

Autorský
zákon

Creative
Commons

Citování

TABLETY DO ŠKOL

— POMŮCKA PRO PEDAGOGA

VE SVĚTĚ DIGITÁLNÍHO VZDĚLÁVÁNÍ

Internet a zákony

LICENCOVÁNÍ
SOFTWARE

BEZPEČNOST,
KYBERŠIKANNA ATD.

Příručka pro ředitele



Facebook

Sexting

Pavel Roubal
2014

esf
evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost

INVESTICE
DO ROZVOJE
VZDĚLÁVÁNÍ

Název projektu: Tablety do škol - pomůcka pro pedagoga ve světě digitálního vzdělávání

Registrační číslo projektu: CZ.1.07/1.3.00/51.0002

Tento produkt je spolufinancován z Evropského sociálního fondu a státního rozpočtu České republiky.

Toto dílo je licencováno pod licencí Creative Commons.

[Uveďte autora – Neužívejte komerčně – Zachovejte licenci].



Obsah

Obsah	3
1 Úvod.....	4
2 Licencování software, textů, obrázků, hudby a videa	5
2.1 Obecné modely licencování software	5
2.2 Modely licencování software firmy Microsoft.....	5
2.3 Další komerční licence	6
2.4 Open Source licence a její využití ve škole, TCO.....	7
2.5 Autorský zákon a texty, obrázky, hudba a video ve výuce i mimo ni	8
2.6 Citování zdrojů (a cloudová služba www.citace.com)	10
2.7 Licence Creative Commons	11
3 Zabezpečení počítače, sítě a přístupu do Internetu, obrana soukromí a osobnosti.....	13
3.1 Technika je na správci sítě	13
3.2 Znalosti a opatrnost potřebují všichni	16
3.3 Zabezpečení školní sítě a přístupu žáků do Internetu	17
3.4 Sociální sítě (Facebook [FB]) – „soukromí neexistuje“ a nic se nedá smazat.....	18
3.5 Kyberšikana a obrana proti ní – nic nesmí být anonymní.....	21

1 Úvod

Sada publikací pro projekt „Učíme digitálně“ obsahuje celkem 4 materiály:

1. Profil Škola 21 a výběrová řízení.
2. Tablety a školní síť.
3. Internet a cloudové služby.
- 4. Licencování software a počítačová bezpečnost.**

Tato část materiálů se zabývá počítačovými licencemi, které zásadním způsobem ovlivňují/omezují využívání programového vybavení i zdrojů na webu.

Bezpečnost uživatelů počítačů je stále důležitější, protože do počítačových uložení se ukládá stále větší část jejich pracovního a osobního „života“.

2 Licencování software, textů, obrázků, hudby a videa

2.1 Obecné modely licencování software

Programy (software) jako celky nikdy nezískáme, vždy dostáváme či kupujeme pouze **licenci** na využití programu na jednom (či více) počítači. Program není obyčejný výrobek, je to tzv. autorské dílo a jeho tvůrci (firma, pro kterou pracují) k němu mají autorská práva.

Licenci k užívání programu můžeme získat zdarma či za poplatek, v licenční smlouvě bývají uvedeny podmínky pro její získání i podmínky a záruky (spíše výhrady záruk), které se k určitému programu vztahují.

Pozor, bezplatné licence některých programů jsou pouze pro domácí použití, ne pro školství

2.1.1 Licenční smlouva

Při instalaci programu většinou musíme odsouhlasit licenční smlouvu s koncovým uživatelem (tzv. EULA – End User License Agreement). Tím dáváme najevo svůj souhlas s licenčním ujednáním, které je proto dobré si předem přečíst. Licenční smlouva je typem obchodní smlouvy, je tedy podřízena zákonu. Jestliže nám tedy tato smlouva něco zakazuje (např. prodat licenci někomu jinému), je toto ustanovení neplatné, protože český zákon to povoluje.

2.1.2 Kontrola užívání legálního softwaru

Kontrolu legálnosti softwaru provádí specializované oddělení Policie ČR. Žádná jiná organizace nemá právo občany kontrolovat. Softwarové firmy vytvořily organizaci BSA, která by se měla zabývat osvětou v oblasti licencování software, někdy však sklouzává až k zastrašování uživatelů.

2.2 Modely licencování software firmy Microsoft

Poznámka: Licencovat operační systémy Windows firmy Microsoft v běžných licenčních programech pro školy není možné. Více informací je uvedeno přímo v kapitole o operačních systémech.

Firma Microsoft nabízí dva typy licenčních programů:

- Jednotlivé licence programů či programových balíčků (MS Office...) na jednotlivé počítače za školní ceny.
- Multilicence mnoha svých programů (kromě OS Windows, viz výše) pro celou školu bez ohledu na počet počítačů/zařízení, cena licence se počítá podle počtu pracovníků školy.

Select Plus pro vzdělávání a School Agreement nebo Open Value Subscription?

<http://www.microsoft.com/cze/education/schools/>

www.microsoft.com/cze/education/schools/

Multilicenční programy

1. Trvalé licence

Trvalé licence Microsoft jsou počítány podle počtu kvalifikovaných zařízení. Existují dva typy trvalých licencí pro akademické zákazníky:

Select Plus pro vzdělávání

Open Licence pro vzdělávání

Škola má licence v trvalém vlastnictví, ale pouze konkrétní verzi, kterou zakoupila; nemá tedy přístup k nejnovějším verzím v případě, že vyjde aktualizace software. Často se tak stává, že škola učí žáky na zásadně zastaralém software a nepřipravuje je efektivně pro budoucnost.

Aby bylo možné software upgradovat, kdykoliv vyjde nová verze, může si škola připlatit [Software assurance](#) (je nutné objednat zároveň s počáteční objednávkou licencí). Jednodušším a ekonomičtější řešením je přejít na pronájem licencí, jehož automatickou součástí je možnost upgradu.

Školy se od modelu trvalých licencí čím dál více odklánějí směrem k pronájmu licencí.

2. Pronájem licencí

Tzv. anuitní licence, tedy licence v pronájmu, jsou počítány podle počtu zaměstnanců školy, kteří pracují aktivně s PC. Zalicencovány jsou pak všechny počítače ve škole (i nové, nakoupené v průběhu roku), kterých většinou bývá více než zaměstnanců.

EES
(Enrolment for Education
Solutions)

OVS - ES
(Open Value Subscription –
Education Solutions)

School Agreement

Pronájem je oblíbeným způsobem pořízení softwaru z důvodu možnosti rozložení plateb a [Software Assurance](#), která mimo jiné nabízí možnost využívat vždy nejaktuálnější verze produktů.

Jednotlivé programy výborně vysvětluje web firmy Microsoft, viz výše. Proto zde uvedeme pouze několik základních poznámek k nim.

Koupit **jednotlivé licence** na počítače/zařízení je možné:

- Jednorázově napořád zaplatit určitou verzi programu a mít ji: **Microsoft Select Plus**
- Platit každý rok poplatek podle počtu aktuálního počtu počítačů/zařízení a mít k dispozici vždy aktuální verze programů: **School Agreement**

2.2.1 Microsoft Select Plus

Díky uzavření rámcové smlouvy s MŠMT ČR tento program může využívat každá škola. Licence jsou trvalé. Nejčastěji se nakupují licence MS Office Standard (2013), v době vzniku materiálu stála licence na jedno zařízení cca 2 000 Kč.

2.2.2 Microsoft School Agreement

Pomocí tohoto programu se pravidelnými ročními platbami licencují vždy nejnovější verze programů firmy Microsoft. Otázkou zůstává, zda na starších zařízeních je reálné provozovat nejnovější programy a zda se celkové platby ve svém součtu vyplatí.

