Pravidla k bezpečnému užívání internetu

1. Pravidla pro děti k bezpečnějšímu užívání internetu

1) Nikdy nesděluj adresu svého bydliště, telefonní číslo domů nebo adresu školy, kam chodíš, jména a adresy rodičů a rodinných příslušníků i jejich telefonní čísla do práce, někomu, s kým jsi se seznámil/a prostřednictvím internetu, jestliže Ti to rodiče (nebo lidé, kteří se o Tebe starají) přímo nedovolí.

2) Pokud se neporadíš s rodiči, neposílej nikomu po internetu fotografii, číslo kreditní karty nebo podrobnosti o bankovním účtu a vůbec žádné osobní údaje.

3) Nikdy nikomu, ani nejlepšímu příteli, neprozraď heslo nebo přihlašovací jméno své internetové stránky nebo počítače.

4) Nikdy si bez svolení rodičů nedomlouvej osobní schůzku s někým, s kým jsi se seznámil/a prostřednictvím internetu. Doma musí bezpodmínečně vědět, kam jdeš a proč. I když Ti rodiče (nebo lidé, kteří se o Tebe starají) dovolí se s takovým člověkem sejít, nechoď na schůzku sám/sama a sejděte se na bezpečném veřejném místě.

5) Nikdy nepokračuj v chatování, když se Ti bude zdát, že se tam probírají věci, které Tě budou přivádět do rozpaků nebo Tě vyděsí. Vždy o takovém zážitku řekni rodičům (nebo lidem, kteří se o Tebe starají).

6) Nikdy neodpovídej na zlé, urážlivé, nevkusné nebo hrubé e-maily. Není Tvoje vina, že jsi tyto zprávy dostal/a. Když se Ti to stane, oznam to rodičům.

7) Nikdy neotvírej soubory přiložené k elektronickým zprávám (e-mailům), pokud přijdou od lidí nebo z míst, které neznáš. Mohou obsahovat viry nebo jiné programy, které by mohly zničit důležité informace a významně poškodit software počítače.

8) Vždy řekni rodičům (nebo lidem, kteří se o Tebe starají) o všech případech nepříjemných, vulgárních výrazů na internetu, totéž platí pro obrázky s vulgární tematikou.

9) Vždy buď sám/sama sebou a nezkoušej si hrát na někoho, kým nejsi (na staršího, na osobu jiného pohlaví apod.).

10) Vždy pamatuj na následující pravidlo a chovej se podle něho: jestliže některá webová stránka bude obsahovat upozornění, že je určena jen pro dospělé nebo jen pro lidi od určitého věku, musí se to respektovat a ti, kteří nevyhovují kritériím nemají takovou stránku otevírat.

11) Domluv se s rodiči na pravidlech používání internetu a poctivě je dodržuj. Především se domluv, kdy můžeš internet používat a jak dlouho.

12) Provždy si zapamatuj další pravidlo: když Ti někdo na internetu bude nabízet něco, co zní tak lákavě, že se to nepodobá pravdě, nevěř mu – není to pravda.

13) Jestliže na internetu najdeš něco, o čem jsi přesvědčen, že je to nelegální, oznam to rodičům.

2. Pravidla pro rodiče k bezpečnějšímu užívání internetu jejich dětmi

1) Nechte se dítětem poučit o službách, které používá, a ujistěte se o jejich obsahu. Tím zlepšete svou znalost internetu.

2) Nikdy svému dítěti nedovolte setkání o samotě s někým, s kým se seznámil na internetu, bez Vaší přítomnosti. Pokud k setkání svolíte, své dítě doprovoďte.

3) Zajímejte se o internetové kamarády svých dětí stejně jako se zajímáte o jejich kamarády ve škole.

4) Základem při komunikaci rodiče s dítětem je otevřenost. Při nepříjemných zkušenostech dítěte s děsivým obsahem nebo nepříjemným člověkem není řešením trestat dítě nebo mu dokonce bránit používat internet, ale poradit mu, jak se v budoucnu nepříjemným zkušenostem vyhnout. Jak se rodič při podobné situaci zachová, určuje, zda se mu dítě svěří i v budoucnu.

