše….

- ✓ Zablokuj útočníka!

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Většina seriózních internetových služeb a mobilních operátorů umožňuje blokovat ohrožujícího uživatele

- ✓ Neposlouchej a řekni ne!
  Neboj se odmítnout, žádá-li po Tobě na internetu něco, do čeho se ti nechce (zaslání fotografií, téma, schůzku).
- ✓ Neodpovídej!
  Na to právě útočník čeká…
- ✓ Ulož zraňující či vydírající zprávy a online obsah jako důkaz
  Pomůže to ilustrovat, co se děje, lze použít jako podklad pro pomoc rodičů, školy, provozovatele, případně Policie.
- ✓ Svěř se!
  I když je to nepříjemné, i když se třeba stydíš za zveřejněný obsah či komunikaci. Špatný je ten, kdo manipuluje, uvádí v omyl a chce ublížit. Svěř se rodičům či jinému dospělému.

Co by mělo dítě vědět o pomoci….

- ✓ Máš právo na pomoc a ochranu, když tě někdo obtěžuje nebo ohrožuje.
- ✓ Svěř se dospělému, kterému důvěřuješ.
- ✓ Hledej pomoc ve škole. Výchovný poradce, metodik prevence nebo školní psycholog by měli poskytnout podporu a zprostředkovat pomoc.
- ✓ Kontaktuj policii. Oddělení informační kriminality je např. na Policejním prezidiu ČR.
- ✓ Policejní Horká linka může zahájit vyšetřování a zastavit pachatele.
  http://aplikace.policie.cz/hotline/
- ✓ Linka bezpečí má zkušené pracovníky, kteří pomohou i v případě elektronického násilí (www.pomoc-online.cz) 116 111, http://www.linkabezpeci.cz/webmagazine/home.asp
- ✓ Dětské krizové centrum má Linku důvěry, kde Ti poradí zkušení odborníci. Non stop linka důvěry 241 484 149, http://www.ditekrize.cz/linka-duvery
- ✓ Horká linka Ti může pomoci se zajištěním důkazů či blokováním útočníka. www.horka-linka.cz
- ✓ Sdružení proti šikaně má poradenskou linku, kde se můžeš také obrátit pro pomoc.

Sexting

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Sextingem rozumíme elektronické zasílání zpráv, obrázků a videí se sexuálním a erotickým obsahem. Fotografie či videozáznam je osobní údaj chráněný zákonem.
Na internetu, jakmile jsou odeslány či uploadovány na internet, žijí svým vlastním životem a nekontrolovaně se šíří. Jejich původce či zobrazená osoba nikdy neví, kdo je uvidí a jak s nimi naloží. Intimní komunikace se snadno přemění v nástroj pomsty, vydírání či veřejného posměchu V USA je sexting trestným činem (mladiství odesílající sexuálně orientovaní se stávají sexuálními delikventy s trvalým záznamem).

Co by měli Vaši žáci vědět?

- ✓ Na svých stránkách, v profilech v sociálních sítích ani kdekoliv jinde na internetu nikdy nezveřejňuj intimní fotografie nebo videa ani např. fotky v plavkách.
- ✓ S webkamerou zacházej velmi opatrně! Používej ji jen v případě, že si jsi naprosto jistý/á, s kým si povídáš, např. při telefonování přes Skype se spolužákem.
- ✓ Při komunikaci ve veřejném chatu nebo v kontaktu s lidmi, které neznáš z reálného života, ji nech raději vypnutou.
- ✓ V žádném případě se před webkamerou nesvlékej.

Kyberšikana

Kyberšikana je jednou z forem psychické šikany. O kyberšikaně hovoříme, pokud agresor oběť úmyslně, zpravidla opakovaně ohrožuje, pronásleduje a týrá psychicky a zneužívá k tomu moderní komunikační nástroje a internet. Primárním cílem útočníka je ublížit oběti. Současné výzkumy uvádí, že zhruba každé desáté české dítě zažilo kyberšikanu jako oběť (podrobně v tematickém materiálu „Elektronická šikana ve školním prostředí, NCBI, 2012).

Kyberšikana a školní šikana se zpravidla prolínají. Kyberútoky u školních dětí proto nelze řešit odděleně, jako ojedinělou událost. Je třeba je posuzovat jako možný ukazatel různě rozvinuté šikany školní.

K elektronické šikaně jsou zneužívány všechny dostupné komunikační kanály. Děti se trápí zasíláním výhružných a urážlivých SMS, opakovaným prozváněním, nepříjemnými hovory. Fotografují a natáčí dehonestující videa a vystavují a sdílejí je na videoportálech a sociálních sítích. Stále častějším jsou online petice a hlasování, falešné profily a webové stránky a další zbraně.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Co by měl pedagog vědět?

- ✓ Oběti kyberšikany se zpravidla dlouho nesvěřují.
- ✓ Nikdo ze zúčastněných nemá zájem na zveřejnění.
- ✓ Nemá smysl říkat dítěti, aby bylo odvážné a samo se bránilo.
- ✓ Výskyt kyberšikany není tolik projevem selhání pedagoga či školy, jako její popření a neřešení.
- ✓ Základem je podpora, řešení musí být soukromé a chránit oběť a svědky.
- ✓ Nikdy nekonfrontujeme oběť s agresory.
- ✓ Kyberšikana a školní šikana jsou složité fenomény, které mají svůj vývoj. Neřešené mohou narůst do fatálních projevů a důsledků

Co by měli Vaši žáci vědět?

- ✓ Ten, kdo někomu úmyslně ubližuje, zesměšňuje ho, vysmívá se mu, vyhrožuje mu, obtěžuje ho či pronásleduje a požívá k tomu mobilní zařízení a internet, se dopouští kyberšikany.
- ✓ Kyberšikana je šikana.Šikana je nepřijatelná.
- ✓ Kyberšikanující aktivity mohou být kvalifikovány jako trestný čin.
- ✓ Děláš si na internetu legraci z ostatních? Pamatuj, že nikdy nevíš, jak mohou Tvé zprávy působit a nakolik mohou ublížit.
- ✓ Posílej jen takové zprávy a obrázky, o kterých 100% víš, že nemohou nikoho zranit.
- ✓ Chovej se na internetu tak, jak by se ti líbilo, aby se ostatní chovali k Tobě.
- ✓ Vždycky požádej o svolení, chceš-li někoho fotografovat či jeho fotografii zveřejnit.
- ✓ Pokud obdržíš posměšnou zprávu o někom druhém, nesdílej ji či nepřeposílej dál. Mohl/a by ses podílet na kyberšikaně. Kyberšikanou se můžeš dopustit trestného činu.