2.2.3 Open Value Subscription

Tento licenční program se nepočítá podle počtu zařízení, ale **podle počtu pracovníků školy**, kteří pracují s počítači. Jeho velkou výhodou je to, že není zapotřebí sledovat licence na každém zařízení, program automaticky pokrývá všechny počítače školy. **Vyplatí se tehdy, pokud škola má poměrně málo zaměstnanců a přitom hodně počítačů.**

2.3 Další komerční licence

Další firmy dodávající software mají své vlastní licenční či multilicenční programy.

- Firma Adobe má školní ceny jednotlivých licencí svých, poměrně drahých, produktů. Zde je zapotřebí zvažovat nutnost pořízení profesionálních verzí (Adobe Photoshop či Premiere) nebo verzí pro běžné uživatele (označených Elements). I tyto „omezené“ verze většinou dobře vyhoví běžným základním či středním školám a jsou výrazně levnější.
- Firma Corel nabízí často balíčky licencí (15+1) svého kreslicího programu Corel Draw.
- Podobně firma Zoner se svým fotoeditorem Zoner Photo Studio mívá akce pro školy, zde se licence dají pořídit na 7, 20 či neomezený počet počítačů.

2.4 Open Source licence a její využití ve škole, TCO

Open Source znamená doslova otevřený zdroj. Takové programy musí být vždy šířeny i s uvedením zdrojových textů, takže každý (kdo má potřebné znalosti) může přesně zjistit, jak takový program funguje. Každý ho také může vylepšit, opravit v něm chybu, použít ho ve svém programu, vždy však musí takový produkt opět distribuovat jako Open Source. Přesné podmínky pak stanovuje licence GPL (General Public Licence – všeobecná veřejná licence). Nejrozšířenější takovou licencí je **GNU/GPL (GNU General Public Licence)**.

Poznámka: Myšlenku svobodného softwaru formuloval v polovině 80. let minulého století Richard M. Stallman, do té doby programátor na univerzitě v USA. Podle R. Stallmana přináší svobodný software uživatelům svobodu ho spouštět, kopírovat, distribuovat, studovat, měnit a zlepšovat. Vychází

z myšlenky, že informace jsou pro člověka základní životní potřebou, podobně jako vzduch nebo voda, a je proto nutné, aby k nim každý člověk měl zajištěn přístup zdarma dostupnými prostředky. Stallman založil projekt GNU, jehož cílem bylo vytvořit svobodný (unixový) operační systém. Systém GNU brzy obsahoval všechny důležité komponenty s výjimkou jádra. To začal vytvářet Linus Torvalds v roce 1991 a časem dostalo název Linux. Kombinací systému GNU a jádra Linux pak vznikl tzv. GNU/Linux systém, který dnes je základem Androidu, používá se na serverech, superpočítačích, oživuje síťové prvky a další IT zařízení.

2.4.1 Využití Open Source programů ve škole

Open source programy jsou z hlediska užití ve škole zdarma. To je jejich zásadní výhoda, nemusíme se starat o počet licencí apod., můžeme je nainstalovat na všechny školní počítače.

Známý open source software [editovat | editovat zdroj]

- operační systémy GNU/Linux, FreeBSD, FreeDOS, ReactOS, OpenSolaris, Android
- databázové servery MySQL, Firebird, PostgreSQL
- webservery Apache, nginx, lighttpd
- ftp server VSFTPD
- mail servery Postfix, Sendmail
- DNS server BIND
- desktopová prostředí GNOME, KDE
- kancelářský software OpenOffice.org, LibreOffice, Novell Evolution, Mozilla Thunderbird
- internetové prohlížeče Mozilla Firefox, Epiphany, Konqueror, Chrome
- monitorovací software Zenoss, nmap, nagios
- bitmapový editor GIMP
- 3D grafický editor Blender
- vektorový editor Inkscape
- program pro sazbu dokumentů Scribus
- multimediální přehrávače VLC media player, Totem, Amarok, Juk, Kaffeine, Rhythmbox,
- multimediální centrum XBMC
- různé kodeky: seznam otevřených kodeků, formátů a kontejnerů
- DOSový audio přehrávač MPXPLAY
- překladáče jazyka „C“ (včetně „C++“ a některých dalších) GCC a OpenWATCOM
- překladáč FreeBASIC
- podcatcher (program pro stahování multimediálních souborů, podcastů) Juice
- archivační a kompresní program 7-Zip
- hry Frozen Bubble, Battle for Wesnoth, OpenArena, MegaGlest, Tux Racer,
- komunikační software Psi (klient), Miranda IM, Pidgin, Empathy, Licq
- editor myšlenkových map FreeMind
- IDE pro vývoj aplikací Eclipse, Netbeans, Anjuta, KDevelop
- prostředí pro vývoj ERP, CRM, SCM aplikací JFire

Otevřený software. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2014-07-21]. Dostupné z:

http://cs.wikipedia.org/wiki/Otev%C5%99en%C3%BD_software

Teoreticky by se dala celá výuka i správa školy postavit na Open Source programech, prakticky to není tak jednoduché.

V podnikové i domácí sféře se Open Source programy ve větší míře neprosadily. Jejich využití s sebou nese náklady na školení uživatelů (které je pro tyto programy často obtížně dostupné), složitější správu, komplikace s přenosem datových souborů jinde dominantních formátů (DOCX, XLSX, PPTX) atd. Tedy to, co firmy nazývají TCO (celkové náklady na vlastnictví) se jeví v tuto chvíli v neprospěch volně šiřitelných programů, i když jsou navenek zdarma.

Navíc rodiče vyžadují/očekávají u žáků znalost Wordu, Excelu a PowerPointu místo práce s textem či tabulkami.

Mnohé volně dostupné programy využíváme běžně a ani nevíme, že jsou to Open Source projekty (prohlížeče Mozilla Firefox, Google Chrome, přehrávače VLC Media Player a MP Player), další stojí minimálně za vyzkoušení, zejména na středních školách (například grafický program GIMP, programovací prostředí Sharp Develop, LMS systém Moodle, kompresní program 7-ZIP, na Open Source systému MediaWiki běží Wikipedie atd.)

2.5 Autorský zákon a texty, obrázky, hudba a video ve výuce i mimo ni

Jsme-li v kontaktu se zákonem, je nejlepší se seznámit s jeho přesným zněním a potom případně s jeho (odborný) výkladem. Autorský zákon má číslo 121/2000 Sb., jeho vyhledání na webu je otázka několika klepnutí myši. Nás zajímají nejvíce paragrafy 30 až 40.

2.5.1 Použití autorských zdrojů (tištěných i z webu) pro svoji výuku

Použití cizích autorských děl pro naše vlastní výukové materiály, tedy pro naše vlastní autorská díla, upravuje §31 s nadpisem **Citace**. Nejlepší bude ho zde citovat:

Do práva autorského nezasahuje ten, kdo:

- a) *užije v odůvodněné míře výňatky* ze zveřejněných děl jiných autorů ve svém díle,
- b) *užije výňatky z díla nebo drobná celá díla* pro účely kritiky nebo recenze vztahující se k takovému dílu, vědecké či odborné tvorby a takové užití bude v souladu s poctivými zvyklostmi a v rozsahu vyžadovaném konkrétním účelem,
- c) *užije dílo při vyučování pro ilustrační účel* nebo při vědeckém výzkumu, jejichž účelem není dosažení přímého nebo nepřímého hospodářského nebo obchodního prospěchu, a *nepřesáhne rozsah odpovídající sledovanému účelu*;

vždy je však nutno uvést, je-li to možné:

- **jméno autora**, nejde-li o dílo anonymní, nebo jméno osoby, pod jejímž jménem se dílo uvádí na veřejnost, a dále
- **název díla a pramen**.

(2) Do práva autorského nezasahuje ani ten, kdo výňatky z díla nebo drobná celá díla citovaná podle odstavce 1 písm. a) nebo b) dále užije; ustanovení odstavce 1 části věty za středníkem platí obdobně.

Poznámka autora: Zákon myslím hovoří poměrně jasně. Přesto raději upozorňuji, že dále uvedený názor není právně závazný, výklad zákona přísluší pouze soudu.

