INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ
Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.

Vzdělávací program

RESTART – (Ne)bezpečný internet pro profesionály

Akreditace – MSMT 40315/2012-201-731 platí do 12.11.2015

Anotace

Tento kurz rozvíjí kompetence učitelů využitím ICT ve výuce na ZŠ a SŠ. Internet jako informační zdroj je pro využití ve výuce lákavý, je ale třeba mít na paměti veškerá rizika, která sebou může přinášet. Učitelé jsou v kurzu na tuto skutečnost upozorněni prostřednictvím ukázek včetně videa a projektu „E-Bezpečí“. Je nutné umět nebezpečí internetového prostředí identifikovat a zajistit ochranu dětí a žáků před jejich dopadem. V dalším kroku pak naučit děti a žáky rizika odhalit a použít vhodné hardwarové, softwarové či jiné nástroje pro tuto ochranu. Při práci využijí učitelé zejména volně šiřitelé programy. Kurz dále nabízí přehled informačních zdrojů na internetu. Velký důraz je kladen na autorská práva a ochranu osobnosti.

Cílová skupina

Pedagogičtí pracovníci škol.

Vzdělávací cíl

Cílem kurzu je posílení profesionalizace učitele při práci s informačními a komunikačními technologiemi, motivace učitele pro dodržování pravidel bezpečné práce na internetu s přenosem těchto dovedností na děti a žáky. V tomto smyslu také šíření příkladů správné aplikace autorského zákona a zákona na ochranu osobních údajů.

Absolvent vzdělávacího programu:

- ovládá obecné informace o nebezpečí internetu
- aplikuje autorská práva, zákon na ochranu osobních údajů
- aktivně řeší hardware resp. softwarovou ochranu na školách
- rozlišuje pojmy: Kybergrooming, SMS Spoofing, Flaming, Kyberstalking, Cyber Bullying – Kyberšikana, Hoax, Spam, Google Bombing, Phishing, Pharming, sociální inženýrství, dětská pornografie a zná způsoby jak jim předcházet resp. jak situaci řešit.

Vyhodnocení akce

Účastníci kurzu nasdílejí dokument k probíranému tématu zpracovaný dle pokynu lektora. Účastníci vyplní evaluační dotazník.

Technické zabezpečení akce

Lektor bude mít k dispozici dataprojektor nebo projekční dotykovou obrazovku, připojení k internetu, PC učebnu s 1 PC učitelským + počet PC dle účastníků.

Výukový materiál pro projekt RESTART, reg. č. CZ.1.07/1.3.00/51.0004

Krajské zařízení pro další vzdělávání pedagogických pracovníků a informační centrum Nový Jičín, příspěvková organizace, Štefánikova 7/826, 741 11 Nový Jičín, IČO 62330403, DIČ CZ62330403

Metodické poznámky ke kurzu

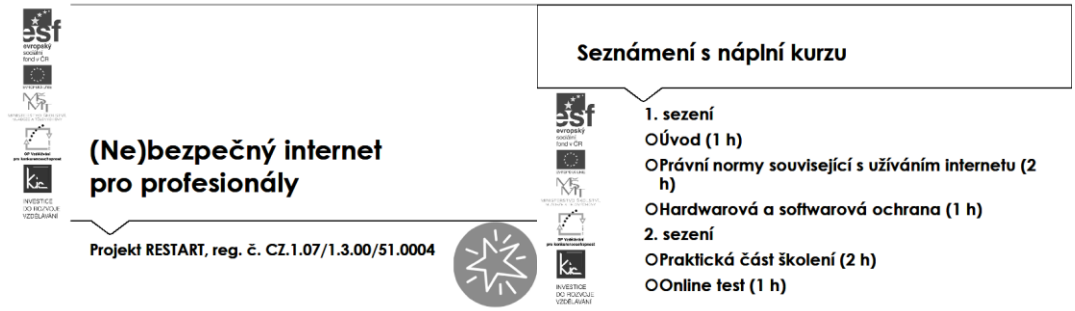
V rámci kurzu se účastníci seznámí s dodržováním pravidel bezpečné práce na internetu s přenosem těchto dovedností na děti a žáky, s právními normami související s užíváním internetu ve výuce a s příklady řešení hardwarové a softwarové ochrany na školách. Důraz je kladen na vysvětlení základních rizik, se kterými se žáci střetávají v každodenním životě při používání vlastních ICT nástrojů.