Co by měli Vaši žáci vědět o ochraně hesel…

- ✓ Svá hesla nikomu nedávej. Ani nejbližším kamarádům. Heslo je jako zubní kartáček, nikomu se nepůjčuje.
- ✓ Zvol si bezpečné heslo, ochráníš tak svůj účet před krádeží.
- ✓ Vol kombinace čísel, znaků, nespojuj je se svými oblíbenými činnostmi. Jako heslo můžeš zvolit i větu.
- ✓ Jsou případy, kdy šikanující útočník rozesílá sprosté nebo nepravdivé zprávy z účtu oběti, do kterého se vloupal. Oběť pak vypadá jako pachatel.
- ✓ Ochrana hesla je ochrana před zneužitím mailu, mobilu, profilu na Facebooku.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Co by měli Vaši žáci vědět, když jim někdo ubližuje online…

- ✓ Máš právo na pomoc a ochranu, když tě někdo obtěžuje nebo šikanuje online.
- ✓ Zablokuj útočníka!
  Většina seriózních internetových služeb a mobilních operátorů umožňuje blokovat ohrožujícího uživatele (Skype, Facebook, Google +, mobilní čísla).
- ✓ Neodpovídej!
  Na to právě útočník čeká…
- ✓ Ulož zraňující zprávy a online obsah jako důkaz.
  Pomůže to ilustrovat, co se děje, lze použít jako podklad pro pomoc rodičů, školy, provozovatele, případně Policie.
- ✓ Svěř se!
  I když je to nepříjemné. Špatný je ten, kdo ubližuje, ne ten, kdo hledá pomoc!

Co by měli Vaši žáci vědět o pomoci…

- ✓ Dětské krizové centrum má Linku důvěry, kde Ti poradí zkušení odborníci. Non stop linka důvěry 241 484 149, http://www.ditekrize.cz/linka-duvery.
- ✓ Horká linka Ti může pomoci se stažením falešného nebo ubližujícího profilu na Facebooku či jinde na internetu či blokováním útočníka. www.horka-linka.cz.
- ✓ Policejní Horká linka může zahájit vyšetřování a zastavit pachatele. http://aplikace.policie.cz/hotline/.
- ✓ Sdružení proti šikaně má poradenskou linku, kde se můžeš také obrátit pro pomoc.

Kyberstalking

Kyberstalking znamená dlouhodobé pronásledování konkrétní oběti prostřednictvím moderních technologií, především zasíláním sms a mailů. Kyberstalker oběť pronásleduje, obtěžuje, vyhrožuje jí nebo jí blízkým osobám a vyvolává v ní tak pocity strachu a omezuje ji. Bývá prostředkem týrání v rámci šikany a kyberšikany

Co by měli Vaši žáci vědět?

Stalking je zakotven v trestním zákoně a je trestným činem (nebezpečné pronásledování, § 354 TZ).

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Online hraní a závislosti

Online hry jsou zejména u chlapců značně rozšířeny. Pokud hry nezobrazují extrémní násilí, nevhodný erotický obsah apod., nejsou samy o sobě špatnou volnočasovou aktivitou. Řada moderních her rozvíjí dovednosti, některé i znalosti. Problém nastává, pokud hraní dítě začne pohlcovat, stává se jedinou aktivitou, u které prožívá uspokojení. V současné chvíli není online závislost kvalifikována jako nemoc, nicméně v americké klasifikaci nemocí (DSM – IV) se již připravuje nová kategorie.

Kdy bychom měli zpozornět? Čas strávený hraním jde na úkor jiných činností – studium, kontakty s přáteli, sportovní, společenské nebo kulturní aktivity, atd. Prostřednictvím hry se dítě vzdaluje realitě, přestává mít zájem o své přátele a kontakty. Přestává spát, hraje i o nocích, zapomíná na tělesné potřeby.
Stejně jako u jiných závislostí jde u nadměrného hraní či jiného užívání internetu o projev jiného, primárního problému. Hraje-li dítě přespříliš, je potřeba pátrat a snažit se o řešení tohoto základního problému. Závislost může být reakcí na opakující se neúspěch a problémy s okolím – k řešení proto nestačí zakázat počítač.

Přehledové list pro žáky

V přehledu základních rizik pro dětské uživatele internetu jsme uváděli přehled toho základního, co by žáci měli vědět, aby jejich surfování bylo bezpečnější. Zkuste spolu s žáky sestavit přehledové listy těchto základních pravidel. Ideální je, pokud je zformulují sami.

Obrázek: přehledové listy pro žáky základních škol vytvořené v komunitním projektu Praha bezpečně online, NCBI, 2012.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Trestněprávní postih dětí a mladistvých

Děti do 15 let nejsou sice odpovědné trestně ani za přestupek, avšak nejsou ani „beztrestné“. Dopustí-li se činu jinak trestného, může jim soud uložit 1 či více tzv. opatření.

V 15-18 letech se dítě nazývá mladistvým, stává se odpovědným za přestupek a je-li dostatečně rozumově a mravně vyspělé, aby mohlo rozpoznat protiprávnost svého jednání nebo ho ovládat, pak i trestně odpovědným. Jím spáchaný trestný čin se nazývá provinění a soud za něj může uložit některé z výchovných (např. napomenutí s výstrahou), ochranných (např. zabrání věci) nebo trestních opatření (např. obecně prospěšné práce nebo odnětí svobody).

Není-li mladistvý dostatečně rozumově a mravně vyspělý, může mu soud uložit za čin jinak trestný ochranné opatření nebo takové opatření k nápravě, které lze uložit dítěti mladšímu 15 let.

Ještě krátce po dosažení 18 let je případné spáchání trestného činu takzvaně ve věku blízkém věku mladistvých polehčující okolností při ukládání trestu.