Co z toho vyplývá:

- Pokud užíváme díla **při výuce ve škole** (tj. výlučně k vyučovacím účelům), můžeme většinou užít celé dílo (viz bod c).
- Pokud vytvoříme dokument (prezentaci, text), který **vystavíme na webu všem (tedy nejen našim žákům)**, jedná se o zveřejnění (našeho) samostatného díla a cizí díla můžeme použít pouze v odůvodněné míře (viz bod a). Co je tato míra, zákon nespecifikuje.
- **Vždy musíme uvést jméno autora, název díla a pramen a to podle normy ČSN ISO 690, která platí od 1. dubna 2011.**

2.5.2 Užití obrázků

Obrázky používáme vždy celé, těžko obhájit nějakou odůvodněnou míru. Můžeme je tedy bez ohledu na práva autora užívat pouze pro vyučovací účely, nikoliv je užívat ve svých dílech.

Obrázky je tedy možné použít:

- **Své vlastní** kresby či fotografie.
- **Pouze z volně dostupných zdrojů**, u kterých je toto užití výslovně povoleno.
- **Po zajištění souhlasu autora** (nebo případně majitele autorských práv).

Užití obrázků je navíc ještě komplikované kvůli *osobnostním právům focených osob a právům majitelů ochranných známek*. Tedy pokud vyfotíme na olympiádě sportovce s dresem s olympijskými kruhy (a na snímku bude sportovec poznat) a tuto fotografii zveřejníme, mohla by se focená osoba domáhat újmy na osobnostních právech a olympijský výbor újmy za užití ochranné známky. A pokud podobný snímek stáhneme z webu a zveřejníme, obdržíme samozřejmě v extrémním případě ještě třetí žalobu od fotografa na ochranu jeho autorských práv.

Tip pro kolegy informatiky: Většina světových IT firem má na svých webech v části press perfektní snímky svých produktů, které je (většinou) možné volně používat za splnění určitých podmínek, například zachování značky na produktu, nespojování s hanlivým textem či jiným obrázkem apod.

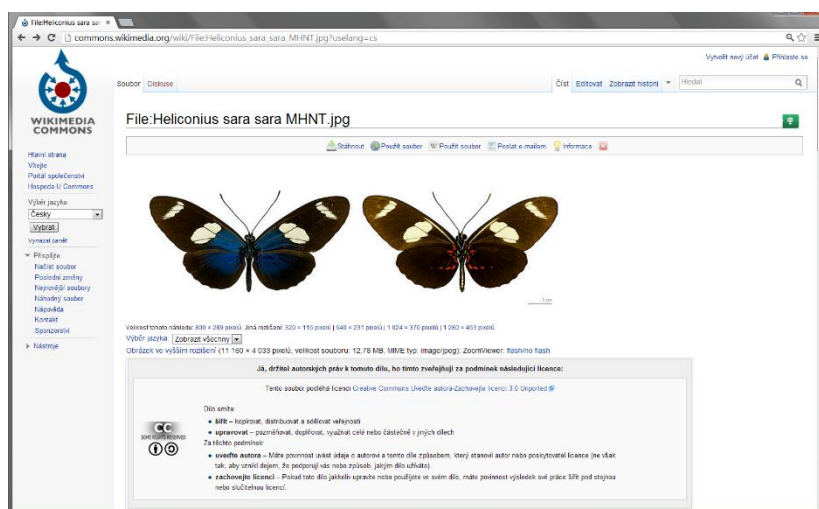
2.5.3 Licence obrázků

Učitel, který použije obrázek, jenž není určen pro vyučovací účely (viz výše) a který bude zveřejněn v nějakém digitálním učebním materiálu, musí mít na zřeteli autorská práva autora snímku. Naštěstí existují lidé, kteří své, někdy velmi kvalitní snímky, dávají k dispozici zdarma. Také některé instituce (NASA.gov apod.) zveřejňují a umožňují dále využít své vynikající snímky. Přesto je zapotřebí znát a respektovat licenci, pod kterou je obrázek zveřejněn. Nejčastěji je pro volné šíření obrázků využívána licence Creative Commons (viz dále), která umožňuje použití obrázku za předpokladu, že výsledné dílo je opět šířeno pod stejnou licencí.

2.5.4 Volně dostupné zdroje obrázků

Nejvíce kvalitních, a pod licencí Creative Commons šířených obrázků, obsahuje projekt Wikimedia Commons, sesterský projekt známé Wikipedie. Najdete ho na webové adrese:

<http://commons.wikimedia.org/wiki>



U každého obrázku na webu Wikimedia.org najdete znění licence stanovující jeho další použití

Další obrazové galerie s volně použitelnými obrázky:

- Obecné: PDphoto – <http://pdphoto.org>, Gimp Savvy – <http://gimp-savvy.com/PHOTO-ARCHIVE>, dále <http://www.freephotobank.org/>
- Galerie výzkumných institucí z oblasti vašeho zájmu. Například na webu NASA (www.nasa.gov) je k dispozici množství velmi kvalitních snímků z oblasti astronomie apod.
- Klipárty: <http://www.openclipart.org/>

Tip: další odkazy na zdroje využitelných obrázků jsou na:

<http://spomocnik.rvp.cz/clanek/10915/TOP-10-ARCHIVU-FREE-OBRAZKU-PRO-UCITELE.html>

2.6 Citování zdrojů (a cloudová služba www.citace.com)

2.6.1 Správné citace obrázků

To, že můžeme obrázek použít, nás nezabývá povinností uvést jeho autora, a to podle normy na citace ČSN ISO 690. Naštěstí pro správné vytvoření citace existují výborné webové nástroje, například web www.citace.com.



Obrázek na webu se cituje stejně jako webová stránka a podle [8] je možné použít buď maximální citaci nebo citaci minimální.

Výše zobrazený obrázek motýlů by v maximální citaci byl citován takto:

DESCOUENS, Didier. File:Heliconius sara sara MHNT.jpg. *Wikimedia Commons* [online]. 2012 [cit. 2012-11-15]. Dostupné z:

http://commons.wikimedia.org/wiki/File:Heliconius_sara_sara_MHNT.jpg?uselang=cs

V minimální citaci pak takto:

[cit. 2012-11-15]. Dostupný pod licencí Creative Commons na WWW:

http://commons.wikimedia.org/wiki/File:Heliconius_sara_sara_MHNT.jpg?uselang=cs

2.6.2 Citování webu, webových stránek a Wikipedie

Pro všechny tyto účely stačí správně zadat údaje do generátoru citací. Důležité je zejména přesně zvolit typ citovaného zdroje, tedy zda se jedná o celý web nebo (častěji) pouze o jednu webovou stránku.

Web

Webová stránka

Příspěvek na webu

Příspěvek na Wikipedii

Jiný dokument

2.6.3 Citování knih

Pokud známe ISBN knihy, stačí do generátoru citací uvést tento údaj a on si sám knihu v integrované databázi knih vyhledá.

Jedním klepnutím získáme správně vygenerovanou citaci:

Údaje Jen povinné údaje

Identifikátory

ISBN*: Vyhledávání ukončeno +

Informatika a výpočetní technika pro střední školy (978-80-251-
Roubal Pavel;

Kniha

ROUBAL, Pavel. *Informatika a výpočetní technika pro střední školy: praktická učebnice*. Vyd. 1. Brno: Computer Press, 2010, 112 s. ISBN 978-80-251-3227-2.

2.7 Licence Creative Commons

Díky svobodnomyslnosti mnoha lidí existují nyní zdroje informací, které jsou legálně zdarma dostupné, a které je navíc možné volně používat v dalších autorských dílech. Vždy je však potřebné se seznámit s přesným zněním licence na zveřejňovaný materiál.

Volná licence někdy není volná úplně:

- Volné užití může být omezeno na nekomerční formu.
- Volné užití může být omezeno na nějaký stát (většinou území USA).
- Volné užití může podmiňovat zveřejnění nově vzniklého materiálu, opět s volně použitelnou licencí.