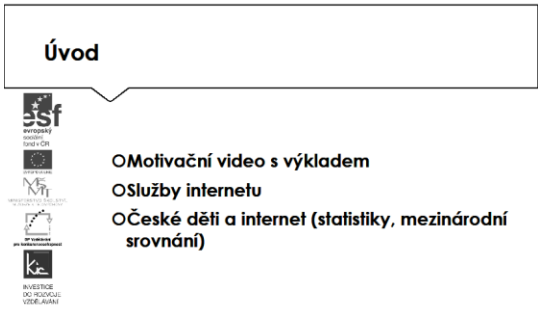
Forma – prezenční forma, hodinová dotace 7 h (7 h prezenčně).

Přehled témat prezenční části výuky (7 h)

1. sezení (rozsah 4 h):

Úvod (1 h): - Motivační video s výkladem - Služby internetu - České děti a internet (statistiky, mezinárodní srovnání)





Lektor tento kurz zahájí motivačními ukázkami, účastníků přehraje:

- video https://www.youtube.com/watch?v=O4VMutqgpZs
- video http://www.e-bezpeci.cz/index.php/temata/videa-k-tematm
- podcast http://cms.e-bezpeci.cz/podcast/?vyber=8

Na základě shlédnutých příspěvku s účastníky zahájí diskusi o problémech, které byly nastíněny, jestli se s nimi osobně již setkali, zda mají informaci, že se s nimi setkali jejich žáci či je řešili ve škole. Jak by

postupovali, pokud by se s takovou situací setkali. Tyto návrhy sepsat na tabuli a při výkladu se s k jednotlivým bodům postupně vracet tak, jak budou řešena v kurzu.

Účastníci kurzu jsou dále seznámeni s výsledky několika průzkumů, které se prováděly ve vzorcích, kde byli respondenty děti z ČR:

- Výzkum České děti na Facebooku http://www.e-bezpeci.cz/index.php/veda-a-vyzkum/1103-czech-children-facebook-research-report-2015 - upozornit na cca 80 % dětí využívá FB, 60 % respondentů mladších 13 let má na FB účet, 90 % respondentů 13-16 let má účet na FB, 33 % respondentů je na FB víc než 3 h denně.
- Projekt E-Bezpečí Pedagogické fakulty Univerzity Palackého v Olomouci (2014) - Výzkum děti a internet: http://www.ceskatelevize.cz/ct24/regiony/1510856-vyzkum-deti-a-internet-40-procent-deti-slo-s-line-znamym-na-schuzku 40 procent dětí by šlo s on-line známým na schůzku
- Čtyřletý celoevropský výzkum EU (2011-2014) Kids Online sledující chování dětí na internetu, za ČR se podílela Fakulta sociálních studií Masarykovy univerzity https://www.online.muni.cz/veda-a-vyzkum/4918-studie-chovani-deti-na-internetu-prinesla-pet-rad-pro-rodice přinesl finální výsledky. České děti (ve věku 9 až 16 let) z něj vyšly jako ty spíše nadprůměrně ohrožené riziky internetu a 5 rad pro rodiče.

Pro účastníky kurzu vybírá lektor z hlavních zjištění:

1. Čím více děti používají internet, tím lepší jsou jejich digitální dovednosti.

2. Čím častěji děti internet používají, tím větší je i riziko újmy.

3. Klíčovou roli v tom, jestli bude internet pro děti přínosný, sehrávají rodiče.

4. Ohroženější jsou spíše mladší děti, zejména dívky a děti s problémy i z reálného světa.

5. Nejvíce děti znepokojuje pornografie, těsně následována násilím páchaným na dětech nebo zvířatech.

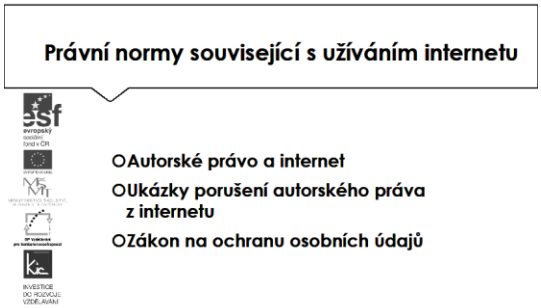
Lektor účastníkům uvede jako zajímavý příklad pro školy aktivitu firmy Google Web Rangers, celkem 7 videolekcí o internetové bezpečnosti http://www.seduo.cz/7-lekci-ktere-z-tebe-udelaji-mistra-internetove-bezpecnosti a projekt, ve kterém žáci učí jiné žáky, jak se chovat na internetu bezpečně.

