

# Příručka pro rodiče

jak zajistit bezpečnost dětí na internetu



Safer  
internet.cz

ins@fe

Podpora projektu:  upc

# OBSAH

## A. Jak používat tento balíček

s. 4



## B. Příručka pro rodiče a vychovatele

s. 5



### 1. Zabezpečení k bezpečnosti

s. 6

### 2. Komunikace

s. 10

### 3. Šikana na internetu

s. 15

### 4. Zábava & stahování

s. 17

## C. Doporučená řešení jednotlivých aktivit

s. 21



### 1. Zabezpečení k bezpečnosti

s. 21

### 2. Komunikace

s. 24

### 3. Šikana na internetu

s. 26

### 4. Zábava & stahování

s. 27

## D. Slovník

s. 29



## E. Užitečné adresy

s. 39





## A. Jak používat tento balíček

***Plánujete-li na jeden rok, zasadte rýži;  
Uvažujete-li v horizontu desetiletí, zasadte strom;  
Plánujete-li na celý život, zajistěte svému dítěti vzdělání.***  
(čínské přísloví)

Vážení rodiče a vychovatelé!

Držíte v rukou balíček věnovaný tématu internetové bezpečnosti, který je určen rodinám s dětmi ve věku 6–12 let. Tato vzdělávací pomůcka vznikla díky přesvědčení, že moderní technologie by neměly vytvářet mezi generacemi propast, ale měly by je sblížovat. Při přípravě jsme vycházeli ze zkušeností společnosti Insafe, celoevropské sítě národních kontaktních středisek, která se zabývají šířením informací o bezpečnosti na internetu. Vznik a výrobu tohoto tematického balíčku podpořila také společnost UPC.

Pokud nejsme opatrní při hraní na hřišti či přecházení silnice, vystavujeme se určitému nebezpečí. A stejně tak číhá nebezpečí na neopatrné uživatele internetu a mobilních technologií. Naštěstí však máme k dispozici nástroje, které nám umožní poznat výhody i možná rizika surfování na webu.

Využijte tento balíček a uče své děti používat internet bezpečně a efektivně. Najdete zde



více než padesát rad týkajících se bezpečnosti a řadu cvičení, při kterých si děti osvojí bezpečné chování na internetu zábavným, zajímavým a neohrožujícím způsobem. Součástí balíčku jsou:

- dvě brožury věnované internetové bezpečnosti: zábavná brožurka pro celou rodinu a příručka pro rodiče
- zlatá pravidla
- rodinný certifikát
- sada samolepek
- 12 situačních kartiček, které si děti mohou rozstříhat

V brožurce pro celou rodinu i v oddílu pro rodiče jsou barevně odlišeny čtyři oblasti, které jsou z hlediska bezpečnosti, na internetu nejdůležitější. Nesou názvy „**Bezpečnost**“, „**Ko-munikace**“, „**Zábava & stahování**“ a „**Šikana na internetu**“. Rodičovská brožura doplňuje zábavnou část určenou pro celou rodinu. Najdete v ní rozšiřující informace, poznámky k aktivitám a návrhy řešení jednotlivých cvičení popsaných na kartičkách.

Rodinná brožura je koncipována tak, aby ji mohli společně používat rodiče a děti. Se čtyřmi zmiňovanými tématy se seznámíte v příběhu dvou dětí, Zdeny a Aleše, jejich rodičů a slečny Heleny, která je na informační technologie velkou odbornicí. Součástí každé kapitoly jsou výukové aktivity – např. úkoly prováděné přímo online či kvízy – a také zlatá pravidla a užitečné odkazy.

Příběh si s dětmi čtete nahlas a společně plňte doporučené úkoly. Na konci každé kapitoly můžete využít situačních kartiček, diskutovat o nich s dětmi a pomoci jim tak probrané téma pochopit do větší hloubky.

Až děti úspěšně dojdou na konec knížky zaslouží si odměnu. Společně se domluvíte na vlastních zlatých pravidlech a všichni podepíšete rodinný certifikát. Nakonec si děti mohou brožurku vyzdobit samolepkami s emotikony.

Zpětná vazba je pro nás velmi důležitá. Proto prosíme neváhejte a se svými dotazy a komentáři se obraťte na projekt Saferinternet.cz (info@saferinternet.cz). Přejeme vám, ať si vy i vaše rodina užijete při kročení internetu co nejvíce zábavy!

S přáním bezpečného surfování,

Pavel Vichtera,  
koordinátor projektu

**Safer**  
internet.cz



## B. Příručka pro rodiče a vychovatele

# 1. Zabezpečením k bezpečnosti



## DOMÁCÍ POČÍTAČ

Domácí počítač může celé rodině sloužit jako skvělý nástroj pro vzdělávání i odpočinek. Pokud chcete chránit bezpečí nejmladších členů domácnosti, umístíte počítač doma do společné místnosti a stanovte, za jakých podmínek a jak dlouhou dobu mohou u obrazovky trávit.

Nezapomínejte, že děti mohou mít přístup na **internet** také u svých kamarádů, v internetových kavárnách apod. Proto je důležité, aby jste se společně dohodli na pevných bezpečnostních pravidlech, která budou platit vždy a všude.

## ZABEZPEČENÍ POČÍTAČE

Počítač si budete schopni zabezpečit, pokud alespoň na základní úrovni porozumíte hrozícímu nebezpečí a budete vědět, jak vzniklé problémy řešit. Užitečné technologické nástroje je třeba nejen využívat, ale také při tom zapojit zdravý rozum. Ten si člověk

podobně jako jiné osobnostní kvality tříbí s rostoucím věkem a zkušenostmi.

Činnosti, které budete vy a vaše děti pravděpodobně na domácím počítači nejčastěji vykonávat, mohou být do určité míry rizikové. Mezi tyto činnosti patří např. používání **USB disků (flash disků)** nebo **CD-ROMů**, otevírání **příloh** a **stahování souborů**. Mluvíme-li o riziku máme na mysli především škodlivé **počítačové programy (malware)**, jejichž cílem je poškodit váš počítač, zcizit vaše osobní informace nebo vám zajistit nevyžádanou publicitu.

Děti se v naší brožuře seznámí s těmito typy škodlivého softwaru: **viry**, **červy**, **trojskými koňmi** a **spywarem**. Zjistí také podle jakých znaků napadený počítač poznají. Dozvědí se, že pokud chtějí zavírování předejít musí se na internet vždy přihlašovat pouze na počítači chráněném nejnovější verzí **antivirového** programu a **anti-spywaru**. Vysvětlíme jim jak obezřetně postupovat při otevírání e-mailových příloh od neznámých odesílatelů, při stahování programů z internetu a používání flash disků a CD-ROMů.

## OCHRANA PROTI SPAMU

90% e-mailů kolujících na internetu jsou **spamy** (nevyžádané e-maily), které mohou velmi snadno ovlivnit vaše děti. Pokud se na **webu** zapojíte do **diskusní skupiny**, **chatu**, **veřejného fóra**, **sociální sítě** nebo vyplníte **online dotazník** a na příslušných stránkách zveřejníte svoji **e-mailovou adresu**, nevyhnutelně se stanete adresáty spamů. Speciální software dokáže z webu stahovat e-mailové adresy, sestavovat jejich seznamy a hromadně na ně rozesílat spamy. Společnosti zabývající se takovou činností obvykle sídlí v zemích bez příslušné legislativy, která by zasílání nevyžádaných e-mailů postihovala!

Spamy nejčastěji nabízejí pornografické materiály, farmaceutické výrobky, pochybné finanční převody, apod. Prostřednictvím spamů se navíc mohou šířit škodlivé programy. Ve většině případů jsou tyto e-maily rozesílány s úmyslem adresáta oklamat. Předkládáme vám několik rad, jak můžete svoji rodinu ochránit:

- Používejte **filtry spamů**. Správce e-mailové adresy obvykle nabízí možnost aktivovat si protispamovou ochranu v e-mailové schránce. S prosbou o podrobnější informace se obraťte na provozovatele serveru, kde máte zřízenou e-mailovou adresu. Pravidelně kontrolujte svoji **složku nevyžádané pošty a spamů** a přesvědčte se, že zde neskončily některé neškodné e-maily. Moderní technologie nejsou neomylné.
- Naučte své děti, aby neotvíraly e-maily od neznámých lidí. Spamy téměř vždy obsahují lákavé nabídky a přílohy. Ukažte jim, jak si mohou přijímání e-mailů zaslaných z určitých adres zablokovat nebo je jednoduše požádejte, aby podezřelé e-maily vždy smazaly.

## SURFOVÁNÍ NA INTERNETU

Internet může být velkým přínosem dokonce i pro velmi malé děti, ať už zde surfují pro zábavu nebo navštěvují vzdělávací **webové stránky**. Na druhou stranu zde narazí na množství stránek s obsahem, který pro uživatele jejich věku vhodný není.

Pro nalezení informací k určitému tématu jsou velmi vhodné vyhledávače. Jelikož však hledání

probíhá na základě zadaných klíčových slov, velmi snadno se dostaneme na stránky s nevhodným obsahem. Nevinně znějící klíčové slovo nás může navést na stránku, která již tak nevinně nevyhlíží a přesto zde zadané slovo figuruje. Chcete-li, aby vaše děti byly při surfování na internetu v bezpečí, máme pro vás několik rad:

- V některém z **operačních systémů** (např. Windows, Linux, Mac OS) vytvořte svému dítěti vlastní uživatelský účet. Na něm si můžete aktivovat funkci s názvem **rodičovská kontrola**.
- Prozkoumejte možnosti rodičovské kontroly u svého internetového **prohlížeče** a vyhledavače. Seznamte se se všemi možnostmi, které vám zde nabízí funkce **ochrana rodiny**.
- Malé uživatele internetu ve vaší péči seznámte s **vyhledavači** vytvořenými přímo pro děti. Příkladem jsou stránky <http://kids.yahoo.com> nebo <http://www.askforkids.com>.
- Adresy webových stránek, které vaše děti navštěvují nejčastěji jim uložte ve složce „**Oblíbené**“ (najdete ji v menu prohlížeče). Svá oblíbená místa na **netu** budou tak moci navštěvovat opakovaně, aniž by musely znovu používat vyhledavač.

Kromě toho, že na svém prohlížeči a vyhledavači aktivujete funkci rodičovské kontroly, můžete také použít přidavný **filtr**, tj. software, který chrání nezletilé uživatele před nevhodným obsahem některých webových stránek. O radu požádejte prodejce nebo si na internetu vyhledejte **zkušební software**. Pamatujte si však, že nic nemůže nahradit péči rodičů a vychovatelů. Technologické nástroje nejsou bezchybné a někdy mohou vyvolat falešný pocit bezpečí. Při jejich používání je třeba nezapomínat na selský rozum.