Různých volných (otevřených) licencí je více, nejčastěji se používají:

Public domain licence je chápána jako možnost nakládat s dílem naprosto volně, tedy užívat ho v libovolných materiálech. Nemá ale přesnou definici.

Creative Commons je skupina licencí, které mohou autoři použít pro své materiály.

Například mohou uvést:

- **by**) [nebo Attribution], což stanovuje povinnost uvést autora původního textu.
- **nc**) [nebo Noncommercial] určuje pouze nekomerční volné použití.
- **nd**) [nebo No Derivative Works] zakazuje změnu původního díla, tedy jeho zahrnutí do odvozených děl.
- **sa**) [nebo ShareAlike] určuje, že díla, ve kterých je takové dílo (nebo z něho odvozené dílo) použito, musí mít stejnou licenci.

Autor může (ale nemusí) použít libovolnou kombinaci omezení: od žádných omezení (uvede CC a nic dále) až po kombinaci všech omezení (uvede CC a zkratkami nebo slovy omezení, například **by**, **nc**, **nd**, **sa**). Tedy pokud je například u fotobanky uvedeno, že obrázky jsou šířeny pod licencí Creative Commons, je třeba u každého snímku číst podrobnější omezení od autora.

GNU Free Documentation License je licence používaná například u svobodné encyklopedie Wikipedia. Stručně řečeno sděluje, že autoři textu neručí za zveřejněné údaje, a určuje, že je možné toto dílo používat za předpokladu, že vzniklé dílo je opět volně dostupné. Pokud je sdělen autor, měl by být vždy uveden, vždy by také měl být uveden zdroj, tj. odkaz na stránku, ze které bylo čerpáno.

Ostatní projekty

Wikipedii provozuje nezisková nadace **Wikimedia Foundation**, která spravuje i řadu dalších otevřených mnohojazyčných **wiki** projektů:

 Wikislovník Výkladový slovník	 Wikizdroje Volně dostupné dokumenty	 Wikicitáty Sbírka citátů	 Wikiknihy Volně dostupné knihy a manuály	 Wikizprávy Otevřené zpravodajství	 Wikiverzita Volně dostupné vzdělání	 Wikidruhy Adresář biologických druhů	 Commons Sdílená sbírka médií	 Wikidata Svobodná databáze vědomostí	 Wikicesty Otevřený cestovní průvodce	 Meta-Wiki Koordinace všech projektů Wikimedia
--	--	---	---	--	--	---	---	---	---	--

3 Zabezpečení počítače, sítě a přístupu do Internetu, obrana soukromí a osobnosti

Mít dnes k dispozici zcela bezpečný počítač vlastně nejde. (Jedině snad jako muzeální kousek, který ovšem nesmí být zapnutý a připojený k žádné síti ☺.) Technickými a organizačními opatřeními je však možné všechna hrozící rizika do značné míry omezit a některá úplně eliminovat.

Zabezpečení počítače je dnes **komplexní problém**, který závisí nejen na technických řešeních, ale do značné míry i na uživatelských návycích a zejména na znalostech každého uživatele počítače. **Proto je velmi důležité mít v této oblasti alespoň základní přehled**, důsledky ztráty nebo odcizení dat mohou být dnes často velmi závažné.

3.1 Technika je na správci sítě

Technická část, zahrnující zejména softwarové nastavení počítače, je věcí odborného pracovníka. Nemusí to být výhradně na tuto oblast školený specialista, každý kvalifikovaný správce sítě by základní nastavení měl být schopen realizovat nebo zkontrolovat.

3.1.1 Aktualizace systému a programů

Dnešní operační systémy a aplikační programy jsou nesmírně složité, neboť obsahují miliony řádků kódu. Je tedy zřejmé, že jsou v nich (právě teď) chyby, o kterých se neví do té doby, než je někdo najde. Takové chyby jsou objeveny každý den a často umožňují napadení počítače.

Po zjištění chyby testery vydá tvůrce programu opravu (tzv. záplatu či aktualizaci) a připraví ji na svém webovém serveru. Náš počítač se o ní díky funkci **Automatické aktualizace** (Windows Update) dozví, záplatu stáhne a systém (program) aktualizuje. To dělá víceméně každý den a mnohé programy už ani uživatelé neinformují a tom, že se pravidelně aktualizují.

Automatické aktualizace všech důležitých programů musí být zapnuté. Kvůli nezáplatovaným chybám v programech by se do počítače mohl přes síť nebo z webové stránky dostat škodlivý kód bez našeho vědomí.

Podobně fungují i aplikace na tabletech a mobilních telefonech, tedy i tato zařízení se neustále aktualizují a stahují nové verze instalovaných programů.

Jinak je to samozřejmě u cloudových aplikací, které se načítají až **v okamžiku použití do prohlížeče webu přes Internet**. Ty jsou aktualizovány provozovateli webových služeb a my se o jejich aktuálnost starat/zajímat nemusíme.

Cloudové služby jsou vždy aktuální díky svým provozovatelům.

3.1.2 Firewall

Každý počítač připojený k Internetu do něho odesílá data s našimi požadavky a přijímá odpovědi (webové stránky, poštu, stažené soubory). Z Internetu by tedy mělo přijít do našeho počítače pouze to, co si (předtím) sami vyžádáme a nemělo by se nikdy stát, že nějaký program z Internetu pronikne bez našeho vědomí do našeho počítače.

Firewall je služba systému, která odděluje jakousi (požární) zdí náš počítač od sítě a dovoluje mu přijmout pouze to, co si sami vyžádáme. Kontroluje příchozí i odchozí komunikaci a v případě, že se mu něco nezdá, komunikaci zakáže a vyžádá si naše schválení či odmítnutí.

Firewall musí být zapnutý a jeho varováním je zapotřebí věnovat pozornost.

3.1.3 Instalace aplikací

Program stažený z jakéhosi obecného webu může obsahovat malware (škodlivé) kódy. **Tento způsob instalace programů je proto minulostí a ve školní síti nemá co dělat.** Pouze odborník může zvážit rizika/přínosy instalace nějaké takové aplikace, zkontrolovat ji a případně (učiteli na jeho počítač) nainstalovat.

Instalace nových programů na školní počítače by měla být vždy věcí správce sítě.

Aplikace na moderní tablety se stahují/instalují pouze z prověřených obchodů (store) jednotlivých firem (viz část o tabletech). Zanesení škodlivého kódu do tabletu je proto velmi nepravděpodobné. Ovšem s instalací programů na školní zařízení souvisí také právní (licenční) otázky, proto je nutné zvážit možnost samostatné instalace potřebných aplikací jednotlivými učiteli a nastavit pro ni nějaká pravidla. Je zřejmé, že pro každý vyučovaný předmět existují (stovky) zajímavých aplikací a bylo by velmi omezující zakázat vyučujícím jejich instalaci, na druhou stranu by správce sítě měl alespoň tušit, jaké aplikace se na školních zařízeních nacházejí.

U tabletů je možnost samostatné instalace aplikací učiteli nutná.



3.1.4 Antivirový program

Nejznámější, a bohužel zatím stále velmi potřebná komponenta zabezpečení počítače. Aktualizovaný systém, funkční firewall a instalace pouze prověřených aplikací ze store by teoreticky mohly znamenat čistý počítač, přesto je tu ještě možnost instalace programů stažených z webu, došlých e-mailem nebo automaticky spuštěných po vložení zavirovaného USB flash disku. **Tedy, stále je možné, že se v našem počítači objeví škodlivý kód a pokusí se spustit (spustíme ho sami).**

V takovém případě antivirový program zablokuje spouštění škodlivého kódu a zobrazí upozornění. Je zřejmé, že antivir může dokonale znát pouze viry, které má popsány ve své virové bázi, musíme proto tuto databázi pravidelně aktualizovat, jinak nás antivir nechrání. Antivir to samozřejmě ví, takže se aktualizuje sám, a to i několikrát denně. Oproti tomu každodenní test počítače dnes není nutný a navíc hodně zpomaluje práci na počítači.