5) Na místo s nevhodným obsahem se může dítě dostat zcela náhodou. Pro tyto případy neexistuje stoprocentní ochrana a vyplatí se spíše vychovávat dítě tak, aby si podobné skutečnosti interpretovalo způsobem odpovídajícím jeho věku, protože s dítětem nemůžete trávit všechen volný čas.

6) Riziko vstupu na stránku s nevhodným obsahem lze snížit jednak prostřednictvím možností zabudovaných přímo do internetového prohlížeče, jednak prostřednictvím speciálních programů obsahujících nepřetržitě aktualizovaný seznam stránek pro děti nevhodných. Tyto programy bývají k dispozici zdarma.

7) Uvažujte o společné e-mailové schránce se svými dětmi.

8) Dávejte si pozor na soubory, které dítě z internetu stahuje a ukládá je na disk.

9) Sledujte, kolik času dítě u počítače stráví. Nepohybuje se ve světě virtuálních her častěji než na hřišti? Nepohybuje se víc na chatu a nekomunikuje s anonymními osobami (skrytými za chatovými přezdívkami) častěji než se svými kamarády Nepozorujete u něj projevy připomínající závislost na chatování či počítačových hrách? Nedovolte, aby virtuální realita dítě příliš pohltila!

10) O radu při výchově dětí ke správnému užívání internetu můžete požádat pedagoga, psychologa či pracovníky internetových firem.

3. Bezpečnost při práci na internetu

Stránky http://www.bezpecneonline.cz/ vám mohou pomoci chránit se před hrozbami internetu. Najdete zde řadu srozumitelných textů rozdělených do témat.

4. Hesla

I to nejlepší zabezpečení na světě je zcela neúčinné, zná-li osoba se zlými úmysly a heslo. Taková osoba pak může dělat všechno, co můžete dělat vy. Někteří lidé používají hesla, která je velmi snadné uhodnout, např. „heslo“. Jiní používají jednoduchá slova, která může uhodnout pomocí programu, který zkouší všechna slova ze slovníku. Pokud používáte stejné heslo na všech stránkách, stačí, aby ho získal jednou – a získá přístup na všechny stránky.

Správné heslo nemusí být ve skutečnosti existujícím slovem. Může jít o kombinaci písmen, číslic a symbolů z klávesnice. Mělo by mít nejméně sedm znaků. Čím delší heslo, tím je obtížnější ho uhodnout. Nesmí obsahovat vaše uživatelské jméno, skutečné jméno ani jméno společnosti. Skládá se z velkých a malých písmen, číslic a symbolů z klávesnice, t. j.: ` ~ ! @ # $ % ^ & ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /). Mějte však na paměti, že – pokud cestujete – některá z těchto znamének může být na klávesnici v zahraničí obtížné zadat. Pravidelně hesla měňte.

Nepracujte bez hesel. Nepoužívejte běžné slovníkové výrazy. Slovo, které použijete jako heslo, by se nemělo vyskytovat v žádném slovníku vašeho mateřského jazyka. Nepoužívejte výrazy, které je snadné uhodnout se znalostí souvislostí, např. oblíbené fotbalové mužstvo, datum narození, jméno partnera, domácích zvířat apod. Nepoužívejte hesla, která jste neobměnili po několik měsíců. Chraňte si svá hesla. Nikdy neprozrazujte své heslo nikomu jinému. Nezadávejte své heslo v situaci, kdy někdo jiný může vidět, co píšete. Používejte různá hesla u různých služeb. Jiné heslo mějte zejména ke své bankovní stránce. Pravidelně své heslo obměňujte. Nepoužívejte opakovaně heslo s drobnou úpravou (např. heslo2, heslo3). Nezapisujte si své heslo. Používejte mnemotechnické pomůcky, abyste si ho zapamatovali. Sestavte např. heslo z prvních písmen každého ze slov tvořících známý citát nebo nahraďte písmena číslicemi (např. „5“ použijte místo písmene „s“, „3“ místo „e“ apod.). Nezasílejte své heslo e-mailem. Žádná solidní firma to po vás nebude chtít. Domníváte-li se, že někdo jiný zná vaše heslo, okamžitě ho změňte.