Filtrační software může být však natolik omezující, že zablokuje i přístup na stránky s naprosto neškodným obsahem. Může se například stát, že se děti nedostanou k materiálům o druhé světové válce, protože půjde o stránky popisující násilí. Navíc pokud je možné nějaký filtr zapnout, dokáží ho chytré děti také vypnout a dokonale zahladit stopy po svých aktivitách. Tyto jejich praktiky odhalíte pouze tehdy, když se sami naučíte počítač a software používat.

Navštivte webové stránky **SIP-Bench**, kde jsou zveřejněny výsledky studie, kterou podpořila Evropská komise. Autoři studie testovali 30 nástrojů pro rodičovskou kontrolu a anti-spamovou ochranu a zjišťovali, nakolik účinně chrání děti ve věku 6–16 let při jejich nejrůznějších aktivitách na internetu před škodlivým obsahem. Sledovány byly tyto aktivity: **prohledávání** internetu, zaslání e-mailů, **přenášení souborů**, chatování a **instant messaging**.

Samotná ochrana před **škodlivým obsahem** nepostačí. Svě děti byste měli naučit, aby nevěřily všemu co na internetu vidí a čtou. V naší zábavné knížce pro celou rodinu jim doporučujeme, aby vždy, když na internetu vyhledávají informace, navštívily nejméně tři webové adresy a uvedené informace porovnaly. Měly by se navíc učit, že kdykoli píšou nějakou práci do školy, je správné v ní systematicky uvádět zdroje informací.

## ZLATÁ PRAVIDLA PRO RODIČE DĚTÍ SURFUJÍCÍCH NA INTERNETU

- Svůj počítač si zabezpečte. Nainstalujte si **firewall** a také antivirový a anti-spyware software, které pravidelně aktualizujte. Věnujte pozornost veškerým **upozorněním**, které tyto programy vygenerují. Zjistěte si zda váš poskytovatel internetových služeb (Internet Service Provider – ISP) nabízí antivirové a anti-spyware nástroje, které můžete využít.

- Ve svém e-mailovém programu použijte filtr spamů a svoji e-mailovou adresu uchovávejte pokud možno v tajnosti, neuvádějte ji na webu. Vyhybte se e-mailům od neznámých odesílatelů a přílohy před otevřením **zkontrolujte antivirovým programem**.
- V maximální možné míře využívejte nástrojů pro rodičovskou kontrolu, které vám poskytuje software vašeho operačního systému a to v internetovém prohlížeči, vyhledávači a e-mailovém programu. Svým dětem vytvořte vlastní **uživatelské účty**. Ochranu soukromí zde nastavte na nejvyšší možnou úroveň (v menu svého prohlížeče vyberte „Možnosti“).
- Zvažte, zda si nepořídit přídatný filtrační software.
- Jakmile se váš počítač začne chovat podivně, může to znamenat, že je zavirovaný. Kontaktujte ihned svého ISP (poskytovatele internetových služeb) nebo jiného odborníka. ISP by také měl být schopen poskytnout rady rodičům.
- Pokud narazíte na internetu na stránky s nevhodným obsahem, oznamte jejich existenci na národní internetovou horkou linku (viz „Užitečné odkazy“).
- Kdykoli vaše děti surfují na internetu a vy si k nim můžete přisednout, udělejte to. Je to skvělá příležitost, jak zahájit diskusi a posílit vzájemnou důvěru. Vezměte to jako výzvu a uče se společně s nimi.
- Nezapomínejte, že bezpečnostní pravidla se týkají jak vašich dětí, tak vás samotných. Vedte děti k tomu, aby vás informovaly, kdykoli uvidí na internetu něco podivného.

## UŽITEČNÉ ODKAZY

Na níže uvedených stránkách projektu Saferinternet.cz [www.internethelpine.cz](http://www.internethelpine.cz) si mohou vaše děti přečíst další užitečné rady a tipy o internetové bezpečnosti.

Chcete-li surfovat bezpečně a tuto činnost si užít, potřebujete určité znalosti: musíte vědět, jaká nebezpečí vám hrozí, jak se můžete chránit a mnoho dalších věcí. Více informací najdete na webových stránkách projektu Saferinternet.cz:

<http://www.bezpecnejionline.cz>

Pokud byste při surfování na internetu narazili na materiály, o kterých jste přesvědčeni, že jsou nelegální můžete zaslat zprávu na českou horkou linku:

<http://www.horkalinka.cz>



## 2. Komunikace



### DÍLKY SKLÁDAČKY

Vzpomínáte si, jak byl pro vás v době dospívání důležitý kontakt s kamarády? Internet nabízí uživatelům řadu nových příležitostí k setkávání s přáteli a umožňuje jim vyjadřovat se a komunikovat mnoha různými způsoby – mohou si zasílat e-maily, **sdílet soubory**, psát vlastní **blogy** nebo se stát členy různých komunit (např. v prostředí MySpace, Facebook, Hi5, Habbohotel atd.). V současné době teenageri využívají moderní technologie nejen proto, aby si vyzkoušeli nové věci, ale také aby navazovali kontakty v prostředí, které považují za soukromé a kde nejsou pod dohledem rodičů.

Kapitola věnovaná komunikaci seznamuje rodiče i děti se způsobem zveřejňování **osobních údajů** a s možnostmi **ochrany soukromí**. Dozvíte se, v čem je online komunikace přínosná a jak se chovat v rizikových situacích, mezi které patří např. kontakt s neznámými lidmi. Problém ochrany soukromí na internetu je velice úzce spojen s vytvářením **účtů & profilů**. Prostřednictvím vlastního účtu máme přístup k online službám.

Na své legitimaci na autobus, permanentce do fitness klubu či jiném průkazu, který používáte v každodenním životě, máte zapsány některé osobní informace. Totéž platí také o online účtech a objednávkách určitých internetových služeb. Zřídit účet či objednat službu si můžete pouze za předpokladu, že uvedete konkrétní informace o své osobě, které se pak stanou součástí vašeho „uživatelského profilu“. Skutečnost, že sami určujete jaké informace o sobě zveřejníte a kdo k nim bude mít přístup, je velmi důležitá.

Chcete-li si chránit své soukromí, neuvádějte lživé informace, ale zvažujte, co se o vás ostatní mají dozvědět. Mladí lidé jsou velmi nadšeni možností komunikovat se svými přáteli po internetu a vytvářet si vlastní online podobu. Ne vždy si však uvědomují, jaké následky může mít zveřejnění soukromých informací.

### VYTVÁŘENÍ PROFILU

Prvním krokem při ochraně osobních informací je vytvoření bezpečného profilu. Je třeba pečlivě rozhodnout, jaké informace v něm uvedete a jaké bezpečnostní nastavení zvolíte.

Pro různé online aktivity si vytvořte různé e-mailové účty. Pokud vaše dítě využívá internetové služby, jako je chatování, instant messaging, psaní blogu apod., naučte ho při těchto aktivitách používat neutrální e-mailovou adresu a **přezdívku**. Chatující dítě tak v adrese nevyzradí celé své jméno.

**Heslo** k účtu vždy udržujte v tajnosti. Vysvětlete dětem, že informace o svých soukromých účtech nemají prozrazovat kamarádům, kteří by jejich důvěry mohli zneužít. Na druhou stranu možná budete chtít znát hesla svých dětí, abyste nad jejich účty měli kontrolu – promluvte si o tom s nimi.

Nezapomeňte si na svém profilu/účtu nastavit **ochranu soukromí**, tj. zadat, že se jedná o informace soukromé, nikoli veřejně přístupné. Pouze tak budete moci určovat, komu se vaše údaje zobrazují a s kým můžete komunikovat. Soukromý profil vám umožňuje nastavit si a měnit svůj seznam kontaktů (tj. **seznam kontaktních adres**). Naučte své děti, aby přijímaly zprávy pouze od osob, které již znají z prostředí mimo internet.

Pokud vaše děti využívají chatovací místnosti, podívejte se zda:

- na komunikaci dohlížejí moderátoři. Nepřítomnost moderátorů znamená nezabezpečené chatování;
- jsou zde nástroje, které umožňují ignorovat či zablokovat kontakt s osobami, se kterými děti chatovat nechťejí;
- jsou na webových stránkách k dispozici funkce „nápověda“ a „zpráva o chybě“, které lze použít, nastanou-li problémy;
- pravidla chatovací služby jsou jasně vymezena a zveřejněna na nepřehlédnutelném místě.

## FOTOGRAFIE A WEBKAMERY

Děti musí pochopit, že fotografie také patří mezi soukromé informace a že pohyb digitálních fotografií po internetu je téměř nemožné ovlivnit. Je velmi jednoduché poslat je do oběhu po síti a měnit jejich podobu (tj. **manipulovat** s nimi). Jakmile byly jednou z počítače či mobilního telefonu odeslány, velmi obtížně se odstraňují, mohou dokonce zůstat online navždy! S **webovými kamerami** je třeba zacházet s velkou opatrností a děti by neměly kamery používat bez dozoru. Chatovací služby s možností použití webových kamer mohou představovat riziko. Vy i vaše děti byste měli své fotografie zasílat pouze lidem, které znáte a kterým důvěřujete. Chcete-li zveřejnit fotografii jiné osoby, požádejte ji o souhlas. Své děti nenechávejte používat počítač s webovou kamerou, pokud jsou v místnosti samy.

## KONTAKT S NEZNÁMÝMI LIDMI

Lidé, které potkáte online, nejsou vždy těmi, za koho se vydávají. Naučte své děti chránit si vlastní soukromí na internetu stejným způsobem, jako to dělají v neinternetovém světě. Určitě jim říkáte, jak se mají chovat k neznámým lidem v běžném životě, proč by se tedy neměly řídit stejnými pravidly i na internetu?

Vaše děti si možná k přátelům z internetu vytvoří silný vztah. Není pro ně vůbec obtížné začít důvěřovat lidem, kteří je sice vůbec neznají, ale zajímají se o ně a mají pro ně pochopení. Velkým lákadlem pro děti je pak možnost se s novými přáteli sejit, aniž by vám cokoli řekly. Děti si často neuvědomují, jak nebezpečná mohou taková setkání být a nepovažují je za problematická. Stávají se velmi snadnou obětí online **groomingu (lákání na schůzky)**. Ze studií vyplývá, že mnoho dětí se na setkání s online „přáteli“ vydává bez doprovodu a o svých schůzkách rodiče neinformují. Chcete-li mít jistotu, že vaše děti takto jednat nebudou, promluvte si s nimi o tomto jevu. Klíčem k řešení možného problému je dobrá komunikace.