Opatření ukládaná dětem mladším 15 let	Výchovná opatření	Ochranná opatření	Trestní opatření
Výchovnou povinnost	Dohled probačního úředníka	Ochranné léčení	Obecně prospěšné práce
Výchovné omezení	Probační program	Zabezpečovací detence	Peněžité opatření
Napomenutí s výstrahou	Výchovné povinnosti	Zabrání věci nebo jiné majetkové hodnoty	Peněžité opatření s podmíněným odkladem výkonu
Zařazení do terapeutického, psychologického nebo jiného vhodného výchovného programu ve středisku výchovné péče	Výchovná omezení	Ochranná výchova	Propadnutí věci nebo jiné majetkové hodnoty
Dohled probačního	Napomenutí		Zákaz činnosti

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

úředníka	s výstrahou		
Ochrannou výchovu			Vyhoštění
Ochranné léčení			Domácí vězení
			Zákaz vstupu na sportovní, kulturní a jiné společenské akce
			Odnětí svobody podmíněně odložené na zkušební dobu (podmíněné odsouzení)
			Odnětí svobody podmíněně odložené na zkušební dobu s dohledem
			Odnětí svobody nepodmíněné

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Online anonymita

Kontakt mezi lidmi se ještě nikdy nezdál tak jednoduchý. Díky online aplikacím je možné si kdykoliv povídat s lidmi z druhého konce světa. Nové komunikační technologie odstranily nejen fyzické, ale i psychologické bariéry: v online komunikaci si lidé dovolí více než při kontaktu tváří v tvář. Jsou otevřenější, upřímnější a troufnou si odhalit detaily ze svého soukromí i lidem úplně cizím. Je to paradox, protože právě na internetu si nikdy nemůžeme být jistí tím, kdo je ve skutečnosti na druhé straně.
V prostředí online komunikace je jednoduché vydávat se za někoho jiného, každá z aplikací totiž poskytuje svým uživatelům určitou míru anonymity:

Veřejné chatovací místnosti – patří k nejrizikovějším komunikačním platformám kvůli vysoké míře anonymity, jejich používání postupně ustupuje sociálním sítím. Přihlášení do chatovacích místností je jednoduché a účelem bývá komunikace a seznámení se lidí, kteří se nikdy předtím neviděli. Chatující většinou nemá možnost ovlivnit, kdo všechno se v chatovací místnosti objeví, ani případně zablokovat obtěžujícího uživatele. Právě v chatovacích místnostech a diskusních fórech mohou agresoři snadno vyhledávat např. oběti pozdějšího kybergroomingu. Chatovací aplikace jsou běžně integrované i v sociálních sítích nebo emailech. ***U nás se nejvíce chatuje na: xchat.cz, Lidé.cz, Líbímseti.cz a nejrůznějších online seznamkách.***

Mobilní telefony - mobilní kontakty obvykle mezi sebou sdílí lidé, kteří se dobře znají. V takovém případě nepředstavuje mobilní telefon zásadnější hrozbu. Pokud se ale číslo mobilního telefonu dostane do ruky cizímu člověku (potenciálnímu agresorovi), komunikace přes mobil se snadno stane důležitým prostředkem navazování intimního vztahu, sexuálně laděné komunikace, lákání na schůzku nebo posílání nevyžádaných zpráv a dalšího obtěžování.

E-Maily - obtěžování, intimní komunikace a lákání k osobnímu setkání může probíhat i prostřednictvím e-mailu. I v tomto případě ale jen za předpokladu, že se e-mailová adresa k agresorovi předtím dostala - buď ji mohl vyčíst např. z profilu v sociální síti, anebo mu ji jeho oběť sdělila dobrovolně - např. v chatu.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Instant Messengery/komunikátory - podle výsledků výzkumu EU Kids online jsou komunikátory prostředkem, kde se nejmladší děti do 10 let seznamují s lidmi, s nimiž se následně setkají osobně. Ve srovnání s veřejnými chatovacími místnostmi sice uživatel má větší vliv na to, s kým komunikuje a může např. zablokovat obtěžující uživatele, ale vzhledem k tomu, že v rámci těchto aplikací často komunikují lidé, kteří se v reálném životě neznají, je zde vysoká hrozba rozvinutí rizikové komunikace s potencionálním agresorem.V ČR jsou rozšířenými komunikátory ICQ nebo např. Skype.

Sociální sítě - z hlediska kybergroomingu představují stále větší hrozbu - podle výsledků výzkumu EU Kids online se totiž děti mezi 9 a 16 lety právě v sociálních sítích nejčastěji seznamují s lidmi, se kterými se později potkávají i tváří v tvář. Seznámení usnadňují profily, kde uživatelé často zcela veřejně poskytují kontaktní údaje, osobní fotografie a informace o svých zvyklostech, které je snadné následně zneužít. V sociálních sítích je také jednoduché vytvořit falešný profil, pomocí něhož agresor vydávající se za někoho jiného naváže důvěrný vztah se svou obětí. Na konci někdy i měsíce trvající komunikace může být osobní setkání s tragickými důsledky. U nás je nejpoužívanější sociální sítí Facebook.com, mezi dospívajícími jsou oblíbené například i sítě Lidé.cz nebo Líbímseti.cz.

Tabu informace

Pravidla ochrany soukromí a základní opatrnost platí i na internetu. Stejně jako by na ulici děti neměly nikomu říkat, kde bydlí, nebo bez uvážení rozdávat svoje telefonní číslo, úsporné ve sdělování osobních informací by měly být i při online komunikaci.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Jednoznačně nebezpečné a primárně ohrožující je sdělovat komukoliv na internetu informaci o místě bydliště, celé jméno, hesla k emailům a profilům v sociálních sítích nebo rodné číslo. Z počítače ani mobilu dítěte by nikdy neměly putovat intimní fotografie nebo videa.

Číslo mobilního telefonu by se nemělo objevovat na veřejně přístupných místech – blozích nebo v otevřených profilech sociálních sítí. Sdělovat by ho děti měly jen lidem, které dobře znají. Informace o věku hlavně u menších dětí na internet nepatří, mohla by být příliš lákavá. Podobně jako vyzývavé fotky.