Právní normy související s užíváním internetu (2 h):

- Autorské právo a internet

- Ukázky porušení autorského práva z internetu

- Zákon na ochranu osobních údajů



V průběhu času se významně rozšířil obsah publikovaný na internetu, objevily se nové nástroje umožňující jednoduché a rychlé sdílení obsahu, ale ne všechny portály kontrolují, zda je s obsahem na internetu nakládáno ve smyslu autorského zákona. Lektor upozorní účastníky kurzu na skutečnost, že takto snadno dostupný obsah může velmi často vést k jeho zneužití ve smyslu např. porušování autorských či majetkových práv.

Účastníkům jsou prezentovány základní pojmy Zákona č. 121/2000 Sb., Autorský zákon. Účastníkům jsou objasněny pojmy „autorské dílo" a uvedeny jeho příklady z praxe:

- věc, konkrétní předmět nebo i jejich ucelený soubor apod.
- nehmotné povahy (hudba či počítačový program).

S účastníky je následně diskutován výčet toho, co není považováno za AD:

- námět díla sám o sobě
- denní zpráva nebo jiný údaj sám o sobě
- myšlenka, postup, princip, metoda, objev, vědecká teorie, matematický a obdobný vzorec, statistický graf a podobný předmět sám o sobě
- ani např. výsledek restaurátorské činnosti.

Účastníci si ve znění zákona individuálně vyhledají výjimky z ochrany podle práva autorského ve veřejném zájmu, např.:

- úřední dílo (např. právní předpis, rozhodnutí, veřejná listina, veřejně přístupný rejstřík, publikace, obecní kroniky, státní symbol apod.)
- výtvory tradiční lidové kultury, není-li pravé jméno autora obecně známo)
- politický projev a řeč pronesenou při úředním jednání.

Vymezení pojmu „autor" je účastníkům prezentováno zejména jako osoba, jejímž výsledkem je tvůrčí činnosti a fantazie je dílo.

Následně jsou s účastníky obdobným způsobem ve znění zákona vyhledány a objasněny pojmy „zveřejnění a vydání díla", „vznik práva autorského" a „osobnostní práva". Zejména je ve vztahu k osobnostnímu právu vhodné uvést právo autora:

- rozhodnout o zveřejnění svého díla
- osobovat si autorství
- rozhodnout, zda a jakým způsobem má být autorství uvedeno.

Účastníkům je vysvětleno, že pokud vzniká dílo jako zaměstnanecké (bude upřesněno dále), bude autor poskytovat právo k nakládání s dílem zaměstnavateli.

Jako velké riziko je účastníkům předloženo nedodržování AZ ve škole a to vč. možných finančních sankcí. Pro dobré pochopení je vhodné uvést jako příklad videa z právnické fakulty publikované na http://is.muni.cz/do/1499/el/seminare/index.html

S účastníky je probrán výčet u majetkových práv – „Právo dílo užít" a doba trvání majetkových práv. Detailně je účastníkům představena část zákona věnovanou § 30 „Volná užití a zákonné licence" a v čem úloha edukace školy vůči „běžnému použití" žáky a učiteli mimo školu.

Volné užití je možné, pokud je pro:

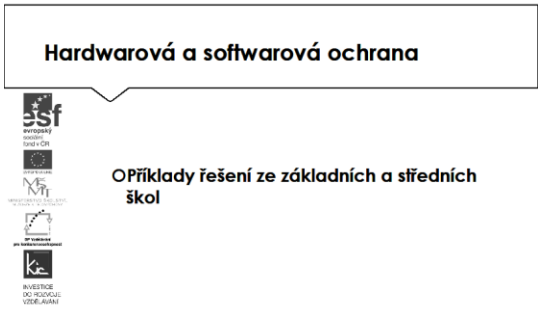
- osobní potřebu (zdůraznit, že toto neplatí např. pro pořízení záznamu audiovizuálního díla při jeho provozování ze záznamu nebo jeho přenosu)
- dočasné vyrobení kopie autorského díla při předvádění počítače apod. zákazníkovi při prodeji
- kopírování tiskového díla (s výjimkou partitury hudebního díla) v copycentru apod.