## NETIKETA

**Netiketa** je synonymem pro slušné chování na internetu. Chceme-li ji dodržovat, musíme se k ostatním chovat stejně tak, jak bychom si přáli, aby se ostatní chovali k nám. Děti si možná neuvědomují, že na internetu mohou nechtěně někoho urazit. Bohužel, někteří lidé používají internet a/nebo mobilní telefony k tomu, aby ostatním ubližovali a obtěžovali je. V takových případech se jedná o internetovou šikanu, která může ohrožovat až jedno dítě ze čtyř (více informací naleznete v kapitole věnované tomuto tématu).

## JAZYK CHATU

Při online chatování používají mladí lidé specifický jazyk plný **emotikonů** a **akronymů**! Některé z nich si můžete prohlédnout v následující tabulce: 😊

Přehled základních akronymů používaných při chatování. Máte-li zájem o více informací, navštivte stránky uvedené v části „Užitečné odkazy“:

121: one to one

AFK: away from keyboard

A/S/L: age, sex, location (or just “ASL”)

BBB: bye bye baby

B4N: bye for now

BBL: be back later

BF: boyfriend or best friend

BFF: best friends forever

C: see?

Comp: computer

CU: see you

CUL: see you later

CYO: see you online

JJ: just joking

K: all right /ok

KFY/K4Y: kiss for you

KISS: keep it simple, stupid

KPC: keeping parents clueless

L8R: later

IRL: in real life

LMIRL: let's meet in real life

LOL: laughing out loud, lots of love

LY4E: love you forever

NE1: anyone

NP: no problem/ noisy parents

OIC: oh, I see

České akronymy se do elektronické komunikace dostaly jen v omezené míře. Mezi nepoužívanější patří:

JJ: jo jo

NN: ne ne

MMNT: moment – počkej chvílku

NJN: no jo no

O5: opět

Z5: zpět

TTJ: tak to jo

TTPJ: tak to potom jo

PP: pápá

NZ: není zač

Emotikony si můžete vytvářet kombinováním interpunkčních znamének a písmen, podobně jako v následujících příkladech:

Smajlík (s nosem nebo bez)

:) nebo :-)  
dvojtečka, (pomlčka), závorka

Smutný obličej (s nosem nebo bez)

:( nebo :-(  
dvojtečka, (pomlčka), závorka

Mrkající obličej (s nosem nebo bez)

;) nebo ;-)  
dvojtečka, pomlčka, závorka

Překvapený obličej (s nosem nebo bez)

:o nebo :-o  
dvojtečka, (pomlčka), malé písmeno o

Široký úsměv (s nosem nebo bez)

:-D nebo :D  
dvojtečka, (pomlčka), velké D

Vyplazený jazyk (s nosem nebo bez)

:p nebo :-p  
dvojtečka, (pomlčka), malé p

## ZLATÁ PRAVIDLA

- Sledujte, jak vaše děti svůj čas na internetu tráví. Požádejte je, ať vám ukáží, jakým způsobem se svými kamarády komunikují.
- Naučte je, jak si na internetu chránit svoji bezpečnost. Měly by vědět, že:
  - si mají vytvářet bezpečné profily, na kterých je možné nastavit si ochranu soukromí;
  - si mají chránit své heslo;

- mají reagovat pouze na zprávy od osob, které znají odjinud než z internetu a pouze tyto osoby také oslovovat;
  - pokud chtějí vložit na internet svoji fotografii nebo fotografii své rodiny, domu nebo školy, musí vždy požádat o souhlas rodičů;
  - soukromé informace, např. telefonní číslo, adresu, školu, sportovní klub apod., smějí sdělovat pouze lidem, které znají dobře z běžného života.
- Rodinný počítač umístíte do obývacího pokoje, abyste měli aktivity svých dětí na internetu pod kontrolou.
  - Společně si vyzkoušejte, že:
    - víte, jak odmítnout nebo si zablokovat příjem zpráv od určité osoby ve svém seznamu kontaktů;
    - na stránkách, které navštěvujete, si umíte zajistit bezpečnost a dokážete zde odeslat zprávu o případných problémech.
  - Budujte si se svými dětmi vztah založený na důvěře. Ujistěte je, že s vámi mohou mluvit i o svých chybách, protože jedině tak můžete společně hledat řešení! Chyby k učení patří.

## UŽITEČNÉ ODKAZY

Stránky „internethelpline“ jsou součástí Národního uzlu bezpečnějšího internetu, provozuje je Linka bezpečí a jsou zaměřeny především na dospívající a děti. Jejich cílem je poskytovat mladým uživatelům internetu nezbytné rady a podporu:

<http://www.internethelpline.cz>

Stránky „Bezpečnej online“ určené především rodičům:

<http://www.bezpecnejonline.cz>

Navštívíte-li stránky wikiHow, porozumíte „tajnému“ chatovacímu jazyku:

<http://www.wikihow.com/Understand-Chat-Acronyms> nebo [http://cs.wikipedia.org/wiki/Seznam\\_zkratek\\_v\\_online\\_diskusich](http://cs.wikipedia.org/wiki/Seznam_zkratek_v_online_diskusich)

Přečtěte si zprávu s názvem „Consult the Eurobarometer 2007“, která se zabývá bezpečnějším internetem pro děti:

[http://ec.europa.eu/information\\_society/activities/sip/eurobarometer](http://ec.europa.eu/information_society/activities/sip/eurobarometer)

# 3. Internetová šikana



## INTERNETOVÁ ŠIKANA VE ŠKOLE

Komunikace prostřednictvím internetu a mobilních telefonů má řadu skvělých výhod. Má však bohužel i své stinné stránky – vaše děti mohou dostávat či rozesílat zprávy, jejichž obsah zraňuje jejich city nebo city někoho jiného. Proto je důležité, aby si osvojily společensky přijatelné chování. Ani vaše vlastní děti totiž nejsou andělci ;-).

Jako **internetovou šikanu** označujeme takové chování, kdy lidé využívají moderní informační a komunikační nástroje k šikanování, obtěžování a urážení jiných jedinců nebo celých skupin. K těmto účelům lze používat e-maily, systém zasílání rychlých zpráv (instant messaging), mobilní telefony či jiné digitální zařízení. Při hraní online her mohou organizátoři šikany útočit na **avatar** vašeho dítěte, např. po něm mohou střílet, zcizit jeho **virtuální vlastnictví** nebo ho přinutit chovat se jinak, než by si jeho majitel přál.

Nejčastěji děti nahlašují problémy, ke kterým došlo poté, kdy ve veřejně přístupném prostředí prozradily některé soukromé informace (např. na veřejných fórech nebo webových stránkách publikovaly vlastní fotografie nebo informace o sobě). Podobně jako v případě šikany ve škole či na hřišti, není takové chování přijatelné. Rodiče, učitelé i děti by měli být ostražiti a reagovat okamžitě. Na rozdíl od klasické **šikany**, virtuální šikana může na dítě působit i v době, kdy se nenachází ve společnosti šikanujících. Ti mohou například kdykoli během dne či noci zaslat výhrůžnou zprávu na domácí e-mailovou adresu nebo mobilní telefon.

Jako rodiče můžete pomoci vytvořit takové prostředí, ve kterém šikana není tolerována. Učte své děti, že být anonymní na internetu neznamená chovat se nezodpovědně. Děti musí znát svá práva i své povinnosti a umět respektovat také práva ostatních.

Vždy vedte se svými dětmi otevřený dialog, abyste společně dokázali mluvit i o jakékoli nepříjemné situaci. Nové technologie, mezi které internet a mobilní telefony patří, mohou samy vyvolat diskusi a poskytnou náměty k přemýšlení!

### ZLATÁ PRAVIDLA:

- Snažte se ochránit své děti před nepříjemnými zkušenostmi – ukažte jim, jak si chránit vlastní soukromí a respektovat soukromí ostatních.
- Naučte děti, aby na urážlivé zprávy neodpovídaly.

- Pomozte dětem pochopit, jaké zprávy a způsoby chování vyvolávají u ostatních nepříjemné pocity a jak lze těmto situacím zabránit.
- Přesvědčte se, že si děti ve svém seznamu kontaktních adres umí zablokovat příjem zpráv od určitého odesilatele.
- Urážlivé zprávy si ukládejte, můžete je potřebovat jako důležitý důkaz.
- Zjistěte si, jaká opatření proti šikaně přijala škola vašeho dítěte. Při potírání klasické šikany a šikany na internetu spolupracujte s učiteli i s ostatními rodiči.
- Buďte v kontaktu s lidmi z okolí vašeho dítěte – seznamte se s jeho kamarády, jejich rodiči, učiteli i spolužáky.
- Vedte svoje děti k tomu, aby vám říkaly o každé zkušenosti z internetového & neinternetového světa, která jim dělá starosti. Ujistěte je, že jste zde pro ně i tehdy, když z neopatrnosti provedou něco špatného a že společně naleznete řešení!
- Ujistěte své děti, že pokud je někdo obtěžuje, nikdy to není jejich vina.

## UŽITEČNÉ ODKAZY

Na těchto webových stránkách zaměřených proti školní šikaně najdete informace, díky kterým šikaně ve škole lépe porozumíte a bude vám jasnější jak jí lze zabránit:

<http://www.protisikane.cz>

V případě nesnází vám pomůže česká asistenční linka na [www.internethelpline.cz](http://www.internethelpline.cz).

Telefonicky ji můžete kontaktovat na čísle **116111**

E-mailová poradna: [pomoc@internethelpline.cz](mailto:pomoc@internethelpline.cz)

# 4. Zábava & stahování



## NA INTERNETU NENÍ VŠECHNO ZLATO, CO SE TŘPYTÍ

Ve virtuálním prostředí na internetu probíhá celá řada aktivit, včetně aktivit komerčních. Jistě svým dětem nekupujete vše, na co vidíte reklamu v televizi nebo co je zaujme v obchodě. Měli byste je tedy také naučit, že není třeba vlastnit každou věc nabízenou na internetu a nelze věřit všem internetovým reklamám. Ty nejčastější nabízejí hudební nahrávky, hry, **vyzváněcí tóny**, počítačové příslušenství či online služby.

Jestliže budete na internetu surfovat společně se svými dětmi, budete mít příležitost vysvětlit jim, že věci jako vyzváněcí tóny, **tapety**, **mp3 nahrávky**, **avatař** apod. jsou zdarma málokdy. Kdykoli narazíte na reklamu tvrdící opak, upozorněte děti na text psaný drobným písmem a ukažte jim, že ne všechna tvrzení na **netu** lze brát doslova.