Mozaika informací

Informace, které o sobě lidé na internetu sdělují, se samy o sobě nemusejí zdát ohrožující, při troše úsilí ale bývá snadné z údajů poskládat celý obrázek o soukromí jednotlivce. Může stačit, že dítě ve svých statusech na sociální síti informuje o svých zvyklostech (v kolik hodin a kterým spojem jezdí do školy, jak tráví víkendy atp.) a zároveň se prezentuje prostřednictvím fotografií. Pro případného agresora potom není obtížné informace propojit a dítě fyzicky vyhledat. Velmi riskantní může být informování o majetkových poměrech rodiny, ať už prostřednictvím fotografií vybavení domácnosti nebo sdělováním informací o rodinných dovolenkových destinacích atp. Existují případy, kdy si agresor dítě vytipuje právě na základě těchto údajů, fyzicky ho napadne, případně unese a rodinu vydírá s cílem majetkově se obohatit.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Blogy, sociální sítě, instant messengery

Blogy a sociální sítě představují v současnosti hojně využívaný komunikační nástroj. Blog je obvykle webovou stránkou jednoho autora, který jejím prostřednictvím sdílí informace. Osobní blog může mít podobu deníku ze života autora, alba fotografií, receptů, zápisníku myšlenek, nebo třeba diskuse s návštěvníky blogu. V případě firemních blogů se sdílí např. i různé akční nabídky atp.

Sociální síť zpravidla nabízí určitou platformu pro vlastní blogy uživatelů zvaných profily - skýtá např. prostor pro nahrávání fotografií, sdílení informací, odkazů, novinek a diskuze s jinými uživateli. Zatímco blog slouží obvykle především k sebeprezentaci autora, sociální sítě ke vzájemné komunikaci uživatelů.

Tzv. instant messengery neboli komunikátory nabízí jakoby stupeň mezi e-mailem a chaty, blogy, sociálními sítěmi. Obvykle umožňuje vyhledávání a ukládání kontaktů na konkrétní osoby a následné sledování jejich přítomnosti. Je-li pak taková osoba tzv. on-line, je možné s ní začít ihned komunikovat bez přítomnosti dalších osob (vyjma těch, kdo jsou přizváni).

Co Vás identifikuje ve světě online

Aby bylo možné připojit se k internetu, je nutné použít nějaké síťové zařízení (např. síťová karta v počítači). Tzv. MAC adresa, kterou každému konkrétnímu síťovému zařízení přiděluje výrobce již při výrobě jako jedinečnou, se za normálních okolností nemění, pokud se uživatel sám nerozhodne ji změnit (to ovšem již vyžaduje určité znalosti z oblasti IT technologií).

Každé zařízení přistupující k internetu má pak svou tzv. IP adresu. Ta je opět vždy jedinečná, podobně jako např. otisky prstů. Na rozdíl od nich se však může v různých časových intervalech (např. po týdnu) měnit (tzv. plovoucí IP adresa), tedy jako by naše otisky prstů byly na rukavicích, které můžeme nosit stále stejné, anebo je čas od času vyměníme. IP adresu přiděluje poskytovatel internetu jako veřejnou (neměnná, jednoznačně identifikuje koncového uživatele) nebo neveřejnou (tzv. dynamická neboli plovoucí). V případě dynamických IP adres je poskytovatel internetu prostřednictvím svých serverů přiřazuje jednotlivým uživatelům ze souboru právě dostupných adres, jakoby následovně. Představme si společnost, mající k dispozici 100 aut s různými SPZ, ale stejné značky i barvy a opatřených logem společnosti. Kdykoliv může za společností přijít její klient s žádostí o užití auta (žádost o přístup na internet). Společnost mu obratem zapůjčí některé ze svých právě dostupných vozidel (přiřadí jeho zařízení IP adresu) a klient odjede (používá internet). Po tento čas ostatní lidé (uživatelé internetu) sice vidí daný vůz (vidí, kdo je poskytovatelem služby), ale již nerozpoznají, který klient právě vůz užívá (vidí IP adresu zařízení, ale tato je pouze dočasná). Jakmile auto vrátí (odpojí se od internetu), společnost má vůz opět k dispozici pro ostatní své klienty a je jen na ní, zda příště

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

přidělí dotyčnému opět zcela identický nebo jiný vůz. Proto může být komplikované zpětně dohledat spojení mezi konkrétní IP adresou a konkrétním koncovým zařízením, avšak není to nemožné. Jedno zařízení může mít současně přiřazeno více IP adres, ale žádná IP adresa se nevyskytuje současně u více zařízení.

Projektové vyučování online bezpečnosti

Projektová výuka je moderní pedagogickou alternativou. Je založená na projektové metodě, tedy systému činnosti žáka a pedagoga, kdy aktivní tvůrčí roli má žák, podporující a poradenské role se ujímá pedagog. Žák si obvykle vybírá téma svého projektu, vyhledává vlastní zdroje materiálů nutných pro řešení projektu, projekt řeší samostatně a sám také prezentuje závěrečný výsledek, čili produkt.

V souvislosti s výchovou k bezpečnému a etickému užívání internetu představuje projektová výuka, takřka ideální prostředek vedoucí ke třem cílům:

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

1) žákům poskytne potřebné vědomosti, které si snáze osvojí v důsledku vlastního aktivního přístupu při jejich vyhledávání
2) díky samostatné práci jim poskytne prostor k získání dovedností jak osvojené vědomosti užívat v praxi
3) v případě opakování projektů, nebo při realizaci dlouhodobého projektu má žák možnost dovednosti zautomatizovat do návyků

Systematická výchova k bezpečnému a etickému užívání v současné školní praxi chybí. Přitom tento typ výchovy má velký význam pro prevenci většiny, nejen kyberprostorových, sociálně patologických jevů. Mladá generace má ve stále větší míře kyberprostorové prožitky propojeny s prožitky běžné reality. IT komunikační styly se u ní promítají do běžné komunikace. Předpoklad, že slušné chování na internetu se promítne do slušného chování v realitě je oprávněný. Na druhou stranu je rovněž oprávněný předpoklad, že žák slušně se chovající v běžném životě, bude se stejným způsobem chovat i při komunikaci internetové. Propojení a jednotné zaměření výchovy k bezpečné a etické komunikaci jak v běžné realitě, tak i v kyberprostoru je logickým vyústěním vývoje výchovného procesu na školách. Nu a výchova, jak je známo, by měla být součástí všech předmětů tedy nejen těch humanitně orientovaných.