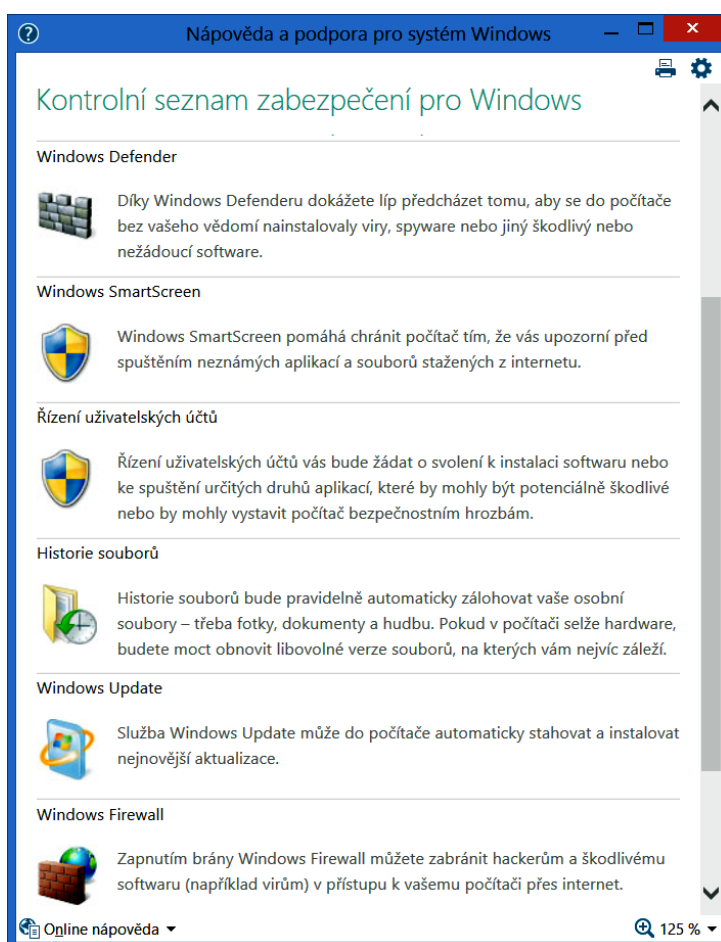
Výběr a instalace antivirového programu je věcí správce sítě. Sledování jeho funkčnosti a aktuálnosti je věcí uživatele počítače.

Antivirový systém Windows Defender je součástí operačního systému Microsoft Windows 8. Komerční antiviry (AVG, AVAST a další) nabízí a horlivě inzerují další bezpečnostní funkce, ale stále platí: základem zabezpečení jsou, více než „dokonalý“ antivir, **znalosti a opatrnost uživatele.**

Nápověda systému Microsoft Windows 8 přehledně vysvětluje jednotlivé oblasti zabezpečení jednotlivého počítače:

3.1.5 Zálohování dat

Pokud selžou bezpečnostní mechanismy nebo prostě technicky „odejde“ pevný disk, ukáže se důležitost pravidelného zálohování dat. Díky školní síti to není zásadní technický problém, zásadnější je ovšem zajištění pravidelnosti záloh.



Pravidelné (automatické) zálohy dat jsou zcela nutné

3.2 Znalosti a opatrnost potřebují všichni

Většina škodlivých kódů (virů, červů atd.) se nešíří díky svému geniálnímu kódu, ale nesmírně jednoduše: **uživatelé si je sami spustí a ještě potvrdí jejich instalaci**. Většina finančních podvodů není provedena dokonalými špiónážními programy, ale tak, že útočník požádá majitele počítače o heslo k jeho bankovnímu účtu a on mu ho pošle! Útoky tohoto typu, které využívají psychologii člověka, bývají označovány jako **sociotechnické útoky**. (Dříve se takovému jednání říkalo podvod, dnes máme na vše odborné pojmy.)

Opatrnost, opatrnost, opatrnost...

3.2.1 Sociotechnické metody

Vycházejí z psychologie člověka, a proto se jim lidé obtížně brání. Znalost základních principů těchto metod a výše zmíněná opatrnost nám dávají dobrý základ pro obranu. Sociotechnické metody využívají několik osvědčených prostředků:

- **Hrají na pocity uživatele** („můžete zachránit nemocného člověka...“) a často **vzbuzují strach** („z vašeho účtu odchází 5.890 Kč, nezaplatil jste 8.658,- Kč, hrozí vám pokuta od Policie ČR atd.“).
- **Nutí jednat okamžitě**, nedávají čas na rozmyšlenou („pokud **okamžitě** nezrušíte transakci, přijdete o...“).

3.2.2 Příklad šíření a fungování viru

Šíření dnešních virů je založeno na sociotechnických podvodech, pěkně to ukazuje příklad jednoho z nejpropracovanějších útoků:

1. Do e-mailové schránky přijde zpráva od exekutora s výpočtem exekuce na nás, v příloze je prý smlouva, na základě které je na nás exekuce uvalena. Samozřejmě musíme reagovat ihned, jinak exekuce proběhne.
2. „Smlouva“ je zkomprimována ve formátu ZIP (proto antiviry zabudované do e-mailových schránek tento vir pustily). Po uložení přílohy na disk a rozbalení ZIP souboru je v něm soubor s příponou **EXE** (tedy **program**, nikoliv dokument).
3. Po spuštění tohoto programu se navenek zobrazí jakási smlouva. (Spuštění by měl kvalitní aktualizovaný antivirový program zabránit a upozornit, že soubor je zavirovaný.) Na pozadí program stáhne a spustí další škodlivý kód, který změní nasměrování adres některých internetových bankovníctví. (Jindy zase začne odesílat soubory a hesla z počítače útočníkovi.)
4. Na podvržené stránce internetového bankovníctví získá díky nám přístupové údaje k našemu účtu. Současně zobrazí výzvu k instalaci „bezpečnostní“ aplikace do našeho chytrého telefonu. Ta potom přepoše zaslaný kód k potvrzení aktivní operace útočníkovi.

Příklad je z obecné oblasti. Ve škole by se mohlo jednat třeba o zasílání přístupových údajů k zadávání známek do školního informačního systému nebo do školní sítě.

Poznámka: Jeden můj kolega, školní informatik, si před časem vytvořil e-mail na jednom z běžně využívaných veřejných serverů a poslal z něho mail všem svým kolegům (jejich e-mailové adresy jsou na stránkách školy) se žádostí o poslání přístupových údajů do školní sítě. Dvě třetiny z nich mu tyto údaje poslalo! Kolik procent by to bylo ve vaší škole?

3.3 Zabezpečení školní sítě a přístupu žáků do Internetu

Tento problém vznikl nedávno a bude nutné ho časem řešit v každé škole. Doby, kdy měli žáci přístup k počítačům připojeným do Internetu pouze v hodinách informatiky, a tedy v době, kdy byli pod dozorem vyučujícího, jsou/budou brzy minulostí.

Mobilní zařízení (žáků) vyžadují možnost blokování přístupu na nevhodné stránky a nejlépe i možnost blokování přístupu do Internetu vůbec.

První otázkou je, zda povolit či nepovolit přístup žákům do školní sítě a do Internetu z jejich soukromých zařízení. Časem nejspíše zjistíme, že je to nutné, že zachovat školu jako (jediné) místo, kde se se svými tablety/mobily/náramky/čtečkami nemohou připojit do Sítě, není možné.

Oddělení žakovské a učitelské wi-fi sítě je samozřejmostí. V okamžiku, kdy povolíme žákům přístup k Internetu bez dozoru, je zapotřebí realizovat další dvě technická opatření:

3.3.1 1. Žádná anonymita

Žakovská zařízení musí být dohledatelná. Tedy každý žák obdrží své uživatelské jméno a heslo do sítě. Na routeru (viz část o připojení k Internetu) běží program, který eviduje, kdy a kam se kteří uživatelé na webu dívali.