5. Počítačová etika

Desatero přikázání počítačové etiky
(převzato z The Computer Ethics Institute)

- ✓ Nepoužiješ počítače ke škodě jiného.
- ✓ Nebudeš ničivě zasahovat do práce druhých lidí.
- ✓ Nebudeš slídit v souborech jiných lidí.
- ✓ Nepoužiješ počítače ke krádeži.
- ✓ Nepoužiješ počítače pro křivé svědectví.
- ✓ Nepoužiješ nebo nepořídíš kopii softwaru, který jsi nezaplatil.
- ✓ Nepoužiješ neoprávněně počítačového zdroje jiných lidí.
- ✓ Nepřivlastníš si intelektuální dílo jiného.
- ✓ Budeš přemýšlet o společenských důsledcích programu, který jsi stvořil.
- ✓ Budeš používat počítače ohleduplně a s úctou.

6. Jak se bránit proti nevyžádaným e-mailům

Co je to spam?

Spam je obecný výraz pro nevyžádaná a nechtěná sdělení, která jsou zasílána na vaši internetovou adresu nebo (ve formě SMS) na váš mobilní telefon. Jinak řečeno, z hlediska elektronické pošty jde vlastně o nežádoucí elektronické "smetí". Spam má zpravidla podobu inzerce či obchodního sdělení reklamního charakteru, přičemž je hromadně rozesílán na obrovská množství (může jít i o miliony) elektronických adres. Sdělení, které spam obsahuje, se vás většinou snaží přesvědčit, abyste navštívili určité internetové stránky, abyste je dále procházeli a abyste si co nejdříve objednali určitý konkrétní produkt nebo službu.

Statistiky vypovídají o tom, že celosvětově je více než polovina odeslaných e-mailů spamem. Velké množství jednotlivců i organizací dnes už má se spamem řadu nepříjemných zkušeností. Kromě toho, že spam způsobuje uživatelům nemálo různých potíží, nese s sebou také navyšování jejich nákladů (např. na systémovou kapacitu počítačů) nemluvě o tom, kolik času zabere jeho následné odstraňování. Spam někdy může být i příčinou poškození vašeho počítače, a co je horší, v současnosti se stále častěji zneužívá k trestné činnosti. Spam bývá rovněž nositelem počítačových virů či jinak škodícího softwaru. Jednou z dalších protizákonných aktivit je tzv. *phishing*. Jde o druh internetového podvodu, jehož cílem je přimět adresáta, aby (neoprávněné osobě) poskytl své důvěrné informace, jako PIN kód, číslo kreditní karty apod. Obsah e-mailů tohoto typu vyvolává přesvědčivý dojem, že odesílatelem je důvěryhodná instituce (například banka či jiný peněžní ústav). Také falešná identita odesílatele dokáže vytvořit dokonalou iluzi solidnosti a spolehlivosti.

Jak se lze vypořádat se spamem?

Jak správně postupovat:

- Vymažte, a to **bez jejich otevírání**, všechny podezřelé e-mailové hlavičky a/nebo e-mailové adresy, které často pocházejí od osob nebo organizací, jež neznáte.
- Otevíráte-li **soubory přiložené k elektronické poště**, buďte opatrní. Mohou obsahovat viry, které se aktivují ve chvíli, kdy je takový soubor otevřen.
- Instalujte na svém počítači kvalitní **antivirový program** a tzv. **firewall**, přičemž nezapomeňte dbát na jejich pravidelnou aktualizaci. Nedostatečně chráněný počítač může být prostřednictvím internetu někým zneužit k tomu, aby se sám stal rozesílatelem dalších spamů, aniž byste vy sami měli sebemenší tušení, že k něčemu takovému dochází. Ve vaší prodejně s výpočetní technikou jsou tyto programy běžně k dostání. Můžete je rovněž získat od vašeho poskytovatele internetového připojení.
- Neváhejte ani s instalací některého z **antispamových filtrů**, které jsou rovněž k dostání v příslušných obchodech. Filtraci spamů si můžete zařídit i prostřednictvím vašeho poskytovatele internetového připojení.
- Zřiďte si současně **několik různých elektronických adres**, přičemž vaši hlavní adresu poskytněte pouze těm osobám a organizacím, které znáte a k nimž máte naprostou důvěru.
- Je-li po vás požadována nějaká důvěrná informace v e-mailu, který podle všeho pochází od vaší banky nebo od jiného peněžního ústavu (například číslo vašeho bankovního účtu nebo přihlašovací kód), **ověřte si telefonicky**, zda takový požadavek skutečně pochází od uvedené instituce: tento typ žádostí je totiž velmi neobvyklý.

- Odesíláte-li svou elektronickou poštou na více e-mailových adres najednou, využívejte funkce **slepých kopií** – ostatní použité adresy se pak příjemcům nezobrazují.
- Příjem spamu můžete ohlásit úřadu, který má kompetence se touto věcí zabývat a disponuje právem takovou činnost penalizovat (viz odkaz na OECD v oddíle Legislativa týkající se spamu).
- Chcete-li mít jistotu, že obsah vašich e-mailů by měl znát pouze a jenom jejich adresát, **kódujte** své důležité e-maily pomocí **šifrovacích programových prostředků**. Je to obdoba zapečetění dopisu odeslaného klasickou poštou.

Čeho bychom se měli vyvarovat:

- **Nenakupujte! Neodpovídejte!** Na spam nereagujte. Neobjednávejte a nekupujte produkty ani služby nabízené touto cestou a nereagujte ani na přihlašovací / odhlašovací (suscribe / unsuscribe) zaškrtávací políčka zobrazená ve spamových e-mailech nebo na odkazovaných webových stránkách. Nákupy, které vycházejí ze spamových nabídek leda podpoří a posílí nekalý spamový byznys. "Odhlášení" (tedy odmítnutí nabídky) slouží v tomto případě pouze k tomu, aby se spamer ujistil, že odeslal svůj e-mail na platnou elektronickou adresu. Takovou adresu pak může zahrnout do své databáze.
- Nereagujte ani na **falešná oznámení o virové nákaze** (tzv. **hoax**). Taková oznámení vás chtějí donutit, abyste učinili opatření proti údajným virům. Ve skutečnosti však o žádnou hrozbu počítačového viru nejde. Naopak samotné otevření této zprávy může váš počítač poškodit. V této souvislosti vás podobné zprávy často vyzývají, abyste je posílali dále, co největšímu počtu lidí. Hoax se tak šíří cestou řetězové reakce a může ohrozit i počítače dalších adresátů.
- Buďte opatrní, poskytujete-li někomu prostřednictvím elektronické pošty či internetu důvěrné informace o vaší osobě (číslo bankovního účtu, PIN kód, přihlašovací heslo apod. Raději si dobře rozmyslete, zda je poskytnutí těchto údajů nezbytné a zda osoba nebo organizace, která po vás takové údaje požaduje, je skutečně tím, za koho se vydává.
- Buďte ostražití i v situaci, kdy dáváte k dispozici vaše kontaktní informace (např. e-mailovou adresu, telefonní číslo, číslo faxu apod.). Dobře si zvažte, komu takové informace dáváte a kdo k nim pak může mít přístup.

zdroj: www.uoou.cz

8. Soukromá elektronická pošta zaměstnanců

Zaměstnancům lze tolerovat využívání počítačové sítě zaměstnavatele pro zasílání soukromých mailů, pokud se stanoví ve vnitřním předpisu určitý limit, např. 10 mailů týdně a podmínky pro posílání této pošty, například