Projektová výuka tím, že staví žáka do centra dění, odstraňuje dělící čáru mezi žákem a pedagogem. Žák již není pouhým aktivnějším nebo pasivnějším konzumentem informací, které mu předkládá pedagog. Z žáka a pedagoga se v procesu výuky stávají partneři, žák vlastním plánováním, prezentací a realizací projektu je hybnou silou, pedagog zastává roli konzultanta. Vzájemná spolupráce učí žáka orientaci v nových situacích, učí jej komunikovat, rozvíjí jeho sociální dovednosti a vede jej k tvorbě pozitivních vztahů. V dobře zvládnutém procesu projektové výuky se vytváří a posiluje přirozená autorita pedagoga, školy i rodičů. Projektová výuka je vhodným prostředkem pro naplňování dvou stěžejních pedagogických zásad. Zásady co nejširšího spojení se životem a zásady individuálního přístupu k žákům.

Samotný projekt představuje komplexní úkol, jehož zdrojem je praktický život. Vychází ze zájmů žáka, které jsou ovlivněny jeho věkem, životním prostředím a dosaženou úrovní dovedností a schopností. Projekt je žákovým dílem.

Projekt zaměřený na prevenci

- ✓ Projekt vychází z obecného tématu (např. „šikana“).
- ✓ Konkrétní podnět projektu vychází z konkrétní situace (např.“ šikana v naší třídě“).
- ✓ Řešeným problémem je obtíž formulovaná otázkou (např. „Jak šikaně zabránit?“, „Je potřeba něco změnit?“)

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- ✓ Dosažení výchovně vzdělávacího cíle je výsledkem vyřešení problému (např. „zlepšili jsme vzájemné vztahy“).

Projektová výuka je náročným typem výuky. Realizace jakéhokoli projektu vyžaduje kvalitní přípravu ze strany pedagoga. Pokus realizovat projekt bez kvalitní přípravy, promyšlení, zvážení časové náročnosti, zajištění prostoru a pomůcek obvykle končí zhroucením projektu, nezájmem žáků, chaotickým průběhem výukových hodin, negativním hodnocením ze strany kolegů a rodičů.

Poznatky z praxe poukazují na skutečnost, že termíny projektová výuka a projekt bývají nadužívány. Za projekt je často označena samostatná práce žáka nebo skupiny žáků na pedagogem zadané téma (např. výroba plakátu varujícího před kyberšikanou).

Za projektovou výuku je možno považovat pouze to pedagogické dění, které má tyto na sebe navazující fáze:

Příprava, plánování projektu:
Plánování projektu zahrnuje níže popsané činnosti bez ohledu na délku trvání projektu.
1. Definování komplexního úkolu, problému k řešení.
2. Zvolení výstupu projektu, jaká bude závěrečná podoba projektu.
3. Časové rozvržení realizace projektu.
4. Určení prostředí, ve kterém bude projekt realizován.
5. Vymezení účastníků projektu, kdo všechno se na něm podílí.
6. Popsání průběhu projektu.
7. Materiální zajištění projektu.
8. Stanovení kritérií hodnocení.

Realizace projektu:
Je daná předem připraveným plánem, postup by měl být prodiskutovaný v přípravné fázi projektu. V průběhu samotné realizace probíhají konzultace, jejichž účelem je prodiskutování nenadálých obtíží, nejasností, nedostupnosti potřebného materiálu, pomůcek, časové tísně apod. Žák si vytváří vlastní projektové portfolio, které obsahuje potřebný materiál.
Tento materiál žák třídí, zpracovává, analyzuje a kompletuje do konečné podoby projektu. Úloha pedagoga je v této fázi projektu daná časovým rozsahem projektu. V případě jednohodinového, jednodenního nebo i jednotýdenního projektu pedagog zaujímá roli poradce, který zpovzdálí sleduje práci žáků a angažuje se pouze na základě žákova podnětu. V případě měsíčního, několika měsíčního či dokonce ročního projektu se úkoly pedagoga rozšiřují o kontrolní a motivační působení. Účast na realizaci dlouhodobého projektu je pro pedagoga náročným úkolem a těžiště zdárného dokončení projektu tkví na něm.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Prezentace projektu:
Je představením konečného výsledku projektu. Součástí prezentace je také zdůvodnění výběru tématu a popis postupu, kterým bylo výsledku dosaženo. Vhodné je uvést obtíže, které bylo nutno překonat a co se na projektu v konečném důsledku realizovat nezdařilo.
Prezentace se odehrává ve formě, která byla naplánovaná při přípravě projektu (písemná, ústní, praktické předvedení díla, individuální nebo skupinová). Prezentace může proběhnout v nejrůznější podobě, rovněž předem naplánované (přednáška, diskusní fórum, uveřejnění ve školním časopise nebo zvláštním sborníku pokud se jedná např. o celoškolní projekt, na internetu, výstava, praktická ukázka apod.)
V přípravné fázi projektu je také naplánováno před kým bude výsledek projektu prezentován (spolužáci, škola, rodiče, sponzor projektu apod.).

Hodnocení projektu:
Probíhá ve dvou rovinách, subjektivní a objektivní. Subjektivní rovinu hodnocení představují žákovi představy, prožitky, myšlenky a pocity související s realizací projektu. Důležitým aspektem je jeho vlastní závěr zda je s realizací projektu spokojen, co mu projekt dal, co vzal a zda bude mít zájem účastnit se dalších projektů. Objektivní rovinu představuje hodnocení pedagoga a užší nebo širší veřejnosti (spolužáci, rodiče, vedení školy, sponzor.
Hodnocení projektu probíhá na základě kritérií stanovených v přípravné fázi projektu (kdo bude hodnotit, co se bude hodnotit, jakým způsobem a v jakém rozsahu). Pedagog nesmí dopustit aby místo hodnocení proběhla kritika.
Součástí hodnocení může být předání odměny, která může být předem vypsána, ale která se může stát i překvapením.