Vědomí, že každá zobrazená stránka je dohledatelná ke konkrétnímu zařízení je pro chování žáků velmi důležité.

3.3.2 2. Filtrování obsahu webu (Content Filtr)

Na školním routeru běží filtr, který využívá databáze nevhodných stránek pro určité věkové skupiny žáků a při zadání URL takové stránky ji odmítne zobrazit. Žádný filtr není zcela dokonalý, nevhodných či nebezpečných stránek jsou miliony, ale naprostou většinu běžných nevhodných webů takový filtr odstíní.

Hlídáme/regulujeme také nevhodné stránky.

Poznámka: Sporná je také možnost nechat žáky stahovat obsah z nejpoužívanějších služeb typu Ulozto.cz. Žáci si tam samozřejmě mohli (doma) nahrát své soubory a ve škole je pak stahují, toto však jde přes webové disky nebo přes službu Uschovna.cz také. Častěji tedy budou asi stahovány kopie autorských děl. Navíc, pokud je adresa serveru již povolena, bude velmi těžké oddělit nezávadný obsah například od pornografie, kterou žáci na podobných serverech také lehce najdou.

3.3.3 3. Možnost odpojit zařízení od Internetu

Užitečná je také možnost moci jednoduše odpojit určitá zařízení (jejich skupiny) od Internetu. Učitel pak má možnost v hodině tuto funkci využít.

3.4 Sociální sítě (Facebook [FB]) – „soukromí neexistuje“ a nic se nedá smazat

Současní žáci potřebují ke svému životu počítač připojený k Internetu stejně jako vodu a vzduch. Tráví u něho, až na výjimky, několik hodin denně, bohužel většinou nikoliv svým sebevzděláváním.

- Téměř třetinu času u počítače tráví na Facebooku.
- Zbytek sledováním videí přes Youtube nebo hraním on-line i off-line her.
- Čas věnovaný hledání informací pro své (školní) vzdělávání je v tuto chvíli zanedbatelný.

Poznámka: Pro ty, kteří FB běžně používají je další text asi do značné míry známý, ale mezi vedoucími pracovníky škol je nejspíše určité procento lidí, kteří z nejrůznějších důvodů svůj účet na FB nemají a mají tedy pouze matnou představu o tom, jak FB vlastně funguje.

3.4.1 Facebook je...

Sociální síť, o tom se v médiích mluví stále. Jako obvykle velmi nepřesně a často zavádějícím způsobem. Facebook (dále FB) je spíše společenská než sociální (ve smyslu sociální práce či dávky) síť, je to síť kontaktů a přátel (a přátel přátel). Z hlediska IT je to skvěle vymyšlený a super profesionálně naprogramovaný webový server, který umožňuje zejména:

- sdílení krátkých příspěvků (statusů) na tzv. zdi uživatele (uprostřed stránky),
- označení těchto statusů a téměř všeho ostatního jako *To se mi líbí* („lajkování“ z anglického *like*), (pod každým příspěvkem),
- sledování přátel, zda jsou zrovna on-line (v pravé části okna),
- zprávy, tj. dále on-line komunikaci pomocí psaných zpráv (chat), tato funkce zahrnuje i možnost přenosu souborů (dole téměř vpravo),
- události, zveřejnění událostí a zvaní přátel na tyto události,
- fotogalerie svých fotografií s možností jejich třídění do alb,
- spouštění aplikací přímo na (své) facebookové stránce,
- a další méně podstatné funkce.



3.4.2 Jak Facebook funguje?

- Každý uživatel si vytvoří (pozve) své „přátele“, ostatní uživatele FB. Najde je a odešle pozvánku, oslovený ji může přijmout či odložit (zatím odmítnout).
- Cokoliv napíše na své stránce nahoře do rámečku **Co se vám honí hlavou** se zobrazí těmto přátelům na jejich zdi. Pokud je jich hodně, FB sám dle vaší předchozí aktivity rozhodne, kterým uživatelům se příspěvek zobrazí.
- Cokoliv oni napíší na svém FB, tak se nám (někdy) zobrazí na naší zdi. FB se stará o to, abychom měli stále nové příspěvky a podle svého uvážení/algoritmu zobrazuje zapisované příspěvky více či méně lidem, právě připojeným uživatelům.

Odpovědět na žádosti o přátelství (10)
Zobrazit odeslané žádosti



Robert

Pracuje ve společnosti Pacov
Jan a další společní přátelé (7)

Potvrdit

Odstranit žádost

A to je v kostce vše. Příspěvky samozřejmě mohou obsahovat obrázky, videa i odkazy na weby (FB sám k nim zobrazí náhledy, malé ukázky). Mezi nimi se pravidelně objevují reklamní příspěvky, ze kterých je FB placen.

Technicky je vše samozřejmě opravdu velmi složité, FB si zapíše nový příspěvek do své databáze, zjistí, kolik máme přátel a kdo to je, podle počtu přátel a jejich aktuální aktivity rozhodne, komu jej pošle na zeď a pak zapíše příspěvek na jejich stránky a zajistí jejich jeho zobrazení. Navíc stále sleduje připojené uživatele (naše přátele) a aktualizuje jejich seznam v pravé části okna. A to vše zvládá pro desítky miliónů současně připojených uživatelů z celého světa.

3.4.3 Jak žáci s FB „pracují“?

Většinou pouze čtou příspěvky ostatních a sledují, kdo je zrovna on-line. Občas někomu napíše zprávu o něčem, či o ničem a jen občas něco sami napíší na zeď. Jelikož příspěvky se stále mění a v případě dostatečného množství přátel (běžný počet je větší než 100 lidí) si máte pokaždé s kým psát, dá se to dělat víceméně neomezenou dobu.

Takže ráno před snídaní se podívají, co se „dělo“ v noci, o přestávce ve škole (odolnější i při hodině) zjistí, co se učí či zrovna dělají „přátelé“, po obědě zjistí, co jim uteklo kvůli výuce (času stráveném) ve škole, pomocí zpráv se ev. s někým na něčem domluví, večer zjistí, co bylo zajímavého odpoledne a v noci se podívají, kdo zrovna nespí a co zajímavého napsal, ev. shlédnou odkazovaná videa a prohlédnou si nové obrázky ve fotogaleriích, případně zahrají kousek hry (mnohé hry vyžadují stálou „péči“ o své postavy, jinak ztrácejí sílu/životy apod.).

3.4.4 Základní nebezpečí: nic se nedá smazat!

Rozebírat se žáky z našeho pohledu nesmyslnost trávení mnoha hodin času „na Facebooku“ je zbytečné. Ovšem zásadní upozornění pro, zejména mladší žáky, je velmi důležité: příspěvek, který napíše (fotka, kterou přiloží) se zobrazí desítkám lidí, které si (kdysi) přidali do přátel. Žáci většinou ví, že (svůj) příspěvek mohou smazat (**z webu Facebooku**, všem pak ze zdi zmizí). Ale jen málokdy si uvědomují, že mezitím si někdo mohl zobrazenou stránku (přiložené fotky) **uložit na disk svého počítače** a z něho samozřejmě my nemůžeme mazat nic.

Jednou publikovaný příspěvek (zveřejněné fotky) mohou mít na SVÉM disku uloženy desítky lidí.

3.4.5 Znalosti jsou jako vždy zásadní

Jakmile žáci (učitelé) pochopí, jak počítače, sítě a Internet (a jeho služby, web, mail atd.) pracují, většinou je samotné brzy napadne, že cokoliv napsané/poslané na web (Facebook) je věčné a nedá se smazat, vzít zpět. A že jejich příspěvky vidí desítky lidí a oni vlastně ani neví, kdo všechno. Zakladatel Facebooku Mark Zuckerberg řekl: „doba soukromí je pryč“, většině žáků to však nevadí (mají pocit, že nic závažného nepíší a že nemají co skrývat).