Pokud si objednáte jakoukoli službu (ať už zdarma či za poplatek), musíte vyplnit **online formulář** a uvést požadované osobní informace. Formuláře vyplňujte, pouze pokud je vám jasné, jakým způsobem budou vámi zadané informace použity. Děti by měly formuláře vyplňovat jediňe ve vaší přítomnosti.

**Vyskakovací okna** se na internetu často používají pro propagaci výrobků. Ne vždy jsou však negativním jevem – záleží, nakolik důvěryhodné jsou samotné stránky, na kterých se objevují. Obecně lze říci, že pokud webovým stránkám důvěřujete, můžete věřit i informacím ve vyskakovacích oknech. V některých oknech se však objevují reklamy na podezřelé výrobky, jiná navádějí uživatele na **online formuláře**, které shromažďují osobní informace. Naučte své děti, aby podezřelá okna zavíraly kliknutím na červený křížek v pravém horním rohu.

## HRANÍ HER NA INTERNETU

Internetové hry vyžadují narozdíl od starších digitálních her **síťové připojení**. Děti si hry mohou hrát z CD/DVD nosičů, na **webových stránkách**, **herních konzolích**, mobilních telefonech či jiných **přenosných zařízeních**.



Mezi online hry patří jak jednoduché, velmi rozšířené hry jako Pacman nebo Tetris, tak hry vycházející z virtuální reality, které hraje několik hráčů najednou online a společně vytvářejí jejich náplň a příběh postav. Okolo řady těchto víceuživatelských her vznikají celé virtuální hráčské komunity. Děti se při hrách tohoto typu dostávají na internetu do kontaktu s neznámými lidmi, což představuje určité riziko (viz kapitola „Komunikace“).

Hraní her hraje ve vývoji dětí významnou roli. Děti si při této činnosti rozvíjejí sociální dovednosti a strategické myšlení a to v prostředí vymezeném určitými pravidly. Mnohé z těchto interaktivních a velmi atraktivních her jsou využívány také pro vzdělávací účely.

Ne všechny digitální hry jsou však kvalitní. Vy sami musíte rozhodnout, jaké hry jsou pro vaše děti nejvhodnější. Zároveň musíte vymezit určitá pravidla a stanovit, jak dlouhou dobu mohou hraním online her strávit, aniž by utrpěly jejich ostatní aktivity.

Systém **PEGI online** je celoevropský systém třídění interaktivních her podle jejich obsahu a věku hráčů. Systém má podporu nejen řady výrobců konzol jako PlayStation, Xbox, Nintendo, ale rovněž vývojových týmů a vydavatelů interaktivních her z celé Evropy. Zařazení do určité kategorie je vždy vyznačeno na obalu hry. Nezapomínejte však, že každé dvanáctileté dítě je jiné.



## ZLATÁ PRAVIDLA

- Vedte svoje děti k tomu, aby navštěvovaly webové stránky, jejichž obsah neporušuje zákon. Vysvětlete jim také, že ne vše je ve skutečnosti takové, jak se na netu na první pohled jeví.
- Vysvětlete dětem, jaká rizika jim hrozí, pokud nebudou při stahování materiálů z internetu obezřetné.
- Přesvědčte se, že je váš počítač dobře zabezpečen. Vždy používejte aktualizovanou verzi antivirového programu.
- Učte své děti ukládat stažené soubory na harddisk tak, že daný soubor před otevřením prověří antivirovým programem.
- Ještě než si cokoli do počítače nainstalujete, přečtěte si text o ochraně soukromých údajů a prohlášení uživatele. Na internetu si ověřte spolehlivost softwaru, který si chcete stáhnout.
- Zavírejte podezřelá vyskakovací okna kliknutím na křížek v pravém horním rohu. Nikdy neklikejte dovnitř okna.

## DĚTI & HRY:

- Stanovte, jak dlouhou dobu mohou vaše děti hraním her trávit.
- Nechte je hrát v obývacím pokoji, kde nad nimi máte kontrolu.
- Sledujte hráčské návyky svých dětí. Hlídáte je na hřišti, proč byste tedy neměli dělat totéž při jejich aktivitách ve virtuálním prostředí?
- Pověďte si s nimi o obsahu hry. Které její prvky jsou podobné realitě a které ne? Co se jim na hře líbí?
- Předtím než svému dítěti hru zakoupíte, zkontrolujte si zda je pro jeho věkovou kategorii vhodná (sledujte označení podle celoevropského systému PEGI nebo národního klasifikačního systému).

### *Pokud vaše děti hrají počítačové hry společně s dalšími hráči:*

- Vyberte jim stránky s přísnými pravidly, které sledují moderátoři.
- Důrazně je vyzvěte, aby své osobní údaje nesdělovaly ostatním hráčům.
- Dbejte na to, aby se s ostatními hráči mimo internet scházeli pokud možno pouze ve vašem doprovodu.
- Vyzvěte děti, aby vám oznamovaly jakékoli šikanování, vyhrožování, používání vulgárního jazyka, zveřejňování nepříjemného obsahu nebo výzvy k setkání v neinternetovém prostředí.
- Pokud vás hra nebo způsob jakým se vyvíjí znepokojuje, odhlaste své dítě ze hry nebo změňte jeho virtuální identitu.

## UŽITEČNÉ ODKAZY

Více informací o internetových hrách a systému PEGI (klasifikačním systému podle věku) se dozvíte na stránkách:

<http://www.pegionline.eu>

Seznam webových stránek z celého světa, kde si můžete hudbu zakoupit legálně:

<http://www.pro-music.org>

Navštivte tyto webové stránky a seznamte se s internetovou hantýrkou:

[http://cs.wikipedia.org/wiki/Seznam\\_zkratek\\_v\\_online\\_diskusich](http://cs.wikipedia.org/wiki/Seznam_zkratek_v_online_diskusich)



C. Doporučená řešení jednotlivých aktivit

# 1. Zabezpečením k bezpečnosti



## POZNÁMKY K AKTIVITÁM

Přiřadte slova k obrázkům: Stolní počítač, podložka pod myš, monitor, reproduktory, webová kamera, tiskárna, USB disk (nebo flash disk), myš, CD-ROM.

*V úvodním cvičení se vaše děti seznámí s různými částmi počítače a s jeho příslušenstvím. Úkol můžete podle svého uvážení rozšířit.*

Požádej rodiče, aby ti poslali e-mail s přílohou nebo si jej pošli sám. Zkus si následující postup: klikni na přílohu pravým tlačítkem a ulož ji na plochu počítače. Zobraz plochu počítače, pravým tlačítkem klikni na ikonu dokumentu a vyber příkaz Najít viry. Když se ujistíš, že je dokument čistý, můžeš jej otevřít. Zapamatuj si: kliknout pravým tlačítkem a ULOŽIT – NAJÍT VIRY – OTEVŘÍT.

*Zašlete e-mail s přílohou na adresu svého dítěte nebo mu pomozte s jeho odesláním. Nechte dítě postupovat podle uvedených instrukcí, tj. kliknout na dokument pravým tlačítkem myši aniž by ho otevřelo. Po uložení dokumentu na plochu nebo do některé složky v počítači, např. do složky s názvem „Moje dokumenty“, mu ukažte, že je nutné na dokument kliknout pravým tlačítkem ještě jednou a před otevřením ho zkontrolovat antivirovým programem. U dítěte tak rozvíjíte návyky nutné pro ochranu vlastní bezpečnosti.*

Poslechni si Heleninu radu a nauč se popsat svou e-mailovou adresu, když ji uvádíš na internetu. Tím zabráníš automatickému stažení adresy a jejímu zneužití pro rozesílání spamů.

Příklad: paja.novak@mujemail.cz = paja tečka novak zavináč mujemail tečka cz

Zkus popsat e-mailové adresy členů své rodiny: tvůj e-mail, rodinný e-mail; mámin e-mail; tátův e-mail

*Nechcete-li, aby vaši veřejnou e-mailovou schránku objevil software pro rozesílání spamů, adresu neuvádějte ve skutečné podobě, ale raději ji popište. Nechte své dítě, aby si tento způsob podle uvedeného příkladu vyzkoušelo. Mějte však na paměti, že děti by neměly vůbec svoji e-mailovou adresu na internetu uvádět. Pokud ji zveřejňují, měly by uvádět takovou, která neprozrazuje celé jejich jméno (viz kapitola „Komunikace“).*

Než bude Helena pokračovat, pomozte to Zdeně pochopit. Podívej se na aktivity uvedené v následujícím rámečku a zakroužkuj ty které můžeš dělat, jenom když je počítač připojen k internetu.

*Velmi malým dětem možná nebude zcela jasné, jaké aktivity vyžadují síťové připojení a jaké ne. Pokud píšeme text, není nutné být připojený na internet, při chatování to však nezbytné je. Hudbu můžete poslouchat z CD nebo z hudebního souboru uloženého v počítači, ale také přímo z internetu. Děti mají za úkol označit pouze ty aktivity, které bez připojení na internet nelze provádět.*

Spolu s rodiči napiš do okna prohlížeče [www.seznam.cz](http://www.seznam.cz). Najdi si informace o tyranosaurovi a zkus zjistit, kdy tento dinosaur na zemi žil. Také si zkus najít hezký obrázek tyranosaura. Nezapomeň si informace ověřit na třech různých stránkách.

*Naučte své děti správným technikám vyhledávání – připomeňte jim, aby nevěřily všemu, co na internetu najdou. Veďte je k tomu, aby si informace vyhledaly nejméně na třech různých stránkách a vzájemně je porovnal. Když píší školní práce, neměly by zapomínat uvádět zdroje informací.*

Spolu s rodiči napiš do okna prohlížeče [www.seznam.cz](http://www.seznam.cz). Potom si najdi informace o nějakém tématu, například o tyranosaurovi, a tři nejzajímavější stránky si ulož mezi své oblíbené. Klikni na nabídku „Oblíbené“ na horní straně okna prohlížeče a přidej stránku ke svým oblíbeným. Můžeš si také vytvořit svou vlastní složku.

*Pokud se děti naučí systematicky si ukládat a třídit odkazy na zajímavé stránky ve složce „Oblíbené“ (ikonu najdete liště v prohlížeči), nebudou muset informace tak často hledat přímo online.*

## POROZUMĚL JSI DOBRĚ?

1: (zabezpečený) 2: (Virem), (neznámého), (stahování), (nakaženého), (CD/DVD), (nezabezpečeném) 3: (divně) 4: (neznámých), (přílohu), (předmětem), (spam) 5: (jedinou), (spamů) 6: (první), (tři), (porovnej), (kdokoli), (zveřejnit), 7: (Antivirus), (anti-spyware) 8: (obsah), (rodičům) 9: (řekni)

## DOPORUČENÁ ŘEŠENÍ SITUACÍ NA KARTIČKÁCH

**SITUACE Č. 1.** Nikdy nesurfuj na internetu, pokud nemáš počítač chráněn nejnovější verzí antivirového programu nebo anti-spywaru. Bylo by to stejné, jako mít hranice bez pohraniční stráže; tvůj počítač by mohl napadnout škodlivé programy, např. viry, trojští koně, červi nebo spyware.