Příprava pedagoga na hodinu projektové výuky obsahuje (jedná se vlastně o **sylabus hodiny**):
* stanovení výchovně vzdělávacího cíle hodiny
* popis naplánovaných činností
* rozbor průběhu hodiny z hlediska času
* výběr metod práce
* volbu forem práce
* soupis potřebných pomůcek.

Smysluplně realizovaná prevence v rámci běžné výuky je postavená na čtyřech pilířích:
- efektivní hodině – založené na vhodně postaveném plánu výuky a použité metod,
- organizačních schopnostech pedagoga,
- autoritě pedagoga,
- dobrém vztahu mezi pedagogem a žákem..

Prevence, jakožto předcházení nežádoucím sociálně patologickým jevům, se v rámci běžné výuky realizuje ve třech úrovních:

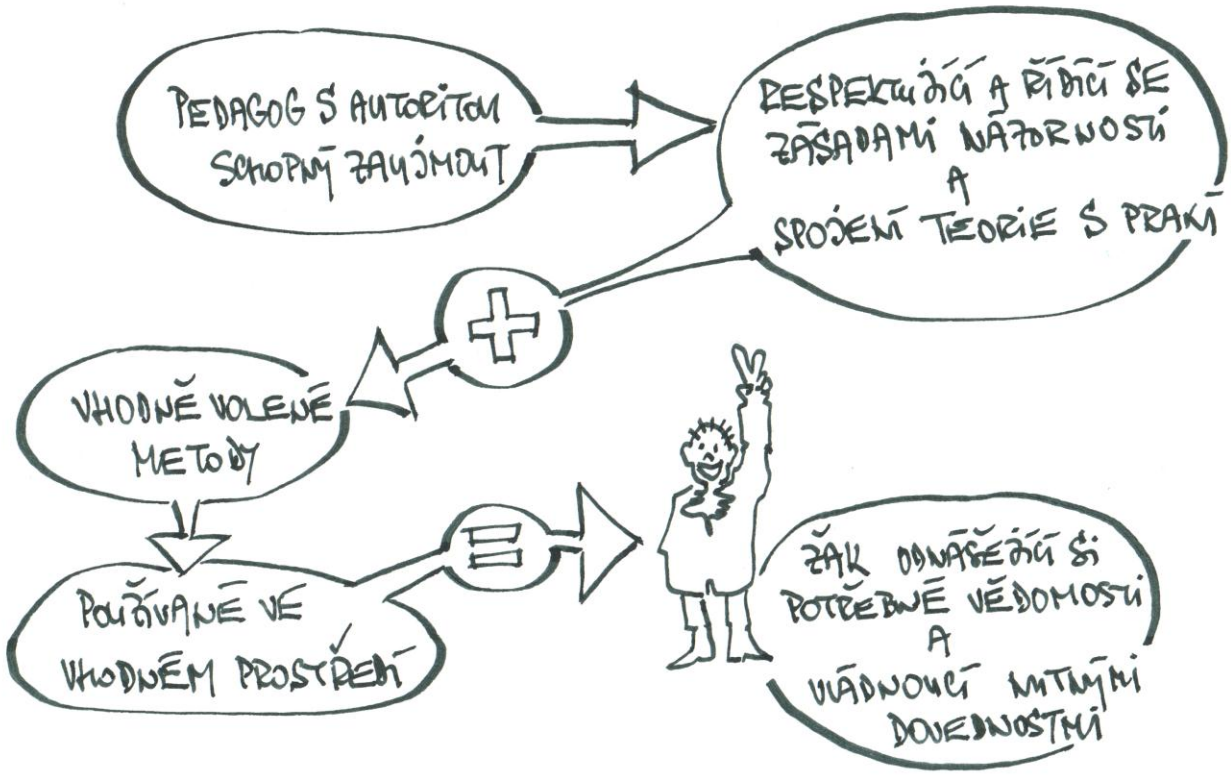
Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- **primární** (předcházení ohrožujícím situacím v celé sledované skupině – škole)
- **sekundární** (zaměřená již na rizikovou cílovou skupinu – třída, skupina žáků ve třídě)
- **terciární** (zaměřená na jedince, u nichž se již negativní jev projevil)

Primární preventivní program se realizuje celoplošně, má působit v rovině výukové, výchovné i psychosociálně poradenské. A zejména – má být efektivní a realizovaný systematicky a dlouhodobě.

V rámci běžné výuky smysluplně realizovaná prevence žákovi předá:

- znalosti nutné k rozpoznání sociálně patologických jevů a závadového jednání vlastního nebo cizího,
- kompetence k řešení problémů souvisejících se sociálně patologickými jevy,
- kompetence ke komunikaci bezpečné a etické,
- kompetence sociální, kdy žák bude umět se svým okolím komunikovat jak kyberprostorově, tak "tváří v tvář".



Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

PŘÍKLAD DOBRÉ PRAXE

Klíčová opatření obsažená v jakémkoli programu primární prevence **obsahují** následující položky:

- zhodnocení situace na škole před zavedením programu a po něm,
- motivaci pedagogů k ochotě působit preventivně, před sociálně patologickými jevy neuhýbat,
- nepřehlížet nejen je ale ani jejich příznaky,
- společné vzdělávání a zejména supervize pedagogického týmu,
- užší realizační tým: zástupce vedení školy, školní metodik prevence, výchovný poradce, školní speciální pedagog nebo psycholog (pokud jsou tyto funkce na škole ustanoveny),
- prevence ve výuce, využívání mezipředmětových vztahů,
- prevence ve školním životě mimo vyučování (školy v přírodě, zájmové kroužky, školní družina),
- spolupráce s rodiči,
- využívání školských poradenských služeb (poskytovaných Pedagogicko psychologickými poradnami nebo Středisky výchovné péče),
- spolupráce se státními institucemi a organizacemi (OSPOD, Policie ČR, Mediační a probační služba ČR, nejrůznější zdravotnická zařízení, např. psychiatrické kliniky nebo léčebny),
- spolupráce s nestátními organizacemi a institucemi působícími na poli prevence,
- spolupráce se školami v okolí (např. formou výměny informací, organizací poradenských a supervizních setkání pedagogů nebo společenských akcí).