Účastníkům je představen další informační zdroj - Vybrané otázky autorského práva pro potřeby škol http://clanky.rvp.cz/wp-content/upload/prilohy/11387/vybrane_otazky_autorskeho_prava_pro_potreby_skol.pdf

Kontrolními otázkami lektora je ověřeno u účastníků rozlišení situací, kdy se jedná o volné užití díla ve škole. V této fázi výkladu je vhodné představit licenci, která umožňuje bezplatné využití díla pod licencí Creative Commons s licenčními prvky (charakteristické prvky této licence stanovil poskytovatel a jsou vyjádřeny v jejím označení, např.: „Uveďte autora“, „Neužívejte komerčně“ a „Zachovejte licenci“).

Na příkladu portálu autori.rvp.cz seznamuje lektor účastníky se způsobem bibliografických citací děl (tištěná média, elektronické dokumenty). A ověří zvládnutí konstrukce citace a provede nácvik použití nástrojů pro tvorbu citací (MS Word – „Vložit citaci“, www.citace.com).

Hardwarová a softwarová ochrana (1 h) - Příklady řešení ze základních a středních škol



Tato část kurzu je ukončena představením dvou řešení, kterými lze zvýšit bezpečnost při práci na zařízeních připojených do internetu. Účastníkům je prakticky předvedeno sw a hw řešení v prostředí českých škol.

Jako první představí lektor softwarové řešení, tj. zejména se účastníci seznámí se službou blokování nevhodného obsahu http://www.i-bezpecne.cz/, dále s omezením obsahu, který mohou děti prohlížet na webu http://windows.microsoft.com/cs-cz/windows-vista/limit-the-content-that-children-can-view-on-the-web pomocí „rodičovské kontroly“ v OS Windows. Toto si prakticky vyzkoušejí a provedou nastavení na jednotlivých počítačích v následujících krocích (postup zapnutí pro standardní uživatelský účet):

- Tlačítko Start, příkaz Ovládací panely - Uživatelské účty a zabezpečení rodiny - Nastavit rodičovskou kontrolu pro všechny uživatele.
- Systém vyzve k zadání nebo potvrzení hesla správce, toto zadejte.

- Zvolte nebo Vytvořit nový uživatelský účet pro tuto kontrolu.
- Rodičovská kontrola - zvolit Zapnuto, vynutit aktuální nastavení.
- Následně lze u uživatelského účtu dítěte upravit co chcete kontrolovat:
    - Časové limity
    - Hry
    - Povolení a blokování programů.

Účastníci postupně vyjmenují, co vše spadá z jejich pohledu pod pojem softwarového zabezpečení počítače, lektor jejich poznatky průběžně zaznamená a komentuje. Zpravidla se objevují pojmy:

- Antivirová ochrana
- Aktualizace systému a programů
- Uživatelské účty a nastavení hesla
- Odstranění škodlivého softwaru
- Spyware
- Zabezpečení bezdrátového připojení
- Nastavení brány Windows Firewall.

Následně představí lektor účastníkům web http://www.bezpecnyinternet.cz/zacatecnik/zabezpeceni-pocitace/default.aspx, kde jsou k tématu uvedeny další možnosti. V případě, že nebylo uvedeno účastníky kurzu, doplní přehled o další nutné kroky ochrany počítače, jako je např.:

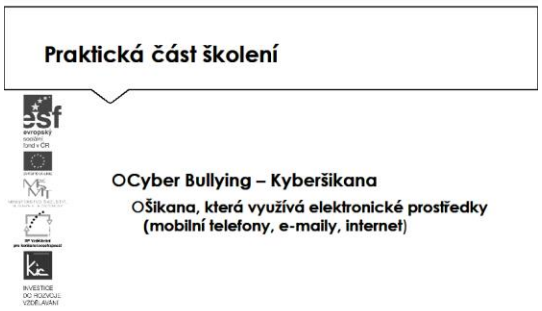
- Zálohování dat
- Šifrování dat.