**SITUACE Č. 2.** Dávej si pozor na e-maily od neznámých lidí, e-maily s přílohami a ty, ve kterých ti odesílatel „nabízí modré z nebe“ – pravděpodobně se jedná o spamy! Spamy mohou tvůj počítač nakazit škodlivými programy, jako jsou viry, trojští koně, červi a spyware. Podezřelé e-maily neotvírej a raději si přijímání zpráv od daného odesílatele zablokuj. To provedeš tak, že na e-mail klikneš pravým tlačítkem myši a z nabídky vybereš „Zablokovat odesílatele“. Jinou možností je e-mail jednoduše vymazat.

**SITUACE Č. 3.** Pokud hledáš informace na internetu, nedůvěřuj hned prvním dobře vypadajícím stránkám, na které narazíš. Navštiv minimálně tři různé adresy a informace porovnej. Pamatuj si, že informace může vytvořit a na webu zveřejnit kdokoli s přístupem na internet. Pokud píšeš zprávu nebo úkol, vždy uveď zdroje informací a použitých obrázků, protože tak to dělají skuteční vědci.

## 2. Komunikace po síti



### POZNÁMKY K AKTIVITÁM

Uvedte, nakolik považujete následující informace za soukromé: telefonní číslo; barva vlasů; jméno; země, ve které žijete; jméno vaší školy; adresa; jméno vašeho domácího mazlíčka; povolání rodičů; vaše e-mailová adresa; vaše fotografie; věk.

*Mají vaše děti stejný pohled na soukromí jako vy? Tři barvy označují různý stupeň soukromí: velmi osobní informace jsou označeny červeně, méně osobní oranžově a nepříliš osobní informace zeleně.*

Pomozte vytvořit Zdeně šikovné heslo. Drže se Heleniných rad.

*Dobré heslo by mělo být sestaveno z náhodně vybraných znaků (čísel, písmen a interpunkčních znamének) a vždy by mělo být uchováno v tajnosti.*

Postupujte jako Zdena a vytvořte si bezpečný profil. Potom jako příklad vytvořte jiný, který bezpečný není.

*Nechte děti nejprve vytvořit bezpečný profil a poté jeho méně bezpečnou verzi, ve které uvedou osobní informace. Připomeňte jim, že samotné sestavení bezpečného profilu jim dostatečnou ochranu nezajistí a že je nutné i později při komunikaci po internetu dbát na svoji bezpečnost.*

Podívejte se na obrázek a napište, co můžete říci o tomhle člověku:

*Jaké informace dokážete z fotografie vyčíst? Děti si často nejsou velké síly fotografií vědomy.*

Podpořte Zdenin nápad a vymyslete tři rady, které by Helena mohla dát Alešovi, „Karkulce v červené mikině“, aby ho ochránila před „vlky na internetu“.

*Ujistěte se, že si děti uvědomují, jak riskantní je navazovat po internetu kontakty s neznámými lidmi.*

Jak byste si přáli, aby se k vám ostatní na internetu chovali? (1..... 2..... 3.....)

*Vysvětlete dětem, že se k ostatním lidem mají chovat tak, jak by si přály, aby se oni chovali k nim.*

**ROZLUŠTĚTE ZAKÓDOVANOU ZPRÁVU:** Podívejte se , co znamenají některé akronymy často používané při chatování.

*V kapitole „Komunikace“ (v části věnované netiketě a jazyku chatu) se s akronymy seznamte podrobněji.*

Pomocí kombinace kláves vytvořte emotikony, které představují tyto výrazy: smajlík – smutný obličej – mrkající obličej – překvapený obličej – široký úsměv – vyplazený jazyk.

Více informací najdete v kapitole „Komunikace“ (v části o netiketě a jazyku chatu).

## POROZUMĚL JSI DOBŘE?

1: (profilem) 2: (soukromí), (zodpovědný) 3: (cizími), (řekni) 4:(Netiketa), (chovali) 5: (Emotikon) 6: (heslo), (8/osmi), (interpunkční) 7: (tajné) 8: (odmítanu) 9: (znáš)

### DOPORUČENÁ ŘEŠENÍ SITUACÍ NA KARTIČKÁCH

**SITUACE Č. 4.** Používáte-li internet, mohou se s vaším profilem nebo s informacemi, které o sobě uvedete, seznámit desítky, stovky, tisíce či dokonce miliony lidí. Proto je velmi důležité pečlivě zvážit, které informace na sebe prozradíte. Osobní informace sděľujte pouze lidem, kterým důvěřujete a dobře je znáte i z neinternetového prostředí.

**SITUACE Č. 5.** Michal pravděpodobně prozradil své heslo kamarádovi a ten se mu po rvačce pomstil tím, že z jeho adresy rozeslal ošklivé e-mailové zprávy. Svě heslo si vždy nechte pro sebe. V opačném případě byste se museli smířit s tím, že cizí lidé budou číst vaše e-maily, vydávat se za vás a říkat věci, které byste sami nikdy neřekli!

**SITUACE Č. 6.** Domluvit si setkání s neznámým člověkem není zrovna moc dobrý nápad. Jestliže jste ale opravdu přesvědčeni, že kamarádovi z internetu můžete věřit, řekněte o schůzce rodičům a domluvte se, že vás jeden z nich doprovodí. Žádnému skutečnému kamarádovi s poctivými záměry to nebude vadit. Problém je to pouze pro ty, kteří něco skrývají.



# 3. Šikana na internetu



## POZNÁMKY K AKTIVITÁM

Namaluj pozvánku, kterou si Aleš ze školy přinesl. Škola si pro celý „Týden“ zvolila také logo a slogan, nezapomeňte je tedy na pozvánku nakreslit.

*Děti mají za úkol zaplnit prázdný rámeček. Ponechte prostor dětské tvořivosti.*

Vezměte si z Aleše příklad a uveďte pět způsobů chování, za které byste udělili „červenou kartu“.

*Diskutujte s dětmi o tom, jaké chování považují za nepřijatelné.*

## POROZUMĚL JSI DOBRĚ?

1: (fair), (kazí) 2: (promluvíš) 3: (dobrý) 4: (virtuální) 5: (zablokuji) 6: (znám)  
7: (neodpověděl)

## DOPORUČENÁ ŘEŠENÍ SITUACÍ NA KARTIČKÁCH

**SITUACE Č. 7.** Tohle určitě není přijatelný způsob používání mobilního telefonu. Zprávy, obrázky či jiné materiály, které by mohly někomu ublížit, nepřešlejte dál. Vždy se k ostatním chovejte tak, jak byste rádi, aby se oni chovali k vám. O situaci, jako je tato, vždy řekněte rodičům či jinému dospělému, kterému důvěřujete.

**SITUACE Č. 8.** Aleš by měl svého kamaráda ujistit, že na šikanování nenese žádnou vinu. Na urážlivé zprávy by jeho kamarád neměl odesilatelovi odpovídat, ale měl by si je uložit jako důkaz a ukázat je rodičům nebo učitelům. Také Aleš by měl o situaci informovat své rodiče, aby ho mohli podpořit v jeho snaze pomoci kamarádovi.

**SITUACE Č. 9.** Netiketa popisuje, jak se chovat k ostatním na internetu, aby se i oni k vám chovali podle vašich představ. Věříme, že toho o ní víte již dost a dokážete Zdeně s úkolem poradit.

# 4. Zábava & stahování



## POZNÁMKY K AKTIVITÁM

Otevřete si svůj oblíbený vyhledávač. Zadejte spojení „vyzváněcí tóny zdarma“ nebo „hry zdarma“ a podívejte se, jaké odkazy vám vyhledávač nabídne. **Některé z adres navštivte. Objevíte nějakou lest?**

*Provedte vyhledávání na základě uvedených klíčových slov a pozorně prozkoumejte, zda na vás obchodníci na nabídnutých webových stránkách nenastražili nějaké pasti. Všimněte si, že informace uvedené malým písmem se v reklamních sloganech neobjevují.*

Jaká je tvoje oblíbená počítačová hra? Ujisti se, že ji tvoji rodiče znají a dokáží ji popsat. Pokud nemají ani ponětí o co ve hře jde, vysvětli jim ji a potom je nech napsat její stručný popis. Povedlo se jim to? Kolik bodů z deseti možných bys jim udělil(a)? .../10. Rodiče mají za úkol do rámečku napsat stručnou charakteristiku oblíbené hry svého dítě. Dítě ji pak ilustruje kresbou.

*Opravdu víte, jaké typy her vaše děti na internetu hrají a jakou hru si oblíbily? Dovolte jim, aby si vás otestovaly!*

## POROZUMĚL JSI DOBRĚ?

1: (zdarma) 2: (formuláře) 3: (pasti) 4: (křížek) 5: (ignorovat) 6: (soukromí) 7: (porad)  
8: (stahuj)

## DOPORUČENÁ ŘEŠENÍ SITUACÍ NA KARTIČKÁCH

**SITUACE Č. 10.** Online dotazník může být dobrá cesta, jak získat zpětnou vazbu od uživatelů. Nicméně, pokud jsou informace o uživateli shromažďovány, musí být uživateli známo za jakým účelem. Poučte své děti, že pokud nerozumí danému formuláři a kontextu informací na stránkách, ať raději dotazník nevyplňují a také ať jsou velmi opatrné s uváděním osobních informací do formulářů (viz. kapitola Komunikace).

**SITUACE Č. 11.** Na internetu existují některé služby zdarma, ale vyzváněcí tóny, tapety, MP3 nahrávky a avatary jsou k dispozici zdarma opravdu výjimečně. Pokud Aleš prozkoumá stránku podrobněji, pravděpodobně objeví text psaný drobnými písmeny, ze kterého se dozví skutečné ceny nabízených služeb. Lidé se často dají nalákat na vyzváněcí tóny, hry a podobné nabídky. Jsou přesvědčeni, že si objednávají „služby zdarma“, ve skutečnosti za ně ale budou muset zaplatit.

