Pravidla chování na webu

1. Internet slouží ve škole jako zdroj informací a podkladů pro výuku a vzdělávání.
2. Prostřednictvím Internetu má každý člen školní komunity (žáci a rodiče, učitelé a všichni další zaměstnanci školy) přístup ke školnímu webu a účast na jeho podobě.
3. Když komunikuješ přes Internet (e-mail, instant messaging, internetová telefonie, chat), dbej ve vlastním zájmu na „Desatero bezpečného Internetu“.
4. Do světa Internetu vstupuj vždy s určitým cílem – nesnaž se jenom „zabít“ čas.
5. Cokoli na Internetu děláš, vždy se snaž poznat něco nového o světě, o lidech a o sobě a rozvíjet své schopnosti.

Kromě mnoha skvělých a úžasných věcí
je Internet ale také místem s temnými kouty,
kde na Tebe, Tvůj počítač, Tvou peněženku
a případně i na Tvůj život či zdraví,
čekají skutečná ohrožení.

Tady je přehled o většině z nich:

1. **Dialer.** Mnoho stránek například s pornografickým či násilným obsahem Tě bez Tvého vědomí přesměruje na vytáčené připojení, kde za minutu zaplatíš třeba 79 nebo i víc korun (a v případě přesměrování do zahraničí pak eur či dolarů). Můžeš se snadno zadlužit na celý život!

2. **Flaming.** Snadno se také může stát, že Tě někdo bude chtít naštvat či urazit, a například do komentáře k Tvému článku na webu nebo blogu Ti napíše nějaké lži či nadávky. Informuj o tom rodiče nebo učitele! Když se naopak ty pustíš do útočníka a začnete spolu „bojovat“, právě vypukl Flame war, čili válka. Buď raději tvůrcem míru.

3. **Grooming**. Buď velmi opatrný/opatrná, když Ti bude na chatu, IM nebo v e-mailu chtít někdo dát nějaké dárky nebo Tě někam vzít či Ti něco ukázat. Mohl by také jenom zneužít Tvé důvěry a ublížit Ti! Také by mohl zneužít Tvé důvěřivosti a ublížit Tvé rodině – například tím, že by z Tebe mohl vymámit různé informace (jak se kdo z rodičů vrací domů) či Ti přímo vzít klíče od bytu a vykrást váš byt. Raději se hned svěř rodičům nebo učitelům, ke kterým máš důvěru!

4. **Hoax.** Možná jsi už obdržel mail či zprávu, žes vyhrál nějakou cenu nebo že Tě někdo žádá o pomoc. Nebo že máš zprávu s nějakým upozorněním (například: „Pozor na nejničivější vir v historii“, „Dnes se nepřipojujte na web, nebo zničíte své PC“ apod.) poslat všem známým či jim rozeslat řetězový dopis (zaručeného) štěstí. Jsou to většinou poplašné zprávy, varování před neexistujícím nebezpečím, které vzbuzují paniku či falešné naděje anebo zneužívají lidské solidarity a jen zatěžují komunikaci v Internetu. Ruce pryč od toho!

5. **Spam.** Někdy máš v poště spoustu zpráv s reklamami na ten či onen výrobek – je to pošta, kterou sis nevyžádal/nevyžádala a kterou nechceš; pošta, která Ti jenom zabírá místo ve schránce a navíc může obsahovat nějaký malware. Ani Ty nerozesílej zprávy takového typu – mohl/mohla by ses navíc dopustit trestného činu!

6. **Spim.** Je totéž, co spam – ale u instant messagingu.

7. **Scam.** Na něj velký pozor – jedná se o různé podvodné hry či loterie, které slibují velké výhry, ale za cenu toho, že se musíš zapojit za určitý finanční obnos, který už nikdy nespatříš (ani výhru…)!

8. **Sociální inženýrství.** Možná jsi slyšel slova jako *phishing* a *pharming*. To první označuje podvodné jednání, kdy Ti přijde například důvěryhodně vypadající mail jakoby od Tvé banky a požaduje jako potvrzení k nějaké transakci ověření totožnosti (čili přístupové údaje k účtu). Když je poskytneš – už jsi bez peněz. To druhé slovo označuje akci ještě rafinovanější: aniž to víš, jsi přesměrován na stránku podvodníka, která vypadá velmi podobně té, ke které ses chtěl připojit a Ty nevědomky zadáváš citlivé údaje (uživatelská jména, hesla, čísla účtů, PINy) a výsledek je stejný. Někdo Tě podvedl a okradl. Nejnovější hit pak je **ransomware.** Přijde Ti mail (obvykle) od policie, že Ti zablokovala počítač, neboť

jsi na webu dělal nějaké nepravosti. Odblokování je možné, ale za nějakou úplatu. Ale: je to jen „jako“ – policie se takto nechová. Mail Ti poslal nějaký škůdce…