V případě hardwarového řešení je školami využíván např. firewall FortiGate s funkčí Web Filtering, který testuje veškerý webový obsah na výskyt známých nežádoucích URL, blokuje nevhodný obsah a nebezpečné Java aplety, cookies, Active X skripty před jejich vstupem do sítě (nezbytnost u služby je možnost přidat další URL). Účastníci diskutují o tom, jak je hw ochráněna jejich školní síť a je jim prezentován příklad problematického routeru a způsob vyřešení jeho zabezpečení na http://www.novinky.cz/internet-a-pc/bezpecnost/339333-je-router-bezpecny-poradi-jednoduchy-test.html

2. sezení (rozsah 3 h):

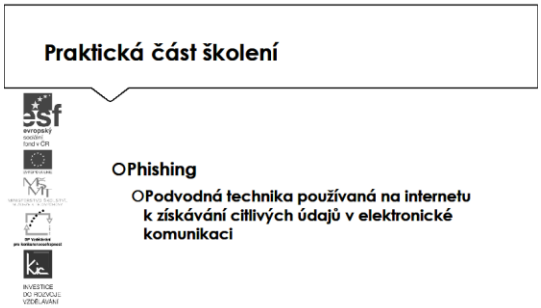
Praktická část školení (2 h): - Kybergrooming, SMS Spoofing, Flaming, Kyberstalking, Cyber Bullying – Kyberšikana, Hoax, Spam, Google Bombing, Phishing, Pharming, sociální inženýrství, dětská pornografie. - Co nás na internetu obtěžuje - diskuse On-line testy získaných znalostí k vybraným kapitolám (1 h)

Tato část kurzu je zaměřena velmi prakticky. Kromě ukázek lektora účastníci také vyhledávají další informace, srovnávají a sdílejí vzájemně ve skupině a doplňují si svůj seznam důležitých odkazů. Lektor zahajuje tuto část zaměřením pozornosti účastníků na pojem kybergrooming, následně kyberstalking, srovnává je v reálném a virtuálním prostoru, s účastníky diskutuje konkrétní zkušenosti ze škol s využitím odkazů na http://www.e-bezpeci.cz/index.php/temata/kybergrooming a http://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking.



Lektor dále diskutuje s účastníky o pojmu kyberšikana, opět srovnává průběh v reálném a virtuálním prostoru, účastníci sdělují své konkrétní zkušenosti ze škol s využitím odkazu na http://www.e-bezpeci.cz/index.php/temata/kyberikana a dále lze využít odkaz z webu MŠMT https://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwipperPgJvLAhXC6HIKHXrsAF8QFghAMAA&url=http%3A%2F%2Fwww.msmt.cz%2Fuploads%2FPriloha_7_Kybersikana.doc&usg=AFQjCNEZqhfFCyjegemTVQQOy9dBYiAn_A&sig2=5bEbRmg4YFdj2-hi7N5A0w Tématu šikany se věnují např. webové stránky českých organizací, proto je lektor účastníkům jednotlivě představí:

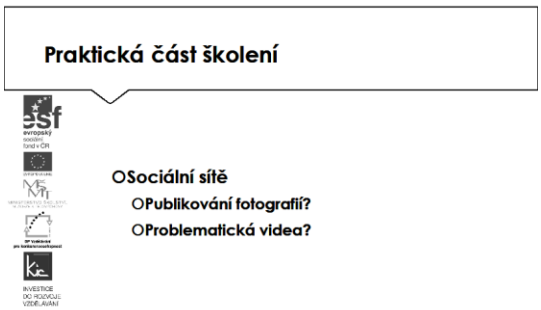
- Společenství proti šikaně, www.sikana.org
- Internet poradna, www.internetporadna.cz
- Sdružení Linka bezpečí (116 111) , www.linkabezpeci.cz
- Amnesty International ČR, www.amnesty.cz.



Toto téma uvede lektor oslovením jednotlivých účastníků a zjišťuje, jak často obdrží e-mail, který je vyzývá k nějaké aktivitě, která by mohla ohrozit např. jejich bankovní účet na internetu (typicky tyto maily byly rozesílány pod pseudohlavičkou České spořitelny či Komerční banky). Lektor proto upozorní na vše, co může takové podvodné jednání pomoci odhalit:

- Mail vypadá věrohodně, působí „opravdově“.
- Mail požaduje zadání uživatelského jména a hesla resp. jiných důvěrných údajů (číslo platební karty, číslo účtu a podobně).
- Pokud mail vypadá podezřele, zadat do vyhledávače věc (subjekt) dopisu.
- Podívat se na web příslušné instituce, zavolat na zákaznickou linku.
- Nepoužívat kontaktní informace z mailu, neklikat na odkazy, neodpovídat na mail.
- Když dojde na nejhorší, okamžitě změnit heslo, kontaktovat banku, sdílet upozornění přátelům.