Součástí každého školního programu primární prevence jsou **rámcově připravené preventivní akční plány** pro jednotlivé typy sociálně patologických jevů:

- narušení mezilidských vztahů agresivitou jedinců nebo skupin (šikana, party a gangy),
- kyberprostorové aktivity (kyberšikana, kybergrooming, sexting, šíření dětské pornografie pornografie, závislost na internetové komunikaci a hraní her i online her),
- autoagrese (sebepoškozování až sebevražda),
- únik z životní reality k sektám, kultům a jiným uskupením (jehovisté, moonisté, hare krišna, satanismus, neonacismus),
- závislosti (alkohol, drogy, hra, počítače),
- juvenilní delikvence (trestná činnost).

Tyto akční plány se posléze podrobně rozpracovávají pro cílové skupiny z řad žáků. Cílové skupiny se obvykle liší intenzitou patologie (mírou zamoření), rozdílností vztahů a ochotou ke změně stavu. Co platí v jedné skupině, často neplatí pro jinou skupinu. Proto cílové skupiny určuje vedení školy na základě provedeného šetření typu sociálně patologického jevu vyskytujícího se na škole.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Slovník pojmů online bezpečnosti

Kyberprostor

- kyberprostor = virtuální svět vytvářený moderními technologiemi (počítači, Internetem, mobilními telefony apod.), oproti světu „reálnému"

- digitální domorodci/přistěhovalci = termínem „digitální domorodci" se dnes zpravidla označují mladí uživatelé online technologií, kteří jsou připojeni takřka nonstop, s technologiemi běžně pracují a využívají je k řešení každodenních problémů a vzájemné komunikaci. Zpravidla bývají vybaveni nejmodernější technikou. „Digitálními přistěhovalci" se zpravidla označují uživatelé, kteří se s moderními technologiemi učí pracovat a vyžívat je k činnostem, které dříve realizovali standardními metodami. Často mají z využívání technologií vetší obavy, přechod do světa online pro ně není tak snadný a v jeho prostředí se zdaleka nepohybují s takovou jistotou, jako digitální domorodci.

- botnet = internetový robot, často tak označována síť infikovaných počítačů řízených z jednoho centra a využívaná internetovými škůdci k útokům na webové stránky, označovaným DOS

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- troll = účastník internetové diskuze, jehož cílem je vyvolat hádku; reaguje kontroverzně, napadá ostatní účastníky diskuze

- počítačová kriminalita, kybernetická kriminalita, kybernalita = zneužití informačních technologií k činnostem v rozporu se zákonem; šíření dětské pornografie, šíření a prodej nelegálních kopií komerčních programů, filmů a hudby, cílené útoky zaměřené na krádeže databází, odcizení přístupových hesel k elektronickému bankovnictví za účelem odčerpání peněz z účtů poškozených uživatelů, útoky vedoucí k odstavení webových stránek, šíření extrémistického a hanobícího obsahu apod.

- facebook = nejrozšířenější sociální síť, určená ke vzájemnému propojování uživatelů a jejich komunikaci, odhaduje se, že v červnu 2013 mělo v jejím prostředí profil 3 900 000 českých uživatelů

- twitter = sociální síť, určená je sdílení krátkých informací, pocitů, zkušeností, zážitků, často s odkazem na jiné internetové zdroje. Zpráva v prostředí Twitteru, tzv. tweet., je omezena svou délkou.

- sociální síť = internetová aplikace, sdružující uživatele za účelem vzájemné komunikace. Nejznámějšími příklady sociálních sítí jsou Facebook, Google+, Lidé.cz nebo např. Spolužáci.cz.

- komunikátor = program určený pro online komunikaci

- instant messenger = program určený k okamžité a rychlé online komunikaci, např. ICQ, Skype, Microsoft live messenger

- závislost na internetu = stav psychické závislosti, vedoucí k nutkavému používání internetu. Závislý jedinec musí být neustále online, neustále kontroluje stav svých profilů na sociálních sítích, komunikaci prostřednictvím komunikátorů nebo instant messengerů, obsah e-mailové schránky apod. Zpravidla si nedokáže představit stav, kdy by byl offline a nacházel se v prostředí/situaci bez možnosti připojení k internetu. V takové situaci je nervózní, nedokáže se soustředit a vykonávat jiné činnosti.

Kyberšikana

- kyberšikana = chování, jehož záměrem je ublížit, ohrozit nebo zastrašovat žáka, případně skupinu žáků prostřednictvím elektronických prostředků

- kyberstalking = pronásledování prostřednictvím online a mobilních technologií

- bullycide (bullying - depresion - suicide)
http://www.youtube.com/watch?v=rn4w8kglX1g&feature=g-vrec&context=G2d31748RVAAAAAAAAAw

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- happy slapping = náhlý nečekaný útok na nic netušící oběť, zpravidla útočníky natočený a umístěný na internet

- falešný profil = profil obsahující nepravdivé údaje o svém uživateli (zpravidla věk a pohlaví)

- krádež účtu = ovládnutí účtu jiným uživatelem zpravidla za účelem škodlivé a nelegální činnosti (pomluvy, hanobení, cílené útoky na jiné uživatele apod.)

Kybergrooming

- kybergrooming = cílená snaha některých uživatelů internetu (tzv. kybergroomerů) kontaktovat zpravidla v prostředí sociálních sítí mladé uživatele a děti a manipulovat jimi komunikativními metodami za účelem jejich vylákání na schůzku v reálném světě a jejich potenciálnímu zneužití. Kybergrooming je jedním z velmi nebezpečných projevů škodlivého chování v prostředí online, vedoucí k fatálním následkům.

- pedofilie ve vztahu ke kybergroomingu = jednou z nejvíce nebezpečných skupin kybergroomerů jsou deviantní pedofilové, jejichž cílem s využitím prostředků groomingu vylákat na schůzku v reálném světě děti a poté je zneužít. Groomeři bývají často velmi inteligentní lidé s vypracovanými metodami, které jsou pro ostatní uživatele s menšími sociálními zkušenostmi snadno uvěřitelné.