Znalosti vedou k opatrnosti. Pokud počítač/Internet chápu jako tajemnou černou skříňku, není možné se kvalifikovaně (s určením důsledků) rozhodovat.

3.4.6 Facebook a soukromí:

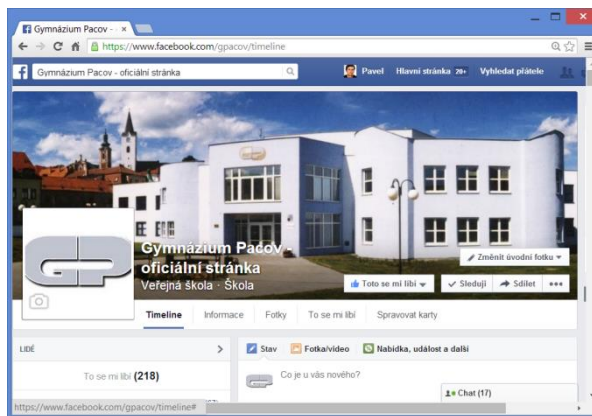
Facebook často své uživatele překvapí tím, že jim nabídne osoby z jejich okolí k přidání do přátel a výrobky, které zrovna jako by potřebovali. Sleduje totiž naši konverzaci, pamatuje si každé kliknutí na *To se mi líbí*, každou napsanou zprávu (i jména v ní uvedená), ví o každé stránce, kterou navštívíme (pokud obsahuje nějaké jeho tlačítko, což je téměř vždy splněno).

Poznámka mírně technická: Facebook pracuje jako databázový systém a každý pokročilejší uživatel nějakého databázového systému (například Bakaláři apod.) ví, že databáze „smazané“ záznamy fyzicky z disku neodstraňují, ale dávají jim pouze příznak: *smazáno, nezobrazovat*. Ovšem tento příznak je možné smazat...

3.4.7 Facebook pro školu?

Většina škol dnes používá svoji Facebookovou stránku jako další médium pro přenos informací o škole směrem k žákům či potenciálním žákům.

Tato forma prezentace má zásadní výhody v dostupnosti základních informací pro žáky současné, bývalé i budoucí (stránka se dá nastavit tak, aby se zobrazila i neuživatelům FB), v jednoduchosti, s jakou se dá naplnit daty a zejména obrazovým materiálem o škole.



Svoji stránku na Facebooku by měla mít každá škola, není složité ji vytvořit a žáci to ocení/uvítají.

3.4.8 Facebook pro učitele?

Měl by mít učitel svůj účet na FB nebo ne? Zde je problém mnohem složitější a nemá jednoduché/jednoznačné řešení:

- Mnozí učitelé prostě FB používají a pak svůj účet samozřejmě mají.
- Jiní se k němu staví skepticky a mají pocit, že FB k ničemu nepotřebují.

Domnívám se, že účet učitele na FB není nutný a jeho přínosnost pro školu/komunikaci se žáky je omezená, a to zejména na základních školách. Na střední škole již nejspíše převažují klady využívání FB učiteli, vždy je ale zapotřebí brát zřetel na omezení a rizika:

Hlavním přínosem učitelů na FB je lepší porozumění svým žákům, kteří v tomto „světě“ žijí.

- Učitel vidí příspěvky a může komunikovat **pouze se žáky, kteří si jej přidají do přátel** (přesněji, zprávy může zasílat i těm, které v přátelích nemá, nemůže s nimi však on-line chatovat). To je zásadní omezení, ani svého třídního učitele nechtějí mít všichni žáci jako „přítele“, dobře vědí, že uvidí (téměř) vše, co napíše a zobrazí, a to nechtějí.
- Učitel tedy může přes FB komunikovat se žáky, s nimiž má i jinak pozitivní vztah (tedy vždy pouze vybranou skupinu žáků, ostatní to mohou výjimečně chápat jako nadřizování). Většinou je to přínosné a efektivní a navázaný vztah se dále buduje.
- Učitel si musí dobře rozmyslet, co napíše do svých příspěvků, jaké zveřejní fotky i co bude „lajkovat“. Nesmí přehánět „sebekontrolu“ aby nepůsobil nevěrohodně, ale také nesmí přehánět otevřenost svých sdělení.

Základní zásada: školní a meziučitelské věci mezi žáky (a tedy ani na FB) nikdy nepatří!

3.5 Kyberšikana a obrana proti ní – nic nesmí být anonymní

Kyberšikana je dnes moderní a hodně skloňovaný pojem. Její řešení není jednoduché. Než však začneme něco „řešit“, je zapotřebí zodpovědět základní otázku:

Jedná se opravdu o (cílený) útok, není to jen „hloupost“ vytvořená z neznalosti? A nechápe postižená strana jako útok něco, co tak nebylo myšleno?

3.5.1 Rozpoznání kyberšikany není jednoduché

Výše uvedené rozdělení není jednoduché, pro další postup je však zásadní. Jednoznačné útoky jsou poměrně zřejmé (z textu či způsobu provedení), neopatrná jednání se posuzují hůře, zejména pokud je postižený chápe jako útok.

Pokud se autor textu nijak neskrývá a texty/obrázky zveřejňuje pod svým jménem, tak je zapotřebí zvažovat, zda jde opravdu o útok nebo ne.

Samozřejmě, útočník si může být naprosto jistý nepostižitelností a tím, že jeho „zprávy“ pro něj nebudou mít žádné důsledky, ale to je spíše výjimečné. Většina žáků ví, že jakékoliv útoky může oběť nahlásit (i Facebooku, nejen škole či rodičům), že je nebude moci zapřít a že pro něho budou znamenat komplikace.

3.5.2 Nevhodné věci je možné řešit ve škole, ne (hned) přes policii

Vyjádření či zpráva, (zejména na Facebooku nebo e-mailové), **kdy jsou autor a příjemce (útočník a oběť) zřejmí**, a kterými se někdo cítí šikanován, je zapotřebí **nejdříve řešit ve škole**. Někdy se ukáže, že útočný úmysl v akci nebyl, nebo útočník svoji akci provedl v okamžitém afektu („naštvaní“) a rád by ji vzal zpět (což už jak je zřejmé z předchozích stran u elektronických médií vlastně nejde).

Pokud k vyřešení nedorazí, následuje kontakt s rodiči a až nakonec ohlášení Policii ČR.

Útoky na sociálních sítích (Facebook...) nejsou příliš časté právě proto, že se nedají provést anonymně. Častější jsou „jemnější ataky“, kdy skupina lidí ve svých příspěvcích „shazuje“ svého spolužáka. Využívají tedy technologie tím samym způsobem, jakým působí ve třídě/škole. Zde je řešení většinou obtížné a vyžaduje dlouhodobý systematický přístup vedení školy.

3.5.3 Zneužívání fotografií, nerespektování osobnostních práv

Dnešní mobily jsou vždy vybaveny fotoaparáty, které „svádějí“ k jejich využívání, či spíše zneužívání. Na své zobrazení jsou pak zejména dospívající žáci (a žákyně) extrémně citliví. Každý z nás má osobnostní práva, která neumožňují/zakazují komukoliv jinému, bez výslovného souhlasu fotografovaného, jeho snímky pořizovat a zveřejňovat.

Fotografování žáků a učitelů jinými žáky bez jejich výslovného souhlasu je zapotřebí přísně zakázat.