K tématu lze rovněž využít odkaz http://www.bezpecnyinternet.cz/zacatecnik/e-mail/default.aspx, který si mohou účastníci individuálně prozkoumat a lektor jim doporučí návod na vytvoření bezpečného hesla http://www.bezpecnyinternet.cz/zacatecnik/hesla/default.aspx



Lektor uvede toto téma průzkumem ve skupině účastníků, kdy se ptá, kdo z nich má účet na některé sociální síti, zda na této síti spolupracují se svými žáky. Jako přehled nejvíce využívaných uvede:

- Facebook
- Lide.cz
- Spoluzaci.cz
- Libimseti.cz
- ASK.fm
- Snapchat

- Instagram
- Pinterest
- WhatsApp

Je důležité akceptovat skutečnost, že téměř všichni žáci účastníků mají účet na některé sociální síti. Proto by účastníci měli vědět, jak žáky naučit bezpečnému chování v tomto prostředí. Mohou porovnat vlastní zkušenost mezi účastníky kurzu, jak k tématu ve výuce přistupují. Ve výuce je doporučeno provést průzkum a sdílet zkušenosti žáků. Pro tento účel může využít celou řadu nástrojů, např.:

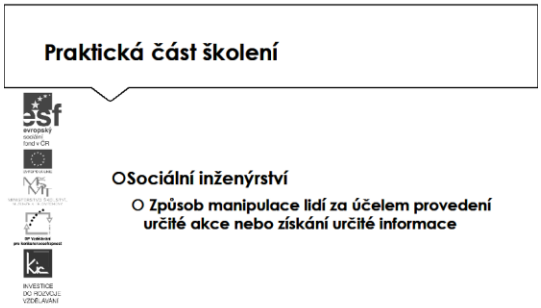
- http://www.e-bezpeci.cz/index.php/temata/socialni-sit
- https://www.youtube.com/watch?v=3QncEyELmTo
- http://www.saferinternet.cz/
- http://www.bezpecne-online.cz/projekt-bezpecne-online/slovnik.html
- http://www.jaknainternet.cz/page/1185/rizika-socialnich-siti/

Účastníci jsou upozorněni také na trestní odpovědnost, která z některých úkonů na sociální síti může vyplynout – publikování fotografií nezletilých, publikování fotografií bez souhlasu, publikování choulostivých snímků nebo videa dětí. Z legislativního rámce je tedy nutné upozornit na porušování Zákona č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů a zákon č. 181/2014 Sb. o kybernetické bezpečnosti.

Účastníci jsou seznámeni s pěknou formou zpracování tématu pro žáky, např. komiksy pro žáky o publikování fotografií http://www.bezpecnyinternet.cz/deti/komiksove-pribehy/komiks-zmatky-a-nehody.aspx nebo vysvětlení pro žáka co jsou sociální sítě http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/default.aspx

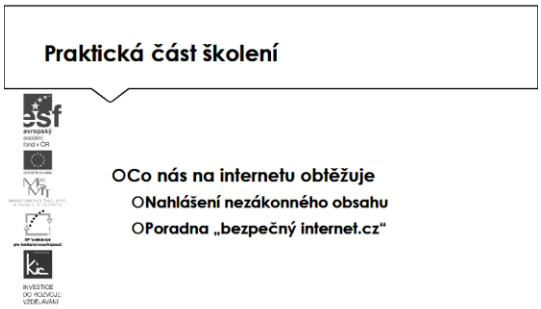
Lektor závěrem shrne, čeho se může týkat ochrana práv ostatních na internetu:

- Vystavování fotek přátel, rodiny a třetích osob
- Ochrana své online reputace
- Krádež identity a jak se jí bránit
- Sdílení obsahu
- Duševní vlastnictví.