9. **Malware**. Zkratka malware znamená malicious software, tedy škodlivý SW. Tímto pojmem se souhrnně označují nežádoucí a nebezpečné programy, které se mohou dostat do počítače bez Tvého vědomí. V počítači pak špehují, co děláš nebo kradou Tvá hesla (spyware), různě škodí nebo otvírají vrátka pro útoky zvenčí (trojské koně a červi), anebo přímo ničí programy či dokonce součástky počítače (viry). Kde se berou?
    a. Často tyto programy dostaneš (i neúmyslně) v poště – buď proto velmi opatrný při otvírání příloh! Otvírej přílohy pouze od známých lidí. Když najdeš soubory s „divným“ názvem nebo se spustitelnou příponou (.com, .exe), raději ho smaž nebo se u známého ujisti, že takový soubor opravdu posílal a nech ho prověřit antivirovým programem! Dávej pozor i na soubory zkomprimované (.zip, .rar a podobné) a v poslední době i na soubory v přenositelném formátu (.pdf). A hlavně neklikej na odkazy – obvykle vedou na podvodné stránky.
    b. Často si je stáhneš z webu, například když stahuješ nějaký nový software. Takový software nikdy neotvírej přímo, ale nejprve si ho ulož, prověř „antiprogramy“ a teprve potom spusť!
    c. Často si natáhneš nějakou „havěť“ do počítače také na „flešce“, „empétrojce“ nebo „cédéčku“ od kamaráda – externí média vždy prověřuj!
    d. Raději se vyhýbej stránkám s asociálním obsahem (pornografie, extremismus, násilí, nelegální software apod.) – lidé, kteří je provozují, většinou nejsou naladěni na to, aby Ti pomohli, ale aby Tě nějak „oškubali“, a proto takové stránky mohou být plné výše uvedených bezpečnostních rizik.
    e. Pozor také na nejrůznější programy typu shareware/freeware, které mohou být zajímavé (i cenné), ale mohou také obsahovat mnohá z výše zmíněných rizik a omezit funkčnost Tvého počítače nebo jej i zničit.

10. *Důležitá poznámka*: Jednotlivé typy škodlivého softwaru se často kombinují, takže nelze ani jednoznačně říci, co je co. Hoax může být spyware či phishing, spyware může fungovat jako dialer, bezelstný

spam může obsahovat červy či trojské koně apod. (Proto začínají kromě „antiprogramů“ na určitá rizika vznikat komplexní balíčky proti veškerému škodlivému softwaru.)

A jak se lze proti těmto ohrožením bránit?

1. Vždy používej „antiprogramy“: antivir, antispyware, antispam a pravidelně jimi svůj počítač prověř.
2. Používej (a správně si nastav nebo nechej nastavit!) osobní firewall.
3. Stahuj pravidelně opravné balíčky svého operačního systému a důležitých programů (internetový prohlížeč, poštovní klient, kancelářské balíky apod.).
4. A zapni blokování vyskakovacích (pop-up) oken a filtruj reklamy.

A nyní to nejdůležitější:

1. AKTUALIZUJ PRAVIDELNĚ všechny „antiprogramy“!
2. ZÁLOHUJ PRAVIDELNĚ data, která jsou pro Tebe důležitá, a případně je ZAŠIFRUJ!
3. PŘEMÝŠLEJ o tom, co na webu děláš a jak se chováš!
4. VZDĚLÁVEJ se neustále, abys znal nová rizika a dovedl se jim bránit!
5. BUĎ raději PŘÍLIŠ OPATRNÝ, než jednoduše naivní!

Poznámka ne úplně pod čarou:
Možná neuškodí informovat občas rodiče nebo vychovatele o tom, co na webu děláš. Třeba si dokonce všimneš, že až si uvědomí, jak odpovědně se chováš, budou mnohem klidnější při Tvém surfování po Internetu.

Poznámka druhá ne úplně pod čarou:
Když na webu objevíš něco, co se Tě zaráží – nepěkného, neslušného, netaktního, násilného, agresivního či odporného – máš možnost se bránit.
Klikni sem: http://www.internethelpline.cz/.