**SITUACE Č. 12.** Aleš by měl mít vždy na paměti, že pokud hraje internetové hry s jinými uživateli, které z neinternetového světa vůbec nezná, měl by svoji identitu udržovat v tajnosti. Neměl by prozrazovat kde bydlí, jakou školu navštěvuje, jaké je jeho příjmení apod. O hrách, které hraje by měl také informovat své rodiče a bez jejich svolení by si neměl nikdy stahovat z internetu žádné nové. Mohly by poškodit domácí počítač.



## D. Slovník

**Adresa (URL):** adresa konkrétní webové stránky nebo souboru na internetu. Neobsahuje speciální znaky ani mezery a k označení jednotlivých adresářů se používají lomítka. První část adresy označuje používaný protokol a druhá specifikuje název IP adresy nebo domény, kde se příslušné internetové stránky nacházejí.

**Adresář:** organizační jednotka, kterou váš počítač používá k řazení složek a souborů do hierarchické struktury. Příkladem jsou sekce „Moje dokumenty“, „Moje obrázky“ apod.

**Akronym:** zkratka vytvořená z prvních písmen slov v určité frázi nebo slovním spojení. Akronymy často používají účastníci chatů, umožňují jim rychlejší komunikaci. Příkladem akronymů jsou např. výrazy LoL, CU, Btw (viz kapitola o komunikaci).

**Anti-spyware:** program bojující proti spywaru. Program kontroluje všechna data přicházející do počítače, vyhledává spywarový software a znemožňuje přístup čemukoli, co by počítač mohlo ohrozit, případně sestavuje seznam podezřelých položek, které mají být vymazány.

**Antivirový program:** počítačový program, který se snaží rozpoznat, izolovat a odstranit počítačové viry a jiný škodlivý software a zamezit jim v proniknutí do počítače. Antivirový program nejprve zkontroluje soubory a vyhledává známé viry a poté upozorní na podezřelé chování počítačových souborů, které se zdají být napadeny.

**Asistenční linka:** e-mailová, někdy též telefonická služba, kterou v některých zemích provozují organizace na ochranu dětí a členové sítě Insafe. Děti se na pracovníky této služby mohou obracet, jestliže narazí na stránky s nelegálním či škodlivým obsahem, a mohou s nimi mluvit o svých nepříjemných či děsivých zkušenostech při používání online technologií.

**Autor:** tvůrce literárního nebo audiovizuálního díla, softwaru, apod. Dílo autora je před nelegálním kopírováním chráněno autorskými zákony.

**Autorská práva:** soubor exkluzivních práv, která stanovují, jak lze dále využívat určitý nápad, práci či informaci. Symbolem pro autorská práva je značka ©.

**Avatar:** profil uživatele, který se skládá z uživatelského jména a obrázku, ikony nebo trojrozměrné postavičky a používá se v online počítačových hrách a virtuálních světech.

**Bezplatný software a volně šiřitelné programy (freeware a shareware):** obecně lze říci, že software je chráněn autorskými právy a nelze ho proto volně stahovat. V případě bezplatného softwaru dal držitel autorských práv souhlas k jeho užívání zdarma. O volně šiřitelném softwaru mluvíme tehdy, kdy držitel autorských práv souhlasí s jeho bezplatným užíváním např. s omezenou funkcí. V některých případech je uživateli dána možnost za užívání shareware dobrovolně zaplatit.

**Blog:** zkratka anglického slova „weblog“. Webové stránky vytvářené jednotlivcem nebo skupinou. Autoři je obvykle denně aktualizují a vkládají na ně texty, fotografie, audiovizuální soubory a odkazy.

**Blogování:** zapisování do blogu a jeho průběžná aktualizace.

**CD-ROM:** akronym vytvořený z výrazu „Compact Disc Read-Only Memory“ („kompaktní disk pouze pro čtení“). Data z disku lze číst pomocí počítače a uložené informace není možné měnit. CD-ROMy se často používají k distribuci počítačového softwaru.

**Cookies:** soubor, který se do vašeho počítače uloží po návštěvě určitých webových stránek. Při každé další návštěvě těchto stránek je cookie zaslán zpět na server, kde jsou webové stránky umístěny. Cookies umožňují uložit vaše nastavení stránek a jsou používány pro uskutečňování prodeje přes internet. Pokud cookies odmítnete, může vám být přístup na některé stránky odepřen.

**Cracker:** člověk, který se ilegálně nabourává do počítačových systémů.

**Crackovat:** prolamovat ochranu autorských práv a pořizovat ilegální kopie komerčního softwaru.

**Červ:** zvláštní druh viru, který sám sebe kopíruje a může se samovolně šířit na velké množství počítačů, napadat síť, snižovat rychlost připojení počítače k internetu, vypnout počítač, apod.

**Dětská pornografie:** zákony v různých zemích definují dětskou pornografii různě. Základní společná definice dětské pornografie říká, že jde o fotografii, na které je osoba v dětském věku zapojena do aktivity prokazatelně sexuální povahy nebo vzniká dojem, že je aktérem takové aktivity.

**Digitální hra:** hra vytvořená autory her a určená pro hraní na počítači. Online hra je definována jako digitální hra, kterou je možné hrát pouze pokud je k dispozici připojení na internet. Může se jednat i o hru pro více uživatelů.

**Diskusní skupina:** viz definice pojmu fórum.

**Domovská stránka:** webová stránka, která se automaticky zobrazí po spuštění internetového prohlížeče. Stejným slovem se označuje také první nebo hlavní stránka ze souboru stránek

vzájemně propojených (viz definice pojmu website).

**E-mail:** prostředek pro písemnou komunikaci po internetu. K zasílaným zprávám je možné přiložit počítačový soubor jakéhokoli typu – text, obrázky, audio nahrávku aj.

**E-mailová adresa:** virtuální místo, na které mohou být doručeny e-mailové zprávy. E-mailové adresy se skládají ze dvou částí, které jsou odděleny znakem @.

**Emotikon:** obrázek či ikona používané k vyjádření pocitů a emocí (např. smajlík). Emotikon lze vytvořit kombinací standardních kláves pro písmena a interpunkční znaménka, nebo použít již připravené obrázky. Ty jsou k dispozici v chatovacích a herních místnostech, na službách pro instant messaging, v mobilních telefonech apod.

**Filtr:** zařízení, které reguluje přístup k informacím či určitým internetovým službám, varuje před problematickými webovými stránkami, vytváří záznamy o pohybu uživatele na internetu a blokuje přístup na nedůvěryhodné stránky. Filtrovací systémy mohou být nainstalovány do samostatně fungujících počítačů, na servery, do telefonů s přístupem na internet apod.

**Filtr spamů:** aplikace, která identifikuje spamy a zabraňuje jejich ukládání mezi došlou poštu v e-mailové schránce.

**Firewall:** je ochranná bariéra, která sleduje a omezuje přenos informací mezi počítačem a sítí nebo Internetem. Poskytuje ochranu proti uživatelům, kteří by se mohli pokusit o přístup k počítači z prostoru vně bez vašeho povolení.

**Fórum:** online diskusní skupina, jejíž členové sdílejí podobné zájmy a na internetu si mohou veřejně zasílat vzkazy k nejrůznějším tématům.

**Grooming (lákání na schůzku):** situace, kdy chatovací místnosti využívají pedofilové. Představují se dětem jako jejich vrstevníci a pokoušejí se je vylákat na schůzku. Navazují hovor s účastníky diskuzí a zjišťují informace o místě jejich pobytu, zájmech, koníčcích a sexuálních zkušenostech. V konverzacích o sexu se nejrůznějšími způsoby snaží děti zaujmout.

**Hacker:** často užívaný termín pro osobu zabývající se crackováním/nabouráváním počítačů (viz definice pojmu “cracker”). V počítačových kruzích toto slovo také označuje počítačového nadšence.

**Hardware:** pevná část počítače odlišná od softwaru, který pracuje na hardwaru. Hardware se dělí na vnitřní části (základní deska, pevný disk a operační paměť), často označované jako komponenty, a části vnější (monitor, klávesnici, tiskárnu atd.), nazývané také periferie počítače.

**Heslo:** tajná posloupnost znaků, která umožňuje uživateli přístup k souboru, počítači, účtu nebo programu a ostatním uživatelům v takovém přístupu zabraňuje (viz kapitola „Komunikace“).

**Horká linka:** telefonická linka nebo internetová služba, kam se lidé mohou obracet a stěžovat si na existenci stránek, jejichž obsah považují za nelegální, a/nebo na nelegální používání internetu. Způsob, jaký se při projednávání stížností postupuje, musí být zcela průhledný, a organizace provozující horkou linku musí mít podporu vlády, průmyslových společností, soudních orgánů a uživatelů internetu v zemi, ve které působí.

**Chat:** systém synchronní komunikace přes internet. Účastníci chatu si vyměňují písemné vzkazy a ke komunikaci využívají nástroje pro chatování a instant messaging (např. MSN).

**Chatovací místnost:** veřejné virtuální prostředí pro komunikaci v reálném čase. Lidé z celého světa se mohou v chatovacích místnostech setkávat a vzájemně komunikovat prostřednictvím vzkazů, které přiší na svém počítači. Pokud vaše děti chatovací místnosti používají, přesvědčte se, že byly vytvořeny speciálně pro uživatele jejich věkové kategorie a že zde komunikace probíhá pod dohledem moderátorů.

**Instant Messaging (IM):** systémy pro rychlou výměnu zpráv – umožňují bezprostřední simultánní elektronickou komunikaci mezi dvěma nebo více uživateli. Pomocí těchto systémů si můžete vybrat pro komunikaci partnery ze seznamu kontaktů. Pokud se některý z vašich kontaktů připojí k internetu, dostanete o tom ihned zprávu.

**Internet:** celosvětová veřejně přístupná síť vzájemně propojených počítačových sítí, prostřednictvím které je možno přenášet a sdílet data. Skládá se z menších domácích, školních, podnikových nebo administrativních sítí, které poskytují různé služby, například informace, e-mail, chat nebo přenos dat.

**Koš:** adresář v počítači, kam se dočasně ukládají vymazané soubory, než jsou nevratně z počítače odstraněny. Stará a nepotřebná data je vhodné z koše pravidelně odstraňovat, aby se uvolnilo místo na pevném disku počítače.

**Krádež identity:** odcizení osobních údajů (např. jména, data narození, čísla kreditní karty) a jejich protiprávní použití.

**Malware:** viz definice pojmu škodlivý software

**Mobil:** zkrácený hovorový výraz pro mobilní telefon, elektronický telekomunikační přístroj, který má stejné základní funkce jako běžný pevný telefon. Dnes má většina mobilních telefonů vestavěný fotoaparát a řada z nich umožňuje i připojení k internetu (placená služba).