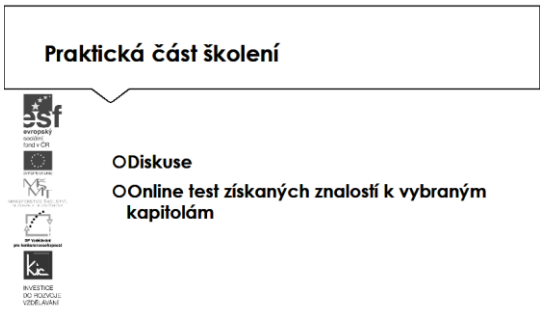


Pro komplexnost informace lektor vysvětlí pojem sociální inženýrství a prezentuje např. na FB, jak může takové sbírání dat probíhat. Uvede příklad prevence využívané u firem „Testy sociálního

inženýrství“, tj. ověřování bezpečnosti organizace např. http://www.systemonline.cz/it-security/socialni-inzenyrstvi-1.htm a s účastníky diskutuje možnost analogického ověřování mezi pracovníky ve škole. Vyhodnocují ve skupině, zda je takový test reálný, zda bude pracovníky školy akceptován a proveden.



V řízené diskusi sestavuje lektor s účastníky návod na bezpečné chování na internetu a první kroky co dělat, když jsme na internetu obtěžováni (totéž doporučí účastníkům formulovat vzhledem k žákům). Zaměří se na stránky, na kterých je popsán postup při obtěžování na FB https://www.facebook.com/help/116326365118751, stránky, na kterých lze provést nahlášení nezákonného obsahu na http://aplikace.policie.cz/hotline/, https://www.internet-hotline.cz/ nebo obtěžujícího chování na internetu na http://www.stopkybersikane.cz/



Účastníkům je předložena zajímavá pomůcka do výuky - Komiksy pro žáky na http://www.bezpecnyinternet.cz/deti/komiksove-pribehy/default.aspx a dále celá řada online testů, ve kterých si mohou ověřit zvládnutí výše uvedených témat a problematiky, popř. je opět začlenit do výuky.

Test pro učitele

http://www.bezpecnyinternet.cz/skoly/zakony/test.aspx

Test pro rodiče

http://www.bezpecnyinternet.cz/rodice/doporuceni-pro-rodice/test.aspx

Test bezpečného chování na internetu

http://www.policie.cz/soubor/iii-soutezni-test-zamereny-na-bezpecny-internet-spravne-odpovedi-pdf.aspx

Test sociální sítě

http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/test.aspx

Test bezpečné on-line komunikace

http://www.bezpecnyinternet.cz/zacatecnik/on-line-komunikace/test.aspx

Test k zabezpečení mailu

http://www.bezpecnyinternet.cz/zacatecnik/e-mail/test.aspx

Test ochrany práv na internetu

http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/test.aspx

Test zabezpečení počítače

http://test.bezpecnosti.cz/

Test zabezpečení organizace na internetu

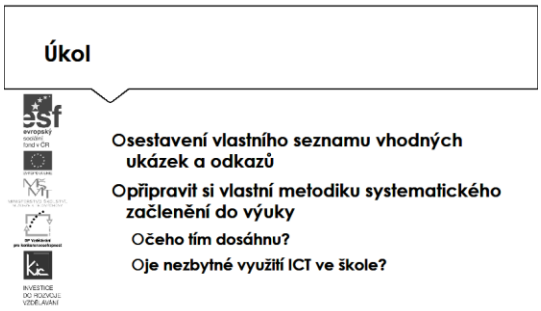
http://tech.ihned.cz/c1-61717370-test-bezpecnosti-umite-si-chranit-svou-firmu-na-internetu

Test zabezpečení počítače

http://www.bezpecnyinternet.cz/zacatecnik/zabezpeceni-pocitace/default.aspx :

Test ochrany dat

http://www.bezpecnyinternet.cz/pokrocily/ochrana-dat/test.aspx



V závěru kurzu bude lektor motivovat účastníky k sestavení vlastního seznamu vhodných ukázek a odkazů a připravit si vlastní metodiku systematického začlenění do výuky, ideálně při revizi ŠVP začlenit do něj s přesahem do dalších vzdělávacích oblastí.

V tomto materiálu může dobře zužitkovat 5 rad pro rodiče z https://www.online.muni.cz/veda-a-vyzkum/4918-studie-chovani-deti-na-internetu-prinesla-pet-rad-pro-rodice, které lze shrnout do hesel:

1. internet jsou výhody i rizika
2. posilujte digitální dovednosti
3. hledejte pozitivní aktivity online světa
4. diskutujte, co na internetu může být problematické
5. nastavte jasná pravidla.

Ve všech částech vzdělávacího programu se předpokládá aktivní práce účastníků.