- zaměstnanec je povinen ukládat soukromou poštu odděleně od služební do složky, kterou všichni zaměstnanci označí jednotně – „soukromá“
- pro soukromou poštu musí zaměstnanci využívat jen svoji soukromou mailovou adresu
- na konci každého týdne musí zaměstnanci tuto soukromou poštu zcela odstranit
- zaměstnavatel je oprávněn ke kontrole těchto podmínek, zejména ke kontrole adresátů a seznamu mailových adres, počtu mailů, názvů mailů „předmět“ a názvů připojených příloh. Není oprávněn ke kontrole obsahu mailů.

7. Jsou webové stránky povinné?

Povinnost zveřejňovat informace způsobem umožňujícím dálkový přístup je dána zákonem č. 106/1999 Sb. o svobodném přístupu k informacím. Ten určuje, které subjekty musí umožnit tento přístup, tedy které musí mít internetové stránky. Patří sem státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce, případně subjekty, kterým to uložil nějaký jiný zákon. **Školy zde uvedeny nejsou.**

Také školský zákon č. 561/2004 Sb. se nezmiňuje o povinnosti škol zveřejňovat informace způsobem umožňujícím dálkový přístup, v jednom případě ukládá tuto povinnost krajským úřadům.

Školský zákon jen v řadě případů ukládá řediteli, aby zveřejnil informace na přístupném místě ve škole nebo školském zařízení (školní vzdělávací program, školní řád, vnitřní řád, termín a dobu pro podání žádostí o přijetí dětí k předškolnímu vzdělávání, termíny přijímacích zkoušek atd.).

Internetové stránky tedy jsou povinné pro střední školy, vyšší odborné školy. Ale jsou velmi účinným komunikačním prostředkem, a i když nejsou "povinné" pro základní a mateřské školy, určitě jsou žádoucí.

Školy také mohou využít ustanovení zmíněného zákona č. 106/1999 Sb., který v § 3 říká, co je to zveřejněná informace:
*(5) **Zveřejněnou informací** pro účel tohoto zákona je taková informace, která může být vždy znovu vyhledána a získána, zejména vydaná tiskem nebo na jiném nosiči dat umožňujícím zápis a uchování informace, vystavená na úřední desce, **s možností dálkového přístupu....***

Tedy tím, že škola umístí na webové (internetové) stránky určité informace, je tím zveřejnila a může prokázat, že tím splnila povinnost, uloženou zákonem.

Na webových stránkách by bylo vhodné umístit řadu důležitých informací, namátkou
- výroční zpráva o činnosti školy,
- školní řád (včetně pravidel pro omlouvání absence žáků, postupu při zjištění, že je žák pod vlivem alkoholu, návykových látek, pravidla hodnocení žáků)
- stravování – zásady přihlašování, ohlašování, odběru jídla během nemoci žáka...
- školní vzdělávací program (zkrácená verze)
- organizace školního roku – prázdniny, zápis do první třídy, přijímací řízení, třídní schůzky
- některé další směrnice – prevence sociálně patologických jevů, minimální preventivní program,
- řád školní družiny, stanovení úplaty, zásady pro možnost snížení či prominutí úplaty
- řád mateřské školy
- formuláře

Při zveřejňování informací musí školy dbát na ochranu osobních údajů podle zákona č. 110/2019 Sb., o zpracování osobních údajů. Pokud zde zveřejňuje fotografie žáků, jejich jména (např. reprezentanti školy v soutěžích, úspěšní řešitelé apod.), měla by k tomu mít podepsaný souhlas zákonných zástupců žáka.

Pokud škola shromažďuje osobní údaje žáků podle zákona (např. v matrice školy), nepotřebuje k tomu souhlas. Zveřejnění údajů na webu ale přesahuje rozsah povolený zákonem, a proto je k tomu nutný souhlas rodičů.