**Mp3:** je kódovací formát pro zvukové soubory. Velikost souboru ve formátu mp3 bývá asi desetkrát menší než u původního zvukového souboru, ale kvalita se blíží kvalitě záznamu na CD. Díky malé velikosti souboru a kvalitnímu zachycení zvuku se formát mp3 stal oblíbenou formou ukládání hudebních souborů pro počítače i přenosné přehrávače.

**Modifikovat/manipulovat:** pozměňovat obrázky, soubory, fotografie nebo ilustrace zjevným nebo skrytým způsobem. V současnosti existuje řada nástrojů, pomocí kterých lze upravovat obsah nebo formu dat, aby se nakonec odlišovala od reality.

**Nastavení zabezpečení (profil):** soubor nastavitelných možností zabezpečení vašeho internetového profilu (viz definice tohoto pojmu). Většinou se tato nastavení týkají otevírání obrázků a souborů, identifikace důvěryhodných poskytovatelů informací a úroveň povolení obsahu nevhodného pro mládež.

**Nelegální obsah:** obsah internetových stránek, který je podle legislativy daného státu protiprávní. Nejčastější typy takového obsahu zahrnují obrázky sexuálního zneužívání dětí, protiprávní aktivity na chatu (např. grooming – lákání na schůzku) nebo publikování materiálů nenávistného nebo xenofobního charakteru.

**Net:** zkratka slova „internet“.

**Netiketa:** pravidla slušného chování při komunikaci na internetu.

**Nevyžádaná pošta:** identické zprávy posílané najednou na e-mailové adresy mnoha lidí, kteří o ně nemají zájem. Vzhledem k tomu, že internet je veřejný prostor, neexistuje v podstatě žádný způsob, jak uživatele před nevyžádanou poštou chránit, stejně jako je nemožné zcela odfiltrovat spamy.

**Oblíbené:** nastavitelná složka v prohlížeči, ve které si můžete ukládat zajímavé odkazy/záložky. Záložky mohou být rozřazeny do podsoček a/nebo označeny klíčovými slovy, což usnadňuje jejich hledání.

**Odkaz:** prvek odkazující na soubor dostupný na internetu (webovou stránku, textový dokument, obrázek, apod.). Kliknutím na odkaz se načte nová stránka nebo nová internetová adresa. Textové odkazy jsou obvykle zobrazovány modrým písmem a podtrženy, ale toto formátování není závazné. Jako odkazy na jiné webové stránky se také často používají obrázky.

**Ochrana rodiny:** funkce nazývaná též „rodičovská kontrola“. Jedná se o nastavení prohlížeče či jiného webového nástroje tak, aby více vyhovoval potřebám dětí. Je možné nastavit filtraci obsahu webových stránek, časový limit, kontrolu her, apod.

**Ochrana soukromí:** soubor nastavitelných vlastností systému, které se nastavují individuálně pro každý účet. Uživatel má možnost určit si míru ochrany svého soukromí a zajistit si ochranu před odhalením osobních údajů, cookies, apod.

**Online formulář:** formátovaný dokument s prázdnými políčky a možností vpisovat informace. Do formuláře v elektronické podobě je možné buď vepsat vlastní text, nebo si vybrat určitou formulaci z předem sestaveného seznamu (rozklikávací nabídka možností). Po odeslání formuláře jsou informace ihned zasílány ke zpracování a zaneseny do databáze.

**Operační systém:** program, který provádí základní funkce počítače a který umožňuje používání ostatních programů. Nejrozšířenější jsou například Windows, Linux nebo Mac OS.

**Osobní údaje:** jakékoli informace, které lze přiřadit určité osobě. Při shromažďování, zpracovávání a přechovávání osobních dat je vždy nutno přesně definovat účel.

**P2P:** síť P2P (z anglického peer-to-peer) umožňují připojeným uživatelům sdílet data, a to jejich nahráváním nebo stahováním – viz definice těchto pojmů. Jedná se pouze o jeden ze způsobů sdílení dat na internetu. Pozor! Některé způsoby sdílení souborů jsou protiprávní.

**Panel nástrojů:** soubor ikon nebo tlačítek, které jsou součástí softwarové aplikace. Panely nástrojů představuje vždy přístupné a snadno použitelné rozhraní pro provádění nejběžnějších operací.

**Počítačový program:** obvykle nazývaný software. Software tvoří strukturovaná sekvence instrukcí napsaná počítačovými programátory, která umožňuje počítači vykonávat jednotlivé úkony. Počítačový software nejčastěji koupíte na CD-ROMu (viz definice tohoto pojmu), což je médium, kde je program fyzicky uložen.



**Počítačový soubor:** archiv/soubor vzájemně souvisejících informací (dokumentů, programů apod.) uložený v počítači pod konkrétním jménem souboru. Počítačové soubory lze považovat za moderní verzi papírových dokumentů, které se uchovávaly ve složkách v kancelářích a knihovnách.

**Port:** je rozhraní na počítači, které se používá k připojení jiného zařízení. Porty mohou být interní nebo externí. Interní porty umožňují připojení k disku, jednotce nebo síti, zatímco externí porty slouží k připojování periferních přístrojů, jako je například tiskárna nebo klávesnice.

**Procesor:** neboli „Centrální řídicí jednotka“ (z anglického „Central Processing Unit, CPU) je ta část počítače, která zpracovává data, vytváří ovládací signály a ukládá výsledky. Spolu s počítačovou pamětí tvoří základní součást počítače.

**Profil:** osobní údaje uživatele uváděné v sociálních sítích, systémech pro rychlou výměnu zpráv, systémech pro online chatování, internetových hrách, apod. Profily mohou být veřejné nebo soukromé a uživatel je může upravovat tak, aby jej co nejlépe reprezentovaly ve virtuálním prostoru.

**Prohlížeč:** program používaný pro zobrazování webových stránek. Mezi nejznámější prohlížeče pro Windows patří programy Internet Explorer, Netscape Navigator a Firefox, pro počítače s operačním systémem Mac OS je to program Safari. Nejnovější verze těchto prohlížečů obsahují nově také možnost nastavení rodičovské kontroly.

**Prohlížení/prohledávání:** využívání prohlížeče k zobrazování webových stránek nebo pouhému surfování na internetu.

**Přenášení souborů:** proces přenášení souborů v počítačové síti. Uživatelé tyto činnosti nejčastěji označují výrazy „nahrávání a „stahování“.

**Přezdívka:** používají se rovněž termíny „uživatelské jméno“ nebo „nick“. Přezdívka je jméno, které si uživatel při využívání internetové služby sám zvolí k označení své osoby. Pod tímto jménem bývá uživatel zanesen v seznamech kontaktů, diskusních skupinách, apod. Pokud si zvolíte vhodnou přezdívku, můžete si na internetu zachovat anonymitu.

**Přihlášení:** souhlas s přijímáním internetové služby – zaslání novinek, používání diskusního fóra, e-mailu, chatové platformy, apod. Uživatelé by měli mít možnost si internetovou službu kdykoli odhlásit.

**Registrace/přihlášení služby:** dobrovolné přihlášení k využívání služby nebo přijímání zpráv, kdy jsou informace zasílány přímo do e-mailové schránky uživatele.

**Příloha:** datový soubor zasílaný společně s e-mailovou zprávou. Prostřednictvím e-mailových příloh se často šíří červi a viry. E-maily s přílohou od neznámých odesílatelů je třeba považovat za podezřelé.

**Připojení k internetu/sítové připojení:** označuje způsoby připojení uživatelů k internetu. Mezi běžně používané způsoby patří ADSL (přes telefonní linku umožňující zároveň telefonování), Wi-Fi (připojení k místní bezdrátové síti), připojení přes poskytovatele kabelové televize nebo prostřednictvím mobilních telefonů.

**Rodičovská kontrola:** viz definice pojmu „ochrana rodiny“.

**Sdílení souborů:** online výměna souborů mezi jednotlivými uživateli. Termín označuje jak

situace, kdy jedinec dává soubor k dispozici ostatním uživatelům (nahrávání), tak proces kopírování dostupných souborů z internetu do vlastního počítače (stahování). Sdílení souborů probíhá nejčastěji prostřednictvím P2P sítí.

**Second Life (Druhý život):** známá trojrozměrná webová komunita provozovaná americkou společností Linden Labs. Uživatelé se účastní života komunity prostřednictvím svých avatarů (viz definice tohoto pojmu), mohou se navzájem ovlivňovat, budovat si domy, zasahovat do prostředí komunity, obchodovat, vydělávat virtuální peníze, apod. Webová adresa komunity je [www.secondlife.com](http://www.secondlife.com)

**Seznam kontaktů/seznam kontaktních adres:** soubor kontaktních adres v programech pro instant messaging či zaslání e-mailů, v online hrách, mobilních telefonech, apod. Kontaktní adresy je možné přidávat, odmítat a mazat.

**SIP-Bench:** výzkum podporovaný Evropskou komisí, který testoval třicet ovládacích a antispamových nástrojů a měřil jejich efektivitu při ochraně dětí před škodlivými obsahy na internetu.

**Skenování:** proces, při kterém se tištěný materiál prostřednictvím skeneru převádí do digitální formy. Takto získané digitální materiály lze následně prohlížet jako elektronické soubory na počítači a sdílet je na internetu.

**Složka:** součást systému souborů, která může obsahovat více souborů a/nebo jiných adresářů/složek! Složky mohou obsahovat větší množství dokumentů a jsou používány pro třídění informací.

**Složka spamů a nevyžádané pošty:** označení místa v e-mailové schránce, kam jsou automaticky ukládány zprávy identifikované jako spamy nebo nevyžádaná pošta.

**Sociální síť:** internetové komunity, jejichž členové mají společné zájmy nebo koníčky a stýkají se a komunikují na internetu prostřednictvím speciálního softwaru nebo služeb (viz stránky sociálních sítí).

**Software:** viz definice pojmu počítačový program.

**Soukromé:** údaje nebo dokumenty patřící soukromé osobě nebo skupině, které nejsou určeny ke zveřejnění, většinou proto, že obsahují něco velmi unikátního nebo osobně citlivého.

**Soukromí:** schopnost uživatele nebo skupiny rozhodovat o přenosu informací o své osobě a zveřejňovat pouze některé z nich. Soukromí je někdy úzce spojeno s anonymitou, tedy přáním uživatele zůstat na internetu nepoznán.

**Spam:** nežádoucí hromadně odesílaný e-mail, většinou komerčního charakteru. Zaslání spamu ostatním uživatelům je jedním z nejčastějších druhů zneužívání internetu.