Nezákonný obsah

- pornografie = neumělecké znázornění lidského těla nebo sexuálního chování za účelem podněcování sexuálního pudu

- dětská pornografie = pornografické materiály, jejichž objekty jsou děti

- extremismus = jednání, ideologie či skupiny mimo hlavní (střední) proud společnosti, kterým je připisováno porušování či neuznávání základních etických, právních a jiných důležitých společenských standardů, zejména ve spojení s verbální nebo fyzickou agresivitou, násilím nebo hrozbou násilí

- proana weby = webové stránky, nabádající k anorexii, která ve svém důsledku může vést k sebepoškozování

- promia weby = webové stránky nabádající k sebepoškozování, především bulimii

Ochrana osobních údajů a osobnosti v online komunikaci

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- IP adresa = číslo, které identifikuje počítač zapojený v počítačové síti. Zkratka IP znamená internetový protokol, což je forma komunikace zařízení zapojených do internetového prostředí

- MAC adresa = jde o jedinečný identifikátor síťového zařízení, MAC adresa je přidělena výrobcem a celosvětově jedinečná

- bot = program vykonávající automaticky různé jednoduché operace. Může jít např. o profil na sociální sítí řízený počítačem, který se vydává za reálnou osobu s cílem získat o uživateli co nejvíce informací, nebo třeba o program rozesílající z e-mailové adresy uživatele bez jeho vědomí spam

- Server = v podstatě počítač poskytující nějaké služby. Může jít o služby lokální (např. obsluha tiskárny) nebo v prostředí sítě (na internetu či v rámci lokální sítě, např. školní): např. správa webových stránek nebo emailů.

- Pharming = využití špatně „přeložené“ IP adresy. Při zadání webové adresy je uživatel nasměrován na podvodný web vydávající se za pravý (např. vstupní stránka k internetovému bankovnictví.

- Phishing = snaha získat dále zneužitelné údaje o oběti (heslo, číslo kreditní karty atp.), nejčastěji formou e-mailu z „důvěryhodného“ zdroje. Např. jakoby žádost banky o zadání hesla k elektronickému bankovnictví kvůli údajnému restartování systému. Vzhledem k velkému počtu oslovených uživatelů se obvykle někdo „chytí“ a údaje zadá

- Spyware = program, který z počítače samotného uživatele monitoruje jeho činnost (vč. např. zadání hesla) a odesílá o ní zprávy. Mnohdy nevědomě nainstalován samotným uživatelem jako skrytá součást jiného programu

- Nigerijské dopisy = podvodné e-maily obvykle přislibující velkou finanční částku výměnou za malou zálohu ze strany adresáta (nebo třeba za poskytnutí jeho čísla účtu)

Autorská práva a internet

- peer to peer sítě = typ počítačových sítí, kdy spolu komunikují přímo jednotliví klienti (uživatelé), někdy bývá také označována jako klient-klient. Nejčastějším obsahem, vyměňovaným přes tento typ sítí, bývají audio nahrávky, filmy a počítačové programy

- softwarový pirát = uživatel, který využívá nelegální kopie komerčních programů, šíří je,

- warez = v počítačovém slangu jde o autorská díla, se kterými se nakládá nelegálně, především jde o počítačové programy, hry a filmy. Nejčastějším prostředím pro šíření warezu je internet.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

- cracky/záplaty = crack je malý program, který slouží k odstraňování ochranných prvků jiných programů za účelem jejich nelegálního používání či šíření. Jde o činnost ve většině zemí nezákonnou. Záplatou je zpravidla označováno softwarové vylepšení, které by mělo odstraňovat chyby předchozí verze softwaru. Často se hovoří o bezpečnostních záplatách, které odstraňují chyby operačního systému Windows anebo internetových prohlížečů.

Technické nástroje online bezpečnosti

- blacklist = v informatice jde o seznam obsahující zakázané položky, zpravidla adresy odesilatelů, od kterých nechceme přijímat zprávy, uživatelů, se kterými nechceme komunikovat prostřednictvím instant messagingu, internetových stránek, které by neměl prohlížeč zobrazovat atd.

- whitelist = seznam položek, které mají zvláštní privilegia, např. doporučené služby, internetové stránky, seznam odesílatelů e-mailů, od kterých nikdy nepřijde nevyžádaná pošta atd.

- rodičovská kontrola = jde o službu filtrace počítačového/internetového prostředí a monitoring jeho provozu při využívání dětmi. Prostřednictvím nástrojů rodičovské kontroly lze např. nastavit blacklist (seznam blokovaných) internetových stránek, na které děti nemají přístup, filtraci webových stránek, které obsahují klíčová slova (např. sex, porno atd.), sledování aktivit dětí v internetovém prostředí (seznam navštívených webů, délku pobytu na jednotlivých stránkách apod.).

Informační zdroje a literatura

- PRŮCHA, J. *Pedagogická encyklopedie* PRAHA, PORTÁL 2009
- *Portál výzkumného ústavu pedagogického* www.vuppraha.cz
- ŠALAMOUN, M. *Ochrana osobních údajů v teorii i praxi* e-kniha
- GLASSER, W. *Terapie realitou* PRAHA, PORTÁL 2001
- NAKONEČNÝ, M. *Sociální psychologie* PRAHA, ACADEMIA 1999
- VÝROST, J., SLAMĚNÍK, I. *Aplikovaná sociální psychologie II* PRAHA, GRADA 2001
- COVEY, S. *7 návyků skvělých teenagerů* PRAHA, PRAGMA 1998
- KRATOCHVÍLOVÁ, J. *Teorie a praxe projektové výuky* BRNO, Masarykova univerzita Brno 2009
- www.prevence.cz

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.

Metodický materiál vznikl v rámci projektu Škola bezpečně online: Zvýšení kvality vzděláván v oblasti bezpečného užívání internetu v Pardubickém kraji.

Registrační číslo projektu: CZ.1.07/1.3.12/04.0016.

Tento projekt je prostřednictvím Operačního programu Vzdělávání pro konkurenceschopnost financován z Evropského sociálního fondu a státního rozpočtu ČR.

Vydalo Národní centrum bezpečnějšího internetu v roce 2012.

Na materiálu spolupracovali
Mgr. Kateřina Lukášová, Mgr. Rastislav Pacák, Mgr. Anna Mašková a Mgr. Jana Brandejsová.

Materiál vznikl v rámci projektu OP VK Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji. Registrační číslo projektu: CZ.1.07/1.3.12/04.0016. Národní centrum bezpečnějšího internetu, 2012.