Fotografování spolužáka v různých situacích a další incidenty vůči soukromí spolužáků mnoho dnešních dětí vůbec nechápe jako něco nenormálního. **Je zapotřebí je vést k respektování soukromí druhých a tuto oblast sledovat.**

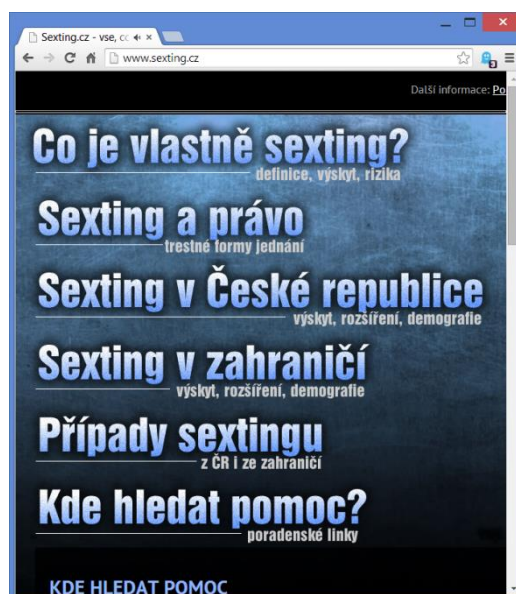
3.5.4 Zřejmé útoky se skrýváním identity

Pokud se útočník od začátku skrývá a využije k útoku anonymní účet na školním počítači, vytvoří si falešnou identitu apod., je jeho záměr někoho úmyslně poškodit zřejmý. V takovém případě je samozřejmě opět zapotřebí zvážit závažnost útoku, nicméně většinou bude zapotřebí spolupráce s IT odborníky pro „vystopování“ útočníka a často spolupráce s Policií ČR.

3.5.5 Sexting

Slovo **sexting** je složeninou vzniklou ze slov sex a textování, a znamená elektronické rozesílání textových zpráv, fotografií či videa se sexuálním obsahem [Zdroj: Co je vlastně sexting, Centrum prevence rizikové virtuální komunikace, Pedagogická fakulta Univerzity Palackého v Olomouci, 2010-2013, on-line. Dostupné z URL: www.sexting.cz].

Typicky se jedná o snímky nahého těla, které vzniknou během partnerského vztahu žáků a které po ukončení vztahu některý z partnerů zneužije.



vá nebo z hlouposti publikuje. Cca 10 % žáků nemá problém s nafocením svých, až erotických, fotografií a podobné procento dětí je ochotno tyto snímky někomu poslat přes Internet. Jestliže mnoho filmů a videí označuje slovem „láska“ projevy dlouhodobě neuspokojeného pohlavního pudu a přihlédneme-li k sociálnímu zázemí mnoha dětí, je zřejmé, že je toto číslo poměrně nízké. Snaha prosadit se a získat „vysněného“ partnera (a někdy i finanční prospěch) za každou cenu se bohužel mezi žáky spíše zvyšuje, než omezuje.

Základní informace:

- Dítě je dle našich zákonů osoba mladší 18 let.
- Děti od 15 let mohou mít intimní styk, ale nesmí se přitom natáčet či fotografovat a zveřejnění takových snímků (i jimi samotnými) je považováno za šíření dětské pornografie.

Případy zřejmého sextingu je nutné řešit s Policií ČR, jedná se o trestný čin.

Nejdůležitější je opět prevence. Žáci by měli vědět, že rozesílání jakýchkoliv fotografií cizích osob může být postihováno a že **pořizování a zejména rozesílání (jakékoliv zveřejnění) fotografií odhaleného těla žáků mladších 18-ti let, které mohou být považovány za pornografické, je závažný trestný čin s právními následky.**

Poznámka autora: Prádlo a plavky? Žáci se při diskuzi na toto téma někdy ptají, jak je to s focením ve spodním prádle a v plavkách. Přesné rozlišení toho, co je a není erotický materiál, je v konečném důsledku u každého případu věcí soudu. Před focením v prádle je však důrazně varuji. Zatímco plavky jsou téměř určitě v pořádku, protože je to oděv určený k nošení na veřejnosti, (spodní) prádlo nikoliv.

3.5.6 Zapojení rodičů

Škola má v prevenci kyberšikany své nezastupitelné místo, mnoho rodičů není schopno své děti kvalifikovaně poučit ani sledovat. To ovšem neznamená, že by rodiče měli být z této problematiky vyřazeni. Naopak, jejich zapojení je zásadní. Protože nemají v této oblasti odborné znalosti, je vhodné jim je nabídnout. Promítnutí odkazů na weby, zabývající se touto problematikou, (viz dále) na třídních schůzkách a zaslání odkazu na tyto stránky e-mailem přiměje část rodičů zabývat se s touto oblastí a umožní jim získat alespoň základní informace.

3.5.7 Vedení/výchova k uvědomělému používání technologií

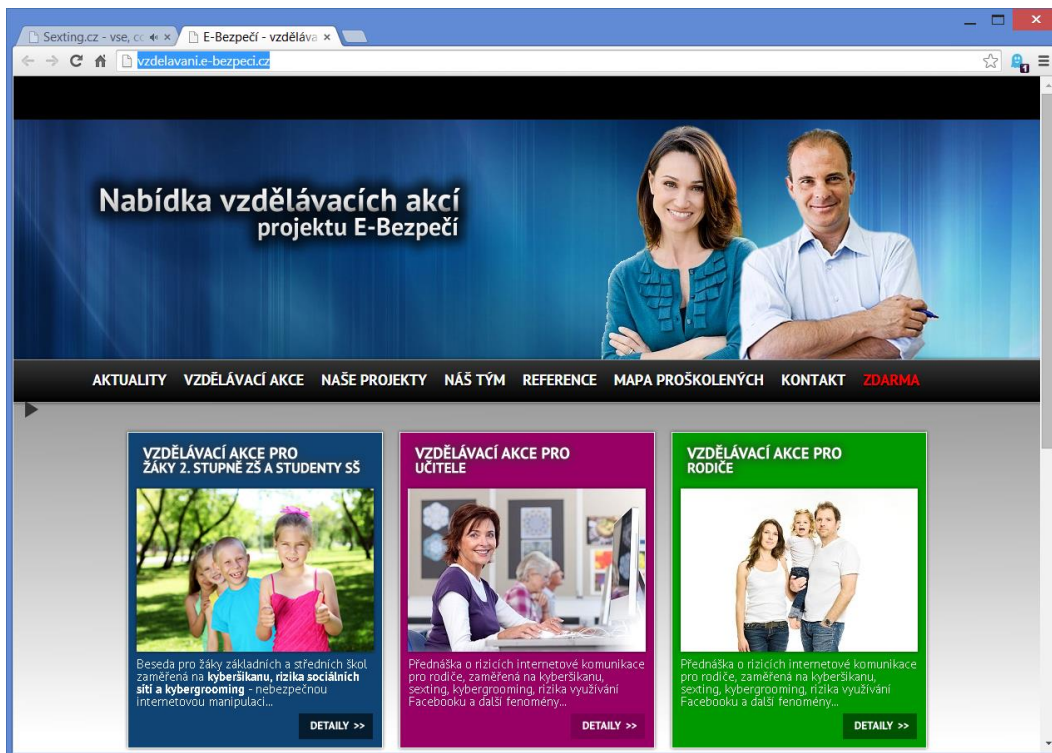
...není věcí pouze předmětu IVT a učitele informatiky. Žáci dnes používají (brzy budou používat) ICT ve všech předmětech. Jsou součástí jejich života mnohem více než u nás dospělých. Dbát na to, ale je nezneužívat, a aby znali rizika s jejich využíváním spojená je nutné a pro jejich život mnohem důležitější než mnoho jiných (odborných) znalostí.

Problematika bezpečného a etického využívání ICT by měla být součástí ŠVP a měla by být sledována nejlépe všemi učiteli.

3.5.8 Další zdroje informací

K výše uvedené problematice existují výborně zpracované webové stránky a instruktážní videa. Určitě se podívejte minimálně na tyto weby:

- www.sexting.cz (viz citace a obrázek výše v textu).
- <http://vzdelavani.e-bezpeci.cz/>



- <http://www.seznamsebezpecne.cz/> Profesionálně a ve spolupráci s Policií ČR zpracovaná videa popisující skutečné případy kyberšikany a zneužívání technologií útočníky a mnoho dalších informací.