**Spyware:** malware připojený k souborům stahovaným z internetu, který se tajně automaticky nainstaluje do počítače, monitoruje aktivity uživatele a odesílá informace třetím stranám. Tyto třetí strany bývají většinou společností, které se zajímají o osobní profily uživatelů, aby jim mohli cíleně zasílat reklamy nebo informace. Může také jít o crackery, kteří chtějí získat přístup k důvěrným údajům a informacím.

**Stahování:** proces kopírování souboru z online služby do vlastního počítače.

**Stránky sociálních sítí:** virtuální platformy, které hostí komunity uživatelů se společnými zájmy nebo koníčky. Členové si musí vytvořit své uživatelské profily a potom mohou prostřednictvím sdílených nástrojů zveřejňovat texty, obrázky a další soubory, psát vzkazy na nástěnku a účastnit se diskusí. Mnoho stránek sociálních sítí neumožňuje vstup osobám mladším 13 let a zahrnuje nastavení zabezpečení profilu.

**Šikana:** ubližování jiné osobě. Může se jednat o opakované poškozování, výhrůžky, sexistické poznámky, fyzické napadání nebo hanlivé výrazy. Šikanovat může jednotlivce nebo skupina osob.

**Škodlivý obsah:** obrázky, texty, dokumenty apod., jejichž obsah může ublížit. Např. fotografie zobrazující násilí nejsou vhodné pro děti a nezletilé osoby a mají na ně škodlivý vliv.

**Škodlivý software (malware):** zkratka pro anglický termín „malicious (tj. zákeřný) software“. Takový software dokáže vniknout do počítače a poškodit jej bez vědomí uživatele. Jedná se o takzvané viry, červy, trojské koně, spyware, nečestný adware a jiné škodlivé nebo nežádoucí aplikace.

**Trojští koně:** zákeřný kód, malware, který do vašeho počítače může nepozorovaně vniknout při provádění zdánlivě neškodných činností, jako jsou hry, nebo dokonce spolu s antivirovými programy. Trojští koně se většinou sami nekopírují, ale mají za úkol proniknout k citlivým datům nebo zničit data. Mohou také vymazat všechna data na pevném disku nebo odcizit důvěrné informace.

**Tapeta:** vzor, obrázek nebo jiná grafika, která se zobrazí na pozadí plochy počítače.

**Uživatelský účet:** existence účtu umožňuje na internetu ověřit vaši totožnost. Přes své uživatelské jméno a heslo máte přístup k online službám. S pomocí svého operačního systému můžete pro každého člena rodiny vytvořit samostatný uživatelský účet.

**Upozornění:** dialogové okno, které se objeví na obrazovce. V okně je uživateli sdělována určitá informace nebo varování před uskutečněním potenciálně nebezpečné operace. Může se jednat např. o oznámení o nové e-mailové zprávě nebo o stavu antivirové ochrany.

**USB disk/flash disk:** malé paměťové médium s vestavěným konektorem USB. Flash disk bývá velmi malý, lehký, snadno připojitelný a přepisovatelný.

**Uživatelský profil:** soubor informací o konkrétním uživateli softwaru, webových stránkách nebo jiných technických nástrojů. Většinou obsahuje informace jako uživatelské jméno, heslo a další údaje (například datum narození, zájmy).

**Víceuživatelské hry:** v angličtině „massive multiplayer games“. Hry, které nabízejí bohatý trojrozměrný svět obydlený tisíci hráči, kteří v něm přijímají role smyšlených postav a soupeří mezi sebou. Většinu této kategorie tvoří hry, kde účastníci tvořivě přijímají role a spolupracují nebo postupují podle daného příběhu.

**Virtuální agresivita (flaming):** nepřátelské a urážlivé chování uživatelů internetu. Obvykle k němu dochází na diskusních stránkách, v chatovacích místnostech nebo dokonce při výměně e-mailových zpráv.

**Virtuální šikana/šikana na internetu:** šikana prováděná prostřednictvím elektronických médií, obvykle systému pro instant messaging a zasílání e-mailů. Může se jednat

o opakované ubližování, výhrůžky nebo sexistické či hanlivé poznámky. Organizátoři internetové šikany mohou zveřejňovat soukromé informace svých obětí nebo na sebe dokonce brát jejich identitu a jejich jménem publikovat určité materiály s cílem obětí očernit či zesměšnit.

**Virtuální vlastnictví:** soubor objektů, které v rámci internetové hry patří konkrétnímu hráči. Každý hráč virtuálně vlastní svůj virtuální majetek prostřednictvím počítačového terminálu, na kterém se tyto předměty zobrazují.

**Virus:** typ zákeřného kódu, malwaru, který je sestaven tak, aby se šířil prostřednictvím činnosti uživatele. Většinou se šíří spolu s přílohami e-mailů, ale také prostřednictvím „infikovaných“ externích paměťových médií (flash disků, CD-ROMů apod.).

**Voice over Internet Protocol (VoIP):** technologie, která po stažení klientského softwaru umožňuje uživatelům využívat internet k hlasové komunikaci. Takové hovory jsou často zdarma pro uživatele, kteří spolu komunikují přes stejného VoIP klienta (například Skype, Voicebuster). Tyto softwary obvykle umožňují také chatování a sdílení souborů.

**Vyhledávač:** nástroj používaný k vyhledávání informací obsažených na webových stránkách. K nejznámějším patří Google nebo Seznam. Vyhledavače obsahují také stránku pro pokročilé nastavení vyhledávání, kde můžete najít i zajímavá nastavení zabezpečení.

**Vyskakovací okno:** okno, které se náhle zobrazí při prohlížení webové stránky nebo po stisknutí funkční klávesy. Vyskakovací okno většinou obsahuje nabídku příkazů a zůstává na obrazovce pouze do chvíle, než některý z příkazů vyberete nebo než je zavřete kliknutím na křížek v pravém horním rohu.

**Vyzvánění tón:** zvuk, kterým mobilní telefon oznamuje příchozí hovor. Existuje široká škála individuálně přizpůsobitelných zvuků a melodií, které si majitelé mobilních telefonů mohou stahovat, většinou za poplatek, a poté používat.

**Web:** zkratka pro spojení World Wide Web (celosvětová síť). Soubor internetových dokumentů ve formátu HTML (HyperText Markup Language), které obsahují odkazy na další dokumenty, grafiku nebo audio a video soubory. Web je součástí internetu.

**Webová kamera:** kamera, která umí přenášet obraz po webu prostřednictvím systémů pro rychlou výměnu zpráv, počítačových videokonferenčních aplikací, chatových platforem apod. Webovou kameru může nahradit digitální fotoaparát, který odesílá snímky na webový server buď průběžně nebo v pravidelných intervalech.

**Webová stránka:** místo na síti World Wide Web. Každé takové místo má svou domovskou stránku, která se při zadání adresy načte jako první. Stránky většinou obsahují odkazy na další soubory nebo stránky. Webové stránky mohou vlastnit a spravovat soukromé osoby, společnosti nebo organizace.

**Zkušební software:** software, který si uživatel může před zakoupením vyzkoušet. Zkušební verze softwaru mají obvykle stejné funkce jako standardní verze, ale lze je používat pouze omezenou dobu.

**Zobrazované jméno:** viz definice pojmu přezdívka

**Zpráva o chybě:** funkce, která umožňuje uživateli veřejného virtuálního prostoru oznámit moderátorovi nebo správci sítě, že se vyskytl problém (technická chyba, nepřijatelné chování uživatelů, nezákonný obsah, apod.).



## E. Užitečné adresy

### SAFERINTERNET.CZ

Hlavní české stránky Národního uzlu bezpečnějšího internetu Saferinternet.cz zaměřené na aktuality a rady v oblasti internetové bezpečnosti. Pokud mají rodiče a učitelé zájem podporovat bezpečné a zodpovědné používání internetu, najdou na stránkách Saferinternet.cz potřebné informace, rady a nástroje: <http://www.saferinternet.cz>

### SAFER INTERNET INSTITUTE

„Safer Internet Institut je česká nevládní organizace, která byla založena s cílem podpořit studium problematiky bezpečnějšího internetu, vytvořit dokumentační středisko osvědčených postupů a přispívat metodicky ke zvyšování povědomí o bezpečnějším používání internetu a nových komunikačních technologií: <http://www.siin.cz>

### HORKÁ LINKA

Chcete-li podat zprávu o materiálech, na které jste na internetu narazili a které podle vašeho názoru porušují zákon, kontaktujte horkou linku: <http://www.horkalinka.cz>. Horkou linku provozuje Národní uzel bezpečnějšího internetu Saferinternet.cz

## LINKA BEZPEČÍ

Linka bezpečí je nejznámější česká linka důvěry pro děti a dospívající do 18 let (studenty do 26 let), kteří mohou využívat její služby krizové intervence po telefonu nepřetržitě 24 hodin denně po celý rok. Pomoci se jim dostane také prostřednictvím e-mailové poradny a chatu, které najdou na webových stránkách:

<http://www.linkabezpeci.cz/>

## INTERNET HELPLINE (POMOC ONLINE)

Linka bezpečí provozuje v rámci národního projektu bezpečnější internet (Saferinternet.cz) asistenční linku <http://www.internethelpline.cz> nebo také <http://www.pomoconline.cz>, která poradí v případě, že se mladí uživatelé dostanou na internetu do nesnází.

## BEZPEČNĚ ONLINE

<http://www.bezpecne-online.cz> jsou národní webové stránky projektu Saferinternet.cz zaměřené na rozšiřování povědomí o bezpečnosti na internetu a šíření informací o nebezpečných praktikách, zejména pokud jde o kybernetickou šikanu, phishing, spyware a krádeže identity a podobně.

## MOBILSTORY.CZ

Stránky, které se věnují problematice bezpečného a etického používání mobilních telefonů a mobilních technologií obecně. <http://www.mobilstory.cz>

## INSAFE

Evropská síť zaměřená na zvyšování povědomí o internetové bezpečnosti. Organizace si klade za cíl poskytovat uživatelům takovou podporu, aby mohli využívat kladných stránek internetu a vyhnuli se potenciálnímu nebezpečí: <http://www.saferinternet.org>



**Safer**  
internet.cz

ins@fe



Podpora projektu: **upc**

*Název: Rodinný balíček o Internetové bezpečnosti • Vytvořila organizace Insafe/Liberty Global-UPC ve spolupráci s projektem Saferinternet Česká republika v roce 2008*

*Prefix: 9789078209 • Id 51950 • ISBN-NUMBER: 9789078209577 • EAN: 9789078209577*

*Copyright: dílo je chráněno licencí „Creative Commons Attribution-Noncommercial-No Derivative Works 3.0 Unported Licence“.  
Popis licence je k dispozici na webových stránkách <http://creativecommons.org/licenses/by-nc-nd/3.0>*